Nways
マルチプロトコル・ルーティング・サービス

ソフトウェア使用者の手引き
バージョン 3.1

SC88-6372-05
英文原典：SC30-3681-07

Nways
マルチプロトコル・ルーティング・サービス

ソフトウェア使用者の手引き
バージョン 3.1

英文原典：SC30-3681-07
SC88-6372-05

お願い

本書の情報をご使用になる前に、xxxiiiページの『特記事項』を必ずお読みください。

第 8 版 (1998 年 6 月)

本書は、IBM Nways マルチプロトコル・ルーティング・サービスのバージョン 3.1 に適用されます。また、新版や TNL で特に指示がない限り、以降のリリースや修正レベルにも適用されます。

原　典： SC30–3681–07
Nways Multiprotocol Routing Services
Software User's Guide
Version 3.1

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 1998.10

目次

図

表

特記事項

本書において、日本では発表されていないIBM製品（機械およびプログラム）、プログラミングまたはサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのようなIBM製品、プログラミングまたはサービスを、日本で発表する意図があることを必ずしも示すものではありません。本書で、 IBMライセンス・プログラムまたは他のIBM製品に言及している部分があっても、このことは当該プログラムまたは製品のみが使用可能であることを意味するものではありません。これらのプログラムまたは製品に代えて、IBMの知的所有権を侵害することのない機能的に同等な他社のプログラム、製品またはサービスを使用することができます。ただし、IBMによって明示的に指定されたものを除き、これらのプログラムまたは製品に関連する稼働の評価および検証はお客様の責任で行っていただきます。

IBMおよび他社は、本書で説明する主題に関する特許権（特許出願を含む）商標権、または著作権を所有している場合があります。本書は、これらの特許権、商標権、および著作権について、本書で明示されている場合を除き、実施権、使用権等を許諾することを意味するものではありません。実施権、使用権等の許諾については、下記の宛先に、書面にてご照会ください。

〒106-0032 東京都港区六本木3丁目2-31
AP事業所
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

商標

以下の用語は、米国あるいはその他の国々における IBM 社の商標です。

拡張同位間通信ネットワーキング機能	IBM	PS/2
AIX	Micro Channel	RS/6000
AIXwindows	NetView	System/370
APPN	Nways	VTAM
BookManager		

UNIX は、米国およびその他の国における登録商標であり、X/Open Company Limited がライセンスを専有しています。

Microsoft、Windows、および Windows 95 ロゴは、Microsoft Corporation の商標または登録商標です。

その他の社名、製品名、およびサービス名は、他社の商標またはサービス・マークです。

まえがき

本書には、ルーター・ユーザー・インターフェースを使用して、Nways 装置に導入された Multiprotocol Routing Services の基本コードを構成および操作するのに必要な情報が記載されています。本書は、以下のプロセスおよび操作を行うのに役立ちます。

- Multiprotocol Routing Services の基本コードの構成、監視、および使用。
- Nways 装置によってサポートされるインターフェースおよびリンク・レイヤー・ソフトウェアの構成、監視、および使用。

本書には、Nways 装置のブリッジング機能およびルーティング機能を構成するのに必要な情報が収められています。本書では、このソフトウェアで提供される機能のすべてについて説明しています。説明されているすべての機能が、どの Nways 装置でも提供されるわけではありません。装置に特有の機能については、該当する章または節に、その制約を示してあります。

本書は IBM 2210 をサポートし、この製品を “ルーター” または “装置” と呼んでいます。本書の例は IBM 2210 の構成を表していますが、実際の出力は本書のものとは異なる場合があります。示されている例は、ユーザーが装置を構成する際に表示される内容のガイドラインとして使用してください。

本書の対象読者

本書は、コンピューター・ネットワークの導入と運用を担当する方々を象にしています。コンピューター・ネットワークのハードウェアおよびソフトウェアを扱った経験があれば役に立ちますが、プロトコル・ソフトウェアを使用する上ではプログラミングの経験は必要ありません。

追加情報の入手: 資料が印刷された後に変更が行われる場合もあります。追加情報がご利用頂ける場合、または資料の印刷後に変更が必要になった場合は、構成プログラム・ディスケットのディスケット 1 のファイル (README という名前のファイル) に変更内容を収めてあります。このファイルは、ASCII テキスト・エディターを使用してご覧ください。

ソフトウェアについて

IBM Nways Multiprotocol Routing Services は、 IBM 2210 (ライセンス・プログラム番号 5801-ARR) をサポートするソフトウェアです。このソフトウェアには、以下に挙げる構成要素が含まれています。

- 基本コード (次のものからできています。)
  - 装置に対してブリッジング、データ・リンク・スイッチ、および SNMP エージェントの各機能を提供するコード
  - 装置に導入されているマルチプロトコル・ルーティング・サービス基本コードの構成、監視、および使用を可能にするルーター・ユーザー・インターフェース。ルーター・ユーザー・インターフェースは、サービス・ポートに接続され

る ASCII 端末またはエミュレーターを介してローカルに、あるいは Telnet セッションまたはモデム接続装置を介してリモートからアクセスされます。

基本コードは工場で 2210 に導入済みです。

- IBM Nways Multiprotocol Routing Services用構成プログラム (*構成プログラム*)。これは、独立型ワークステーションからの装置の構成を可能にする、グラフィカル・ユーザー・インターフェースです。構成プログラム にはエラー検査およびオンライン・ヘルプ情報が含まれます。

  構成プログラムは、工場で事前にロードされてはいません。ソフトウェア受注の一環として、装置とは別に出荷されます。

  IBM Nways Multiprotocol Routing Services用構成プログラムは、FTP で入手することもできます。サーバー・アドレスおよびディレクトリーについては、 *Nways マルチプロトコル・アクセス・サービス、ルーティング・サービス、スイッチ・サービス 構成プログラム 使用者の手引き* SC88-6657 を参照してください。

本書における表記法

本書では、コマンド構文とプログラム応答を示すために、以下の表記法を使用します。

1. コマンドの省略形は以下のように示されます。

   ```
   reload
   ```

   この例では、コマンド全体 (reload) を入力しても、その省略形 (rel) を入力しても構いません。
2. キーワードの選択項目は大括弧で囲み、or (または) という語で区切っています。例:

   ```
   command [keyword1 or keyword2]
   ```

   パラメーターの値として、キーワードの 1 つを選択してください。
3. オプションの後に続く 3 つのピリオドは、オプションの後にユーザーが追加データ (たとえば、変数) を入力することを意味します。例:

   ```
   time host ...
   ```

   この例では、コマンドの説明として、ピリオドの位置にホストの IP アドレスを入力します。
4. コマンドの応答として表示される情報の中で、オプションの省略時値はそのオプションの直後にある大括弧に入れて示します。例:

   ```
   Media (UTP/STP) [UTP]
   ```

   この例では、STP を指定しない限り、媒体は UTP に省略時設定されます。
5. キーボードのキーの組み合わせは、以下のように表示されます。
   - **Ctrl-P**
   - **Ctrl -**
6. キーボードのキーの名前は、次のように表示されます。例: **Enter**
7. 変数 (すなわち、ユーザーが定義するデータを表すのに使用される名前) は、イタリック体で表示されます。例:

File Name: *filename.ext*

IBM 2210 Nways マルチプロトコル・ルーターの資料

以下のリストには、IBM 2210 をサポートする資料が示してあります。

運用およびネットワーク管理

SC88-6372

Nways マルチプロトコル・ルーティング・サービス ソフトウェア使用者の手引き バージョン 3.1

この資料には、以下に関する説明が記載されています。

- ルーターとともに出荷される IBM Nways Multiprotocol Routing Services のソフトウェアの構成、モニター、および使用
- マルチプロトコル・ルーティング・サービス コマンド行ルーター・ユーザー・インターフェースの使用による、ルーターとともに出荷されるリンク・レイヤー・プロトコルならびにネットワーク・インターフェースの構成および監視

SC88-6371

Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻 バージョン 3.1

SC88-6687

Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 2 巻 バージョン 3.1

上記の両資料では、マルチプロトコル・ルーティング・サービス コマンド行ルーター・ユーザー・インターフェースをアクセスおよび使用して、ルーターと共に出荷されるルーティング・プロトコル・ソフトウェアを監視および構成する方法を説明しています。

これらの資料には、装置がサポートするプロトコルのそれぞれについての情報が含まれています。

SC88-6373

IBM Nways イベント・ログ・システム・メッセージの手引き

この資料には、発生する可能性のあるエラー・コードのリストを挙げ、説明およびエラーを訂正する場合の推奨処置が併記してあります。

構成

オンライン・ヘルプ

構成プログラムのヘルプ・パネルは、プログラム機能、パネル、構成パラメーター、およびナビゲーション・キーの理解に役立ちます。

SC88-6657

Nways マルチプロトコル・アクセス・サービス、ルーティング・サービス、スイッチ・サービス 構成プログラム 使用者の手引き、

この資料では、構成プログラムの使用法を説明しています。

GG24-4446

IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios

この資料には、IBM Nways Multiprotocol Routing Servicesを使用してプロトコルを構成する方法の例が挙げてあります。

安全

SD21-0030

Caution: Safety Information - Read This First

この資料には、IBM 2210 の導入および保守に適用される注意および危険のただし書きが記載されています。

以下のリストは、IBM 2210 Nways マルチプロトコル・ルーター ライブラリーの資料をタスク別に並べています。

計画および導入

GA88-6228

IBM 2210 Nways マルチプロトコル・ルーター 計画とセットアップの手引き

1Sx 型および 1Ux 型の場合を除いて、この資料は 2210 と共に出荷されます。この資料では、導入の準備方法、2210 の導入方法、初期構成の実行方法、および導入結果の検査方法について説明しています。

この資料には、危険のただし書きおよびその他の安全上の注意が記載されています。

GC30-3867

IBM 2210 Models 1Sx and 1Ux Installation Guide

この資料は、2210-1Sx 型および -1Ux 型と共に出荷されます。 この資料では、導入の準備方法、2210 の導入方法、初期構成の実行方法、および導入結果の検査方法について説明しています。

この資料には、危険のただし書きおよびその他の安全上の注意が記載されています。

診断および保守

SY27-0345

IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual

この資料は 2210 と一緒に出荷されます。 2210 に関する問題を診断し、修理する方法を示しています。

IBM 2210 ソフトウェア・ライブラリーの変更の要約

変更の内容は、以下のとおりです。

- **新しい機能**
  - ネットワーク・アドレス変換 (NAT) - リモート・ワークステーションは、単一の IP アドレスを使用して、ルーターの背後にある異なる宛先に到達することが可能になります。
  - バーチャル・ルーター冗長度プロトコル (VRRP) - このプロトコルを実行している LAN 上のルーターは、相互にバックアップすることができます。

- IP、IPX、および AppleTalk は、同じ装置上の異なるインターフェースを使用してルート指定できるようになりました。

- **拡張機能**
  - APPN
    - 拡張ボーダー・ノード・サポート
    - TN3270E サブエリア接続性サポート
  - 基本サービス
    - ネットワーク・インターフェースの最大数が増えました。
    - イベント・ログ・システム (ELS) の拡張
  - BGP
    - **reset** コマンドのサポート
  - DLSw
  - 動的再構成
  - フレーム・リレー - 暗号化をサポートするようになりました。
  - IP
    - ファイアウォールをサポートするためのセキュリティーの拡張
    - セキュリティーをサポートするためのフィルターの拡張
    - ブリッジ・ネットワークでの IP ルーティング
    - APPN/HPR、SNA/DLSw、および TN3270 サーバーに対するバージョン 4 優先順位設定およびフィルター・サポート
    - **reset** コマンドのサポート
  - IPX
    - **reset** コマンドのサポート
  - OSPF
    - RFC 2178 のサポートの拡張
    - **reset** コマンドのサポート
  - RLAN
    - L2TP の拡張
  - セキュリティーの拡張
    - TACACS+/RADIUS 認証および会計
      - ルーターへのログインを制御するために TACACS+/RADIUS を使用可能にすることができます。
  - X.25 - ヌル・カプセル化のサポート
    - X.25 は ISDN BRI D チャネル (X.31 と同様に) を介して伝送できるようになりました。

- **説明と訂正**

  本書で加えられた技術上の変更個所には、左側欄外に縦線 (|) を引いて示してあります。

資料の再構築中

本版より、当資料およびその他のソフトウェア資料の改編を進めています。改編の目的は次のとおりです。

- 資料を再編成する。
- 不必要または冗長な情報を除去する。
- 検索しやすくする。
- 情報をより分かりやすくする。

この再編成の一環として、次の情報が移動されました。

- **BGP の使用および構成**

  これは以下のように移動されました。

  移動元 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻 バージョン 3.1*

  移動先 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 2 巻 バージョン 3.1*

- **NHRP の使用および構成**

  これは以下のように移動されました。

  移動元 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻 バージョン 3.1*

  移動先 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 2 巻 バージョン 3.1*

この作業は、版を重ねながら進めていきます。この再編成についてご意見がおありの方は、本書の巻末のご意見記入用紙にご記入の上、郵便またはファックスでお送りください。

第1部 ソフトウェアの概要および使用

第1章 開始

この章では、IBM 2210 Nways マルチプロトコル・ルーター (2210) および マルチプロトコル・ルーティング・サービスに関連する以下のコンポーネントの使用を開始する方法について説明します。

- ルーター・コンソール端末
- ルーター・ソフトウェア (Multiprotocol Routing Services)
- ルーター・ソフトウェア・ユーザー・インターフェース

この章は、以下の節に分かれています。

- 『始める前に』
- 『現行リリースへの移行』
- 4ページの『ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス』

始める前に

開始する前に、以下のチェックリストを参照して、ルーターが正しく導入されているかどうかを検査してください。

チェックリスト

- 必要なハードウェアはすべて導入済みですか。
- コンソール端末 (ビデオ端末) はルーターに接続してありますか。

  重要: サービス・ポート接続端末を使用して IBM 2210 の構成または監視を行い、サービス端末が読み取り不能である場合は、構成の中のいくつかのパラメーターを変更する必要があります。 (IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual の “Service Terminal Display Unreadable” を参照してください。)
- ルーターは、該当するネットワーク・インターフェースやケーブルを使用してネットワークに接続してありますか。
- 必要なハードウェア診断はすべて実行しましたか。

以上の手順に関する詳細については、いずれも*IBM 2210 Nways マルチプロトコル・ルーター 計画とセットアップの手引き* を参照してください。

現行リリースへの移行

新しいコード・レベルへの移行についての詳細は、*Service and Maintenance Manual* を参照してください。

ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス

ルーター・コンソールからルーター・ユーザー・インターフェースを使用して、ルーターのネットワーキング・ソフトウェア (Multiprotocol Routing Services) の機能の監視や変更を行うことができます。ルーターはローカル・コンソールおよびリモート・コンソールをサポートしています。

ローカル・コンソール

ローカル・コンソールは、EIA 232 (RS-232) ケーブルによって直接接続されるか、あるいはモデムを介してルーターに接続されます。初期ソフトウェア導入時に、ローカル・コンソールを使用することが必要になる場合があります。初期セットアップ接続の後は、IP 転送が使用可能になっている限り、Telnet を介して接続することができます。(IP 転送を使用可能にする方法の詳細については、*プロトコルの構成と監視解説書* を参照してください。)

構成したルーターを初めて始動すると、画面にブート・メッセージが表示され、続いてオペレーターのコンソール (OPerator's CONsole) つまり OPCON プロンプト (*) が表示されます。 * プロンプトはルーターが OPCON コマンドを受信する準備ができていることを示しています。

ユーザーのマルチプロトコル・ルーティング・サービス・ソフトウェアは、工場で事前に構成されている場合があります。その場合、ローカル・コンソールを使用して初期構成を行う必要はありません。ただし、マルチプロトコル・ルーティング・サービスが工場で事前構成されていない場合は、2210 のサービス・ポートに接続された ASCII 端末を使用して、最初にその構成を行う必要があります。

重要: 不要情報、ランダム文字、逆疑問符、または端末を 2210 サービス・ポートに接続できないなどの問題が生じる場合、さまざまな原因が考えられます。以下に、それらの原因の一部のものをリストします。

- サービス・コンソール上に不要情報またはランダム文字が生じる最も一般的な原因は、ボー・レートが IBM 2210 と同期していないことです。

  2210 が特定のボー・レートに設定されている場合、端末または端末エミュレーターは、それと同じボー・レートに設定する必要があります。

  IBM 2210 が通信速度自動選択 (これがデフォルト) に設定されている場合は、端末の break キー・シーケンスを押して **Enter** を押します。

  PC 端末エミュレーターの一般的な BREAK キー・シーケンスは Alt-B です (端末エミュレーターの資料を参照してください)。 ASCII 端末はほとんどに **Break** キーが付いています (しばしば **Ctrl** キーと一緒に使用されます)。
- 端末または装置 (AC) の接地の欠陥
- 端末と IBM 2210 間の EIA 232 (RS-232) ケーブルの欠陥、不適正なシールド、または不適正な接地
- 端末または端末エミュレーターの欠陥
- IBM 2210 システム・ボードの欠陥
- 高レベルの電磁気干渉 (EMI)

- 送電線外乱

(*IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual* の “Service Terminal Display Unreadable” を参照してください。)

2210 が初期構成された後は、IP が使用可能である限り、ルーターの操作にローカル・コンソールを使う必要はありません。

ルーター・ソフトウエアによって、コンソールの活動は自動的に処理されます。ソフトウェアをアップグレードするときには、ローカル・コンソールを使用することが必要になる場合もあります。ローカル・コンソールの接続と構成に関しては、*IBM 2210 Nways マルチプロトコル・ルーター 計画とセットアップの手引き*、GA88-6228 を参照してください。

リモート・コンソール

リモート・コンソールは、標準リモート端末プロトコルを使用して、ルーターに接続されます。リモート・コンソールの機能は、ローカル・コンソールの場合と同じですが、 IBM 2210 が工場で事前構成されていない場合の初期構成には、ローカル・コンソールを使用する必要がある点が異なっています。

Telnet 接続

ルーターは、Telnet クライアントと Telnet サーバーの両方をサポートします。ルーター上のリモート・コンソールが Telnet サーバーの役を務めます。 OPCON (*) プロセスで **telnet** コマンドを使用して、ルーターから別のルーターまたはホストに接続するときは、ルーターは Telnet クライアントの役を務めます。

リモート・ログイン名およびパスワード

リモート・ログイン時には、ルーターはプロンプトによって、ログイン名およびパスワードの入力を指示します。リモート・コンソールからルーターにログインするときは、ルーターの **status** コマンドを使用することによって、ログイン名を表示することができます。

リモート・ログインまたはローカル・ログイン

ローカル・コンソールへのログインは、ホスト・システム上で Telnet を開始し、ルーターに接続する必要がある点を除けば、リモート・コンソールへのログインの場合と同じです。リモート・ログインの場合は、 5ページのステップ 1 から始めます。ローカル・ログインの場合は、 6ページのステップ 3 から始めます。

リモート・コンソールからログインする場合は、次のようにします。

1. ホスト・システム上で Telnet を開始して、ルーターに接続する。ホスト・システムとは、リモート端末が接続されているシステムのことです。
2. ルーターの名前またはインターネット・プロトコル (IP) アドレスを提供する。

   ルーター名を使用する場合は、ネットワークにネーム・サーバーがあることが必要です。次の例に示すように、ルーター名または IP アドレスを出します。

   ```
   % telnet brandenburg
   ```

または

```
% telnet 128.185.132.43
```

ここまでは、リモート・ログインとローカル・ログインには相違はありません。

3. プロンプトで指示されたら、ログイン名とパスワードを入力する。

```
login:
Password:
```

ログイン名はあるがパスワードはないということもあり得ます。パスワードは、ルーターへのアクセスを制御します。パスワードが設定されていない場合は、`Password:` プロンプトで **Enter** キーを押します。ログインは自動的には設定されません。セキュリティーのために、CONFIG プロセスで **add user** コマンドを使用して、ユーザー名とパスワードを設定することができます。詳細については、**add user** 構成コマンド (61ページ) を参照してください。リスタートして、変更をアクティブにするのを忘れないでください。

注: 初期プロンプトが表示されてから 1 分以内にログイン名と有効なパスワードを入力しなかった場合、または間違ったパスワードを 3 回連続して入力した場合、ルーターは Telnet 接続を切断します。

4. **Enter** キーを押して、メイン・プロンプトのアスタリスク (*) を表示する。

Enter キーを数回押すか、または **Ctrl-P** を押さないと、* プロンプトが表示されないことがあります。

この段階に達すれば、キーボードからのコマンドの入力を始めることができます。コマンド行に入力した最後の文字を削除するときは **後退** キーを押します。コマンド行の入力全体を削除してコマンドを再入力できるようにするには、**削除**キーまたは **Ctrl-U** を押します。前に入力したコマンドにアクセスする方法については、24ページの『GWCON および CONFIG コマンド行のコマンド活動記録』 を参照してください。

Telnet クライアント上でローカル Telnet コマンドを使用して、Telnet 接続をクローズすることもできます。

注: VT100 端末を使用している場合、**後退** キーを押すと目に見えない文字が挿入されるので、このキーは押さないようにしてください。その代わりに、**削除** キーを使用してください。

5. 7ページの『ルーターの終了』 の説明に従って、ルーターを終了します。

ルーターのリスタート

動的に構成されないユーザー構成可能パラメーターを変更した場合は、必ずルーターをリスタートして、変更を有効にする必要があります。そのためには、OPCON **restart** コマンドを入力します。 たとえば、次のように入力します。

```
* restart

Are you sure you want to restart the gateway? (Yes or [No]): yes
```

ルーターの終了

* プロンプトに戻って、Telnet 接続をクローズします。たとえば、次のように入力します。

```
IP Config> exit
Config> Ctrl-P
* logout

%
```

Telnet クライアント上でローカル Telnet コマンドを使用して、Telnet 接続をクローズすることもできます。

ユーザー・インターフェース・システムの説明

ルーター・ソフトウェア (Multiprotocol Routing Services) は、さまざまなプロセスおよびハードウェア装置間の CPU の使用をスケジュールするマルチタスク処理システムです。ルーター・ソフトウェアは、次のようなものです。

- タイミングおよびメモリー管理を行い、ユーザーがルーターの動作パラメーターの表示および変更を行うことができる、ローカルとリモートの両方のオペレーター・コンソールをサポートします。
- さまざまなユーザー・インターフェース・プロセス、すべてのネットワーク・インターフェース・ドライバー、およびルーターと共に購入されたすべてのプロトコル転送プログラムを含む、機能モジュールで構成されます。

第 1 レベル・ユーザー・インターフェースの定義

ソフトウェアへのユーザー・インターフェースは、メイン・メニュー (プロセス) といくつかの補助メニュー (プロセス) で構成されます。これらのメニューは、ソフトウェアの複数のレベルのプロセスに関連しています。

第 1 レベルのプロセスは、OPCON プロセスと CONFIG-ONLY プロセスから成っています。ほとんどの場合、OPCON プロセスを使用して第 2 レベルにアクセスし、IBM 2210 で実行する基本サービス、機能、インターフェース、およびプロトコルを構成または操作します。

第 2 レベルのプロセスは、**status** コマンドによってリストされるプロセスから構成されます。 talk*pid* コマンドを使用して、第 2 レベルのプロセスにアクセスできます。ソフトウェア内には使用できないプロセスもあります。プロセスの概要については、12ページの表1 を参照してください。

8ページの図1 は、各種のプロセスを示し、ルーター・ソフトウェアの構造内でのそれらの配置を示しています。

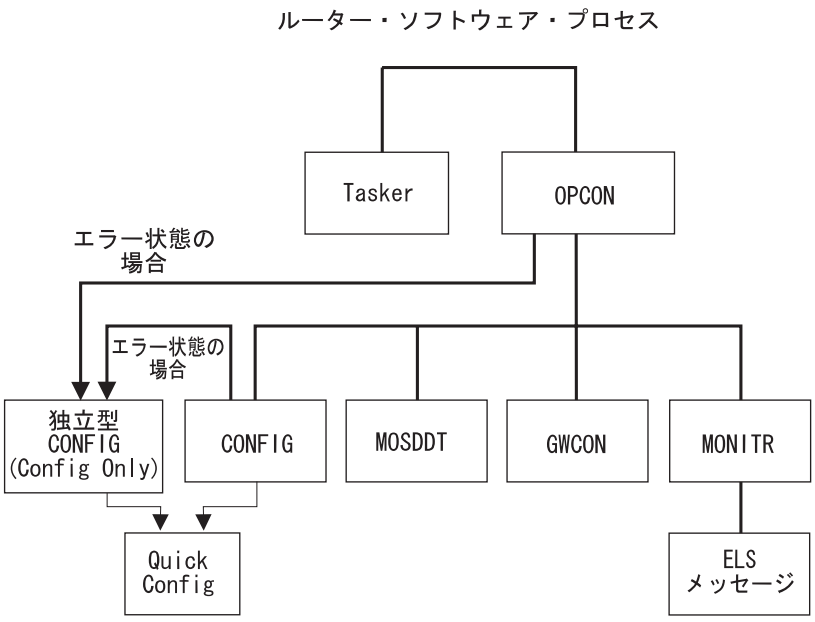


図 1. Multiprotocol Routing Services

図2 は、さまざまなプロセス・レベル間の関係の例を示しています。

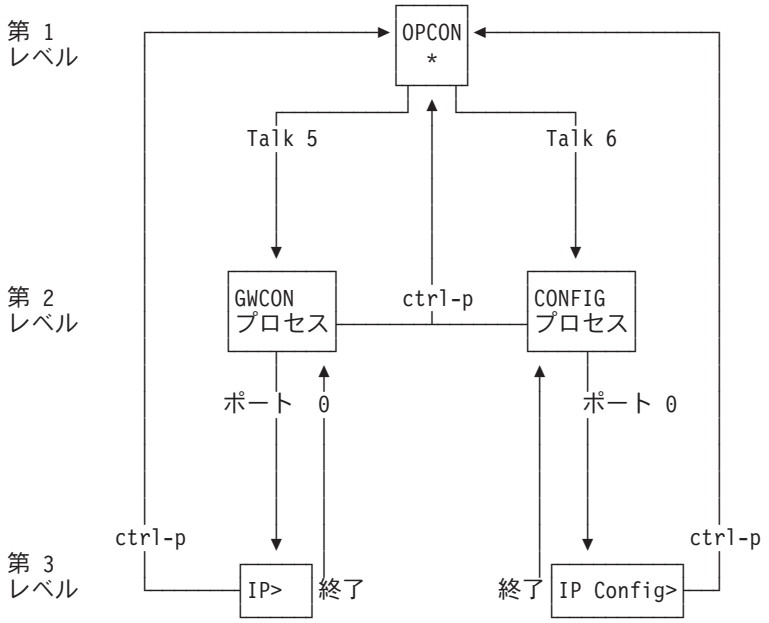


図 2. プロセスとコマンドの関係

注: 図2 には、各プロセス・レベルにアクセスしたり、各プロセス・レベルから戻ったりするのに使用される種々のコマンドも示されています。

OPCON についての詳細は、29ページの『第3章 OPCON プロセスおよびコマンド』を参照し、CONFIG-ONLY についての詳細は、45ページの『Config-Only モード』 を参照してください。

ROPCON プロセスは、リモート・コンソールからの処理を行うもので、基本的には OPCON プロセスと同じです。

クイック構成プロセス

クイック構成 (つまり、Quick Config) では、特定のオペレーティング・システム・コマンドを処理しなくても、ルーターの部分を即時に構成することができます。構成をもたないルーターを初期ロード、スタート、またはリスタートすると Config-Only に入り、そのプロセスから Quick Config メニューにアクセスできます。ルーターに装置が構成されており、その装置にプロトコルが構成されていない場合、ルーターは自動的に Config-Only でスタートし、その後で Quick Config に入ります。

また、CONFIG プロセスから **qconfig** コマンドを使用して Quick Config に入ることもできます。

システム・セキュリティー

add user コマンドを使用して、ログイン許可をもつ複数のユーザーを追加することもできます。セキュリティー問題についての詳細、および **set password** コマンドと **add user** コマンドの説明は、48ページの『ユーザー・アクセスの構成』 を参照してください。

第2章 ソフトウェアの使用

この章では、ソフトウェアの使用法について説明します。この章は次の各節に分かれています。

コマンドの入力

コマンドを入力する場合は、以下の点に留意します。

- 入力できるコマンドの中で、そのコマンドを固有に識別するのに十分な文字数を順次に入力します。たとえば、**reload** コマンドを実行する場合は、最小限として **rel** と入力する必要があります。コマンド構文について説明した章で、必要な最小文字数を下線で示してあります。
- コマンドは大文字・小文字の区別をしません。
- コマンド (および後続のオプション) の先頭文字を入力するだけで、コマンドを実行できる場合があります。たとえば、* プロンプトで **s** と入力し、その後に続けて **Enter** キーを押すだけで、**status** コマンドが実行されます。

プロセスへの接続

ルーターを開始すると、コンソールにブート・メッセージが表示されます。次に、OPCON プロンプト (*) が画面に表示され、これで OPCON プロセスに入ったので OPCON コマンドの入力を開始できることが示されます。これが異なるプロセスとの通信を行うコマンド・プロンプトになります。

コンソールをプロセスに接続するには、以下のようにします。

1. * プロンプトで **status** コマンドを入力して、プロセスのプロセス ID (PID) 番号を見つける。

   status コマンドは、プロセス ID (PID)、プロセス名、およびプロセスの状態など、ルーター・プロセスに関する情報を表示します。 **status** コマンドを出すと、次の例のような表示が得られます。

```
* status
Pid  Name      Status TTY  Comments
1    COpCn1    RDY    TTY0
2    Monitr    DET     --
```

```
3    Tasker    RDY     --
4    MOSDDT    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    Ezystrt   IDL     --
8    ROpCn1    IDL    TTY1 128.185.210.125
9    ROpCn2    IDL    TTY2
10   CES3      IDL     --
11   TOUT      IDL     --
12   L2S3      RDY     --
13   L3L2      RDY     --
14   LLL2      RDY     --
15   S3CE      RDY     --
```

2. **talk** *pid* コマンドを使用する。ただし、*pid* は、接続したいプロセスの番号です。 (これらのコマンドおよび他の OPCON コマンドの詳細については、29ページの『第3章 OPCON プロセスおよびコマンド』 を参照してください。)

   注: リストされたどのプロセスにもユーザー・インターフェースがあるとは限りません (たとえば、**talk 3** プロセス)。 **talk 4** コマンドは、IBM サービス技術員が使用するためのものです。

プロンプトの識別

各プロセスは、それぞれ異なるプロンプトを使用します。プロンプトを見れば、コンソールが接続されているプロセスが分かります。 (**talk** *pid* コマンドを入力してもプロンプトが表示されない場合は、**Return** キーを数回押してください。)

以下のリストは、3 つのメイン・プロセスのプロンプトを示しています。

表 1. プロセス、目的、アクセスするコマンド

プロセス	レベルと目的	アクセスするためのコマンド	入力プロンプト
OPCON	レベル 1 - すべての 2 次レベルへのアクセス	**Ctrl-P**	アスタリスク (*)
CONFIG	レベル 2 - 基本サービスの構成、および第 3 レベルの構成へのアクセス	**talk 6**	Config >
GWCON	レベル 2 - 基本サービスの動作と監視、および第 3 レベルの動作と監視へのアクセス	**talk 5**	正符号 (+)
MONITR	レベル 2 - メッセージの表示	**talk 2**	(なし)
MOSDDT	レベル 2 - 診断環境	**talk 4**	$
注: talk 4 コマンドの入力は、サービス技術員の指示のもとで行ってください。			

OPCON プロンプト・レベルで、キーボードからコマンドの入力を開始できます。コマンド行に入力した最後の文字を削除するときは **後退** キーを使用します。コマンド行の入力全体を削除してコマンドを再入力できるようにするには、**Ctrl-U** を使用します。前に入力したコマンドにアクセスする方法については、24ページの『GWCON および CONFIG コマンド行のコマンド活動記録』 を参照してください。

ヘルプの入手

上記のプロンプトのいずれも、そのレベルで利用可能なコマンドのリストという形でヘルプを得ることができます。このためには、**?** (**help** コマンド) を入力して、**Enter** を押します。 **?** は、現行プロンプト・レベルから利用可能なコマンドをリストするのに使用します。通常は特定のコマンド名の後に **?** を入力すると、そのオプションをリストすることもできます。たとえば、* プロンプトで **?** を入力すると、以下のように表示されます。

```
*?

BREAKPOINT

DIVERT output from process
FLUSH output from process
HALT output from process
INTERCEPT character is
LOGOUT
MEMORY statistics
RESTART
 RELOAD

STATUS of process(es)
TALK to process
TELNET to IP-Address
```

下位レベル環境の終了

ソフトウェアは複数レベルの構造になっているので、2210 を構成または動作するときには、2 次、3 次、およびさらに下位レベルの環境に入ります。すぐ上のレベルに戻るためには、**exit** コマンドを入力します。 2 次レベルに達するためには、2 次レベルのプロンプト (Config> または +) が得られるまで繰り返し **exit** を入力します。

たとえば、IP プロトコル構成プロセスを終了する場合は、次のように入力します。

```
IP config> exit
Config>
```

1 次プライマリー (OPCON) 到達する必要がある場合は、インターセプト文字 (デフォルトでは **Ctrl P**) を入力します。

OPCON に戻る方法

OPCON プロンプト (*) に戻るには、**Ctrl-P** を押します。 OPCON に戻ってからでなければ、別のプロセスと通信することはできません。たとえば、GWCON プロセスに接続されているときに CONFIG プロセスに接続したい場合、まず **Ctrl-P** を押して OPCON に戻る必要があります。 **Ctrl-P** キーの組み合わせは、デフォルトの*インターセプト文字* です。

第 3 レベル以下のレベルのプロセスからインターセプト文字 (デフォルトのインターセプト文字は **Ctrl-P**) を使用して * プロンプトに戻った場合、次回に **talk** コマンドを使用すると、再び第 3 レベル・プロセスに入ります。ルーターを再初期化すると、このリンクはなくなります。

構成に関する推奨事項

2210 の構成は、初めて構成するのか、既存の構成に基づいて構成を作成するのか、あるいは構成を更新するだけなのかによって異なります。以下の節は、ユーザーのニーズに応じて、最良の手順を使用するためのガイドとして使用してください。

初めて構成を作成する場合

この手順は、構成する 2210 と似たような構成をもつ 2210 が他に存在しないものと想定しています。また、2210 を箱から取り出したばかりであることも想定しています。この手順は順序付けて示してありますが、実際の構成は (ステップ 3 以降) どのような順序で行っても構いません。

IBM 2210 を初めて構成する場合は、次のようにします。

1. 構成する 2210 を調べて、構成する必要があるインターフェースを確認する。これは後で使用するので、メモしておいてください。
2. 4ページの『ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス』 の説明に従って、2210 に接続する。
3. 最初に、47ページの『クイック構成』 または 947ページの『付録A. クィック構成リファレンス』 で説明している Quick Config を使用して、2210 のポートと少なくとも装置の内部 IP アドレスを構成する。装置に Telnet 通信を行なうために必要な最小構成を行います。
4. 基本サービス (ブート・オプションなど) を構成する。 16ページの『構成プロセスへのアクセス、CONFIG (Talk 6)』 の説明に従って、構成プロセスにアクセスします。
5. インターフェースを構成する。 18ページの『ネットワーク・インターフェース構成プロセスへのアクセス』 の説明に従って、インターフェース構成プロセスにアクセスします。
6. 必要な機能を構成する。 22ページの『機能の構成プロセスおよび動作プロセスへのアクセス』 の説明に従って、機能構成プロセスにアクセスします。
7. この装置を通して実行するプロトコルを構成する。 23ページの『プロトコルの構成プロセスおよび動作プロセスへのアクセス』 の説明に従って、プロトコル構成プロセスにアクセスします。

   注: 最小限として、このステップで IP を構成します。
8. 6ページの『ルーターのリスタート』 の説明に従って、ルーターをリスタートする。

既存の構成に基づいて構成する場合

この節では、以下の方法について説明します。

- 稼働中の 2210 の構成に基づいて構成する
- 2210 の構成を永続的に更新する
- 2210 の稼働時に、2210 の構成を一時的に更新する

既存の構成に基づく構成

新規の 2210 に構成するものと同じインターフェース、機能、およびプロトコルを使用している 2210 がすでに存在する場合は、既存の 2210 に基づいて構成することにより、構成の時間を節約することができます。このタイプの構成は、コマンド行インターフェースまたは 2210 に付属の構成プログラムのいずれかを使用して行うことができます。いずれの場合も、2210 は実動ネットワークに組み込まれていないものと想定しています。

コマンド行インターフェースを使用して、既存の構成に基づいて構成する場合は、以下の手順で行います。

1. 使用する構成のコピーを入手する。
   a. OPCON (*) プロンプトで **talk 6** と入力する。
   b. `Config>` プロンプトで **boot** と入力する。
   c. `Boot config>` プロンプトで **copy** と入力する。詳細については、87ページの『第7章 ブート CONFIG プロセス』 を参照してください。
2. 構成する 2210 に接続する。
3. 15ページのステップ 1 で入手した構成を、 TFTP を使用して 2210 にロードする。87ページの『第7章 ブート CONFIG プロセス』 を参照してください。
4. 構成を更新する。
5. 2210 をリスタートする。

構成プログラムを使用して、既存の構成に基づいて構成する場合は、以下の手順で行います。

1. 構成プログラムを開始する。
2. この構成の基にする 2210 から構成を取り出す。
3. 新規の構成のために必要な変更を行う。この変更には、アドレス、ホスト名、ユーザー、およびその他の項目が含まれます。
4. 構成を、取り出した元の名前とは別の名前で保管する。
5. この構成を、構成する 2210 に送信する。
6. 2210 をリスタートする。

構成プログラムの使用法についての詳細は、*Nways マルチプロトコル・アクセス・サービス、ルーティング・サービス、スイッチ・サービス 構成プログラム 使用者の手引き* SC88-6657 を参照してください。

構成の永続的な更新

構成を永続的に更新する場合は、以下の手順で行います。

1. 4ページの『ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス』 の説明に従って、更新する 2210 にアクセスする。 `*` プロンプトが表示されるはずです。
2. **talk 6** コマンドを入力して、構成プロセスにアクセスする。
3. 該当するコマンドを入力して、変更する領域の構成を行う第 3 レベルのプロセスにアクセスする。

4. **exit** を必要な回数入力して、構成プロセスに戻る。
5. 2210 をリスタートする。

構成の一時的な更新

構成を永続的に更新できるようになるまでの期間、2210 の一部の動作特性を一時的に変更することができます。この機能により、ただちに変更を行って、問題の解決や性能の向上を図り、ピーク期間中の停止を回避することが可能になります。後で構成の永続的な更新を行い、停止をスケジュールし、装置をリスタートして、変更を有効にすることができます。

構成を一時的に更新するには、以下の手順で行います。

1. 4ページの『ローカルおよびリモート・コンソールを使用してのソフトウェアへのアクセス』 の説明に従って、更新する 2210 にアクセスする。 * プロンプトが表示されるはずです。
2. **talk 5** コマンドを入力して、動作/監視プロセスにアクセスする。
3. 該当するコマンドを入力して、変更する領域を監視する第 3 レベルのプロセスにアクセスする。
4. **exit** を必要な回数入力して、動作/監視プロセスに戻る。
5. **Ctrl-P** を入力して、* プロンプトに戻る。
6. 7ページの『ルーターの終了』 の説明に従って、ルーターを終了する。

第 2 レベルのプロセスへのアクセス

すべてのインターフェース、機能、およびプロトコルには、以下のプロセスにアクセスするためのコマンドがあります。

- インターフェース、機能、またはプロトコルを初期構成して使用可能にしたり、後で構成変更を行うための *構成* プロセス
- 各インターフェース、機能、またはプロトコルに関する情報を表示したり、構成を一時的に変更したり、あるいは構成変更をアクティブにしたりするための動作/監視プロセス

また、一部の基本システム・サービスも、第 2 レベル・プロセスを通して構成または動作することができます。これらの機能を実行するためのコマンドについては、43ページの『第5章 構成 (CONFIG) プロセスおよびコマンド (Talk 6)』 および 133ページの『第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』 で説明しています。

次の節では、第 2 プロセスにアクセスする手順について説明します。

構成プロセスへのアクセス、CONFIG (Talk 6)

各プロトコル構成プロセスには、ルーターの CONFIG プロセスを通してアクセスします。 CONFIG はルーター・ユーザー・インターフェースの第 2 レベルのプロセスで、第 3 レベルのプロセスとの通信を可能にします。第 3 レベルのプロセスの例としては、プロトコル・プロセスがあります。

CONFIG コマンド・インターフェースは、いくつかのレベル (モードと呼ばれる) で構成されています。プロトコル構成コマンド・インターフェースは、CONFIG インターフェースのモードです。各プロトコル構成インターフェースには、それぞれ独自のプロンプトがあります。たとえば、TCP/IP プロトコル・コマンド・インターフェースのプロンプトは `IP config>` です。

以下の項では、これらの手順についてさらに詳細に説明します。

CONFIG プロセスに入る方法

OPCON から CONFIG コマンド・プロセスに入り、CONFIG プロンプトを表示させるには、OPCON **talk** コマンドと CONFIG の PID を入力します。 CONFIG の PID は 6 です。

```
* talk 6
```

コンソールに CONFIG プロンプト (`Config>`) が表示されます。このプロンプトが表示されない場合は、再度 **Return** キーを押してください。

クイック構成プロセス: クイック構成 (つまり、Quick Config) では、特定のオペレーティング・システム・コマンドを処理しなくても、ルーターの部分を即時に構成することができます。 CONFIG プロセスから **qconfig** コマンドを使用すると、Quick Config メニューに入ります (47ページの『クイック構成』を参照してください)。

ルーターのリスタート

CONFIG を介してプロトコル・パラメーターに対して行われる変更は、動的な変更を含んでいるネットを起動するか、あるいはルーター・ソフトウェアをリスタートするまでは、有効になりません。

ルーターをルーターするには、OPCON **restart** コマンドを入力します。たとえば、次のように入力します。

```
*
restart
```

Are you sure you want to restart the router? (Yes or No): **yes**

動作/監視プロセスへのアクセス、GWCON (Talk 5)

インターフェース、機能、またはプロトコルに関する情報を表示したり、実行中にパラメーターを変更したりするためには、動作 (監視) プロセスにアクセスし、これを使用して行うことが必要です。動作コマンド・インターフェースは、GWCON インターフェースのモードです。 GWCON モード内では、各インターフェース、機能、またはプロトコル・インターフェースには、それぞれ独自のプロンプトがあります。たとえば、TCP/IP プロトコルのプロンプトは `IP>` です。

注: このプロセスで変更したパラメーターは、2210 の動作コードを再ロードすることが必要になったイベント (電源異常など) の後、あるいは**restart** コマンドを入力した後は、アクティブのままにはなりません。

以下の項では、これらの手順についてさらに詳細に説明します。

GWCON コマンド・プロセスに入る方法

OPCON から GWCON プロセスに入り、GWCON プロンプトを表示させるには、OPCON **talk** コマンドと GWCON の PID を入力します。たとえば、次のように入力します。

```
* talk 5
```

これにより、GWCON プロンプト (+) がコンソールに表示されます。このプロンプトが表示されない場合は、再度 **Return** キーを押してください。

第 3 レベルのプロセスへのアクセス

第 2 レベルにアクセスした後で、IBM 2210 のインターフェース、機能、およびプロトコルを構成または動作するために、第 3 レベルでコマンドを入力することが必要になる場合があります。以下の節では、第 3 レベルのプロセスにアクセスする方法について説明します。

ネットワーク・インターフェースの構成プロセスと動作プロセスへのアクセス

この節では、ネットワーク・インターフェースの構成プロセスおよび動作プロセスにアクセスし、プロセスを開始する方法について説明します。これらのプロセスにアクセスすると、ルーターで使用されているネットワーク・インターフェースのソフトウェア構成可能パラメーターを変更したり、監視したりすることができます。

ネットワーク・インターフェース構成プロセスへのアクセス

ルーターの構成プロセスにアクセスするには、以下の手順を使用します。このプロセスにより、特定のインターフェースの構成 プロセスにアクセスすることができます。

1. OPCON プロンプトで、OPCON **talk** コマンドと CONFIG の PID を入力する。(このコマンドの詳細については、29ページの『第3章 OPCON プロセスおよびコマンド』 を参照してください。)

   ```
   * talk 6
   ```

   talk 6 コマンドを入力すると、CONFIG プロンプト (Config>) がコンソールに表示されます。最初に **CONFIG** に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

   add device コマンドを使用して、ネットワーク・インターフェースを作成します。 **add device** コマンドは、自動的にインターフェース番号を割り当て、以下のタイプの装置をサポートします (**add device ?** と入力すると、サポートされる装置タイプが表示されます)。

   a. ダイヤル回線

      次の例は、ダイヤル回線インターフェースを追加します。

      ```
      Config> add device dial-circuit
      Enter the number of PPP Dial Circuit interfaces [1]?
      Adding device as interface 8
      Base net for this circuit[0]?4
      ```

```
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 8" command to configure circuit parameters
```

b. 次の例は、ダイヤルイン回線を追加します。

```
Config>add device dial-in
Enter the number of dial-in interfaces [1]?
Adding device as interface 5
Base net for this circuit [0]? 5
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 5" command to configure circuit parameters
```

c. 次の例は、ダイヤルアウト回線を追加します。

注: ダイヤルアウト装置タイプは、ソフトウェア・ロードに DIAL 機能が含まれている場合にのみサポートされます。

```
Config>add device dial-out*
Enter the number of dial-out interfaces [1]?
Adding device as interface 6*
Base net for this circuit [0]? 4
Defaulting Data-link protocol to Dial-out*
Use "net 6" command to configure circuit parameters*
```

d. マルチリンク PPP

次の例は、マルチリンク PPP インターフェースを追加します。

```
Config>add device multilink-ppp
Enter the number of Multilink PPP interfaces [1]?
Adding device as interface 7
Defaulting Data-link protocol to PPP
Use "net 7" command to configure circuit parameters
```

注:

a. 基本ポート、ならびに機能スロットがあるモデルの機能スロットに挿入されたアダプターのポートについては、インターフェースは自動的に作成されるので、**add device** コマンドを使用する必要があるのは、バーチャル・インターフェースを作成するときだけです。以下の例は、追加できるバーチャル・インターフェースのタイプを示しています。

b. シリアル・アダプターまたはダイヤル回線用のインターフェースを作成する場合、デフォルトのデータ・リンク・タイプは PPP になりますが、 **set data-link** コマンドを使用して、データ・リンク・タイプを変更することができます。シリアル・ポートおよびダイヤル回線でサポートされるデータ・リンク・タイプについては 20ページの表2 を参照し、80ページの **set data-link** コマンドの説明をお読みください。

2. Config > プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。次のような表示が出ます。

```
Config> list devices

Ifc 0 Ethernet                      CSR  81600, CSR2  80C00, vector 94
Ifc 1 WAN X.25                      CSR  81620, CSR2  80D00, vector 93
Ifc 2 WAN X.25                      CSR  81640, CSR2  80E00, vector 92
Ifc 3 WAN PPP                       CSR 381620, CSR2 380D00, vector 125
Ifc 4 WAN Frame Relay               CSR 381640, CSR2 380E00, vector 124
Ifc 5 Token Ring                    CSR 600000, vector
95
```

3. インターフェース番号を記録する。
4. CONFIG **network** コマンドと、構成するインターフェースの番号を入力する。 たとえば、次のように入力します。

```
Config> network 1
```

該当する構成プロンプト(たとえば、トークンリングの場合は TKR Config>)がコンソールに表示されます。

注: ネットワーク・インターフェースは、すべてがユーザーによる構成が可能とは限りません。構成できないインターフェースの場合は、次のようなメッセージが出ます。

```
That network is not configurable
```

インターフェース構成の表示: 同じインターフェース構成プロンプトから、 **list** コマンドを使用して、選択したインターフェースに特定の構成情報をリストすることができます。たとえば、次のように入力します。

```
TKR Config> list

Token-Ring configuration:

PACKET SIZE (INFO FIELD): 4472
Speed:                    16 Mb/sec
Media:                    Shielded

RIF Aging Timer:          120     Source Routing:          Enabled
MAC Address:              000000000000
```

ネットワーク・インターフェースの構成: IBM 2210 のネットワーク・インターフェースの構成についての詳しい情報は、本書の該当する章を参照してください。

表2 は、ネットワーク体系と各体系でサポートされるインターフェースをリストしています。

表 2. ネットワーク体系とサポートされるインターフェース

ネットワーク体系	サポートされるインターフェース
ATM	IBM 2210 用のデュアル・ポート・シリアル・インターフェース (25 Mbps)
802.5 トークンリング	IBM 2210 トークンリング 4/16 インターフェース
イーサネット	IBM 2210イーサネット・インターフェース
ISDN	以下の、IBM 2210 用シリアル・インターフェース 基本インターフェース (BRI) PRI/チャネル化 T1/J1 インターフェース * PRI/チャネル化 E1 インターフェース * **注:** アスタリスク (*) が付いているインターフェースは、ISDN またはチャネル化インターフェースかとして使用できます。
ポイント・ポイント	IBM 2210 用のシリアル・インターフェース、ダイヤル回線インターフェース、 4 ポートまたは 8 ポート WAN 集線アダプターでサポート。
フレーム・リレー	IBM 2210 用のシリアル・インターフェース、ダイヤル回線インターフェース、 4 ポートまたは 8 ポート WAN 集線アダプターでサポート。
X.25	IBM 2210 用のシリアル・インターフェース、4 ポートおよび 8 ポート WAN 集線アダプターおよびダイヤル回線でサポート
SDLC リレー	IBM 2210 用のシリアル・インターフェース、4 ポートおよび 8 ポート WAN 集線アダプターでサポート、ダイヤル回線インターフェース

表 2. ネットワーク体系とサポートされるインターフェース (続き)

ネットワーク体系	サポートされるインターフェース
SDLC	IBM 2210 用のシリアル・インターフェース、4 ポートおよび 8 ポート WAN 集線アダプターおよびダイヤル回線でサポート
V.25bis	IBM 2210 用のシリアル・インターフェース、 4 ポートおよび 8 ポート WAN 集線アダプターでサポート
V.34	IBM 2210 用のシリアル・インターフェース、4 ポートまたは 8 ポート WAN 集線アダプター、または 4 ポートおよび 8 ポート内蔵モデムでサポート
ダイヤルアウト	V.34 基底インターフェースを介した DIAL および Telnet ダイヤルアウトをサポート
ダイヤルイン	PPP ダイヤル回線インターフェース。構成パラメーターのデフォルトでは DIAL をサポートする
マルチリンク PPP (MP)	物理インターフェースではサポートされない。ISDN バーチャル・インターフェース上でのみサポートされる。
L2TP	レイヤー 2 トンネル伝送プロトコル (L2TP) を通して、バーチャル PPP DIAL 接続をサポート

注:

1. PPP ダイヤル回線インターフェースは、ISDN、V.25bis、または V.34 ネットワークを基本ネットワーク・インターフェースとして使用できます。
2. FR ダイヤル回線インターフェースは、ISDN または V.25bis ネットワークを基本ネットワーク・インターフェースとして使用できます。
3. ダイヤルアウト回線インターフェースは、V.34 ネットワークを基本ネットワーク・インターフェースとして使用できます。
4. ダイヤルイン回線インターフェースは、ISDN または V.34 ネットワークを基本ネットワーク・インターフェースとして使用できます。
5. SDLC ダイヤル回線は、V.25bis を基本ネットワーク・インターフェースとして使用できます。
6. X.25 は、ISDN B チャネルを基本ネットワーク・インターフェースとして使用できます。

ネットワーク・インターフェース・コンソール・プロセスへのアクセス

特定のインターフェースに関連する情報を監視する場合は、以下の手順を使用して、インターフェース・コンソール・プロセスにアクセスします。

1. OPCON プロンプトで、OPCON **talk** コマンドと GWCON の PID を入力する。たとえば、次のように入力します。

   ```
   * talk 5
   ```

2. GWCON プロンプト (+) がコンソールに表示される。最初に GWCON に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。
3. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

```
+ configuration

Portable M68360 C Gateway [not configured] S/N 207
Multiprotocol Routing Services
5801-ARR Feature 5xxx V1 R2.0 PTF 0 RPQ 0
Boot ROM version  1.20     Watchdog timer enabled    Auto-boot enabled

Time: 13:34:56    Thursday     March 9, 1995       Console baud rate: 9600

Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge

Num Name  Feature
1   BRS   Bandwidth Reservation
2   MCF   MAC Filtering

3 Networks:
Net Interface  MAC/Data-Link         Hardware         State
0   Eth/0      Ethernet/IEEE 802.3   SCC Ethernet     Up
1   PPP/0      Point to Point        SCC Serial Line  Up
2   PPP/1      Point to Point        SCC Serial Line
UP
```

4. GWCON **network** コマンドと監視したいインターフェースの番号を入力する。たとえば、次のように入力します。

```
+ network 2
X.25>
```

この例では、X.25 コンソール・プロンプトがコンソールに表示されます。ここで X.25 コンソール・コマンドを入力して、X.25 インターフェースに関する情報を表示させることができます。

ネットワーク・インターフェースの監視: 2210 のネットワーク・インターフェースの監視についての詳しい情報は、本書の該当する章を参照してください。

機能の構成プロセスおよび動作プロセスへのアクセス

マルチプロトコル・ルーティング・サービスの機能の構成プロセスおよび動作プロセスにアクセスするのに役立つように、この節ではこれらの手順の両方について概説します。

機能プロセスへのアクセス

プロトコル構成プロセスおよびネットワーク・インターフェース構成プロセス以外の、マルチプロトコル・ルーティング・サービスの特定の機能に関する構成コマンドにアクセスする場合は、 CONFIG プロセスから **feature** コマンドを使用します。

プロトコル・コンソール・プロセスおよびネットワーク・インターフェース・コンソール・プロセス以外の、特定の機能に関するコンソール・コマンドにアクセスする場合は、GWCON プロセスから **feature** コマンドを使用します。

使用しているソフトウェア・リリースで使用可能な機能のリストを表示させるには、**feature** コマンドの後に疑問符を入力します。たとえば、次のように入力します。

```
Config> feature ?

WRS
BRS
MCF

Feature name or number [1] ?
```

特定の機能の構成プロンプトまたは動作プロンプトにアクセスするには、それぞれ Config> または + (GWCON) プロンプトで、**feature** コマンドに続けて機能の番号または短縮名を入力します。たとえば、次のように入力します。

```
Config> feature mcf

MAC filtering user configuration

Filter Config>
```

72ページの表8 は、使用できる機能の番号と名前をリストしています。

機能の構成プロンプトまたは動作プロンプトにアクセスしたら、その機能の特定コマンドの入力を開始することができます。直前のプロンプト・レベルに戻るには、機能のプロンプトで **exit** コマンドを入力します。

プロトコルの構成プロセスおよび動作プロセスへのアクセス

この節では、プロトコルの構成プロセスおよび動作プロセスにアクセスする方法について説明します。

プロトコル構成プロセスに入る方法

CONFIG プロンプトから、必要なプロトコル構成プロセスに入るには、次のようにします。

1. CONFIG プロンプトで **list configuration** コマンドを使用して、ソフトウェアのコピーとして購入したプロトコルの番号と名前を表示する。 **list configuration** コマンドの出力例については、73 ページを参照してください。
2. Config> プロンプトで、構成したいプロトコルの番号と短縮名 (たとえば、IP、IPX、および ARP) を指定して **protocol**コマンドを入力する。 プロトコル番号と短縮名は **list configuration** コマンドの画面から入手します。次の例では、IP プロトコル構成プロセスにアクセスするためのコマンドが入力されています。

   ```
   Config> protocol IP
   ```

   または

   ```
   Config> protocol 0
   ```

   これにより、プロトコル構成プロンプトがコンソールに表示されます。次の例は、IP プロトコル構成プロンプトを示しています。

   ```
   IP config>
   ```

これで、このプロトコルの構成コマンドの入力を開始することができます。特定のプロトコル構成コマンドの詳細については、*Protocol Configuration and Monitoring Reference* の該当するプロトコルのセクションを参照してください。

要約すると、**protocol** コマンドを使用すると、ルーターに導入されているプロトコル・ソフトウェアの構成プロセスに入ることができます。 **protocol** コマンドは、プ

ロトコルのコマンド・プロセスに入ります。 protocol コマンドを入力すると、指定されたプロトコルのプロンプトが表示されます。このプロンプトから、そのプロトコル特定のコマンドを入力できます。

プロトコル動作プロセスに入る方法

GWCON プロンプトからプロトコル・コンソール・プロセスに入るには、次のようにします。

1. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。 たとえば、次のように入力します。

```
+ configuration

Portable M68360 C Gateway BENNY S/N 207
Multiprotocol Routing Services
5801-ARR Feature 5xxx V1 R2.0 PTF 0 RPQ 0
Boot ROM version  1.10     Watchdog timer enabled    Auto-boot enabled
Time: 13:43:04    Thursday     March 9, 1995       Console baud rate: 9600

Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
7   IPX   Netware IPX
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
26  DLS   Data Link Switching

Num Name  Feature
1   BRS   Bandwidth Reservation
2   MCF   MAC Filtering

3 Networks:
Net Interface  MAC/Data-Link         Hardware            State
0   TKR/0      Token-Ring/802.5      IBM Token-Ring      Up
1   FR/0       Frame Relay           SCC Serial Line     Down
2   PPP/0      Point to Point        SCC Serial Line
Up
```

2. 構成情報に表示されている必要なプロトコルのプロトコル番号と短縮名を指定して、GWCON **protocol** コマンドを入力する。

   次の例では、IP プロトコル・コンソール・プロセスにアクセスするためのコマンドが入力されています。

```
+ protocol 0
```

   または

```
+ protocol IP
```

   これにより、プロトコル・コンソール・プロンプトがコンソールに表示されます。次の例は、IP プロトコル・コンソール・プロンプトを示しています。

```
IP>
```

これで、このプロトコルのコマンドを入力し始めることができます。特定のプロトコル・コンソール・コマンドの詳細については、*Protocol Configuration and Monitoring Reference* の該当するプロトコルのセクションを参照してください。

GWCON および CONFIG コマンド行のコマンド活動記録

コマンド活動記録には、ユーザーが GWCON (Talk 5) または CONFIG (Talk 6) コマンド行メニューから入力したコマンドが、最大で最後の 50 個が入っています。

逆方向および順方向の検索キーを使用して、以前に入力したコマンドを再度呼び出すことができます。また、熟練したユーザー向けに、一連の特定コマンドを反復して使用できる機能も用意されています。

コマンド活動記録内のコマンドの反復

GWCON または CONFIG メニュー内の任意のコマンド行プロンプトで **Ctrl-B** (backward) または **Ctrl-F** (forward) を押すと、現行のコマンド行が、コマンド活動記録内の前のコマンドまたは次のコマンドと置き換わります。コマンド活動記録は、GWCON と CONFIG の両方に共通です。つまり、GWCON メニューで入力したコマンドを CONFIG 内から検索したり、CONFIG メニューで入力したコマンドを GWCON から検索するといったことが可能です。

コマンド活動記録には、最新に入力されたコマンドが、最大で最後の 50 個が入っています。リスタート後に 3 つのコマンドしか入力していない場合、**Ctrl-F** または **Ctrl-B** を押すと、この 3 つのコマンドだけが循環します。それまでに 1 つもコマンドを入力していない場合、**Ctrl-F** または **Ctrl-B** を押すと、『ベル』 がなります。このベルは、次行の先頭を越えてさらに後退キーを押そうとしたときに鳴るものと同じものです。

注: **Ctrl-U** を押して打ち切られたコマンドは、コマンド活動記録には入力されません。

2 つの類似したコマンドを入力する場合は、

```
display sub les
display sub lec
```

次のようにします。

display sub les と入力して、**Enter** を押します。

Ctrl-B (Backward) を押すと、現在の行が次の行で置き換えられます。

```
display sub les
```

Backspace を押して、『s』 を 『c』 で置き換えます。

display sub lec となるので、 **Enter** を押します。

コマンド活動記録内の一連のコマンドの反復

上級のユーザー向けに、特定の一連の GWCON または CONFIG コマンドを簡単に反復使用することができる追加機能が提供されています。コマンド活動記録の中の C1, C2,...,Cn を*反復シーケンス* と呼びます。この機能は、あるタスクの中で複数のコマンドを反復して使用する必要がある場合に、単に **Ctrl-B** および **Ctrl-F** だけを使うよりも便利なことがあります。コマンド C1 で **Ctrl-R** (repeat) を入力して、*反復シーケンス* の開始をセットします。続いて **Ctrl-N** (next) を入力して、反復シーケンス内の次のコマンドを取り出します。コマンドは自動的に入力されるのではなく、現行のコマンド行に置かれるので、ユーザーはそのコマンドを修正したり、入力したりすることができます。

必要な動作を実行する反復シーケンスを作成するために、初めに **Ctrl-N** (next) を使用して取り出される最初のコマンドは、**Ctrl-R** (repeat) を使用してセットされた反復シーケンスの開始方法によって異なったものになります。

Ctrl-R を使用して反復シーケンスの開始をセットするには、次の 2 通りの方法があります。

1. C1 を最初に入力するときにセットする
2. **Ctrl-B** または **Ctrl-F** を使用してコマンド活動記録から C1 を取り出したときにセットする。

コマンドの入力時に反復シーケンスを開始

コマンド C1 を入力するときに **Ctrl-R** を入力し、次にコマンド C2, C3... Cn を入力した場合、 **Ctrl-N** を入力すると、コマンド C1, C2, ... Cn, C1, C2, ... Cn, C1, ... が連続的にコマンド行に置かれます。

例 1 では、反復シーケンスの開始は、最初のコマンドの入力時にセットされています。ユーザーは事前に、GWCON に入力するのと同じコマンドを CONFIG で反復する必要があることを知っています。

例 1

1. シーケンスの最初のコマンドを入力するときに、**Ctrl-R** (repeat) を使用して、反復シーケンスの開始をセットする。

   ```
   *talk 5
   +event Ctrl-R
   ```

   ここで **Enter** を押して、反復シーケンスをセットします。
2. シーケンス内の後続のコマンドを入力する。

   ```
   Event Logging System user console
     ELS>display sub les
     ELS>display sub lec
     ELS>exit
     +
   ```
3. これと同じコマンドを CONFIG に入力するために、

   Ctrl-P (デフォルトの OPCON インターセプト文字) を押して、CONFIG に行く。

   ```
   +-pressCtrl-P-
   *talk 6
   Config>Ctrl-N for NEXT to retrieve the start of
          this sequence-
   Config>event Enter
   Event Logging System user configuration
   ELS config>Ctrl-N for NEXT to retrieve the next
              command in sequence-
   ELS config>display sub les Enter
   ELS config>Ctrl-N for NEXT to retrieve the next
              command in sequence-
   ELS config>display sub lec Enter
   ELS config>Ctrl-N for NEXT to retrieve the next
              command in sequence-
   ELS config>exit Enter
   Config>
   ```

すべてのコマンドの入力後に反復シーケンスを開始

一方、最初に C1, C2, ... Cn を入力した場合は、**Ctrl-B** または **Ctrl-F** を使用して C1 を取り出します。 **Ctrl-R** を入力し、**Ctrl-N** を入力すると、コマンド C2,..., Cn, C1, C2,..., Cn, C1,...,Cn がコマンド行に連続して置かれます (例 2 を参照)。 C1 が取り出されたときには、C1 はすでにコマンド行に置かれており、最初の **Ctrl-N** で再度呼び出す必要はないので、最初の C1 はバイパスされます。

例 2 では、すべてのコマンドを入力した後で、反復するシーケンスの最初のコマンドを取り出します。一連のコマンドが GWCON で入力されており、同じシーケンスを CONFIG で反復する必要があります。

例 2

1. 以下のコマンドを GWCON に入力する。

```
*talk 5
+event
Event Logging System user console
ELS>display sub les
ELS>display sub lec
ELS>exit
+
```

2. これと同じコマンドを CONFIG に入力するために、**Ctrl-P** (デフォルトの OPCON インターセプト文字) を押して、CONFIG に行く。

```
+Ctrl-P-
*talk 6
Config>Ctrl-B four times to retrieve the start of
        the four command sequence in this example-
Config>event
Config>event Ctrl-R for REPEAT to set the start of
             the repeat sequence-
 Config>event Enter
 Event Logging System user configuration
 ELS config>Ctrl-N for NEXT to retrieve the next
             command in sequence-
 ELS config>display sub les Enter
 ELS config>Ctrl-N for NEXT to retrieve the next
             command in sequence-
 ELS config>display sub lec Enter
 ELS config>Ctrl-N for NEXT to retrieve the next
             command in sequence-
 ELS config>exit Enter
 Config>
```

29ページの『第3章 OPCON プロセスおよびコマンド』 に記述されているように OPCON **intercept** コマンドを使用して OPCON インターセプト文字をデフォルト文字の **Ctrl-P** からコマンド活動記録制御文字の**Ctrl-B**、**Ctrl-F**、**Ctrl-R**、または **Ctrl-N** に定義し直した場合には、OPCON インターセプト文字が優先されます。たとえば、インターセプト文字を **Ctrl-F** に変更した場合、**Ctrl-F** はコマンド活動記録を順方向に検索するのではなく、OPCON プロンプト (*) に戻します。

第3章 OPCON プロセスおよびコマンド

この章では、OPCON プロセスについて説明します。この章は次の各節に分かれています。

- 『OPCON とは』
- 31ページの『OPCON プロセスへのアクセス』
- 31ページの『OPCON コマンド』

OPCON とは

オペレーター・コンソール・プロセス (OPCON) は、ルーター・ソフトウェア・ユーザー・インターフェースのルート・レベルのプロセスです。 OPCON の主な機能は、どのプロセスをコンソールに接続するかを制御することです。 OPCON コマンドを使用して、以下のことが行えます。

- プロセスからの出力を操作する
- インターセプト文字を変更する
- ルーター・メモリーの使用状況に関する情報を表示する
- ルーター・ソフトウェアをリスタートする
- ルーター・ソフトウェアを再ロード (リブート) する
- 基本 LAN スイッチ・コンソールに戻る
- 他のルーターまたはホストに Telnet 接続する
- すべてのルーター・プロセスに関する情報を表示する
- 2 次レベルのプロセスと通信する
- MOS システム・デバッグ・ツールにエスケープする

第4章 OPCON の構成

この章では、OPCON インターフェースの構成コマンドおよび動作コマンドについて説明します。この章は、次の節に分かれています。

- 『OPCON プロセスへのアクセス』
- 『OPCON コマンド』

OPCON プロセスへのアクセス

初めてルーターを開始すると、コンソールにブート・メッセージが表示されます。次に、OPCON プロンプト (*) がコンソールに表示され、OPCON プロセスがアクティブになり、OPCON コマンドを受け入れる準備が整ったことを示します。

OPCON プロセスでは、ルーターの動作パラメーターのすべてを構成、変更、および監視することができます。 OPCON プロセスにいるときは、ルーターはデータを転送しています。ルーターがブートされて OPCON に入ると、著作権ロゴとアスタリスク (*) プロンプトが、ローカル接続されたコンソール端末に表示されます。これが OPCON (OPerator's CONsole) プロンプトで、第 2 レベルのプロセスへのアクセスを可能にする、メイン・ユーザー・インターフェースです。

OPCON で行われるルーターの動作パラメーターの変更の一部のものは、ルーターを再初期化しなくても、即時に有効になります。変更が有効にならない場合は、* プロンプトで **restart** コマンドを使用します。

* プロンプトで入力できる広範なコマンド・セットが用意されており、これらを使用して、各種の内部ソフトウェアの状況を検査したり、ルーターのインターフェースおよびパケット転送の性能を監視したり、さまざまな動作パラメーターを構成したりすることができます。

OPCON コマンド

この節では OPCON コマンドについて説明します。各コマンドについて、説明、構文の要件、および例を示します。 OPCON コマンドの要約を 表3 に示します。これらのコマンドを使用するには、OPCON プロセスにアクセスし、OPCON プロンプト (*) で該当のコマンドを入力します。

表 3. OPCON コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Breakpoint	MOS システム・デバッグ・ツールに入ります。
Divert	プロセスからの出力をコンソールまたは他の端末に送ります。
Flush	プロセスからの出力を廃棄します。
Halt	プロセスからの出力を中断します。
Intercept	デフォルトの OPCON インターセプト文字を設定します。
Logout	リモート・コンソールをログアウトします。

表 3. OPCON コマンド (続き)

コマンド	機能
Memory	ルーターのメモリーの使用状況を報告します。
Pause	EasyStart を一時中止します (EasyStart の場合のみ)
Restart	ルーター・ソフトウェアをリスタートします (再ロードはしません)。
Status	すべてのルーター・プロセスに関する情報を示します。
Stop	EasyStart を停止し、Config Only モードに入ります (EasyStart の場合のみ)。
Talk	別のルーター・プロセスに接続し、そのコマンドの使用を可能にします。
Telnet	別のルーターに接続します。

Breakpoint

breakpoint コマンドは、MOS デバッグ・ツール内の情報のトラップする、メモリーを検査する、区切り点を配置する、あるいはメモリー・ダンプを取るのに使用します。このコマンドを使用するのは、ソフトウェア専門の担当者のみに限定します。

このコマンドを呼び出すときに見張りタイマーがオンになっている場合、見張りタイマーが作動すると、コア・メモリーの内容がダンプされます (ダンプ処理が使用可能になっている場合)。すべてのルーティング・プロセスが一時停止されます。

breakpoint コマンドは、ローカル・コンソールから出さなければなりません。

注: このコマンドは、ソフトウェアの動作を完全に停止するので、通常の動作中はこのコマンドを使用してはなりません。誤って **breakpoint** コマンドを入力してしまった場合は、素早く **Esc** を押してから **p** を押してください。

構文:

breakpoint

Divert

divert コマンドは、指定のプロセスからの出力を指定の端末に送信するのに使用します。 このコマンドを使用すると、複数のプロセスの出力を同じ端末に着信転送し、出力を同時に見ることができます。 **divert** が通常使用されるのは、MONITR 出力メッセージを特定の端末に転送する場合です。ルーターで着信転送が許されるのは、特定のプロセスだけです。

このコマンドを入力した後に PID と tty# (出力端末の番号) を入力します。これらの値は、OPCON status コマンドを使用して入手することができます。端末番号は、ローカル・コンソール (tty0) またはリモート・コンソール (tty1, tty2) の 1 つのいずれかです。次の例は、MONITR プロセス (2) で生成されたイベント・ログ・システム・メッセージをリモート・コンソール *tty1* (1) に送信する場合を示しています。

イベント・メッセージは、コマンドを入力している最中であっても、即時に表示されます。コマンドが混同されるのを防止するために、ディスプレイとキーボードにはそれぞれ別々のバッファーが用意されています。次の例は、**divert 2 1** コマンドの実行後、 MONITR プロセスが TTY1 に接続されたことを示しています。出力を停止したい場合は、**halt 2** と入力します。 **halt** コマンドについては、33ページの『Halt』で説明しています。

構文:

divert *pid tty#*

例: divert 2 1

```
Copyright Notices:
Copyright IBM Corp. 1994, 1997
MOS Operator Control


* divert 2 1

* status
Pid  Name      Status TTY  Comments
1    COpCN1    IOW    TTY0 gzs
2    Monitr    IDL    TTY0
3    Tasker    RDY     --
4    MOSDDT    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    Ezystrt   IDL     --
8    ROpCN1    IDL    TTY1
9    ROpCN2    RDY    TTY2 jlg@128.185.40.40
10   CES3      IDL    --
11   TOUT      IDL    --
12   L2S3      IDL    --
13   L3L2      IDL    --
14   LLL2      IDL    --
15   S3CE      IDL    --
```

Flush

flush コマンドは、MONITR プロセスの出力バッファーを消去するのに使用します。一般的に、このコマンドは MONITR の FIFO バッファーの内容を表示する前に使用され、メッセージがスクロールして画面から消えるのを防止します。累積されたメッセージは廃棄されます。

ルーターで着信転送が許されるのは、特定のプロセスだけです。 *pid* と *tty#* を入手するには、OPCON **status** コマンドを使用します。次の例では、**flush 2** コマンドを実行すると、MONITR プロセスの出力は SNK (フラッシュ済み) に送信されます。

構文:

flush *pid*

例: flush 2

```
* status
Pid  Name      Status TTY  Comments
1    COpCN1    IOW    TTY0 gzs
2    Monitr    IDL    SNK
3    Tasker    RDY     --
4    MOSDDT    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    Ezystrt   IDL     --
8    ROpCN1    IDL    TTY1
9    ROpCN2    RDY    TTY2 jlg@128.185.40.40
```

Halt

halt コマンドは、指定のプロセスからのすべての後続の出力を、そのプロセスに対して **divert**、**flush**、または **talk** OPCON コマンドが出されるまで中断するのに使用します。 ルーターは、すべてのプロセスを転送できるわけではありません。 **Halt** は、

プロセスからの出力のデフォルトの状態です。このコマンドで使用する PID を入手するには、OPCON **status** コマンドを使用します。次の例では、**halt 2** コマンドの実行後は、MONITR プロセスは TTY1 に接続されなくなります。イベント・メッセージも表示されなくなります。

構文:

halt *pid*

例: halt 2

```
* status
Pid  Name      Status TTY  Comments
1    COpCN1    IOW    TTY0 gzs
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDDT    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    Ezystrt   IDL     --
8    ROpCN1    IDL    TTY1
9    ROpCN2    RDY    TTY2 jlg@128.185.40.40
```

Intercept

intercept コマンドは、 OPCON インターセプト文字を変更するのに使用します。 インターセプト文字とは、OPCON プロセスに戻るために、他のプロセスから入力する文字です。デフォルトのインターセプト・キーの組み合わせは **Ctrl-P** です。

インターセプト文字は、制御文字で***なければなりません***。 (シフト 6) 文字に続けて、インターセプト文字として使用する英字を入力します。

注: インターセプト文字は、Return キーまたは印刷可能文字に設定しないでください。OPCON インターセプト文字を、デフォルトの **Ctrl-P** からコマンド活動記録制御文字の 1 つ (**Ctrl-B**、 **Ctrl-F**、**Ctrl-R**、または **Ctrl-N**) に変更した場合、OPCON インターセプト文字が優先されます。

たとえば、インターセプト文字を **Ctrl-F** に変更した場合、**Ctrl-F** はコマンド活動記録を順方向に検索するのではなく、OPCON プロンプト (*) に戻ります。前に入力した GWCON または CONFIG コマンドにアクセスする方法については、 24ページの『GWCON および CONFIG コマンド行のコマンド活動記録』 を参照してください。

構文:

intercept *character*

例: intercept ^u

この例から、インターセプト文字は **Ctrl-U** になっています。

Logout

logout コマンドを使用すると、logout コマンドを入力したユーザーの現行セッションが終了します。コンソール・ログインが使用可能になっている場合、このコマンドにより、次のユーザーは許可ユーザー ID/パスワードの組み合わせを使用してログイ

ンすることが必要になります。コンソール・ログインが使用可能になっていない場合は、OPCON プロンプトが再び表示されます。

構文:

logout

Memory

memory コマンドは、ルーターのグローバル・ヒープ・メモリーの使用に関する情報を入手したり、表示したりするのに使用します。この表示を見れば、ルーターが効率的に使用されているかどうかを判断することができます。メモリー使用状況の例は、図3 を参照してください。

構文:

memory

例:

```
memory
Number of bytes:  Busy = 319544, Idle = 1936, Free = 1592
```

Busy 現在割り振られているバイト数を示します。

Idle 以前に割り振られていたが解放され、再利用できるバイト数を示します。

Free 初期の空き記憶域から一度も割り振られたことのないバイト数を示します。

注: Idle と Free メモリーの和が、使用可能な合計ヒープ・メモリーに等しくなります。

図3. メモリーの使用状況

Pause (EasyStart のみ)

pause コマンドは、EasyStart 機能を中断するのに使用します。このコマンドはルーターをデバッグするときにのみ使用します。デバッグ・セッションが完了した後は、**restart** コマンドを入力してルーターをリスタートし、EasyStart 機能を再開します。ルーターは再び EasyStart に入ります。

構文:

pause

例:

```
pause
Entering EasyStart operation. Type 'stop' to terminate.
ELS messages are automatically displayed in this mode.

EasyStart>

  EZ.001: Starting.
  EZ.007: Waiting up to 6 seconds for devices to pass self-test.
pause
* restart
Are you sure you want to restart the gateway? (Yes or [No]):  yes


Copyright Notices:
Copyright IBM Corp. 1994, 1997

MOS Operator Control
Entering EasyStart operation. Type 'stop' to terminate.
ELS messages are automatically displayed in this mode.

EasyStart>

EZ.001: Starting.
EZ.007: Waiting up to 60 seconds for devices to pass self-test.
BTP.010: net 0, int TKR/0, Sent client request (htype: 6)
BTP.011: net 1, int FR/0, Could not snd client req because: Ifc not up
BTP.011: net 2, int FR/1, Could not snd client req because: Ifc not up
BTP.011: net 3, int FR/2, Could not snd client req because: Ifc not up
```

Restart

restart は、ソフトウェアを再初期化するのに使用します。 ソフトウェアを再初期化すると、バスがリセットされます。これにより、接続しているネットワーク・インターフェースは自己テストを行い、すべてのルーティング・テーブルが消去され、ルーター内のパケットは廃棄されます。リスタートする前に、リスタートの確認を求めるプロンプトが出ます。

注: リモート・コンソールからこのコマンドを使用すると、すべてのルーター・プロセスがリスタートするので、Telnet セッションは失われます。

構文:

restart

例:

```
restart
Are you sure you want to restart the gateway (Yes or No)? Yes

Copyright Notices:
Copyright IBM Corp. 1994, 1997
MOS Operator Control
*
```

Status

status コマンドは、すべてのルーター・プロセスに関する情報を表示するのに使用します。 **status** コマンドの後に PID を入力することにより、必要なプロセスだけを選択して、その状態を見ることができます。次の例は、すべての状態を表示しています。

構文:

status *pid*

例: status

```
Pid  Name      Status TTY  Comments

1    COpCN1    IOW    TTY0
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDDT    DET     --
5    CGWCon    IOW     --
6    Config    IOW    TTY1
7    Ezystrt   IDL     --
8    ROpCN1    IOW    TTY1 128.185.46.101
9    ROpCN2    RDY    TTY2 128.185.46.104
```

Pid PID を指定します。これは OPCON との間でトークするためのプロセスであり、特定プロセスの状態に関する情報を要求する STATUS コマンドの引き数として使用することができます。

Name プロセス名を指定します。通常は、プロセスで実行中のプログラムの名前に対応しています。

Status

次のいずれか 1 つを指定します。

IDL プロセスがアイドルで、何らかの外部事象 (非同期入出力など) が完了するのを待っています。

RDY プロセスがレディー状態で、CPU の使用を待っていることを示します。

IOW プロセスが同期入出力 (通常は、予期する標準入力) が完了するのを待っています。

DET プロセスの出力が表示可能な状態にあり、プロセスはディスプレイ・コンソールに接続されるのを待っているか、その出力が指定コンソールに着信転送されるのを待っていることを示しています。

FZN プロセスがエラーのために凍結されていることを示します。これは通常、プロセスが、障害のある装置または間違って構成されている装置を使おうとしていることを意味しています。

TTY*n* プロセスが現在接続されている出力端末 (もしあれば) を指定します。

TTY0 ローカル・コンソール

TTY1 または TTY2
Telnet コンソール

SNK プロセスはフラッシュされた。

Two dashes (--)
プロセスは停止された。

Comments

ユーザーが Telnet を使用してログインするときに提供した、ユーザーのログイン IP アドレスを指定します (ROpCon)。

Stop (EasyStart のみ)

stop コマンドは、EasyStart 機能を停止して、Config-only モードに入るのに使用します。 Config-only モードについての詳細は、45ページの『Config-Only モード』 を参照してください。

構文:

stop

例:

```
stop
EasyStart>  EZ.001: Starting.
  EZ.007: Waiting up to 6 seconds for devices to pass self-test.
stop  EZ.006: All dlinks/parameters tried but failed; resetting to def values.
  EZ.009: *** Restarting Router ***

No Protocols Configured. Entering Quick Config

Router Quick Configuration for the following:
o   Interfaces
o   Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing/Transparent Bridge (SR/TB)
        Source Routing Transparent Bridge (SRT)
o   Protocols
        IP (including OSPF, RIP and SNMP)
o   Booting

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

*********************************************************
Interface Configuration
*********************************************************

Type 'Yes' to Configure Interfaces
Type 'No' to skip Interface Configuration
Type 'Quit' to exit Quick Config Configure Interfaces? (Yes, No, Quit):
[Yes] q

Quick Config Done

Config (only)>
```

Talk

talk コマンドは、GWCON、MONITR、または CONFIG のような他のルーター・プロセスに接続するのに使用します。 新しいプロセスに接続した後は、そのプロセスに特定のコマンドを送信し、そのプロセスから出力を受信することができます。ただし、TASKER または OPCON プロセスとは接続できません。

PID を入手するには、OPCON **status** コマンドを使用します。第 2 レベルのプロセス (CONFIG など) に接続した後で * プロンプトに戻るには、インターセプト文字 **Ctrl-P** を使用します。

構文:

talk *pid*

例: talk 5

第 3 レベルのプロセス (IP Config または IP など) を使用しているときに、第 2 レベルに戻るには **exit** コマンドを使用します。

Telnet

telnet コマンドは、別のルーターまたはリモート・ホスト (*ip address*) にリモート接続するのに使用します。唯一のオプション・パラメーターは、エミュレートしたい端末タイプです。

ルーターは最大 5 つの Telnet セッションを持つことができます。2 つのサーバー (ルーターへの着信) と 3 つのクライアント (ルーターからの発信) です。

注: 純粋なブリッジング環境で Telnet を使用する場合は、ホスト・サービスを使用可能にする必要があります。

構文:

telnet *ip-address terminal-type*

例: telnet 128.185.10.30 or **telnet 128.185.10.30 23** or **telnet 128.185.10.30 vt100**

```
Trying 128.185.10.30  ...
Connected to 128.185.10.30
Escape character is '^]'
```

存在しない IP アドレスに Telnet 接続すると、ルーターは次のように表示します。

```
Trying 128.185.10.30  ...
```

Telnet コマンド・モードに入るには、エスケープ文字列 (どのプロンプトでも **Ctrl-]**) を入力します。

```
telnet>
```

ルーターに telnet するときは、次のようにします。

- コマンド行に入力した最後の文字を削除するには ← **後退** キーを押す。

  注: VT100 端末を使用している場合、← **後退** キーを押すと、 目に見えない文字が挿入されるので、このキーは押さないようにしてください。最後の文字を削除するときは **Delete** キーを押してください。
- コマンド行の入力全体を削除してコマンドを再入力できるようにするには、`telnet>` プロンプトで **Ctrl-U** を押す。

Telnet コマンド・モードは、以下のサブコマンドから構成されます。

close 現行接続をクローズします。

display
動作パラメーターを表示します。

mode 逐次行モードまたは逐次文字モードに入ることを試みます。

open サイトに接続します。

quit Telnet を終了します。

send 特殊文字を送信します (続く場合は、'send ?')。

set オペレーティング・パラメーターを設定します (続く場合は、'set ?')

status 状態情報を印刷します。

toggle オペレーティング・パラメーターを切り替えます (続く場合は、'toggle ?')。

z Telnet を中断します。

? ヘルプ情報を印刷します。

status および **send** サブコマンドでは、ユーザーが別のホストに接続されているかどうかに応じて、2 つのレスポンスのうちの 1 つになります。たとえば、次のように入力します。

ホストに接続されている場合:

```
   telnet>    status
Connected to 128.185.10.30    Operating in character-at-a-time mode.    Escape character is ^].


   telnet>    send ayt
```

注: send コマンドが現在サポートするのは ayt だけです。

ホストに接続されていない場合:

```
   telnet>    status
   Need to be connected first.

   telnet>    send ayt

   Need to be connected first.
```

リモート・ホストへの接続をクローズし、Telnet セッションを終了するには、**close** サブコマンドを使用します。 **telnet** コマンド・モードを終了し、接続をクローズして Telnet セッションを終了するには、**quit** サブコマンドを使用します。

```
telnet>    close
```

または

```
telnet>    quit

logout
*
```

第2部 基本サービスの概要、構成、および使用

第5章 構成 (CONFIG) プロセスおよびコマンド (Talk 6)

この章では CONFIG プロセスについて説明し、以下の節が含まれています。

CONFIG とは

構成プロセス (CONFIG) は、ルーター・ユーザー・インターフェースの第 2 レベルのプロセスです。 CONFIG コマンドを使用して、次のことが行えます。

- 構成パラメーターを設定または変更する
- ハードウェア構成にインターフェースを追加または削除する
- Boot CONFIG コマンド・モードに入る
- クィック構成モードに入る
- 構成情報を消去、リスト、または更新する
- コンソール・ログインおよびモデム制御を使用可能または使用不可にする
- プロトコル環境を含めて、第 3 レベルのプロセスと通信する

注: 新しいコード・レベルへの移行については、「保守の手引き」の 『新規コード・レベルへの移行』 の章を参照してください。

CONFIG では、ルーターの不揮発性構成メモリーに記憶されている構成情報を表示したり、変更したりすることができます。システム・パラメーターおよびプロトコル・パラメーターに加えた変更は、ルーターをリスタートするか、ルーター・ソフトウェアを再ロードするまでは有効になりません。 (詳細については、29ページの『第3章 OPCON プロセスおよびコマンド』 の OPCON **restart** および **reload** コマンドを参照してください。)

CONFIG コマンド・インターフェースは、いくつかのレベル (モードと呼ばれる) で構成されています。各モードには、それぞれ独自のプロンプトがあります。たとえば、TCP/IP プロトコルのプロンプトは `IP config>` です。

自分が通信しているプロセスおよびモードを知りたい場合は、**Return** キーを押すと、プロンプトが表示されます。この章で説明する一部のコマンド (**network** や **protocol** など) では、CONFIG の種々のレベルにアクセスし、それを終了することができます。CONFIG プロセスから出すことができるコマンドのリストについては、55ページの表 5 を参照してください。

EasyStart の使用

EasyStart モードはルーターの構成を自動的に BOOTP サーバーからダウンロードします。このプロセスの間、ルーターは EasyStart> プロンプトおよびプロセスを追跡する ELS メッセージを表示します。

1. ネットワーク管理者はダウンロード構成のレコードで BOOTP サーバーをセットアップします。ネットワーク管理者は、使用しているルーター・タイプに有効な構成ファイルを使用して、BOOTP サーバーを構成することが必要です。 BOOTP サーバーの構成についての詳細は、118ページの『コンソール端末を使用したBOOTP』 を参照してください。
2. ルーターをオンにすると、BOOTP を使用して IBD またはネットワークから自動的にロードします。

   動作ソフトウェアが実行を開始すると、ルーターに装置やプロトコルがなにも構成されていない場合 (新規のルーターなど)、EasyStart が起動します。起動時には、装置は自動的にデフォルト・パラメーターを使用して構成に入ります。

注: デフォルトの装置は構成されているが、プロトコルが構成されていない場合、EasyStart がスタートします。

手操作で EasyStart に入ることはできませんが、Config プロンプトで以下のようなコマンドを入力することによって、ルーターを EasyStart に入れることができます。

```
Config>clear all
You are about to clear all non Device configuration information.
Are you sure you want to do this (Yes or [No]): yes
non Device configuration cleared

Config>clear device
You are about to clear all Device configuration information
Are you sure you want to do this (Yes or [No]): yes
Device configuration cleared

*restart
Are you sure you want to restart the gateway? (Yes or [No]):  yes

Copyright Notices:
Copyright IBM Corp. 1994, 1997

MOS Operator Control Entering EasyStart operation.
Type 'stop' to terminate.
ELS messages are automatically displayed in this mode.

EasyStart>

  EZ.001: Starting.
  EZ.007: Waiting up to 30 seconds for devices to pass self-test.

stop
  EZ.009: *** Restarting Router ***


No Protocols Configured. Entering Quick Config

Router Quick Configuration for the following:
o   Interfaces
o   Bridging
        Spanning Tree Bridge (STB)
```

EasyStart の中で **stop** を入力すると、ルーターはリスタートし、自動的にクイック構成に入ります。クイック構成についての詳細は、79ページの『Qconfig』 を参照してください。

EasyStart の中で **pause** を入力すると、ルーターは EasyStart プロセスを中断します。 **restart** を入力すると、プロセスは再開されます。 EasyStart を中断するのは、デバッグする場合だけに限ってください。

Config-Only モード

Config-Only モードは、ルーターの起動時の障害の原因になる不適切な構成を解消するための 1 つの手段です。 Config-Only モードを使用するのは、装置またはデータ・リンクを変更するため (つまり、サポートされない装置の場合)、またはルーティング・テーブル・サイズ、パケット・サイズ、および受信バッファー割り当てなどメモリーの使用量を削減する場合 (つまり、*no memory* 障害の場合) に***限ります***。

注: Config-Only が用意されているのは、構成上の問題によってルーターに panic、check、fail、または detect の障害が起きたときに、構成コマンドのサブセットを使用するためです。一般的なルーター構成では、Config-Only モードは使用***しない*** ようにしてください。装置関連コマンドの多くは Config-Only モードでは使用不可になっており、障害の原因になる場合もあるからです。

Config-Only モードに自動的に入る

ルーターの動作中またはルーターの初期化中に問題を検出すると、Config-Only モードに入ります。

次いずれかの状態で、ルーターは Config-Only モードに入ります。

- ソフトウェア・ロードが装置構成に一致していない。具体的に言うと、ソフトウェア・ロードによってサポートされていない装置またはデータ・リンクを構成しようとしています。
- 装置が構成されているが、プロトコルが構成されていない。
- すべてのルーター・インターフェース情報の削除

サポートされない装置が構成されたために、ルーターが CONFIG-Only モードに入った場合は、次のようにします。

- 装置情報を変更して、ルーターに導入 (サポート) されているハードウェアに一致させるか、または、サポートされない装置を 『ヌル装置』 に変更する。
- `Config (only)>` プロンプトから **Restart** コマンドを入力する。
- ルーターは自動的に OPCON (*) に入る。

プロトコルまたは装置が構成されていない場合 (デフォルトの装置を除く)、ルーターは EasyStart に入ります。詳しい情報は、44ページの『EasyStart の使用』 を参照してください。

Config-Only モードに手動で入る

Config-Only モードに入るには、次の処置のいずれかを行います。

- 構成せずにルーターを再ロードする。
- インターフェースを構成せずにルーターを再ロードする。
- プロトコルを構成せずにルーターを再ロードする。

CONFIG (Talk 6) プロセスの使用

注: 自動ブートが使用可能のときに、ソフトウェアのロード中に **Ctrl-C** を押した場合、テキストは表示されずに、直接 bootstrap monitor > プロンプトに進み、46ページのステップ 1 はスキップされます。そうでない場合には、次のようなテキストが表示されます。

```
PROM Load/Dump Program * Revision: 1.15 *
Copyright IBM Corp. 1994, 1997
Host **VL-51*  loading
Using Ethernet at ( 81600, 94).
Trying host 128.185.210.125, via 128.185.123.28
      file loads/latest-gen.rbx2-multisna.ldc
·loading
·.....................................................
·...
```

1. ブート情報が欠けている場合、ソフトウェアは IBD からロードします。最初の IBD ファイル (config ファイルなど) が無効の場合、ソフトウェアは手動ロード・プロンプトに進みます。

   ```
   No valid boot records found, attempting IBD load
   Loading using IBD Load Image "vl2-15.cfg"
   Bad record header 0

   No valid server configured -- Entering manual mode
   Device types available:

            IBD
            Token Ring
            WAN

   Device type:
   ```

2. **Ctrl-C** を押して、ブートストラップ・モニターに進みます。 > プロンプトが表示されます。

   ```
   Bootstrap Monitor v1.15
   Copyright IBM Corp. 1994, 1997
   >
   ```

3. Config-Only モードにブートします。

   ```
   >bc

   PROM Load/Dump Program * Revision: 1.15 *
   Copyright IBM Corp. 1994, 1997
   Host **VL-51*  loading

   Device types available:

           IBD
           Ethernet
           WAN

   Device type [Ethernet]:
   Connector Type (AUI/RJ45) [AUTO_CONFIG]:
   Interface IP address [128.185.123.51]: 10.1.155.22
   IP mask [FFFFFF00]:
   Boot from host [128.185.210.125]:
   Via gateway [128.185.123.28]: 43
   Boot file name [loads/latest-gen.rbx2-multisna.ldc]:

   Using Ethernet at (     0, 0).
   Trying host 128.185.210.125, via 128.185.123.28
         file loads/latest-gen.rbx2-multisna.ldc
   ·loading
   ·.....................................................
   Starting at 1040010

   The Standalone Configuration Process.  You are here because
   The watchdog timer timed out and/or Autoboot not selected

   Config (only)>
   ```

初期スタート時に装置が構成されていない場合、ルーターは Config-Only モードで立ち上がります。プロトコルが構成されていない場合、ルーターは Config-Only モードで立ち上がり、自動的にクィック構成に入ります。

詳細については、117ページの『第9章 ブート・オプション』 を参照してください。

クイック構成

クィック構成 (Quick Config) は、ルーター・ロードに存在する 各種の装置 (インターフェース)、ブリッジング・プロトコル、ルーティング・プロトコル 、およびブート・レコードを構成するのに必要な最小限の 1 組のコマンドを提供します。また、一部のインターフェース、ブート情報、および対応するハードウェア機構が導入されている場合は、コンソール・モデム制御の構成を行うこともできます。また、WRITE_READ_TRAP アクセスをもつ SNMP コミュニティーを構成することもできます。これにより、初期設定時に、構成プログラムが SNMP SET コマンドを使用して構成を転送することができるようになるので便利です。

表4 は、クィック構成がサポートするものをリストしています。

表 4. クイック構成の機能

装置	ATM プロトコル	ブリッジング・プロトコル	ルーティング・プロトコル	ブート	ダイヤル回線
トークンリング、イーサネット、PPP、FR、マルチリンク PPP	LAN エミュレーション	STB、SRT、SRB	IP、IPX、DNA IV	TFTP、BootP、	FR、PPP、ダイヤルアウト、ダイヤルイン

Quick Config は、ショートカットを提供して、既存の構成プロセスを補足します。このショートカットにより、構成プロセスを終了して別の構成プロセスに入らずに、これらの装置、ブリッジング・プロトコル、ルーティング・プロトコル、およびブート・レコードに必要な最小数のパラメーターを構成することが可能になります。その他のパラメーターは、選択されたデフォルトに設定されます。

ルーターのクイック構成が必要になる状態としては、次のものがあります。

- 構成メモリーがブランクであるか、破壊されている (次のいずれかの状態が生じた場合など)
  - ルーターを初めて構成する場合
  - 電圧変動によって構成メモリーが破壊された場合
  - ルーターの CPU ボード (構成メモリー・チップが組み込まれている) が交換された場合
- デモンストレーションで、ルーターの機能を実証するためにルーターをクイック構成する必要がある場合
- ベンチマーク・テストで、各種のテストを進める (ルーターのオペレーティング・システム・コマンドについて学習する必要はない) 場合

Quick Config は、以下のように動作します。

- デフォルト値を示しながら一連の質問をする。
- 通常モード・コマンド・セットの詳細構成へのショートカットを提供する。

Quick Config は、構成質問に対するユーザーの応答に基づいて、多数のデフォルト・パラメーターを設定します。 Quick Config で構成できないものは、これを終了した後で、Config を使用して構成することができます。

CONFIG (Talk 6) プロセスの使用

Quick Config の内部から Quick Config 情報を削除することはできません。ただし、いったん終了して Quick Config に戻るか、一部の Quick Config 質問への応答として **restart** コマンドを入力するかのいずれかにより、情報を訂正することができます。

Quick Config ソフトウェアの使用についての詳しい説明は、 947ページの『付録A. クィック構成リファレンス』 を参照してください。

Quick Config に入るには、EasyStart から自動的に入る方法と、手動で入る方法の 2 通りがあります。

Quick Config モードに自動的に入る

EasyStart モードの中で **stop** を入力すると、ルーターは自動的にクイック Config モードに入ります。

Quick Config で構成できないものは、Quick Config を終了した後で、CONFIG プロセスを使用して構成することができます。

Quick Config 情報は削除することはできませんが、Quick Config を終了した後で再び Quick Config に戻って、それを訂正することは可能です。

Quick Config モードに手動で入る

ルーターのオペレーティング・システム・コマンドを学習する必要はないベンチマーク・テストで、至急再構成してルーターの機能を実証したい場合は、手動で Quick Config に入ることができます。

Quick Config に入るには、`Config>` プロンプトで **qconfig** と入力します。

Quick Config モードの終了

Quick Config を終了するには、任意のプロンプトから **r** を入力し、リスタートします。 **no** を入力するまでは照会に従って進み、その後で **q** と入力して終了します。ルーターは `Config (only)>` または `Config>` プロンプトに戻ります。

ユーザー・アクセスの構成

ルーター構成プロセスでは、最大 50 個のユーザー名、パスワード、および許可レベルを使用することができます。各ユーザーにパスワードと許可レベルを割り当てることが必要です。許可には*管理*、*操作*、および*監視* の 3 つのレベルがあります。

詳細については、**add user** コマンドの項を参照してください。

技術サポートへのアクセス

システム管理者が最初に新規ユーザーを追加するとき、技術サポート・アクセスを追加したいかどうかを尋ねられます。 yes と応答すると、ユーザーがシステム管理者として持っているのと同じアクセス特権が、技術サポートに対しても認められます。

このためのパスワードはソフトウェアによって自動的に選択され、サービス技術員に知らされます。このパスワードは **change user** コマンドを使用して変更できますが、パスワードを変更すると、カスタマー・サービスはリモート・サポートを提供できなくなります。 **change user** コマンドの使用についての詳しい説明は、63ページの『Change』 を参照してください。

予備インターフェースの構成

ときには、装置をリスタートせずに、新規インターフェースをそのブリッジングおよびルーティング・プロトコルと共に構成することが必要になる場合があります。装置上に多数の ***予備インターフェース*** を構成しておくことによって、これを実現できます。予備インターフェースは、次のような場合に便利です。

- ダイヤル回線を装置に追加する場合

  予備インターフェースを使用して、新規の V.25bis または ISDN ダイヤル回線を既存の V.25bis または ISDN インターフェースに追加します。
- ATM LAN エミュレーション・クライアントを追加する場合

  予備インターフェースを使用して、トークンリングまたはイーサネット ATM LAN エミュレーション・クライアントを既存の ATM インターフェースに追加します。

予備インターフェースを構成するには、以下のようにします。

1. **talk 6** と入力して、CONFIG プロセスにアクセスする。
2. **set spare-interfaces** コマンドを使用して、予備インターフェースの数を構成する。
3. **Ctrl-P** を押して、CONFIG プロセスを終了する。
4. 装置をリスタートする。

例:

```
*talk 6
Config> set spare 2
Config>
*restart
Are you sure you want to restart the gateway? (Yes or [No]) yes
```

装置をリスタートすると、予備インターフェースは空き装置として導入されます。

予備インターフェースの 1 つを使用するには、次のようにします。

1. **talk 6** と入力して、CONFIG プロセスにアクセスする。
2. **add device** コマンドを使用して、ダイヤル回路を追加する。。
3. インターフェースを構成するため、または ATM LAN エミュレーション・クライアントを追加するために、**net** コマンドを使用して予備インターフェースを構成する。
4. **protocol** および **feature** コマンドを使用して、種々のプロトコルおよび機能を構成する。
5. **Ctrl-P** を押して、CONFIG プロセスを終了する。
6. **talk 5** と入力して、GWCON プロセスにアクセスする。
7. **activate** コマンドを使用して、新規インターフェースをネットワークにオンラインにする。

CONFIG (Talk 6) プロセスの使用

次の例は、IP プロトコルが使用可能にされた新規ダイヤル回線を構成し、起動する方法を示しています。ダイヤル回線と IP プロトコルの構成は示されていません。

例:

```
*talk 6
Config> add device dial-circuit
Config> net 6
Circuit configuration
Circuit config>

⋮
 Here you would configure the dial circuit

Circuit config> exit
Config> protocol ip
IP>


⋮
 Here you would configure the IP protocol on the dial circuit.

⋮
IP>exit
Config>
*talk 5
+ activate 6
```

予備インターフェースの制約事項

以下の状況下では、**activate** コマンドを使用して、新規インターフェースをネットワークにオンラインにすることはできません。

- すでに **delete interface** コマンドを入力した場合。***いずれかの*** インターフェースを削除した場合は、装置をリスタートする必要があります。予備インターフェース (リストに ***null*** と表示) は削除できません。
- 予備インターフェースが、プロトコルまたは機能を使用可能にする唯一のインターフェースである場合。プロトコルまたは機能は、既存のインターフェース上ですでに使用可能にされていないと、予備インターフェースで使用することはできません。
- 新規の予備インターフェースのヘッダー・サイズまたはトレーラー・サイズが、他のインターフェースのサイズより大きい場合
- 新規インターフェース用の受信バッファーを割り当てるためのメモリーが不十分である場合

このような場合には、装置をリスタートしないと、新規インターフェースをオンラインにすることはできません。

以下のインターフェースは、予備インターフェースとして構成することは可能ですが、**activate** コマンドを使用してネットワークにオンラインにすることはできません。

- SDLC リレー
- PPP マルチリンク・マスターおよび専用リンク・ネット

装置をリスタートしないと、これらのインターフェースをオンラインにすることはできません。

以下のプロトコルは、予備インターフェース上で構成することは可能ですが、**activate** コマンドを使用してネットワークにオンラインにすることはできません。

- LNM
- OSI/DECnet V
- XTP

注: 構成プログラムを使用している場合は、以下の手順を実行して、予備インターフェースを使用できるようにします。

1. 装置の予備インターフェースの構成変更を行う。
2. 装置上で **activate** コマンドを入力して、予備インターフェース、プロトコル、または機能をオンラインにする。
3. 構成プログラムを使用して、構成を検索する。
4. 検索した構成を、構成プログラム・データベースに保管する。

また、機能にも制約があります。制約は次のとおりです。

APPN	予備インターフェースでこのプロトコルをアクティブにするためには、最初にインターフェースを起動し、次に起動されたインターフェース上でプロトコルを構成することが必要です。
帯域幅予約 (BRS)	予備インターフェースに BRS を構成するには、各ネットワーク・インターフェースの BRS を使用可能にして、フレーム・リレー回線をアクティブにしてから、予備インターフェースを起動することが必要です。予備インターフェースを起動した後、BRS 構成コマンドを使用して、トラフィック・クラスを追加したり、トラフィック・クラスにプロトコルを割り当てるなどの変更を加えることができます。
DECnet IV	予備インターフェースでこのプロトコルをアクティブにするためには、最初にインターフェースを起動し、次に起動されたインターフェース上でプロトコルを構成することが必要です。構成変更をオンラインにするには、DECnet IV **set** コマンドを使用します。
フレーム・リレー	• ダイヤル回線の基本ネットがすでにアクティブになっていないと、FR ダイヤル回線インターフェースを起動することはできません。 • 予備インターフェースに必要なフレーム・サイズ、MAC ヘッダー、またはトレーラーが、すでに基本ネットに割り当てられている他のダイヤル回線よりも大きい場合、FR ダイヤル回線の起動は失敗します。 • 装置のデータ圧縮がすでにアクティブになっていないと、データ圧縮用に定義された予備インターフェースのデータ圧縮は機能しません。
BGP	新しい近隣ノードを起動するには、BGP **reset neighbor** コマンドを使用します。
IPX	予備インターフェースの静的ルート、静的サービス、およびフィルター・リストをアクティブにするには、**reset** コマンドを使用します。
PPP	• 装置のデータ圧縮がすでにアクティブになっていないと、データ圧縮用に定義された予備インターフェースのデータ圧縮は機能しません。 • 装置のブロック・バッファーが小さすぎて 1500 バイト PPP MRU をサポートできない場合、予備 PPP インターフェースを起動することはできません。 • ダイヤル回線の基本ネットがすでに起動されていないと、PPP ダイヤル回線インターフェースを起動することはできません。 • 予備インターフェースに必要なフレーム・サイズ、MAC ヘッダー、またはトレーラーが、すでに基本ネットに割り当てられている他のダイヤル回線よりも大きい場合、PPP ダイヤル回線の起動は失敗します。

ブリッジング
- ブリッジングがすでにアクティブになっていない場合
- 予備インターフェースに NetBIOS フィルターが定義されている場合
- 予備インターフェースにより、ブリッジ・パーソナリティーまたは動作が変更される場合 (たとえば、純粋な TB ブリッジに SR ポートを追加したり、SR-TB 変換が使用可能になるなど)

IP
アクセス制御およびパケット・フィルターの構成変更をオンラインにするには、reset IP コマンドを使用します。

WAN 復元/ WAN 再ルート
以下のいずれかの条件に適合する場合、予備インターフェースは起動できません。
- 予備インターフェースが WRS 1 次として構成されており、構成済みの WRS 2 次が、すでに WRS 1 次、WRR 1 次、または WRR 代替である場合
- 予備インターフェースが WRS 1 次として構成され、構成済みの WRS 2 次が、すでに他の WRS 1 次を復元するために起動されている場合
- 予備インターフェースが WRS 2 次として構成されており、構成済みの WRS 1 次が、すでに WRS 2 次、WRR 1 次、または WRR 代替である場合
- 予備インターフェースが WRS 2 次として構成されており、構成済みの WRS 1 次が、すでに他の WRS 2 次を復元するために起動されている場合
- 予備インターフェースが WRR 1 次として構成されており、構成済みの WRR 代替が、すでに WRS 1 次、WRS 2 次、WRR 1 次、または WRR 代替である場合
- 予備インターフェースが WRR 代替として構成されており、構成済みの WRR 1 次が、すでに WRS 1 次、WRS 2 次、または WRR 代替である場合
- 予備インターフェースが WRR 代替として構成されており、構成済みの WRR 1 次が、すでに他の WRR 代替による復元が起動されている場合

インターフェースのリセット

ときには、装置をリスタートせずに、ネットワーク・インターフェースを、そのブリッジングおよびルーティング・プロトコルとともに、構成変更することが必要になる場合があります。 **reset** コマンドを使用すると、ネットワーク・インターフェースを使用不可にした後、新しいインターフェース、ブリッジングおよびルーティング構成パラメーターを使用して使用可能にすることができます。

インターフェース、プロトコル、および機能の構成パラメーターの変更は、CONFIG プロセス (talk 6) コマンドを使用して行います。 talk 6 コマンドは、構成メモリーの内容に影響を与えます。構成変更をアクティブにするには、 GWCON プロセス (talk 5) **reset** コマンドを出します。

インターフェースのリセットは、以下の手順で行います。

1. CONFIG プロセス (talk 6) にアクセスする。
2. **net** コマンドおよび他のコマンドを使用して、構成パラメーターを変更する。
3. **protocol** および **feature** コマンドを使用して、インターフェースに基づく構成パラメーターを変更する。
4. **Ctrl-P** を押して、CONFIG プロセスを終了する。

5. GWCON プロセス (talk 5) にアクセスする。
6. **reset** コマンドを使用して、インターフェースおよびインターフェース上のプロトコルと機能をリセットする。

例:

```
*talk 6
Config>net 1
PPP Config>

. . . change PPP parameters . . .

PPP Config>exit
Config>protocol ipx
IPX Config>

. . . change IPX parameters on the PPP interface . . .

IPX Config>exit
Config>
*talk 5
+reset 1
Resetting net 1 PPP/0...successful
```

注: 構成プログラムを使用している場合は、以下の手順を実行して、予備インターフェースを使用できるようにします。

1. 装置上のインターフェースの構成変更を行う。
2. **reset** コマンドを入力して、インターフェース、プロトコル、および機能パラメーターをリセットする。
3. 構成プログラムを使用して、構成を検索する。
4. 検索した構成を、構成プログラム・データベースに保管する。

インターフェースのリセットに関する制約事項

以下の条件下では、**reset** コマンドを使用してネットワーク・インターフェースをリセットすることはできません。

- すでに **delete interface** コマンドを入力した場合。いずれかのインターフェースを削除した場合は、装置をリスタートする必要があります。
- ハードウェアまたはデータ・リンク・タイプを変更した場合。たとえば、データ・リンク・タイプを PPP からフレーム・リレーに変更した場合などです。
- より大きい MTU を構成した場合
- インターフェース上にルーティング・プロトコルまたはブリッジングを構成したが、そのルーティング・プロトコルまたはブリッジングが現在、装置上でアクティブになっていない場合

このような場合には、装置をリスタートしないと、構成変更をオンラインにすることはできません。

以下のタイプのインターフェースは、構成パラメーターを変更することはできますが、**reset** コマンドを使用してその構成変更をオンラインにすることはできません。

- ATM
- PPP マルチリンク・マスターと専用のリンク・ネット
- ISDN BRI
- ISDN PRI

- X.25
- SDLC
- SDLC リレー
- V.25bis

これらの構成変更をオンラインにするためには、装置をリスタートする必要があります。

以下のプロトコルおよび機能は、構成パラメーターを変更することはできますが、**reset** コマンドを使用してその構成変更をオンラインにすることはできません。

- AppleTalk
- Vines
- OSI/DECnet V
- LNM
- XTP
- WAN 復元
- WAN 再ルート

これらの構成変更をオンラインにするためには、装置をリスタートする必要があります。

また、機能にも制約があります。制約は次のとおりです。

PPP ダイヤル回線	PPP ダイヤル回線は、ダイヤル回線パラメーターを変更した場合は、リセットできません。
フレーム・リレー・ダイヤル回線	フレーム・リレー・ダイヤル回線は、ダイヤル回線パラメーターを変更した場合は、リセットできません。
圧縮	圧縮は、大きいサイズのヘッダーおよびトレーラーを必要とします。すでに他のインターフェース上で圧縮が使用可能になっていない場合、ヘッダーおよびトレーラーのサイズが小さくなり過ぎる可能性があります。この場合、インターフェース上の圧縮は自動的に使用不可になり、ELS メッセージがログに記録されます (インターフェースのリセット全体が失敗するのではなく)。
ブリッジング	• ブリッジングがすでにアクティブになっていない場合 • リセットするインターフェースに NetBIOS フィルターが定義されている場合 • インターフェースのリセットにより、ブリッジ・パーソナリティーまたは動作が変更される場合 (たとえば、純粋な TB ブリッジに SR ポートを追加したり、SR-TB 変換が使用可能になるなど)
BGP	近隣ノードの構成変更をオンラインにするには、BGP **reset neighbor** コマンドを使用します。
APPN	構成変更をオンラインにするには、**activate_new_config** コマンドを使用します。
IPX	静的ルート、静的サービス、およびフィルター・リストの構成変更をオンラインにするには、IPX **reset** コマンドを使用します。
DNA IV	構成変更をオンラインにするには、DNA IV **set** コマンドを使用します。
SNMP	構成変更をオンラインにするには、SNMP **revert** コマンドを使用します。

第6章 CONFIG プロセスの構成

この章では、CONFIG プロセスの構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

- 『CONFIG への出入り』
- 『CONFIG コマンド』

CONFIG への出入り

OPCON (*) から CONFIG に入るには、次のようにします。

1. OPCON プロンプトで **status** コマンドを入力して、CONFIG の PID を見つける。 (**status** コマンドの出力例は、11ページを参照してください。)

   ```
   * status
   ```

2. OPCON **talk** コマンドと CONFIG の PID を入力する。

   ```
   * talk 6
   ```

コンソールに CONFIG プロンプト (Config>) が表示されます。ここで CONFIG コマンドを入力することができます。このプロンプトが表示されない場合は、再度 **Return** キーを押してください。 CONFIG を終了して OPCON プロンプト (*) に戻るには、インターセプト文字を入力します。 (デフォルトは **Ctrl-P** です。)

CONFIG コマンド

この節では、個々の CONFIG コマンドについて説明します。各コマンドごとに、説明、構文の要件、および例を示します。 CONFIG コマンドの要約を 表5 に示します。

CONFIG 環境にアクセスした後、Config> プロンプトで構成コマンドを入力します。

表 5. CONFIG コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	インターフェースをルーター構成に追加するか、またはユーザーをルーターに追加します。
Boot	Boot CONFIG コマンド・モードに入ります。
Change	ユーザーのパスワード、またはこのインターフェースに関連するユーザーのパラメーター値を変更します。インターフェースのスロット/ポートも変更します。
Clear	構成情報を消去します。
Delete	インターフェースをルーター構成から削除するか、または構成済みのユーザーを削除します。
Disable	リモート・コンソールからのログインを使用不可にします。
Enable	リモート・コンソールからのログインを使用可能にします。
Environment	2 つのサービス・ポートがある場合、ルーターの動作環境を監視します。

表 5. CONFIG コマンドの要約 (続き)

コマンド	機能
Event	イベント・ログ・システム構成環境に入ります。
Feature	通常のプロトコルおよびネットワーク・インターフェースの構成プロセスの外部の、独立したルーター機能の構成コマンドへのアクセスを提供します。
List	システム・パラメーター、ハードウェア構成、ユーザーの (PPP ユーザーを含む) を表示します。
Network	指定されたネットワークの構成環境に入ります。
Patch	ルーターのグローバル構成を変更します。
Performance	基本プロセッサーの使用状況の統計のスナップショットを提供します。
Protocol	指定されたプロトコルのコマンド環境に入ります。
Qconfig	Quick Config プロセスを開始します。
Set	バッファー、ホスト名、非活動タイマー、パケット・サイズ、プロンプト・レベル、予備インターフェースの数、ボー・レート、ログの後処理とレベル、リスタート回数、ロケーション、および連絡担当者など、システム全体のパラメーターを設定します。
Time	システム時刻を維持し、コンソールに表示します。
Unpatch	変更した変数をデフォルト値に復元します。
Update	構成の現行バージョンを更新します。

Add

add コマンドは、インターフェースを構成に追加したり、ユーザー・アクセスのために使用します。 このコマンドは、不注意で構成を消失した場合、装置レコードを再作成するのにも使用されます。

構文:

add device . . .
isdn-address . . .
ppp-user
tunnel-profile
user . . .
v25-bis-address
v34-address

device *device_type*

add device コマンドは、ダイヤル回線インターフェースのような仮想インターフェースを作成するのに使用します。インターフェースの装置タイプ (device_type) を入力する必要があり、その他の構成パラメーターの入力も求められる場合があります。構成パラメーターおよびサポートされる装置タイプについては、20ページの『ネットワーク・インターフェースの構成』を参照してください。

add device ? と入力すると、サポートされる装置タイプのリストが表示されます。

ネットワーク・インターフェースに関連する装置およびプロトコル構成情報はすべて、インターフェース番号別に保管されます。インターフェース番号を変更すると、プロトコル内の装置構成情報の大部分が無効になります。

```
Config> add device dial-circuit
Adding device as interface 8
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 8" command to configure circuit parameters
```

isdn-address *address-name network-dial-address network-subdial-address*

ルーターと通信する ISDN エンドポイントのローカル番号とリモート番号を追加します。

address-name

何でもかまいません (ポートの記述など)。

network-dial-address

ローカル・ポートまたは着側ポートの電話番号です。

network-subdial-address

インターフェースを PBX に接続したときに解釈される、電話番号の追加部分 (内線番号など)。このパラメーターはオプションです。

注: 句読点 (括弧やダッシュなど) も使用できますが、句読点は有効文字とはみなされません (ルーターは数字だけを使用します)。

```
Example: add isdn-address line 1 local
Assign network dial address [0 - 32 digits]? 1 2345 67
Assign network subdial address [0 - 19 digits]? 98765
```

ppp_user

ユーザー・プロファイルをローカル PPP ユーザー・データベースに追加します。 PPP 認証プロトコル、PPP 暗号化、または LAN へのダイヤルイン・アクセス (DIAL) 機能を使用している場合、あるいはユーザーがダイヤルアウト機能を使用することを許可している場合、装置がローカルで PPP ユーザー・データベースを保管して管理するようにしたいときには、PPP ユーザーを構成する必要があります。 PPP ユーザー情報を RADIUS、TACACS、または TACACS+ サーバーから入手するようにしたい場合は、ローカル PPP ユーザーを構成する代わりに、認証機能を構成する必要があります。

装置上にローカルに保管されるユーザー・プロファイルは、以下から構成されます。

User Name

ユーザーを識別する名前

Password

ユーザーおよび装置に認知されるパスワード。パスワードは、最大 31 文字の長さで、任意の英数字を使用できます。パスワードは大文字小文字の区別をします。

Will this user be tunnelled?

このダイヤルイン・ユーザーを LNS 宛先にトンネル伝送する必要があるかどうかを指定します。 『yes』 と応答した場合は、LNS に関する情報の入力を求めるプロンプトが出ます。

Hostname to use when connecting to this peer:

トンネルの設定時に ID として LNS に渡される、この LAC のローカル・ホスト名を指定します。

Tunnel Server endpoint:
このユーザーのトンネル伝送先の LNS の IP アドレスを指定します。

Type of Route
『Host Route』 または 『Net Route』 です。

ホスト・ルートは通常、単一ユーザー・アクセスの場合に使用します。ネット・ルートは通常、ネットワーク・アクセスの場合に使用します。ネット・ルートの場合は、ネットマスクも入力できます。

User IP Address
ユーザーに割り当てられる IP アドレス

要求された場合にダイヤルイン・クライアントに提供される、ユーザー・プロファイルに基づく IP アドレスです。 2210 には、ダイヤルイン・クライアントの IP アドレスを入手するさまざまな方法があります。詳細については、480ページの『IP 制御プロトコル』を参照してください。

Net-Route Mask
ネットワーク・ユーザーのマスク

ダイヤルイン・ユーザーが、DIAL 使用可能の PPP インターフェースに接続している場合、ルーターは PPP セッションの間、自動的にそのクライアントに一時的な静的ルートを追加します。通常、この静的ルートは 255.255.255.255 のネットマスクを持っています。これは、その PPP リンクの反対側は単一の IP ホストであることを意味しています。ただし、このネットマスクは指定変更することが可能です。マスクを構成した場合、そのマスクは一時ルートを追加するときに使用されます。たとえば、小規模なルーターが、ホスト間の単一ルートを使用して、DIAL 使用可能のルーターにダイヤルインする場合を考えてみます。この小規模オフィス・ルーターへの単一ルートは、ユーザー・プロファイルに基づいて自動的に導入されるので、2 つのホスト間のルーティング・プロトコルを構成する必要はなくなり、低速リンク上でのルーティングによる通信量のオーバーヘッド軽減することができます。

Hostname
動的 DNS を使用するためにプロキシー DHCP サーバーに送信されるホスト名。詳細については、663ページの『第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用』を参照してください。

Time-Allotted
DIAL ユーザーに接続できる時間の長さ。これは、このセッションの合計時間を指しており、非活動タイマーと混同しないようにしてください。

有効値 0 - 71 827 788 分 (0=無制限)

デフォルト値: 0

Callback type
コールバック方式。『Roaming』 または 『Required』のいずれかです。

Dial-Out
ダイヤルアウトを使用可能にします。

このパラメーターは、DIAL ダイヤルアウト・ダイヤルアウトを使用するクライアント専用です。 PPP ユーザーのダイヤルアウトを使用可能にすると、このユーザーはダイヤルアウト回線のモデム・プールにアクセスできるようになります。詳細については、663ページの『第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用』を参照してください。

Encryption
暗号化を使用可能にします。

構成している装置に接続できる各リモート・ルーターまたは DIAL クライアントの PPP ユーザーを追加します。

PPP ユーザー名、パスワード、IP アドレス、および暗号化キー (そのユーザーに対して暗号化を使用可能にする必要がある場合) を入力するように求められます。

DIAL 機能がソフトウェア・ロードに含まれている場合、これは DIAL ユーザーであるかどうかを尋ねられます。

- DIAL クライアントのユーザーを追加している場合は、ホスト名、ルート・タイプ、ネットワーク・マスク、接続時間、コールバック情報、およびダイヤルアウト機能を入力するように求められます。
- DIAL クライアントのユーザーを追加しているのでない場合は、ルート・タイプ、ネット・ルート・マスク、ホスト名、割り当てられた時間、コールバック、およびダイヤルアウト機能は該当しないので、これらの機能を使用不可にしてユーザー・プロファイルが作成されます。

詳細については、663ページの『第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用』を参照してください。

入力パラメーターは、次のように使用されます。

- PPP ユーザー名とパスワードは、PPP 認証時に使用されます。 474ページの『PPP 認証プロトコル』 を参照してください。
- 暗号化キーは、PPP 暗号化制御プロトコル (ECP) によって使用されます。873ページの『第66章 暗号化の概説』 を参照してください。
- IP アドレスは、ユーザーに割り当てられるアドレスです。

  要求された場合にダイヤルイン・クライアントに提供される、ユーザー・プロファイルに基づく IP アドレスです。 2210 には、ダイヤルイン・クライアントの IP アドレスを入手するさまざまな方法があります。詳細については、480ページの『IP 制御プロトコル』を参照してください。
- ネットマスクは、ダイヤルイン・ユーザーがネットワーク・タイプである場合に入力します。単一ユーザーの場合、デフォルトのマスクは 255.255.255.255 です。

  ダイヤルイン・ユーザーが、DIAL 使用可能の PPP インターフェースに接続している場合、ルーターは PPP セッションの間、自動的にそのクライアントに一時的な静的ルートを追加します。通常、この静的ルートは

255.255.255.255 のネットマスクを持っています。これは、その PPP リンクの反対側は単一の IP ホストであることを意味しています。ただし、このネットマスクは指定変更することが可能です。マスクを構成した場合、そのマスクは一時ルートを追加するときに使用されます。たとえば、小規模なルーターが、ホスト間の単一ルートを使用して、DIAL 使用可能のルーターにダイヤルインする場合を考えてみます。この小規模オフィス・ルーターへの単一ルートは、ユーザー・プロファイルに基づいて自動的に導入されるので、2 つのホスト間のルーティング・プロトコルを構成する必要はなくなり、低速リンク上でのルーティングによる通信量のオーバーヘッド軽減することができます。

- 動的 DNS を使用するためにプロキシー DHCP サーバーに送信されるホスト名。詳細については、663ページの『第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用』を参照してください。
- 割り当てられた時間は、PPP ユーザーが接続したままでいられる時間の長さを制限します。
- コールバック・パラメーターは、ルーターがユーザーをコールバックするかどうか、およびコールバックするときの番号を指定します。詳細については、477ページの『PPP コールバックの構成』を参照してください。

最大 500 の PPP ユーザーを追加できます。

例: ホスト・ルートを使用する PPP ダイヤル・ユーザーの追加

```
Enter name:  []? dialshost
Password:
Will 'dialshost' be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before password expiry[0-1000] [0]?
IP address: [0.0.0.0]?
Enter hostname for dynamic DNS:  []?
Give 'dialshost' default time allotted ? (Yes, No): [Yes]
Enable callback for 'dialshost' ? (Yes, No): [No]
Will 'dialshost' be able to dial-out ? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:
Disable 'dialshost' ? (Yes, No): [No]
```

例: ネット・ルートを使用する PPP ダイヤルの追加

```
Enter name:  []? dialsnet
Password:
Enter again to verify:
Will 'dialsnet' be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute] n
Number of days before password expiry[0-1000] [0]?
IP address: [0.0.0.0]?
Net mask: [0.0.0.0]?
Enter hostname for dynamic DNS:  []?
Give 'dialsnet' default time allotted ? (Yes, No): [Yes]
Enable callback for 'dialsnet' ? (Yes, No): [No]
Will 'dialsnet' be able to dial-out ? (Yes, No): [No]
Enable encryption for this user/port (y/n)  No]:
Disable 'dialsnet' ? (Yes, No): [No]
```

例: ダイヤルなしの PPP の追加

```
Enter name:  []?
nodialsnet
Password:
Enter again to verify:
Will 'nodialsnet' be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes] n
Number of days before password expiry[0-1000] [0]?
IP address: [0.0.0.0]?
Enable encryption for this user/port (y/n) [No]:
Disable 'nodialsnet' ? (Yes, No): [No]
```

例: PPP トンネル伝送ユーザーの追加

```
Enter name:  []? tunneluser
Will 'tunneluser' be tunneled? (Yes, No): [No] y
Enter hostname to use when connecting to this peer: []?
Tunnel-Server endpoint address: [0.0.0.0]?
```

tunnel *tunnel_name*

IP ネットワーク通したルーターへのトンネル同位間アクセスを指定します。これにより、この同位 (相手) はルーターへのトンネル伝送 PPP セッションを開始できるようになります。トンネルを構成するには、以下のものを指定する必要があります。

Name トンネル伝送の同位のホスト名

Hostname to use when connecting to this peer
この同位に接続するときに使用するローカル・ホスト名。この名前は、同位上のホストの名前を識別するのに使用します。

Shared Secret
LAC と LNS 間で共有される機密。トンネルの両側で正確に一致していることが必要です。

Tunnel-Server endpoint
トンネル伝送の同位 (LAC または LNS) の IP アドレス

user *user_name*

ルーターへのユーザー・アクセスを許可します。最高 50 のユーザーに、ルーターへのアクセスを許可することができます。各 *user_name* は 8 文字で、大文字小文字を区別します。

最初のユーザーが追加されると、コンソール・ログインが自動的に使用可能にされます。追加された各ユーザーに、表6 に定義されている許可レベルの 1 つを割り当てる必要があります。

ユーザーを追加した場合は、ログイン認証をローカルに設定します。そうでない場合は、リモート・サーバーを使用しなければなりません。

表 6. アクセス許可

許可レベル	説明
システム管理者 (A)	構成およびユーザー情報を表示し、構成およびユーザー情報を追加/変更/削除します。システム管理者は、どのルーター機能にもアクセスできます。
オペレーター (O)	ルーター構成の表示、統計の表示、システム中断の有無を調べるテストの実行、ルーターの動作の動的変更、およびルーターのリスタートを行います。オペレーターは、固定されたルーター構成を変更することはできません。処置はすべて、システム・リスタートによってやり直すことができます。
モニター (M)	ルーターの構成および統計を表示しますが、ルーターの動作を変更したり、中断したりすることはできません。
技術サポート	パスワードを忘れたときに、サービス技術員がルーターにアクセスできるようにします。ユーザーに割り当てることはできません。

注: ユーザーを追加するには、管理許可が必要です。ユーザーを追加した後でルーターを再初期化する必要はありません。

例:

```
add user John
Enter password:
Enter password again:
Enter permission (A)dmin, (O)perations, (M)onitor [A]?
Do you want to add Technical Support access? (Yes or [No]):
```

Enter password
ユーザーのアクセス・パスワードを指定します。 80 字の英数字に限定され、大文字小文字を区別します。

Enter password again
ユーザーのアクセス・パスワードを確認します。

Enter permission
ユーザーの許可レベル (A、O、または M を指定します (61ページの表6 を参照してください)。

Do you want to add Technical Support access?
これのオプションは、ダイヤルイン・アクセスがロードされている場合にのみ適用されます。 61ページの表6 を参照してください。

v25-bis-address
ルーターと通信するローカルおよびリモートの V.25bis エンドポイントの番号を追加します。ネットワーク・アドレス名 は、ポートの記述など、任意のもので構いません。最大 23 字までの印刷可能 ASCII 文字列を使用できます。 *network-dial-address* は、ローカル・ポートまたは着信ポートの電話番号です。詳細については、581ページの『第41章 V.25bis ネットワーク・インターフェースの使用』 を参照してください。

注: 句読点 (括弧やダッシュなど) も使用できますが、句読点は有効文字とはみなされません (ルーターは数字だけを使用します)。

```
Example: add v25-bis-address
remote-site baltimore 1-909-555-0983
```

v34-address
ルーターと通信するローカルおよびリモートの V34 エンドポイントの番号を追加します。ネットワーク・アドレス名 は、ポートの記述など、任意のもので構いません。最大 23 字までの印刷可能 ASCII 文字列を使用できます。 *network-dial-address* は、ローカル・ポートまたは着信ポートの電話番号です。最大 31 文字までの、接続されたモデムの有効なダイヤル文字を入力できます。詳細については、601ページの『第43章 V.34 ネットワーク・インターフェースの使用』を参照してください。

注: 句読点 (括弧やダッシュなど) も使用できますが、句読点は有効文字とはみなされません (ルーターは数字だけを使用します)。

Example: `add v34-address`

```
Assign address name [1-23] chars []? remote-site-baltimore
Assign network dial address [1-20 digits][]? 1-909-555-1234
```

Boot

boot コマンドは、Boot CONFIG コマンド環境に入るのに使用します。 Boot CONFIG 情報については、87ページの『第7章 ブート CONFIG プロセス』を参照してください。

構文:

boot

Change

change コマンドは、構成内のインターフェースの変更、ユーザー自身のパスワードの変更、またはユーザー情報の変更を行うのに使用します。

構文:

change　　device . . .
　　password
　　ppp_user . . .
　　tunnel-profile

device dial-circuit
装置インターフェースを *NULL* インターフェース (構成情報が無視されるインターフェース) に変更したり、元はダイヤル回線インターフェースであった NULL インターフェースをダイヤル回線インターフェースに戻したりすることができます。

例:

```
change device dial-circuit
Interface number [0]? 3
Defaulting Data-link protocol to PPP
```

例:

```
change device null
Interface number [0]? 1
```

password
現在ログ・インしているユーザーのパスワードを変更します。

注: ユーザー・パスワードを変更するには、管理許可が必要です。

Example:

```
change password
Enter current password:
Enter new password:
Enter new password again:
```

Enter current password
現行パスワードを指定します。

Enter new password
新規パスワードを指定します。

Enter new password again
確認のために、新規パスワードを再び指定します。確認のために指定したパスワードが直線に指定した新規パスワードに一致しない場合、旧パスワードが有効のままになります。

ppp_user
特定の PPP ユーザーに関する情報を変更します。

構文:

change ppp_user encryption-key

parameters

password

encryption-key

PPP ユーザーの暗号化キーを変更します。次の例は、暗号化キーを変更するためのダイアログを示しています。

例 - 暗号化キーの変更

```
Config>change ppp_user encryption-key
Enter user name:  []? leslie
Enable encryption for this user/port (y/n) [No]:y
Encryption key should be 16 characters long.
Encryption Key (16 characters ) in Hex(0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex(0-9, a-f, A-F):
User 'leslie' has been updated
Config>
```

parameters

ユーザーのすべての ppp-user オプションを変更します。このパラメーターは **add ppp_user** と同様に動作します。ただし、[] 内に示されている値は現行値であり、change コマンドは変更の確認を行ったり、変更時にリストを再表示したりしません。 **add ppp_user** コマンドの詳細については、 56ページの『Add』 を参照してください。

password

PPP ユーザーのパスワードを変更します。

例 - パスワードの変更

```
Config>change ppp_user password
Enter user name:  []? sam
Password:
Enter password again:
User 'sam' has been updated
Config>
```

user 以前に **add user** コマンドを使用して構成したユーザー情報を変更します。

注: ユーザーを変更するには、管理許可が必要です。

例:

```
change user
User name: []
Change password? (Yes or No)
Change permission? (Yes or [No])
```

tunnel-profile

トンネル伝送の同位 (相手) の構成を変更します。

```
Config>change tunnel-profile
Enter name:  []? lac.org
Enter hostname to use when connecting to this peer: [lns.org]?
set shared secret? (Yes, No): [No]
Tunnel-Server endpoint address: [11.0.0.1]? 11.0.0.2

profile 'lac.org' has been updated
Config>
```

Clear

clear コマンドは、ルーターの構成情報を不揮発性構成メモリーから削除するのに使用します。

考慮事項: このコマンドは、サービス技術員に連絡してから使用してください。

構文:

clear

- all
- ap2 (AppleTalk 2)
- arp (ARP)
- asrt (Adaptive Source Route Protocol)
- appn (Advanced Peer-to-Peer Networking)
- atm (Asynchronous Transfer Mode)
- auth (Authentication)
- bgp (Border Gateway Protocol)
- boot
- brs (Bandwidth Reservation)
- cmprs (Data Compression)
- dls (Data Link Switching)
- device
- dialer-circuit
- dn (DECnet)
- dvmrp (Distance Vector Multicast Routing Protocol)
- els (Event Logging System Information)
- environment
- fr (Frame Relay)
- hdlc
- ip (IP)
- ipx (Novell IPX)
- isdn
- osi (OSI)
- ospf (OSPF routing protocol)
- ppp (Point-to-Point)
- sdlc
- snmp
- srb (Source Route Bridge)
- srly (SDLC Relay)

stb (Spanning Tree Bridge)

tcp/ip-host

time (Time of day information)

user

v25bis

v34

vines (Banyan VINES)

wrs (WAN Restoral feature)

x25

xtp

プロセスを不揮発性構成メモリーから消去するときは、**clear** コマンドとプロセス名を入力します。装置情報を除いて、すべての情報を構成メモリーから消去するときは、**clear all** コマンドを使用します。装置情報を含めて、すべての情報を消去するときは、**clear all** コマンドを使用し、次に **clear device** コマンドを使用します。

clear user コマンドは、ルーター・コンソール・ログイン情報を除いて、すべてのユーザー情報を消去します。これは、デフォルト値が 『disabled』 であっても、使用可能のままにされます (使用可能として構成した場合)。

注:

1. ユーザー情報を消去するには、管理許可が必要です。
2. ソフトウェア・ロードに組み込まれているものに応じて、リストに他の項目が含まれている場合があります。

例: `clear els`

```
You are about to clear all Event Logging configuration information
Are you sure you want to do this (Yes or No):
```

注: 上記のメッセージは、どのパラメーター構成を削除している場合も表示されます。

Delete

delete コマンドは、構成に保管されている装置のリストからインターフェースまたは一定範囲のインターフェースを除去するため、あるいはユーザーを除去するために使用します。 **delete** コマンドを使用するには、管理許可が必要です。

構文:

delete

interface . . .

isdn-address

ppp_user . . .

tunnel

user . . .

v25-bis-address

v34-address

interface [*intfc#* **or** *intfc#range***]**
インターフェースを削除するには、インターフェースまたはネットワークの番号をコマンドの一部として入力します。 (削除できるのは、**add device** コマンドを使用して追加した装置だけです。) ルーターが割り当てるインターフェース番号を入手するには **list device** コマンドを使用します。

delete interface コマンドは、そのインターフェースの装置構成とプロトコル情報を削除します。ただし、ルーターはリスタートされるまで、前の構成の実行を続けます。

一定範囲のインターフェースを削除する場合は、下の例に示すように、範囲の最初と最後のインターフェースをハイフンで区切って指定します。

```
delete interface 13-21
```

プロンプトで指示されたときに、インターフェース番号またはインターフェース番号の範囲を指定することもできます。

isdn-address *address-name*
前に追加された ISDN アドレスを削除します。

注: *address-name* にスペースが含まれている場合 (たとえば、**remote site XYZ**)、コマンドを 1 行に入力することはできません。 `delete isdn-address` と入力して **Return** を押します。次に、プロンプトで指示されたら、名前を入力します。

ppp_user *user_name*
PPP ユーザー・データベースからユーザーを削除します。

tunnel-profile
トンネル・プロファイル・データベースからトンネルを削除します。

user *user_name*
指定されたユーザーの、ルーターへのユーザー・アクセスを削除します。

v25-bis-address *address-name*
前に追加された V25bis アドレスを削除します。

注: *address-name* にスペースが含まれている場合 (たとえば、**remote site Baltimore**)、コマンドを 1 行に入力することはできません。 `delete v25-bis-address` と入力して **Return** を押します。次に、プロンプトで指示されたら、名前を入力します。

v34-address *address-name*
前に追加された V34 アドレスを削除します。

注: *address-name* にスペースが含まれている場合 (たとえば、**remote site New York**)、コマンドを 1 行に入力することはできません。 `delete v34-address` と入力して **Return** を押します。次に、プロンプトで指示されたら、名前を入力します。

Disable

disable コマンドは、リモート・コンソールからのログインを指示するプロンプトが出されるのを防止し、モデム制御を使用不可にします。また **disable** コマンドは、指定されたインターフェースも使用不可にします。ルーターにサービス・ポートが 2 つある場合、**disable modem-control** コマンドを使用するときには、**service1** または **service2** のいずれかを指定します。

インターフェースを使用不可にするときも、disable コマンドを使用できます。

構文:

disable console-login
interface . . .
modem-control

console-login
物理コンソール上でユーザー ID とパスワードの入力をユーザーに求めることを使用不可にします。デフォルトは使用不可です。

interface *interface#*
restart コマンドが出された後、指定されたインターフェースは使用不可にされます。 デフォルトは enabled (使用可能) です。

modem-control [service1 or service2]
コンソールでポートのモデム制御回線の監視を使用不可にします。デフォルトは disable (使用不可) です。ルーターに 2 つのサービス・ポートがある場合、どちらのサービス・ポートにモデムを接続したかを示すために、**service1** または **service2** のいずれかを指定します。*両方* のサービス・ポートを使用不可にする場合は、それぞれ別々に使用不可にします。

Enable

enable コマンドは、リモート・コンソールからのログインを許可し、モデム制御を使用可能にし、指定されたインターフェースを使用可能にするのに使用します。

enable modem-control carrier-wait または **enable modem-control ring-wait** を指定します。サービス・ポートが 2 つあるルーターの場合は、**service1** または **service2** も指定します。

構文:

enable console-login
interface . . .
modem-control

console-login
物理コンソール上でユーザー ID とパスワードの入力をユーザーに求めることを使用可能にします。これはセキュリティーに役立ちます。管理ユーザーを構成せずにこの機能を使用可能にすると、次のようなメッセージが表示されます。

```
Warning: Console login is disabled until an
administrative user is added.
```

重要: コンソール・ログインを使用可能にする前に、コンソール・ログインを使用不可にして、構成を保管してください。ログイン認証が Radius または Tacacs+ を使用しているリモート・サーバーに設定されていて、ルーターが認証サーバーに到達できない場合には、ルーターへのアクセスは拒否されます。コンソール・ログインを使用不可にしておくことにより、ロックアウト状態を防止できます。

interface *interface#*

restart コマンドが出された後、インターフェースは使用可能になります。

modem-control [carrier-wait or ring-wait] [service1 or service2]

物理コンソールがモデムを介してルーターに接続されている場合、物理コンソールでログインするためにルーターをセットアップします。このコマンドを使用する前に、必ず次のことを行ってください。

- モデムを自動応答に設定する。
- コンソールのボー・レートがモデムのボー・レートと等しいことを確認する。
- モデムをルーターに接続しているケーブルが正しく構成されていることを確認する。
- ATE0 コマンドを使用して、エコーをオフにする。
- ATQ1 コマンドを使用して、クァイエット・モードで稼働する。
- 必要なジャンパーがすべてセットされていることを確認する。詳細については、ルーターの *使用者の手引き* を参照してください。

ログアウトすると、ルーターは自動的にモデムを停止します。また、モデムを使用中に、モデムがルーターから切り離されると、ルーターはユーザーをログアウトします。

enable modem-control carrier-wait および **enable modem-control ring-wait** コマンドの両方について、サービス・ポートを指定します。サービス・ポートを 2 つ持つルーターの場合は、どちらのサービス・ポートにモデムを接続したかも示すために、**service1** または **service2** を指定します。*両方の* サービス・ポートを使用可能にする場合は、それらを別々に使用可能にします。

注: すべての構成をクリアし、ルーターをリスタートしないと、モデム制御を使用可能にした後でルーターとコンソールを接続することができません。

Request to Send を送信する前に、モデムからの carrier-detect 信号を待つようにルーターに指示することができます。これはモデム制御の標準的な方法です。

Request to Send または Data Terminal Ready を実行する前に、ring-indication 信号を待つようにルーターに指示することができます。これは初期のハンドシェークを必要とする国のために提供されています。

例:

```
Config> enable modem-control carrier-wait service1
```

Environment

注: このコマンドはサービス・ポートが 2 つあるルーターの場合に***のみ*** 呼び出されます。

環境システムでは、ルーターの動作温度を監視することができます。高温と低温の限界値を構成できます。ルーターの動作温度がこれらの限界値の 1 つを超えた場合、ルーターの動作温度が超えた限界値より低くなる (高温状態の場合)、または高くなる (低温状態の場合) まで、ルーターは周期的に ELS イベントを出します。

極度に暑い条件下では、チップはルーターをリセット状態に保ち、動作は停止されます。ルーターの正常な動作を保証するために、温度チップはルーターを -55°C ～ +85°C (-67°F ～ +185°F) の範囲で動作するようにします。ただし、ルーターの稼働に影響するのは上限だけです。85°C 以上になると、温度チップはルーターを遮断し、80°C 以下になるまでルーターは再稼働しません。極度の低温はルーターの稼働を中断させることはありませんが、チップが記録できる最低温度は -55°C です。

environment コマンドは、`ENV config>` プロンプトを表示します。

構文:

environment

環境コマンド

表 7. 環境コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	システム・パラメーター、ハードウェア構成、ユーザーの (PPP ユーザーを含む) を表示します。
Set	バッファー、ホスト名、非活動タイマー、パケット・サイズ、プロンプト・レベル、予備インターフェースの数、ボー・レート、ログの後処理とレベル、リスタート回数、ロケーション、および連絡担当者など、システム全体のパラメーターを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List: **list** コマンドは、環境の設定値を表示するのに使用します。

構文:

list

例: `list`

```
Current Ambient Temperature: 53C (127F)

Recalculate temperature interval:  30 seconds (approx)

High Temperature Alarm Threshold:   80C (176F)
Low Temperature Alarm Threshold:     0C (32F)
 (Hysteresis value: +/- 5C)
```

ヒステリシス は、アラート条件がクリアされるために必要な温度変化の量です。サービス・ポートが 2 つある装置の場合は、ヒステリシス値は ± 5 度に固定されます。たとえば 75°C の高温限界値が指定される場合、75 度以上になると ELS メッセージを受け取ります。温度が 70 度より低くならないとその条件はクリアされません (75 - 5 = 70)。 -10°C の低温限界値が指定される場合は、-10 度以下になると ELS メッセージを受け取ります。温度が -5 度以上になると、ELS メッセージを受け取らなくなります (-10 +5 = -5)。

Set: **set** コマンドは、システムが警報状態を警報する上限と下限の温度を設定します。

注: リセット温度レベルは工場で設定されています。これは変更することができません。

構文:

set high-temp-threshold
low-temp-threshold
recalc-temp-interval

high-temp-threshold *degrees_celcius*
ルーターがリセットする前に ELS メッセージを受け取る高温を設定します。ルーターが自動的にリセットする前にいくつかの ELS メッセージを受け取れるようにするために、この値は最大値 (85°C) よりも 10°C ほど低くすることが必要です。

low-temp-threshold *degrees_celcius*
ELS メッセージを受け取る低温を設定します。いくつかの ELS メッセージを受け取れるようにするために、この値は最小値 (-55°C) よりも 10°C ほど高く設定することが必要です。ルーターは低温の条件下では、自動的にリセットしません。

注: 温度範囲は、ルーターが置かれている環境によって異なります。 70 ページで説明している **environment** コマンドを使用して、ルーターの自然の動作温度範囲を調べてください。

recalc-temp-interval *seconds*
連続する温度読み取りの時間間隔を設定します。

有効値: 10 ～ 86400 秒

デフォルト値: 60

Event

event コマンドは、イベント・ログ・システム (ELS) 環境に入り、コンソールに表示されるメッセージを定義できるようにします。 ELS についての説明は、153ページの『第12章 イベント・ログ・システム (ELS) の使用』 を参照してください。

構文:

event

Feature

feature コマンドは、プロトコルおよびネットワーク・インターフェースの構成プロセスの外部の特定ルーター機能の構成コマンドにアクセスするのに使用します。

構文:

feature [*feature#* or *feature-short-name*]

すべての 2210 機能には、次の方法で実行されるコマンドがあります。

- 機能を初期構成して使用可能にしたり、後で構成変更を行うために、構成プロセスにアクセスする。
- 各機能に関する情報を表示したり、一時的な構成変更を行うために、コンソール・プロセスにアクセスする。

これらのプロセスにアクセスする手順は、すべての機能で同じです。この手順を以下で説明します。

使用しているソフトウェア・リリースで利用可能な機能のリストを入手するには、**feature** コマンドの後に疑問符を入力します。

機能の構成プロンプトにアクセスするには、**feature** コマンドを入力し、その後に続けて機能番号または短縮名を入力します。 表8 は、指定できる機能番号と名前をリストしています。

表 8. IBM 2210 機能番号と名前

機能 番号	機能 短縮名	アクセスする 機能構成プロセス
0	WRS	WAN 復元/再ルート
1	BRS	帯域幅予約
7	CMPRS	データ圧縮
9	DIALS	LANへのダイヤルイン・アクセス
10	AUTH	認証
12	LAYER	レイヤー 2 トンネル伝送プロトコル

機能の構成プロンプトにアクセスしたら、その機能特有の構成コマンドの入力を開始することができます。 CONFIG プロンプトに戻るには、機能の構成プロンプトから **exit** コマンドを入力します。

List

list コマンドは、すべての網インターフェースの構成情報またはルーターの構成情報を表示するのに使用します。

構文:

list configuration

devices

isdn-address

patches . . .

ppp_users . . .

tunnel-profile

users . . .

v25-bis-address

v34-address

devices [*device* **or** *devicerange***]**

インターフェース番号とハードウェア・インターフェースの関係を表示します。このコマンドは、**add** コマンドを出して装置が正しく追加されているかどうかを検査するのにも使用できます。

また、次の例に示すように、一定範囲の装置をリストするように指定することもできます。

```
list dev 2-5Ifc 2 WAN X.25                      CSR  81640, CSR2  80E00, vector
92
Ifc 3 WAN PPP                          CSR 381620, CSR2 380D00, vector 125
Ifc 4 WAN Frame Relay                  CSR 381640, CSR2 380E00, vector 124
Ifc 5 Token Ring                       CSR 600000, vector 95
```

注: インターフェース番号またはインターフェースの範囲を指定しないと、すべてのインターフェースが表示されます。

例: list devices

```
Ifc 0 Ethernet                         CSR  81600, CSR2  80C00, vector 94
Ifc 1 WAN X.25                         CSR  81620, CSR2  80D00, vector 93
Ifc 2 WAN X.25                         CSR  81640, CSR2  80E00, vector 92
Ifc 3 WAN PPP                          CSR 381620, CSR2 380D00, vector 125
Ifc 4 WAN Frame Relay                  CSR 381640, CSR2 380E00, vector 124
Ifc 5 Token Ring                       CSR 600000, vector 95
```

注: 注記されている受信バッファー数は、受信バッファーのデフォルト値からの例外報告です。 **set receive buffers** コマンドについては、80ページの『Set』 で説明しています。

configuration

ルーターに関する構成情報を表示します。

例: list configuration

```
Hostname: acctg
Maximum packet size: [autoconfigured]
Maximum number of global buffers: [autoconfigured]
Number of spare interfaces: 0
Number of Restarts before a Reload/Dump: 64
Logging disposition: detached
Console baudrate:  9600 (Autobaud)
Console inactivity timer (minutes): 0
Physical console login: disabled
Modem Control Enabled, using CARRIER-WAIT type control
Contact person for this node: [none]
Location of this node: [none]

Configurable Protocols:
Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
4   DN    DNA Phase IV
6   VIN   Banyan VINES
7   IPX   NetWare IPX
8   OSI   ISO CLNP/ESIS/ISIS
9   DVM   Distance Vector Multicast Routing Protocol
10  BGP   Border Gateway Protocol
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol
20  SDLC  SDLC/HDLC-Relay
22  AP2   AppleTalk Phase 2
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
24  HST   TCP/IP Host Services
```

```
25  LNM   Lan Network Manager
26  DLS   Data Link Switching
27  XTP   X.25 Transport Protocol
28  APPN  Advanced Peer-to-Peer Networking [HPR]
29  NHRP  Next Hop Routing Protocol
30  APPN  Advanced Peer-to-Peer Networking [ISR]

Configurable Features:
Num Name  Feature
0   WRS   WAN Restoral
1   BRS   Bandwidth Reservation
2   MCF   MAC Filtering
6   QOS   Quality of Service
7   CMPRS Data Compression Subsystem
8   NDR   Network Dispatching Router
10  AUTH  Authentication
12 LAYER L2TP

27616 bytes of configuration memory free
```

isdn-address

現行 ISDN アドレス構成を表示します。

```
Example: list isdn-address
Address assigned name     Network Address     Network Subdial Address
---------------------     ---------------     -----------------------
remote site XYZ            1 2345 67           98765
```

patches

patch コマンドを使用して入力されたパッチ変数の値を表示します。

例:

```
list patches
Patched variable             Value

ping-size                    60
ping-ttl                     59
ip-default-ttl               60
ethernet-security            3
rip-static-suppress          3
```

ppp_users

特定の PPP ユーザー・プロファイル・パラメーターをリストします。

例: List of PPP users when DIALs is not in the software load

```
Config> list ppp_users
List (Name, Verb, User, Addr, Encr):

       PPP User Name: joe
     User IP Address: Interface Default
          Encryption: Not Enabled
```

例: List of PPP users when DIALS is in the software load

```
Config> list ppp_users
List (Name, Verb, User, Addr, Call, Time, Dial, Encr):

       PPP User Name: joe
     User IP Address: Interface Default
      Net-Route Mask: 255.255.255.255
            Hostname: <undefined>
       Time-Allotted: Box Default
      Call-Back Type: Not Enabled
            Dial-Out: Not Enabled
          Encryption: Not Enabled
```

list ppp_users を入力すると、ソフトウェアは以下の 1 つを入力するように求めるプロンプトを出します。

Name データベース内のすべての名前をリストします。

Verb 各ユーザーの詳細情報をリストします。各ユーザー・プロファイルに関するすべての情報をリストします。

User 単一ユーザーに関する詳細情報をリストします。

Addr (address)
各ユーザーのアドレス情報 (IP アドレス、ネットマスク、およびホスト名を含む) をリストします。

Call (callback)
各ユーザーのコールバック情報 (コールバックのタイプと番号を含む) をリストします。

Time 各ユーザーに構成された許容時間をリストします。

Dial (dialback)
各ユーザーのダイヤルアウト状況をリストします。

Encr (encryption)
各ユーザーについて、暗号化が使用可能かどうかをリストします。

tunnel-profile
トンネル・プロファイル・パラメーターを表示します。

例:

```
Config>list tunnel-profile
Tunnel Name     Server Endpoint  Type      Medium    Local Hostname
lac.org         11.0.0.1         L2TP      IP        lns.org
lns-1           11.0.0.170       L2TP      IP        lac-1

2 records displayed.

Config>
```

Tunnel Name
構成された同位 (相手) の名前を指定します。

Server Endpoint
同位の IP アドレス

Type 同位間接続のタイプを指定します。

Medium
トンネル伝送に使用されるプロトコルを指定します。

Local Host Name
同位に接続するときに使用する、構成済みの名前を指定します。

users システムにアクセスするように構成されたユーザーを表示します。

例:

```
list users
USER            PERMISSION
joe             operations
mary            administrative
peter           monitor
```

v25-bis-address
現行の V25bis アドレス構成を表示します。 V25bis アドレス構成は、ローカル・ポート (シリアル・ライン・インターフェース) または着側ポートのネットワーク・アドレスとネットワーク・アドレス名から構成されます。ネットワーク・アドレスは、ローカル・ポートまたは着側ポートの電話番号です。ネットワーク・アドレス名は、ポートの記述など、任意のもので構いません。詳細については、581ページの『第41章 V.25bis ネットワーク・インターフェースの使用』 を参照してください。

```
Example:
list v25-bis-address
Address assigned name            Network Address
```

```
---------------------           ---------------
v25-1                           8982800
v25-2                           8980001
westboro                        1-666-555-4444
```

v34-address

現行の V34 アドレス構成を表示します。詳細については、601ページの『第43章 V.34 ネットワーク・インターフェースの使用』を参照してください。

```
Example:
list v34-address
Local Network Address Name    = v403
Local Network Address         = 1-508-898-2403
```

Network

network コマンドは、サポートされるネットワークのネットワーク・インターフェース構成環境に入るのに使用します。 インターフェース番号またはネットワーク番号をコマンドの一部として入力します。 (インターフェース番号を入手するには、CONFIG **list device** コマンドを使用します。) 該当する構成プロンプト (たとえば、TKR Config>) が表示されます。必要なネットワーク・インターフェース・タイプの構成についての詳しい説明は、本書のネットワーク・インターフェース構成の章を参照してください。

構文:

network *interface#*

注:

1. ユーザー構成可能パラメーターを変更した場合は、必ずルーターを**リスタート**
2. ネットワーク・インターフェースは、すべてがユーザーによる構成が可能とは限りません。ユーザーが構成できないインターフェースの場合は、メッセージ `That network is not configurable.` を受け取ります。

Patch

patch コマンドは、ルーターのグローバル構成を変更するのに使用します。パッチ変数は不揮発性メモリーに記録され、即時に有効になります。ルーターを次回にリスタートするまで待つ必要はありません。このコマンドを使用するのは、一般的でない構成を扱う場合だけに限ります。普通に構成するものは、やはり特定の構成コマンドを使用して処理すべきです。以下に示すのは、このリリースで文書化され、サポートされている現行のパッチ変数のリストです。

構文:

patch bgp-subnets
dls-ignore-lfs
ethernet-security
filter-nr
ip-default-ttl
ip-mtu
lnm-link-via-tbport

more-lines

mosheap-lowmark

ospf-import-rate

ping-size

ping-ttl

ppp-echo

relax-jate

rip-static-suppress

bgp-subnets *new value*

BGP スピーカーが近隣にサブネット・ルートを公示するようにしたい場合は、*new value* を 1 に設定します。デフォルトは 0 です。

dls-ignore-lfs *new value*

1 に設定すると、回線の設定時に、DLSw は発信元ルーティング・フレーム内の 『最大フレーム』 サイズ・ビットを無視します。これにより、これらのビットを正しく設定しない一部の旧 LAN プロダクトに伴う回線設定の問題を回避することができます。デフォルトは 0 です。

ethernet-security *new value*

非ゼロ値に設定すると、データ部分が物理最小値の 60 バイト未満のイーサネット・パケットに適用される埋め込みをゼロにします。セキュリティー上の理由から、これが必要になる場合があります。デフォルト値: 0。

ip-default-ttl *#_of_packets*

ルーターによって発信されるパケットで使用される TTL。デフォルト値は 64 です。

注: set ttl IP 構成コマンドを使用して、このパラメーターを設定することをお勧めします。 (*Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻 バージョン 3.1* の 『IP の使用および構成』 の章の 『Set』 の節を参照してください。) このパッチ変数は、旧リリースの構成との互換性のために残されています。

ip-mtu *bytes*

このパラメーターは、IP MTU サイズを指定された値に制限します。このパラメーターが設定されている場合、ネットワーク・インターフェースの IP MTU サイズは、ip-mtu の値とそのネットワーク・インターフェースに構成されているフレーム・サイズに収まる最大値のうちの小さい方の値に設定されます。

lnm-link-via-tbport *new value*

LNM がイーサネット透過型ブリッジ (TB) ポートを介してトークンリングにリンクできるようにします。

1 に設定されている場合、LNM リンクは許可されます。

0 (デフォルト) に設定されている場合、LNM リンクは許可されません。

more-lines *#_of_lines*

IP ルーティング・テーブルをリストするときにコンソールに表示される行数。『more pipe』 (¦) を使用する。

mosheap-lowmark *new value*

このパラメーターは、空き MOS ヒープ・メモリーのパーセント値を指定します。この値に達すると、装置は out-of-memory (メモリー不足) エラーが近づいていることをオペレーターに知らせます。この通知により、装置がエラーを受け取って停止する前に、オペレーターは MOS ヒープ・メモリーを解放する処置を取ることができます。

オペレーターは通知を受け取ると、ルーターを再構成してリブートすることによって、ネットワークの故障率を最小化することができます。このパラメーターを 0 に指定すると、この警告は抑止されます。

有効値: 0 ～ 100

デフォルト値: 10

ospf-import-rate *rate*

1 秒当たりのインポートされるルートの数

ping-size *bytes*

IP> **ping** コマンドによって送信される ICMP PING パケットのデータ部分 (つまり、IP ヘッダーと ICMP ヘッダーを除いた部分) のサイズ。デフォルト : 56 バイト。 (PING データのサイズは、 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻 バージョン 3.1*) 『IP の監視』 の章の 『Ping』 の項に説明されている **ping** コマンドのパラメーターとして入力することもできます。)

ping-ttl *seconds*

IP>**ping** コマンドによって PING で送信されるTTL (存続時間)。デフォルト : 64 (TTL は、 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻 バージョン 3.1* の中の 『IP の監視』 の章の 『Ping』 の節で説明されている **ping** コマンドのパラメーターとして入力することもできます。

ppp-echo *new value*

1 に設定すると、装置はどの PPP インターフェースでも PPP エコー要求を送信しません。リモート装置を動作可能に維持するために、PPP エコー要求は PPP 保守の一部としてリモート装置に送信されます。 PPP を低速ラインで実行しており、そのラインを大きなデータ・パケットの転送に使用しているので、PPP インターフェースをアップに保つのに十分な頻度で PPP 保守パケットが交換されない場合に、この変数を使用可能にすることを考慮してください。

relax-jate

JATE ISDN 制限を緩和します。

rip-static-suppress *new value*

非ゼロ値に設定すると、インターフェースに IP config> **enable send static** コマンドが与えられない限り、静的ルートはそのインターフェースを介して RIP によって公示されなくなります。これは **enable send static** コマンドの意味を変更します。 rip-static-suppress が 0 (デフォルト) のときは、RIP を介して公示されるルートのリストは、そのインターフェースの RIP フラグによって指定されたルートの集合になります。

注: 変更したいパッチ変数は、完全な名前を指定する必要があります。パッチ名に省略構文を使用することはできません。

Performance

性能のために構成環境に入るには、GWCON> プロンプト (+) で **performance** コマンドを使用します。詳細については、221ページの『第14章 性能の構成および監視』を参照してください。

Protocol

ルーターに導入されているプロトコル・ソフトウェアの構成環境に入るには、Config> プロンプトで **protocol** コマンドを使用します。

構文:

protocol [*prot#* or *prot_name*]

protocol コマンドに続けて、必要なプロトコル番号または 短縮名を入力すると、プロトコルのコマンド環境に入ることができます。このコマンドを入力すると、指定したプロトコルのプロンプトが表示されます。このプロンプトから、そのプロトコル特定のコマンドを入力できます。 Config> に戻るには、**exit** コマンドを入力します。

注:

1. ソフトウェア・ロード内のプロトコルの名前と番号を見たい場合は、Config> プロンプトで **list configuration** と入力します。
2. ユーザー構成可能パラメーターを変更した場合は、ルーターをリスタートして、変更を有効にする必要があります。これを行うには、OPCON プロンプト (*) で **restart** コマンドを入力します。

   CONFIG を通して加えた変更は、不揮発性メモリー内の構成データベースに保管され、ルーターをリスタートすると再び呼び出されます。

Qconfig

qconfig コマンドは、Quick Config を開始するのに使用します。 Quick Config では、インターフェース、ブート・レコード、ならびにブリッジングおよびルーティング・プロトコルのパラメーターを、それぞれ別々の構成環境に入らずに構成することができます。

構文:

qconfig

注: ルーターに用意されている Quick Config ソフトウェアの使用についての詳しい説明は、947ページの『付録A. クィック構成リファレンス』を参照してください。

Set

set コマンドは、システム全体の種々のパラメーターを構成するのに使用します。

構文:

set contact-person . . .
baudrate
data-link . . .
down-notify . . .
global-buffers
hostname
inactivity-timer
input-low-water
location . . .
logging disposition
packet-size
prompt-level
receive-buffers
restart-count
spare-interfaces

baudrate
コンソールのボー・レートを設定します。有効なオプションは、0 (通信速度自動選択)、300、1200、2400、4800、9600、 19200、および 38400 です。

contact-person *sysContact*
この管理 SNMPノードの連絡担当者の名前または識別番号を設定します。*sysContact* 名の長さは、最大 80 字に制限されます。

この変数は、情報のためだけのものであり、ルーターの動作には影響しません。システムの SNMP 管理 ID として有用です。

data-link *type interface#*
シリアル・インターフェースのデータ・リンク・タイプを選択します。 *type* は次のいずれかです。

- FRAME-RELAY
- PPP
- SDLC
- SRLY
- V25BIS
- V34
- X25

*Interface #*は、構成するインターフェースの番号です。

注: 内蔵モデムの場合、データ・リンク・パラメーターは変更できません。

down-notify *interface# # of seconds*

ユーザーは、インターフェースをダウンとして宣言するまでの秒数を指定することができます。通常の保守パケット間隔は 3 秒で、保守障害が 4 回検出されると、インターフェースはダウンとして宣言されます。

set down-notify コマンドを主に使用するのは、 OSPF を使用して IP ネットワークを介して LLC トラフィックをトンネル伝送するときです。インターフェースがダウンした場合、インターフェースをダウンとして宣言するまでに時間がかかるために、OSPF はただちにそれを検出することはできません。そのため、LLC セッションはタイムアウトを開始します。 down-notify タイマーを低い値に設定すれば、OSPF はより早くインターフェースのダウンを検知できるようになります。これにより、代替ルートを迅速に選択して、LLC セッションのタイムアウトを防止することが可能になります。

注: シリアル・リンクの一方の端で **set down-notify** コマンドを実行する場合、リンクの他方の端でも同じコマンドを実行する必要があります。そうしないと、リンクがアップにならず、アップに保てないことがあります。

Interface#

構成するインターフェースの番号です。

# of seconds

ダウンしたインターフェースがダウンとしてマーク付けされるまでに経過する最大時間を指定するダウン通知タイム値です。値を大きくすると、ルーターは一時的な接続問題を無視することになり、値を小さくすると、ルーターはより迅速に反応するようになります。値の範囲は 1 〜 300 秒で、デフォルトは 0 (3 秒間に設定) です。ダウン通知タイムを 0 に設定すると、そのインターフェースのデフォルト時間に復元されます。

list devices コマンドは、デフォルト値がオーバーライドされているインターフェースのダウン通知タイムを表示します。

global-buffers *max#*

グローバル・パケット・バッファー (ローカル発信パケットに使用されるパケット・バッファー) の最大数を設定します。デフォルトでは、バッファーの最大数 (最高 1000) を自動構成します。デフォルトに復元するには、この値を 0 に設定します。 global-buffers の設定値を表示したい場合は、**list configuration** コマンドを使用します。

hostname *name*

ルーター名を追加または変更します。ルーター名は識別のためだけのものであり、ルーター・アドレスには影響を与えません。 *name* は、以下に適合していなければなりません。

- 78 文字未満で、大文字・小文字を区別する。
- IBD 内のルーターの構成メモリーに保管する前に設定する。

inactivity-timer *#_of_min*

非活動タイマーの設定値を変更します。このコマンドで指定された時間の間、リモート(または、物理) コンソールが非活動状態の場合、非活動タイマ

ーはユーザーをログアウトします。このコマンドは、ログインを必要とするコンソールにのみ適用されます。デフォルト設定値の 0 は非活動タイマーをオフにし、どんなに長時間コンソールが非活動状態のままでも、ログオフは行われないことを示します。

input-low-water *interface# low_ #_of_receive_buffers*

受信バッファー数またはパケット数の下限値をインターフェース単位で構成して、デフォルトをオーバーライドすることができます。

空バッファー数が下限値または最低水準値に等しいかそれ以下になると、バッファーを節約するようにバッファー割り当て方法が変更されます。パケットを受信したときに、インターフェースの現行値が最低水準値より小さい場合、そのパケットはフロー制御 (除去) 可能になります。

値の範囲は 1 ～ 255 です。デフォルトは、プラットフォームと装置の両方に依存します。値を 0 に設定すると、自動構成されたデフォルトに復元されます。

*Interface #*は、構成するインターフェースの番号です。 *Low # of receive buffers* は、最低水準値です。

値を下げると、このインターフェースからのパケットが、輻輳 (ふくそう) したネットワーク上に送信された場合に、除去される確率が低くなります。ただし、値を下げたために、受信待ち行列が頻繁に空になるほどパケットが除去されると、性能に悪影響が生じることがあります。値を上げると、これとは逆の影響があります。

下限設定値を表示するには、GWCON プロンプト (**+**) で **QUEUE** または **BUFFER** コマンドを入力します。

location *sysLocation*

SNMP ノードの物理ロケーションを設定します。 *sysLocation* 名の長さは 80 文字に制限されます。この変数は、情報のためだけのものであり、ルーターの動作には影響しません。システムの SNMP 管理 ID として有用です。

logging disposition *setting*

デフォルトのログ後処理の SRAM レコードを変更します。このコマンドは MONITR プロセスに影響します (つまり、始動時のデフォルト設定値を変更します)。

ログ後処理 *settings* は、以下のとおりです。

- **console** は、コンソールに書き込みます (OPCON **divert 2 0** コマンドと同等です。)
- **detached** は、データを保留し、印刷しません (OPCON **halt 2** コマンドと同等です)。
- **flush** はデータを廃棄します (OPCON **flush 2** コマンドと同等です)。

ルーターのコンソール・ポートに印刷端末が接続されている場合、ログ後処理を **console** に設定してルーターをリスタートすると、始動メッセージのハード・コピーを入手することができます。

packet-size *max_packet_size_in_bytes*

グローバル・バッファーおよび受信バッファーの最大サイズを設定または変更します。値 0 を最大パケット・サイズとして指定した場合、インターフェ

ースの受信バッファー・サイズは、そのインターフェースに構成されているパケット・サイズになり、グローバル・バッファーのパケット・サイズは自動構成されます。非ゼロ値を指定した場合、構成された値がグローバル・バッファー・パケット・サイズとして使用され、この最大パケット・サイズより大きいパケット・サイズが構成されているインターフェースは、それぞれの受信バッファーの最大パケット・サイズを使用します。値 0 (自動構成) がデフォルトです。

重要: このコマンドは、サービス技術員の直接の指示のもとでのみ使用してください。パケット・サイズを小さくする目的では***絶対に*** 使用しないでください。大きくする場合に***のみ*** 使用してください。

prompt-level *user-defined-name*

ユーザー定義の名前をすべてのオペレーター・プロンプトへのプレフィックスとして追加し、ホスト名と置き換えます。

user-defined-name は、文字、数字、およびスペースを任意に組み合わせて、最大 80 字まで使用できます。また、特殊文字も、表9 に説明されている追加機能を要求するのに使用できます。

例:

```
set prompt
What is the new MOS prompt [y]? AnyHost 99
AnyHost 99 Config>
```

表 9. Set Prompt Level コマンドによって提供される追加機能

特殊文字	Set Prompt Level コマンドによって提供される追加機能

$n	ホスト名を表示します。これは、ホスト名をプロンプトに含めたい場合に便利です。たとえば、次のように入力します。
	`Config> set prompt`
	`What is the new MOS prompt [y]? $n`
	`hostname:: Config>`

$t	時刻を表示します。たとえば、次のように入力します。
	`Config> set prompt.`
	`What is the new MOS prompt [y]? $t`
	`02:51:08[GMT-300] Config>`

$d	現在の年月日を表示します。たとえば、次のように入力します。
	`Config> set prompt.`
	`What is the new MOS prompt [y]? $d`
	`26-Feb-1997 Config>`

$v	ソフトウェア VPD 情報を、次のような形式で表示します。 `program-product-number Feature xxxx Vx.x PTFx RPQx`
$e	ユーザー定義プロンプト内のこの組み合わせの後 の 1 文字を消去します。
$h	ユーザー定義プロンプト内のこの組み合わせの*前* の 1 文字を消去します。
$_	ユーザー定義プロンプトに復帰を追加します。
$$	$ を表示します。

表 9. Set Prompt Level コマンドによって提供される追加機能 (続き)

特殊文字	Set Prompt Level コマンドによって提供される追加機能

注: これらのコマンドを組み合わせて使用することができます。たとえば、次のように入力します。
`Config> set prompt`
`What is the new MOS prompt [y]? $n::$d`
`hostname::26-Feb-1997 Config>`	

receive-buffers *interface# max#*

ほとんどのインターフェースの私用受信バッファー数を調整します。

範囲は 5 ～ 255 です。

注: このコマンドは、ISDN プライマリー・レート・インターフェースには適用できません。. ISDN PRI の場合、受信バッファーの数は、B チャネル当り 5 つに固定されており、T1 の場合は 115、E1 の場合は 150 です。

(一部の装置では、 表10 に示すように、最大値にさらに制約があります。) デフォルトに復元するには、値を 0 に設定します。インターフェースの受信性能を上げたい場合は、 **set receive-buffers** コマンドを使用して行うことができます。さらに、このコマンドを使用して、ルーターが高速インターフェースから低速インターフェースに多数のパケットを転送しているときに、フロー制御による廃棄数を減らすこともできます。このコマンドの効果は、GWCON **buffer** コマンドで表示して見ることができます。**重要 :** このコマンドは、サービス技術員の直接の指示のもとでのみ使用してください。

表 10. インターフェースのデフォルトおよび最大設定値

インターフェース	デフォルト値	最大値
ATM	80	80
ETH	50	50
シリアル	24	24
TKR	40	120

restart-count

ダンプ (使用可能な場合) や再ロードを行う前に、重大エラーが原因でのルーターのリスタート回数を設定します。一般に、restart-count は変更すべきではありません。デフォルト値は 64 です。

spare-interfaces ***n***

この装置の予備インターフェースの数 ***n*** を定義します。詳細については、49ページの『予備インターフェースの構成』を参照してください。

Time

time コマンドは、2210 システム・クロックと日付を設定し、それらの値をユーザー・コンソールに表示するのに使用します。これらの値を使用して、ELS メッセージにタイム・スタンプを表示することができます。

注: 2210 には、ルーターの再初期化後に日付と時刻を維持するハードウェア・クロックが内蔵されています。

構文:

time host . . .

list

offset

set . . .

sync . . .

host *IP_address*

時刻ソースとして使用される RFC 868 準拠のホストの IP アドレスを設定します。これは、現在の時刻が入っているデータグラムを使用して、UDP ポート 37 の空のデータグラムに応答するホストのアドレスです。

list 構成された時刻関連のすべてのパラメーターを表示します。これには、現在の時刻 (設定されている場合) および時刻ソース (最後に受信した時刻の発信元のオペレーターまたは IP アドレス) が含まれます。

```
Example: time list
05:20:27  Wednesday December 7, 1994
Set by: operator
Time Host:  131.210.4.1
Sync Interval: 10 seconds GMT
Offset:  -300 minutes
```

offset *minutes*

GMT グリニッジ標準時）からの時間帯のオフセットを分単位で定義します。GMT の西側の値は負になることに注意してください。たとえば、EST (米東部標準時) は GMT より 5 時間早いので、コマンドは **time offset -300** となります。

有効値: -720 ～ 720

デフォルト値: 0

set **<***year month date hour minute second***>**

現在の時刻を入力するように求めます。このコマンドで時刻全体を指定しなかった場合は、残りの値の入力を求めるプロンプトが出ます。次の例に示すように、日付を変更することができます。

```
Example: time set
year [1996] 1997
month [12]?
date [6]? 7
hour [11]? 12
minute [3]?
second [2]?
```

sync *seconds*

ルーターが現在の時刻を時刻ホストにポーリングするする期間を秒数で設定します。

Unpatch

unpatch コマンドは、**patch** コマンドで入力したパッチ変数の値をデフォルト値に復元するのに使用します。 76ページの『Patch』 の **patch** コマンドを参照してください。

構文:

unpatch *variable_name*

注: 必ず、復元するパッチ変数の長名を指定することが***必要*** です。

Update

update コマンドは、新しいソフトウェア・ロードを受け取ったときに、構成メモリーを更新するのに使用します。

構文:

update version-of-SRAM

ソフトウェアに添付されているリリース通知の指示に従ってください。 **update** コマンドは、新規ソフトウェアをロードするときに最後に入力するコマンドです。このコマンドを入力すると、構成メモリーを更新中であることを示すメッセージがコンソールに表示されます。

```
Updating configuration memory to V15.2 [X104]
```

第7章 ブート CONFIG プロセス

この章ではブート CONFIG プロセスについて説明します。本章には、以下の節が含まれています。

ブート CONFIG とは

ルーターの不揮発性構成データベース・メモリーには、ルーターのブートおよびダンプ機能を制御するデータが入っています。ブート CONFIG コマンドを使用して、このデータを変更することができます。

ブート CONFIG コマンドを使用すると、次のことができます。

- ブートおよびダンプ構成データベースの項目を追加、変更、または除去する。
- ネットワーク・メモリー・ダンプを使用可能または使用不可にし、ダンプ・ファイルに固有の名前を割り当てる。
- TFTP プロトコルを使用して、ルーター・メモリーとリモート・ホストの間で構成情報を転送する (**TFTP** コマンドまたは **copy** コマンドを使用)。
- 現行のブートおよびダンプ構成データベースを表示する。
- ファイル・イメージを統合ブート装置 (IBD) に保管する。
- 現行イメージを IBD に保管する。
- ブート CONFIG コマンド環境から抜けて CONFIG プロセスに戻る。
- IBD の内容をリストする。
- IBD からファイルを削除する。
- ローカル・ルーター・メモリーと別のローカル・ルーター・メモリーまたはホスト・ファイル・システムの間でファイルをコピーする。
- システム・パラメーターおよびプロトコル・パラメーターに加えた変更をすべて保管する。

ブート CONFIG を用いてシステム・パラメーターおよびプロトコル・パラメーターに加えた変更が有効になるのは、ルーターをリスタートしたとき、またはルーター・ソフトウェアを再ロードしたときです。

ブートの構成

ブート・ファイルはロード・イメージ・ファイルと同じものです。ブート・ファイルにはソフトウェア・ロードが入っており、ホスト・サーバーまたは IBD に常駐し

ています。ホスト・サーバーは、たとえば、IP プロトコルおよび TFTP を実行している任意の PC、ルーター、またはワークステーションです。ブート構成データベースには、**add** コマンドを用いて構成して、各ブート・ファイルごとに 1 つの項目を入れることができます。各項目には、ホスト・サーバーのアドレス、次のホップ・ルーター、およびブート・ファイルのタイムアウト、パス、およびファイル名が含まれます。

各ブート・ファイルのパスと名前を指定することにより、ブート構成データベースに複数のブート・ファイルを構成することができます (98ページの『Add』で説明する **add** コマンドを使用して)。複数のホスト・サーバーがある場合、1 つのホスト・サーバーがネットワーク経由で接続できないときには、別のホスト・サーバーを使用してルーターをブートすることができます。

ブートを構成するには、以下の手順で行います。

1. `Boot config>` プロンプトから **add address** コマンドを使用して、ブートを実行したいインターフェースを指定するアドレス・レコードを追加する。
2. `Boot config>` プロンプトから **add boot-entry** コマンドを使用してブート・レコードを追加し、ホスト・アドレス、次のホップ・ルーター (必要な場合)、およびホストのパスとファイル名を指定する。

ブート・サーバーとしての装置の使用

装置はブート・サーバーとして機能することもできます。 IBD がない装置では、IBD のあるルーターからロード・ファイルまたはブート・ファイルを入手することができます。この場合は、**add boot-entry** コマンドを使用して、ブート・ファイルにルーターの場所を指定します。このコマンドにはロード・ファイルの全パス名を必ず組み込んでください。ロードが IBD 内にあるルーターの場合、これは `IBD/`*`filename`* になります。

BOOTP 転送プロセスの働き

BOOTP (RFC 951 に文書化されています) は、ルーターまたはディスクのないワークステーションが、その IP アドレス、ブート・ファイルの場所、およびブート・サーバー名知るために使用するブートストラップ・プロトコルです。 装置は、*BOOTP クライアント* として、あるいは別の装置の *BOOTP リレー・エージェント* として機能することができます。以下の項では、これらの 2 つのプロセスについて説明します。

BOOTP クライアントとしての装置

装置が BOOTP クライアントとして機能するのは、ブート・ファイルおよびブート・サーバーの場所を見つける必要があるときです。ユーザーが装置のブート PROM 構成レコードを特別に構成して、ルーターが BOOTP クライアントとして機能できるようにすることもできますし、ブート時に有効なファイル名およびブート・ファイルとブート・サーバーの場所への有効なパスがない場合は、ルーターが BOOTP クライアントになることもできます。この 2 つの条件のいずれかが存在するとき、ルーターは LAN インターフェースの 1 つを介して、ブート・ファイルおよびブート・サーバーのパス名をもつ *BOOTP サーバー* に UDP パケットを同報通信します。

以下に、BOOTP クライアントの転送プロセスを説明します。

1. BOOTP クライアントは、その MAC アドレス (イーサネットまたはトークンリング) を BOOTP パケット (UDP パケット) にコピーし、それをローカル LAN 上でブロードキャストします。 BOOTP は UDP の最上位で稼働します。
2. BOOTPサーバーは要求を受信し、そのデータベースにあるクライアントのイーサネット・アドレスを調べます。見つかった場合、クライアントの IP アドレス、そのブート・ファイルの場所、およびブート・サーバー名を含む BOOTP 応答にフォーマットします。次に、この応答は LAN を介して BOOTP クライアントに送り返されます。

   注: BOOTP サーバーに到達するまでにいくつかのホップが必要な場合は、BOOTP リレー・エージェントがそのパケットを受け取ります。 BOOTP リレー・エージェントについては、次の項で説明します。
3. ルーターが BOOTP 応答パケットを受け取ると、そこに含まれている情報を使用して、ブート・サーバーに TFTP 要求を開始します。

BOOTP リレー・エージェントとしての装置

BOOTP 要求が BOOTP サーバーに到達するまでにいくつものホップを必要とする場合、BOOTP リレー・エージェントが知っている BOOTP サーバーすべてに IP 経由でパケットを送ります。 IP を介してパケットが送信されている間に、他のルーターがこれを受信すると、そのパケットを検査してそれが BOOTP パケットかどうかを判別し、知っている BOOTP サーバーの方へパケットを回送します。以下に、BOOTP リレー・エージェントの転送プロセスを説明します。

1. ローカル BOOTP リレー・エージェントとして機能する装置は、BOOTP クライアントから BOOTP 要求を受信し、チェックサムを変更し、リレー・エージェントの IP アドレスを BOOTP 要求の本体にコピーして、パケットに IP ヘッダーを付け、そのパケットをすべての BOOTP サーバーに送ります。
2. BOOTP サーバーがその要求を受け取ると、クライアントの MAC アドレスをデータベースの中で探します。サーバーがクライアントのアドレスを見つけると、クライアントの IP アドレス、そのブート・ファイルの位置、およびブート・サーバー名を含めた BOOTP 応答にフォーマットします。次に、その応答が BOOTP リレー・エージェントに送られます。
3. BOOTPリレー・エージェントは応答を受け取り、クライアントのために ARP テーブル内に登録してから、応答を BOOTP クライアントへ転送します。
4. クライアントは、BOOTP 応答パケットに含まれているブート・サーバーへの TFTP 要求を開始するための情報を使用して、ブートを続けます。

BOOTP 転送の使用可能/使用不可

ルーターでの BOOTP 転送を使用可能または使用不可にするには、 IP 構成プロンプトで、次の該当するコマンドを入力します。

```
IP Config> enable bootp
IP Config> disable bootp
```

BOOTP を使用可能にする場合、次の値を入力するようにプロンプトで指示されます。

- BOOTP 要求が経由するアプリケーション・ホップの最大数

これは、パケットを転送できる BOOTP リレー・エージェントの最大数です。BOOTP サーバーへの IP ホップの最大数では***ありません***。このパラメーターの標準値は 4 です。

- BOOTP 要求を転送する前にクライアントが再試行する秒数。このパラメーターは*通常は使用されません*。 このパラメーターの標準値は 0 です。

BOOTP 要求を受け付けると、ルーターはその BOOTP 要求を各 BOOTP サーバーに転送します。 BOOTP に複数サーバーが構成されている場合、転送するサーバーはパケットを複写します。

BOOTP サーバーの構成

BOOTP サーバーは、*bootpd* daemon をもつ AIX または UNIX ホスト、あるいは DOS ホスト (FTP ソフトウェアから利用可能なソフトウェアを実行) です。 BOOTP サーバーには、このサーバーが担当するすべての BOOTP クライアントと、それぞれの関連の IP アドレス、ブート・ファイルの場所、およびブート・サーバー名をリストした 1 つのファイルが収められています (ネットワーク管理者が管理します)。

BOOTP サーバーは、BOOTP 要求を受け取ると、クライアントの MAC アドレスと、サーバーの BOOTP ファイルにある MAC アドレスとを突き合わせます。一致した場合、サーバーは BOOTP 応答を構成し、クライアントの IP アドレスと、ブート・サーバーおよびブート・ファイル名の場所を追加します。一致しない場合、パケットは廃棄されます。

ルーターの構成に BOOTP サーバーを追加するには、IP 構成プロンプトで次のコマンドを入力します。

```
IP Config> add BOOTP-SERVER [IP address of server]
```

複数のサーバーを構成することができます。さらに、サーバーのネットワーク番号のみを知っている場合、あるいは複数のサーバーが同じネットワーク・セグメント上に存在する場合は、 `IP config>>` プロンプトで **enable directed-broadcast** コマンドを入力して、サーバー用のブロードキャスト・アドレスを構成することができます。

トリビアル・ファイル転送プロトコル (TFTP) の使用

TFTP は、インターネット UDP プロトコル上で実行されるファイル転送プロトコルです。この実現では、ルーターの不揮発性構成メモリー、統合ブート装置 (IBD)、およびリモート・ホストの間で、複数の TFTP ファイル転送を同時に行うことができます。

TFTP では、以下のことが可能です。

- ルーターからサーバーへの構成ファイルの保管
- サーバーからルーターへの構成ファイルのコピー
- IBD への構成のコピーまたはファイルのロード

TFTP 転送には、クライアント・ノードとサーバー・ノードが関与します。クライアント・ノードは、ネットワーク上に TFTP 要求を生成します。ルーターはクライアン

ト・ノードとして機能し、Boot Config> プロセスの **copy** コマンドを使用して、ルーター・コンソールから TFTP 要求を生成します。

注: **tftp** コマンドと **copy** コマンドは、同じ機能を持っていますが、構文は異なります。

このクライアントは、構成メモリーに保管されている構成ファイルのコピーまたは IBD に保管されているファイルを転送することができます。

サーバーは、TFTP 要求を受け取ってサービスを提供する任意の装置 (たとえば、パーソナル・コンピューター (PC)、ルーター、またはワークステーション) を使用できます。ルーターがサーバーとして動作する場合、転送はユーザーに透過的に行われます。 ELS サブシステム tftp メッセージ・ログを使用すると、進行中の転送を見ることができます。

注: ファイル・サーバーまたはルーターは、ファイルを他のルーターの不揮発性構成メモリーまたは IBD にコピー することはできません。ルーターに書き込みを行うには、宛先のローカル Boot config>> プロンプトから **copy** コマンドを使用します。

copy コマンドを使用するときは、次の点に注意してください。

- 装置構成に IP プロトコルが組み込まれており、構成済みの IP アドレスが少なくとも 1 つは必要です。また、ルーターが CONFIG-Only モードで動作していてはなりません。
- 装置の構成メモリーが空の場合 (つまり、装置の初期導入時、SRAM が破壊されている場合など) は、次のパラメーターを設定して、装置の構成を復元する必要があります。
  1. 装置のホスト名を設定する。
  2. 保存されている構成を用いて、装置が各ホストに到達できるように IP を構成する。 IP 構成コマンドについては、 *プロトコルの構成と監視解説書* で説明しています。
- TFTP 転送の発信元 IP アドレスは、装置 ID です。デフォルトでは、この ID は装置のネットワーク・インターフェースの 1 つの構成済み IP アドレスになります。ルーター ID を変更するには、IP Config> プロンプトで **set router ID** コマンドを入力します。
- すべての TFTP データ転送は、512 バイトの長さです。 512 バイト未満のデータ転送は、転送の終わりを示します。プロトコル、クライアント、またはリモート・ホストにエラーがあると、転送を終了させるエラー・パケットが生成されます。
- 構成ファイルをダウンロードする場合は、ファイルをアップロードしたときと同じタイプのルーターにダウンロードしてください。

注: この TFTP は、他のルーターに *copy* することはできません。

各 TFTP 転送には、クライアントとサーバーの UDP ポート番号が付いています。クライアント・ノードがサーバーへの最初の要求を生成するときに、クライアント・ノードの未使用の UDP ポート番号が、クライアント・ノードとしてランダムに選択されます。サーバー・ポートは UDP ポート番号 69 (10 進数) になります。サーバー上で TFTP サーバーが稼働している場合、UDP ポート 69 を監視します。サーバ

ーがネットワークから要求を受信すると、サーバー上の現在未使用の UDP ポート番号が、ホスト・ポートとしてランダムに選択されます。この 2 つの UDP ポート間で、ファイル転送が行われます。

リモート・ホストまたはルーターからの構成ファイルへのアクセス

リモート・ホストまたはルーターから構成ファイルへアクセスするには、以下の手順で行います。

1. Boot config>>プロンプトで、**copy**と入力し、 **Enter** を押す。
2. source filename [CONFIG]? プロンプトで、リモート IP アドレスとパス名を指定する。

   これは TFTP ホスト、または IBD 内にファイルが入っている別のルーターです。
3. destination filename [Config]? プロンプトで、**Enter** を押す。

   Enter を押すことによって、デフォルトのファイル名 CONFIG. を受け入れます。たとえば、次のように入力します。

```
Boot config>copy
source filename[CONFIG]?128.185.210.125:loads/configs/vl-28.cfg
destination filename [CONFIG]?
COPYing from "128.185.210.125:loads/configs/vl-28.cfg" to
"CONFIG"
COPY succeeded
```

IBD のファイル名の定義

IBD に保管されている各ファイルまたはイメージ には、それに関連した固有の *loadname* が必要です。 IBD のファイル名には、ファイル名の他に、完全パス名を含めることができます。

例 1: test.cfg

例 2: /usr/loads/test.ldc

次の例は、Boot config> プロンプトでファイルを IBD に保管する方法を示しています。

例: copy 128.185.210.125:/usr/config/test.cfg ibd/test.cfg

ルーターは、ファイル名定義の一部として任意の印刷可能 ASCII 文字を受け入れますが、次の 2 つの例外があります。

- ファイル名は、数字で始めることはできません。
- ファイル名に RETURN または LF (改行) 文字を含めることはできません。

文字列にはスペースを含めることができますが、この文字は目に見えないので、使用しないことをお勧めします。別のユーザーが必須のスペースを抜かしてファイル名を入力しようとすると、エラー・メッセージを受け取ることになります。

注: IBM 2210 を他のルーターのサーバーとして使用する場合には、ブート・ルーター上の **add boot-entry** コマンドを使用して、ロード・ファイルに完全パス名を必ず組み込んでください。

下の表に、ファイル名拡張子に関する規則を示します。

表 11. ファイル名の拡張子に関する規則

ファイルのタイプ	ファイル名の拡張子
構成	.cfg
ロード	.ldc

ファイル転送時の IBD に関する考慮事項

IBD にファイルを転送する場合、次の事項を考慮してください。

- 全ロードは、IBD の 1 つのバンクには収容できません。
- ロードを保管するために複数のバンクが必要な場合、連続する番号の空のバンクにのみ書き込みます。たとえば、ロードが大きすぎてバンク 2 に収容しきれない場合、バンク 3 が空の場合にのみ、ロードはバンク 3 に保管されます。
- 大きなロードを保管するために隣接バンクを利用できない場合、コンソールに `TFTP Disk Full` メッセージが表示され、そのロードは保管されず、IBD は変更されないままになります。バンクに部分的に保管されたロードは除去されます。

構成ロードの妥当性検査

イメージが装置の構成メモリーに書き込まれる前にイメージを検査するには、次の 2 通りの方法があります。

- 最初の方法は、保存されているイメージおよび復元されるイメージのそれぞれのプラットフォーム・タイプに、装置がマジック・ナンバー と呼ばれる識別コードを割り当てます。この番号が一致しない場合は、転送は打ち切られ、コンソールに `Bad Magic Number` というメッセージが表示されます。
- 2 番目の方法は、最初にイメージを保存した装置のホスト名と、イメージを復元する装置のホスト名が比較されます。このホスト名が一致しないと、転送は打ち切られ、コンソールに以下のメッセージが表示されます。

  ```
  COPY error -
  Got hostname "<hostname>" - is this okay (Yes or [NO])? no
  ```

  したがって、ホスト名が一致しなくても、別の装置から構成を導入することができます。構成は、使用している装置のモデルに適合する正しいものであることが必要です。

  RAM スペースの不足が原因で転送が正常に行われないときは、コンソールにエラー・メッセージが表示されます。

特定時刻にイメージをロード

ユーザーに不都合な特定の日時に装置にロードしたい場合があります。 **timedload activate** コマンドを使用すると、指定した時刻に装置がロードを実行するように構成することが可能です。装置にスケジュールされているロード情報を表示したり、スケジュールされたロードを取り消したりするコマンドも用意されています。これらのコマンドについては、97ページの『ブート CONFIG コマンド』 を参照してください。

ダンプの構成

2210 の重要な機能は、ソフトウェア・クラッシュやハードウェア障害が原因でシステム・リセットが行われるとき、あるいはリセット・ボタンを押したときに、システム・メモリーおよびプロセッサー・レジスターの内容を他のホストへダンプできることです。

ダンプを構成するには、`Boot config>` プロンプトから以下のことを実行します。

1. *アドレスを追加する。*

   これはブートの構成で使用したブート・アドレスと同じで構いません。

2. *ダンプ項目を追加する。*

   これは、ダンプ・ファイルを受信するホストまたはサーバーの場所です。 **add dump-entry** コマンドを使用して、ダンプ項目を追加することができます。ダンプ・ファイルの平均サイズは 8 MB です。

3. *ダンプを使用可能にする。*

   ダンプを使用可能にするには、**enable dumping** コマンドを使用します。ダンプを使用不可にするには、**disable dumping** コマンドを使用します。

ダンプ・ファイル

ダンプ・ファイルには、システム・メモリーとプロセッサー・レジスターの内容が入っています。

装置がクラッシュし、ダンプが使用可能になっているときは、TFTP を使用して、メモリーの内容がリモート・ホストに書き込まれます。各ダンプ項目には、ホスト・サーバーおよびパスの場所、タイムアウト、およびダンプ・ファイルのファイル名が含まれています。

ダンプ・ファイル名に固有の文字列を自動的に追加するように、装置を構成することも可能です。こうすると、既存のダンプ・ファイルが後続のダンプによって上書きされるのを防ぐことができます。ただし、ダンプ・ファイルに固有の名前を付けると、連続的にダンプが行われた場合、サーバーのディスクがいっぱいになる可能性があります。 TFTP サーバーによっては、固有の命名はセキュリティー要件に反することもあります。また、一部のサーバーでは、サーバー上にすでに存在しているファイルにしか、ダンプを書き込むことができません。

ダンプ・ファイルは診断のためにだけ使用します。装置のダンプ機能および固有の命名機能を使用可能にするのは、カストマー・サービス技術員の助言があった場合だけにしてください。

TFTP サーバー、ブートおよびダンプ・ディレクトリー

ブート・ファイルおよびダンプ・ファイルを入れるために、宛先サーバー上にディレクトリーを作成する必要があります。これらのディレクトリーはホスト・サーバーに常駐し、ブート・ディレクトリーはグローバルに読み取り可能で、ダンプ・ディレクトリーはグローバルに書き込み可能でなければなりません。ブートおよびダンプ機能は、TFTP プロトコルを使用します。ユーザーの TFTP サーバーには、その他の制約事項がある場合があります。

ソフトウェア / コードの導入

サーバーから IBD へ新規のロード・モジュールをダウンロードするには、次のステップで行います。

1. 装置が到達可能なサーバーにロード・ファイルをインストールする。サーバー上で TFTP デーモンが稼働していることを確認してください。装置のルーター・コンソールで、以下のコマンドを入力します。
2. OPCON プロンプト (*) で:
   a. **status** と入力し、Config プロセス ID (PID) を表示する。

      ```
      * status
      ```

   b. **talk** と Config PID を入力して、Config> コマンド環境にアクセスする。

      ```
      * talk 6
      ```

3. Config> プロンプトで、**boot** と入力する。これにより、Boot config> コマンド環境にアクセスします。

   ```
   Config> boot
   Boot config>
   ```

4. Boot config> プロンプトで **add address** と入力して、装置がブートできる IP アドレスを指定する。これは、使用できるようにしたい各インターフェース対して、1 回だけ行う必要があります。新規のロード・モジュールを取得するたびに行う必要はありません。

   続いて、次の情報を求められます。

   - Interface number ルーターがファイルを転送するのに使用するインターフェースの番号です。
   - New address このインターフェースの IP アドレスです。
   - Net mask このインターフェースのネットワーク・マスクです。

   ```
   Boot config> add address
   Which interface is this address for [0]?
   New address [0.0.0.0] ?
   Net mask for this interface [255.255.255.0]?
   ```

   以下のステップは、ブート・アドレスを追加した場合にだけ必要です。ブート・アドレスを構成済みの場合は、以下のステップを省略して、 95ページのステップ 9 へ進んでください。

5. **Ctrl-P** を押して、 OPCON プロンプト (*) に戻る。
6. OPCON プロンプトで、**restart** と入力する。
7. **talk** と Config PID を入力する。
8. Config> プロンプトで **boot** と入力して、Boot config> コマンド環境に戻る。
9. Boot config> プロンプトで、**tftp get** と入力する。これで、ロード・モジュールのファイル転送を開始します。

   次の情報を求められます。

   - Local filename ローカル・ファイル名として、IBD 内の新規ロードのファイル名を入力します。
   - Remote host リモート・ホストとして、サーバーの IP アドレスを入力します。
   - Host filename ホスト・ファイル名として、ホスト・マシン上の完全なパスとファイル名を指定します。

```
Boot config> tftp get
Local filename []?  ibd/newloadfile
Remote host []?
Host filename []?
```

10. Boot config> プロンプトで、**list boot-entries** と入力する。こうすると、IBD 内のロード・モジュールがリストされます。

    ```
    Boot config> list boot-entries
    ```

    このロード・モジュールを受け取る前に使用していた IBD 内のロード・モジュールの項目番号をメモしておいてください。

    ブート・データベースで、ルーターはロード・モジュールを入手する場所を調べます。データベースには、複数の項目を入れることができます。通常は、最初の項目は IBD 内のロード・モジュールで、2 番目の項目はリモート・ホストまたはルーターのロード・モジュールです。

11. Boot config> プロンプトで **change boot** と入力して、ブート・データベースのポインターをロードしたばかりのモジュールに変更する。これにより、次回にルーターをリブートしたときに使用されるロード・モジュールが決まります。

    ```
    Boot config> change boot
    ```

    次に、IBD 内で使用していた以前のモジュールの項目番号を求められます。これは、96ページのステップ 10 でメモした項目番号です。ブート項目番号は、通常は ″1″ になります。

    ```
    Change which entry?: 1
    ```

12. 新規ロードのファイル名を入力する。これは、IBD に保管するために 95ページのステップ 9 で指定した名前です。ファイル名は大文字・小文字を区別します。

    ```
    remote host or IBD load name:
    ```

13. **exit** と入力する。

    ```
    Boot config> exit
    ```

14. **Ctrl-P** を押して、 OPCON プロンプト (*****) に戻る。
15. **restart** と入力して、″change boot″ コマンドによる構成変更が有効になっていることを確認する。
16. **reload** と入力して、装置に新規ロード・モジュールをロードする。
17. 新規ロードを確認した後、直前のロードを消去して、IBD 内に将来のロードのためのスペースを作成することができます。
    a. **talk 6** と入力する。
    b. **boot** と入力する。

       ```
       Config> boot
       ```

    c. **list ibd** と入力して、バンクの内容をリストする。前のロードが保管されていたバンクの番号をメモしておいてください。

       ```
       Boot config>list ibd
       ```

    d. **erase** と前のロード名またはバンク番号を入力する。たとえば、バンク 36 ～ 50 を消去するには、次のように入力します。

       ```
       Boot config> erase 36-50
       ```

第8章 ブート CONFIG の構成

この章では、ブート CONFIG 構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

- 『ブート CONFIG の開始と終了』
- 『ブート CONFIG コマンド』

ブート CONFIG の開始と終了

ブート CONFIG コマンド環境へ入るには、CONFIG の **boot** コマンドを使用します。ルーターのソフトウェアは、初期ロード時には OPCON プロセスで動作し、* プロンプトが表示されます。 * プロンプトから、次のようにします。

1. **talk 6** と入力する。
2. `Config>` プロンプトで、**boot** と入力する。
3. `Boot config>` プロンプトで、**?** を入力する。コマンドのリストについては、98ページの『Add』を参照してください。

   CONFIG プロセスに戻るには、**exit** と入力します。

ブート CONFIG コマンド

この節では、ブート CONFIG コマンドについて説明します。各コマンドごとに、説明、構文の要件、および例を示します。 表12 は、ブート CONFIG コマンドの要約を示しています。

ブート CONFIG 環境にアクセスした後、`Boot config>` プロンプトでブート構成コマンドを入力します。

表 12. ブート CONFIG コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	指定されたインターフェース、ホスト・ブート項目、またはホスト・ダンプ項目に、ブート・インターフェースの IP アドレスを追加します。
Change	ブート・インターフェース IP アドレス、ネットワーク・ブート項目データ、またはネットワーク・ダンプ項目データを変更します。
Copy	リモート構成ファイルとホスト間で、あるいはルーター内の各資源の間で、ブート・ファイルおよび構成ファイルをコピーします。
Describe	IBD 内に保管されているロード・ファイル・イメージに関する情報を表示します。
Delete	ネットワーク・ブート・インターフェース・アドレス、ホスト・ブート項目、またはホスト・ダンプ項目を削除します。

表 12. ブート CONFIG コマンド (続き)

コマンド	機能
Disable	ダンプ・ファイルのメモリー・ダンプまたは固有の命名を使用不可にします。
Enable	ダンプ・ファイルのメモリー・ダンプまたは固有の命名を使用可能にします。
Erase	IBD バンクに保管されているイメージを消去します。
List	すべてのネットワーク・ブート・アドレス、すべてのブートおよびダンプ構成データ、IBD の内容、BOOTP 名の設定値、およびスケジュールされたイメージ・ロード情報を表示します。
Load	IBD または RAM からブート・ファイルをコピーするか、またはリモート・ホストから RAM にブート・ファイルをコピーします。
Store	RAM から IBD にブート・ファイルをコピーします。
Timedload	特定の日時に装置にイメージをロードすることをスケジュールしたり、スケジュールされたロードを取り消したり、あるいはスケジュールされたロード情報を表示したりします。
TFTP	装置メモリーまたは IBD とリモート・ホストとの間で TFTP ファイル転送を開始します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、装置の構成データベースにブート/ダンプ・パラメーターを入れるのに使用します。

構文:

add address
boot-entry
bp-device
dump-entry

address

装置がブートまたはダンプできるインターフェースまたは装置の IP アドレスを指定します。 **add address**コマンドを使用する場合、次の情報を提供するかまたはそのデフォルト値を受け入れる必要があります。

- ネットワーク・インターフェースのインターフェース番号
- IP アドレス
- ネットワーク・マスク

インターフェース番号 (Ifc#) を入手するには、CONFIG **list devices** コマンドを使用します。このコマンドについては、43ページの『第5章 構成 (CONFIG) プロセスおよびコマンド (Talk 6)』で説明しています。

注: アドレスを追加しないと、装置はネットワーク上でブートまたはダンプを行えなくなります。

以下の点に注意してください。

- 入力する最初のアドレスは、入力した最初のブート項目に対応し、2 番目のアドレスは 2 の項目に対応するというようになります。
- 複数のブート項目で同じ IP アドレス (インターフェース) を使用することができます。
- **add boot-entry**、**add dump-entry**、および **load remote** コマンドを使用する場合は、このコマンドを入力する必要があります。

```
Example: add address
Which interface is this address for [0]?
New address [0.0.0.0] ? 128.185.1.2
Net mask for this interface [255.255.255.0]?
```

boot-entry

装置が TFTP ホスト・サーバーを見つけて、ブート・イメージ・ファイルを検索するために必要な情報を指定します。装置をブートするには、いくつかの方法があります。

- ルーターが自身の IBD に保管されているソフトウェアを使用してブートする場合、IBD ロード名を構成の最初のブート項目として指定することが必要です。複数のブート装置を構成することもできます。ロード名は **list ibd** コマンドを使用して入手してください。ロード名は、大文字・小文字を区別します。

  ```
  例: add boot-entry
  remote host or IBD loadname [0.0.0.0]? 128.185.30.0
  via gateway (0.0.0.0 if none) [0.0.0.0]?  0.0.0.0
  timeout in seconds [3]?  10
  file name [ ]?  loads/Y21.ldc
  ```

- 装置が TFTP サーバーに保管されているソフトウェアを使用してブートする場合は、リモート TFTP ホスト・サーバーの IP アドレスを指定することが必要です。 TFTP ホスト・サーバーは、IBD をもつ別の装置でも構いません。
- TFTP ホスト・サーバーがリモート・ネットワーク (ブートを行うルーターとは直接接続されていない) にある場合には、ホスト・サーバーに向けての次のホップ (ルーター) の IP アドレスを指定する必要があります。

表 13. Add Boot Entry パラメーター

remote host or IBD loadname?	リモート・ホストの IP アドレスまたは IBD ロード名。 **注:** IBD ロード名は、英字で始まっていなければなりません。そうしないと、システムはその文字列を IP アドレスと解釈します。
via gateway?	最初のホップ・ルーターの IP アドレス (存在する場合)。 TFTP ホスト・サーバーが、直接接続されたネットワーク上にある場合には、0.0.0.0 と応答します。
timeout in seconds?	再伝送が行われる前に、装置が待つ時間の長さを指定します。デフォルト値は 3 秒です。極度に遅いブート・パスの場合は、もっと長い時間を設定することが必要になる場合があります。

表 13. Add Boot Entry パラメーター (続き)

file name?	TFTP ホスト・サーバー上のブート・イメージ・ファイルの完全なディレクトリー・パスと名前。 (完全ディレクトリー・パスを必要としない機械もあります。デフォルトでは、 パスは `tftpboot/` であるもと想定しますが、これはユーザーからは見えないので、パスが `/tftpboot/loads/name` のときは **loads/name** と入力します。) – UNIX ベースのオペレーティング・システムに保管されているファイルを参照するときは、前向きスラッシュ "/" を使用し、ファイル名は大文字・小文字の区別が必要です。パスの先頭に前向きスラッシュ (/) が必要な場合には、二重の前向きスラッシュ (//) を使用します: `128.185.15.1//tftpboot/loads/name`. – DOS ディスク上に保管されているファイルを参照するときは、前向きバック・スラッシュ "\" を使用し、ファイル名は大文字・小文字の区別をしません。

注: 現行のブート構成のリストを表示するには、ブート CONFIG **list boot** コマンドを入力します。

```
Example: list boot-entry
remote host or IBD loadname [0.0.0.0]?  10.0.0.5
via gateway (0.0.0.0 if none) [0.0.0.0]?  12.0.0.7
timeout in seconds [3]  10
file name [ ]  loads/v1.ldc
```

bp-device

BOOTP (ブート・プロトコル) 装置から装置のソフトウェアを取り出すために、以下のような BOOTP ブート機能を提供します。

- 装置が構成されていないか、装置の自動ブート構成情報が欠けており、しかも自動ブート・スイッチが使用可能に設定されている場合、装置は自動的にすべての LAN インターフェース上の BOOTP を使用してブート情報を取り出そうと試みます。
- 自動ブート時には、最初に装置はブート項目に提供されている情報を使用して、ロード・イメージ・ファイルを取り出そうと試みます。ブート項目の情報からロード・イメージ・ファイルを取り出せなかった場合、次に装置は BOOTP を使用してブートを試みます。
- **add bp-device** コマンドで選択されるインターフェースは、ネットワーク内の BOOTP サーバーの位置によって異なります。
- BOOTP を使用して、直接接続されたシリアル・インターフェースを介してブートすることはできません。

```
Example: add bp-device
Which interface number [0]? 1
```

dump-entry

ダンプ・ファイルを受け取るリモート・ホストの IP アドレスを指定します。**add dump-entry** コマンドを入力するときに、次の情報を提供する必要があります。

remote host?	ダンプ・ファイルが保管されるリモート・ホストの IP アドレス。通常はブート・サーバーと同じです。
via gateway?	ホストがリモート・ネットワーク上にある (ブート装置に直接接続されていない) 場合は、ホストに向けての次のホップ (ルーター) の IP アドレスを指定することが必要です。ホストが直接接続ネットワーク上にある場合は、0.0.0.0 と答えます。

timeout in seconds?	再伝送が行われる前に、装置が待つ時間の長さを指定します。デフォルト値は 3 秒です。極度に遅いブート・パスの場合は、もっと長い時間を設定することが必要になる場合があります。
file name?	基本ダンプ・パスとファイル名 (固有の接尾部を付けることができます)。

ダンプ構成リストを表示するには、 **list dump-entries** コマンドを入力します。

例:

```
add dump-entry
remote host [0.0.0.0]? 128.185.162.30
via gateway (0.0.0.0 if none) [0.0.0.0]? 128.185.160.3
timeout in seconds [3]?
file name []?  c:\dump\gertrude.dmp
```

Change

change コマンドは、情報を削除して再追加するのではなく、既存のアドレス、ブート項目、およびダンプ項目情報内の項目を変更します。 **change** コマンドを使用する代わりに、情報を削除して再入力することもできます。

構文:

change address
boot-entry
bp-device
dump-entry

address

以前に追加したブート・インターフェースまたは装置の既存アドレスを変更します。 **change address**を入力するときは、次の情報を提供する必要があります。

- アドレス項目番号
- ネットワーク・インターフェースのインターフェース番号
- IP アドレス
- ネットワーク・マスク

注: ブート CONFIG の **list** コマンドを入力すると、この情報の一部のもの (アドレス項目番号など) がコンソールに表示されます。インターフェース番号 (Ifc#) を入手したい場合は、CONFIG **list devices** コマンドを使用します。 (このコマンドについては、 43ページの『第5章 構成 (CONFIG) プロセスおよびコマンド (Talk 6)』で説明しています。)

例:

```
change address
Change which entry [1]? 1
Which interface is this address for [0]? 1
New address [192.9.1.1]? 128.185.162.1
Net mask for this interface [255.255.255.0]?
```

boot-entry

以前に追加したネットワーク・ブート・ファイルに関する構成を変更します。 **change boot-entry** コマンドを入力するときは、次の情報を提供する必要があります。

- ブート項目番号
- リモート・ホストの IP アドレス
- 最初のホップ・ルーターの IP アドレス (存在する場合)
- TFTP 再送タイマー値
- ブート・ファイル名 (現行ファイル名と異なる場合)

注: ブート CONFIG の**list boot-entries** コマンドを入力すると、この情報の一部のものが (ブート項目番号など) コンソールに表示されます。

例:

```
change boot-entry
change which entry [1]?
remote host [18.123.0.16]?
via gateway (0.0.0.0 if none) [0.0.0.0]?
timeout in seconds [3]?
file name [user/lib/gw/gwimage.ldb]?
```

bp-device

BOOTP 装置であるインターフェースを変更します。インターフェースの項目番号を入手するには、**list boot-entries** コマンドを使用します。

例:

```
change bp-device
Change which entry [1]?
Which interface is this entry for [1]?
```

注: BOOTP プロトコルと関連のプロセスについての詳細は *プロトコルの構成と監視 解説書* の中の IP プロトコルの構成と監視に関する章を参照してください。

dump-entry

以前に追加したネットワーク・ダンプ・ファイルに関する構成を変更します。 **change dump-entry** コマンドを入力するときは、次の情報を提供する必要があります。

- ダンプ項目番号
- リモート・ホストの IP アドレス
- 最初のホップ・ルーターの IP アドレス (存在する場合)
- TFTP 再送タイマー値
- 基本ブート・ファイル名 (現行ファイル名と異なる場合)

注: この情報を表示するには、ブート CONFIG の**list dump-entries** コマンドを使用します。

例:

```
change dump-entry
change which entry [1]? 1
remote host [18.123.0.16]?
via gateway (0.0.0.0 if none) [0.0.0.0]?
timeout in seconds [3]?
file name [user/lib/gw/gwimage.ldb]? c:\dump\debug1.dmp
```

Copy

copy コマンドは、リモート・ルーターとホストの間でブート・ファイルおよび構成ファイルをコピーするのに使用します。 **copy** コマンドを使用するためには、装置に IP が構成されており、少なくとも 1 つのインターフェース上で稼働していることが必要です。装置は Config-only モードであってはなりません。

構文:

copy config

[ibd or *filename*]

[*host-ip-address* or *filename*]

例 1 - リモート・ルーターからのコピー

```
Boot config> copy
source filename [CONFIG] 128.185.110.30/ibd/Y17.ldc
destination filename  IBD/Y17.ldc
```

Source filename および *destination filename* は、次のいずれかでなければなりません。

config 構成メモリー

ibd/filename
IBD にあるファイル名。完全なパス名を指定してください。

IP address/remote
TFTP ホストにあるリモート・ファイル

path and filename
完全なパス名を指定してください。

注: IBD にファイルをコピーするときには、ファイルは連続した空きバンクの最も大きい集合に入れられます。バンクが利用不能の場合は、コンソールに `COPY error - TFTP Disk Full or IBD full` というメッセージが表示されます。

上の例では、128.185.110.30 の IP アドレスをもつリモート・ルーターからソース・ファイルを入手します。 IBD のファイル名は Y17.ldc. です。ここではコロン (:) は区切り文字として使用されています。 *destination* のファイル名は Y17.cfg です。

例 2 - リモート・ホストからのコピー

```
Boot config> copy
source filename [CONFIG]  128.185.110.30/router/loads/2210.02.cfg
destination filename ibd/2210.02.cfg
```

上の例では、ソースはパスとファイル名が指定されています。宛先は IBD です。

例 3 - 装置内でのコピー

```
Boot config> copy
source filename [CONFIG] config
destination filename [CONFIG]? ibd/2210.02.cfg
```

上の例では、ソースは構成メモリーです。宛先は IBD です。

config copy と入力して **Enter** キーを押したと同じ結果が得られます。ただし、ソース・ファイル名を求めるプロンプトは表示されません。

[ibd or *filename***]**
IBD からブート・ファイルまたは構成ファイルをコピーします。ファイル名を含める必要があります。

[*host-ip-address* **or** *filename***]**
リモート・ホストからブート・ファイルまたは構成ファイルをコピーします。ファイル名を含める必要があります。

Delete

delete コマンドは、ブートおよびダンプの構成データベースから項目を除去するのに使用します。

構文:

delete address
boot-entry
bp-device
dump-entry

address *#*
ブートおよびダンプの構成データベースからインターフェース・アドレス項目を除去します。

delete address コマンドを入力すると、削除したい項目を尋ねるプロンプトが表示されます。アドレス・エントリー番号は、`Boot config>>` プロンプトで **list address** コマンドを入力したときに各行に表示される最初の番号です。

削除されたことを確認するには、**list** コマンドを使用します。

例:

```
delete address
Delete which entry [1]?
```

boot-entry
ブートおよびダンプの構成データベースからブート項目を除去します。**delete boot-entry** コマンドを入力すると、削除したいブート項目を尋ねるプロンプトが表示されます。ブート項目番号は、`Boot config>>` プロンプトで **list boot-entries** コマンドを入力したときに各行に表示される最初の番号です。

削除されたことを確認するには、**list** コマンドを使用します。

例:

```
delete boot-entry
Delete which entry [1]? 2
```

bp-device
BOOTP 装置として指定されたインターフェースを除去します。

例:

```
delete bp-device
Delete which entry [1]?
```

注: BootP プロトコルと関連のプロセスについての詳細は *プロトコルの構成と監視 解説書* の中の IP プロトコルの構成と監視に関する章を参照してください。

dump-entry

ブートおよびダンプの構成データベースからダンプ項目を除去します。**delete dump-entry** コマンドを入力すると、削除したい項目を尋ねるプロンプトが表示されます。ダンプ項目番号は、Boot config>> プロンプトで **list dump-entries** コマンドを入力したときに各行に表示される最初の番号です。

削除されたことを確認するには、**list** コマンドを使用します。

例:

```
delete dump-entry
Delete which entry [1]?
```

Describe

describe コマンドは、IBD に保管されているイメージに関する情報を表示するのに使用します。

構文:

describe *loadname*

loadname

指定されたロード名に関する以下の情報を表示します。

- 著作権情報
- サポートされるプロトコル、機能、およびデータ・リンク・タイプ
- サポートされるネットワーク・インターフェース

例:

```
describe ibd/test.ldb

             Copyright Notice .....


IBM 2210 Bridging Router   V1 R2.0[Y69]    Wed Mar 8 10:24:20 1995

Software configuration: Expanded Multi-Protocol DLSw
Includes:
  Internet Protocol - IP & OSPF
  Novell - IPX
  AppleTalk Phase 2 - AP2
  Banyan VINES - VIN
  Adaptive Source Routing Transparent Bridge - ASRT
    with NETBIOS Name Caching & Filtering
  Data Link Switching - DLSw
  SDLC Relay - SRLY
  Frame Relay
  PPP
  X.25
  V.25bis
  WAN Restoral/Reroute - WRS
  Bandwidth Reservation - BRS
  MAC Filtering - MCF
```

Disable

disable コマンドは、メモリー・ダンプおよびダンプ・ファイルの固有の命名を使用不可にするのに使用します。

構文:

disable dumping

unique-naming

dumping

システム障害の発生時に装置がネットワークへのメモリー・ダンプを実行するのを抑止します。このコマンドを入力した後、ブート CONFIG の**list all** コマンドを使用してダンプ設定値を確認してください。 **enable dumping** コマンドを入力するまで、ダンプは抑制されます。 **Disable dumping** がデフォルト設定です。

unique-naming

ダンプ・ファイルの自動固有命名を抑制します。このコマンドを入力した後、ブート CONFIG の**list all**コマンドを使用して、固有命名の設定値を確認してください。 **enable unique-naming** コマンドを入力するまで、固有命名は抑制されます。 **Disable unique-naming** がデフォルト設定です。

Enable

enable コマンドは、メモリー・ダンプおよびダンプ・ファイルの固有命名を使用可能にします。 **add dump-entry** コマンドで供給されたデータを使用したダンプ操作をオンにするには、このコマンドを使用する必要があります。ダンプを使用可能にするのは、装置に原因不明の問題が生じた場合だけにすることが必要です。ダンプ・ファイルは非常に大きくなり、 ディスク・スペースを大量に消費する可能性があります。インターネットを介して大きなダンプ・ファイルをダンプ・ホストに転送するのには、かなりの時間がかかります。

構文:

enable dumping

unique-naming

dumping

システム障害の発生時に装置がネットワークへのメモリー・ダンプを実行するのを可能にします。このコマンドを入力した後、ブート CONFIG の**list all** コマンドを使用してダンプ設定値を確認してください。 **disable dumping** コマンドを入力するまで、ダンプは使用可能です。

unique-naming

ダンプ・ファイルの固有命名を使用可能にします。ダンプ時に、構成済みダンプ・ファイル名に 1 ～ 5 文字のランダムな接尾部 (16 進数) が追加されます。

このコマンドを入力した後、ブート CONFIG の**list all**コマンドを使用して、固有命名の設定値を確認してください。 **disable unique-naming**コマンドを入力するまで、ダンプ・ファイルには固有の名前が組み込まれます。

Erase

erase コマンドは、保管されているイメージまたは IBD バンクを消去するのに使用します。

構文:

erase [*loadname* または *bank-number*]

loadname または **bank-number**

保管されているイメージまたは IBD バンクを消去します。 **erase** コマンドの後に、ロード名またはロードが入っているバンク番号 (1 〜 64) を入力します。消去されたことを確認するには、**list ibd** コマンドを使用します。 10 回の試行しても消去が正常に行われない場合、装置はそのバンクに障害のマークを付けます。

IBD パラメーター:

IBD サイズ: 4 MB

バンク・サイズ: 64 KB

開始バンク番号: 1

終了バンク番号: 64

ロード・イメージ・ファイルが大きくて 2 つ以上のバンクにまたがっている場合は、バンク番号を指定すると、ロード・イメージ・ファイルが部分的に消去されることになる場合があります。

例 1:

```
erase test
Erasing bank 5 ...
Banks 1-4 contain ...
Banks 5-7 have been erased
```

例 2:

```
erase 2
Are you sure you want to erase bank 2? (Yes or [No]): yes
Erasing bank 2 ...
Banks 5-7 has been erased
```

例 3:

```
erase
Loadname or Bank Number: 4
Are you sure you want to erase bank 4? (Yes or [No]): yes
Erasing bank 4...
Bank 1 contains load "vl-29.cfg" which use 131094 bytes
     Loaded using TFTP over IP
     Filename config
     Host 0.0.0.0
Banks 2-3 contain load "vl-22.cfg" which uses 1832848 bytes
     Manual Booted using TKR-4/16 at (80001000, 72) as  10.1.155.29
     Filename loads/latest-gen.c5-multisna.ldc
     Host 128.185.210.125, Gateway 10.1.155.43
Bank 4 has been erased
```

消去が正常に行われなかった場合は、障害を示すメッセージが、障害を生じたバンクとともにコンソールに表示されます。ルーターがリスタートされていない場合は、**list** コマンドを使用して、障害情報を表示することができます。ルーターは、障害のあるバンク内のイメージを参照するブート・レコードを自動的に削除することは***ありません***。

ブート時に、ブート PROM がイメージを見つけられない場合は、メッセージを表示して、次のブート・レコードを試行します。

List

list コマンドは、現行のブートおよびダンプ構成データベース、IBD の内容、およびスケジュールされたイメージ・ロード情報を表示するのに使用します。

構文:

list

addresses

all

boot-entries

bp-device

dump-entries

ibd

view

addresses

add address コマンドを使用して入力されたすべてのネットワーク・ブート・インターフェースの IP アドレスとサブネット・マスクを表示します。

例:

```
list addresses
Interface addresses:
1: 192.9.1.1 on interface 0, mask 255.255.255.252
2: 192.9.223.39 on interface 2, mask 255.255.255.0
```

all

すべてのブートおよびダンプ構成データ、ならびにダンプ、固有命名機能、およびスケジュールされたイメージ・ロード情報の現行設定値を表示します。

例:

```
Interface Addresses:

 Boot files:
  1: "/u/steve/vl/load/vl060694/vl.X11.ldc" on 216.1.2.100 via 0.0.0.

 BOOTP over interface(s): 0
 Dumping disabled
 Unique-naming disabled
 Dump to:

 Banks 1-19 contain load "vl.X11.ldc" which uses 1199272 bytes
      Loaded using TFTP over IP
      Filename /u/steve/vl/load/vl060694/vl.X11.ldc
   Host 216.1.2.100
Banks 20-48 have been erased
Bank 49 in unknown(AA) state
Banks 50-57 contain load "vl051894.ldc" which uses 508492 bytes
Loaded using TFTP over IP
Filename /u/steve/vl/load/vl051894/vl051894.ldc
   Host 216.1.2.100
Banks 58-64 have been erased

Time Activated Load Schedule Information...

 The router is scheduled to reload as follows.

 Date: April 1, 1997
 Time: 13:00
 Remote host IP address: 1.1.1.2
 Via gateway: 0.0.0.0
 Timeout in seconds: 10
 Filename: /tftpboot/vl3.img
 Interface adress: 0
 New address: 1.1.1.1
 New mask: 255.255.255.0
```

boot-entries

ブート・ファイル構成を表示します。

例:

```
list boot-entries
1: /usr/lib/gw/this-dn.ldb on 192.9.1.2 via 0.0.0.0 for 3 secs
2: /usr/lib/gw/this.ldb on 192.9.2.2 via 192.9.1.4 for 3 secs
3: IBD load "test"
```

bp-device

以前に **add bp-device** コマンドを使用して追加されたインターフェースをリストします。

例:

```
list bp-device
BOOTP over interface(s): 0 1
```

dump-entries

ダンプ・ファイル構成を表示します。

ibd IBD の内容を表示します。 GWCON **boot information** コマンドと同様の情報を提供し、ファイルのロード名とファイルのロード元のホスト・サーバーを表示します。さらに、必要な場合には、IBD の消去済みおよび障害のあるバンクおよび障害のあるチップも表示されます。

例:

```
list ibd
 Bank 1 contains load "2210-29.cfg" which uses 131094 bytes
   Loaded using TFTP over IP
   Filename config
   Host 0.0.0.0
 Banks 2-3 contain load "vl/load-ver2.ldc" which uses
      1652961 bytes
   Loaded using TFTP over IP
   Filename loads/vl/load-ver2.ldc
   Host 128.185.210.125
 Bank 4 contains load "vl/load-ver4.cfg" which uses 131084 bytes
  Loaded using TFTP over IP
  Filename CONFIG
  Host 0.0.0.0
```

『Loaded using TFTP over IP』 は、このローカル・コマンドから IBD への **copy** コマンドが使用されたことを暗黙的に示しています。

view スケジュールされたイメージ・ロードの時刻、日付、およびその他の情報を表示します。

例:

```
list view
Time Activated Load Schedule Information...

  The router is scheduled to reload as follows.

  Date: April 1, 1997
  Time: 13:00
  Remote host IP address: 1.1.1.2
  Via gateway: 0.0.0.0
  Timeout in seconds: 10
  Filename: /tftpboot/vl3.img
  Interface address: 0
  New address: 1.1.1.1
  Network mask for this interface: 255.255.255.0
```

Load

load コマンドは、ローカルまたはリモート・ソースから装置のメイン・メモリーにブート・ファイルをコピーするのに使用します。 **load** コマンドの結果は、* プロンプトから **reload** コマンドを実行した場合と同じです。

構文:

load local . . .

remote . . .

local *loadname*

以前に保管したロード・イメージ・ファイルを装置の IBD から取り出して、ルーターのメモリーに入れます。ロード名は、IBD 内に保管されているロード名の 1 つと一致していなければなりません。ロード名は、大文字・小文字を区別します。

IBD をセットアップするには **add boot-entry** コマンドを使用します。これには最高で 5 分ほどかかります。

IBD 内にロード・ファイルがないと、**load local** コマンドは正常に行われません。

例:

```
load local
Loadname:  ibd/softrel.ldc
```

注: ソフトウェアは、ロード・ファイルが見つからない場合はブート・モニターに行き、ブート・スイッチの設定に応じて、自動ブートまたは手動ブートを実行します。

remote

リモート・ホストから RAM へブート・ファイルをロードします。リモート・ロードを実行するには、次のようにします。

1. Boot config> が表示された後、**load remote** コマンドを入力し、プロンプトで指示されたら、リモート・ホスト・アドレス、リモート・パス名、最初のホップ・アドレス、および TFTP タイムアウトを入力します。
2. 次にロードの確認を求めるプロンプトが出ます。 **no** を入力すると、コマンドは取り消されます。 **yes** を入力すると、リモート・ホストから RAM にブート・ファイルがロードされます。

例:

```
load remote
Remote Host Address [0.0.0.0]? 128.185.210.125
Remote Pathname[]? /loads/v1.ldc
First Hop Address[0.0.0.0]? 128.185.208.38
TFTP Timeout Value [3]?
Are you sure you want to reload the gateway(Yes or No): yes
```

Remote Host Address

ブート・ファイルが入っているホストの IP アドレス

Remote Pathname

ロードしたいブート・ファイルのパス名とファイル名

First Hop Address

他のネットワークに転送する最初のホップ・ルーターのアドレス。リモート・ホスト・アドレスが直接接続されたネットワーク上にない場合には、これを指定する必要があります。そうでない場合は、デフォルト値の 0.0.0.0 を使用します。

TFTP Timeout Value

TFTP パケットの再転送の時間間隔。低速のネットワークやシリアル回線を介してブートする場合、長い時間値 (デフォルト値の 3 より長い時間値) を指定することが必要になる場合があります。

Store

store local コマンドは、IBD の消去済みバンクに圧縮イメージを保管するのに使用します。保管されたバイト数がコンソールに表示されます。イメージが保管されたことを確認するには、**list ibd** コマンドを使用します。

注: ルーターは、バンク 1 ～ 4 に順番にイメージを保管します。 4 つのバンクすべてがいっぱいの場合は、エラー・メッセージを受け取ります。バンク内にスペースを作成するには、 **erase loadname** または **erase bank-number** コマンドを使用します。

装置のロード・イメージ・ファイルは、 IBD に保管されるときに圧縮されます。ロード・イメージ・ファイルは、消去されていない IBD には上書きせず、また IBD の終わりを越えると書き込みを試みません。比較が失敗した場合は、オペレーターに通知され、影響を受けた IBD は消去されます。

ロード名の長さは最大 80 文字の任意の名前が可能で、英字で始まり、大文字・小文字を区別します。

構文:

store local *loadname*

loadname

指定されたイメージを IBD の消去済みバンクに保管します。

例:

```
store local
Loadname: test
Will start storing at bank #2
.
.
.
Number (dec) bytes used
Boot config>
```

Timedload

timedload コマンドは、装置へのイメージ・ロードをスケジュールする、スケジュールされたロードを取り消す、またはスケジュールされたロード情報を表示するのに使用します。

このコマンドにより、サポート技術員が不在のときでも、ネットワーク通信量のピーク期間を外して装置へのロードを実行することが可能になります。

構文:

timedload activate

deactivate

view

activate

装置へのイメージ・ロードをスケジュールします。 **add boot-entry** および

add address コマンドと同様に、イメージのソースを説明する情報の入力を求められます。パラメーターについての詳細は、98ページの『Add』を参照してください。

Time of day to load image

装置が新しいイメージをロードする日付と時刻を指定します。この値は *YYYYMMDDHHMM* 形式で指定します。ただし、

YYYY は 4 桁の年号です。

注: 装置の現在の月が 12 月のときは、年号データは現行年または翌年でなければなりません。また、装置の現在の月が 1 月～11 月のときは、年号データは現行年でなければなりません。

MM は 2 桁の月です。

MM の有効値: 01 ～ 12 (01 は 1 月を表します)

DD は 2 桁の日です。

DD の有効値: 01 ～ 31 (MM の値によって異なります)

HH は 2 桁の時間 (24 時間計) です。

HH の有効値: 00 ～ 23

MM は 2 桁の分です。

MM の有効値: 00 ～ 59

以下に、種々のソースからのロードをスケジュールする例を示します。

例 1: リモート・ホストからのロード

```
Boot config>
timedload activate
Time Activated Load Processing...

  Remote host IP address or IBD load name [0.0.0.0]  1.1.1.2
  Via gateway (0.0.0.0 if none) [0.0.0.0]? 0.0.0.0
  Timeout in seconds [10]? 10
  File name []? /tftpboot/vl3.cce
  Do you want to configure an interface address? (Yes, No, Quit): [No] yes
  Which interface do you want to configure an address to boot over [0]? 0
  New address [0.0.0.0]? 1.1.1.1
  Network mask for this interface [255.255.255.0]?  255.255.255.0
  Config filename [CONFIG] ? ibd/vl3.cfg
  Time of day to load image (YYYYMMDDHMM) []?  199703191630
  The load timer has been activated.
```

例 2: IBD からのロード

```
Boot config> timedload activate
Time Activated Load Processing...

  Remote host IP address or IBD load name [0.0.0.0] ibd:vl3.cce
  Time of day to load image (YYYYMMDDHMM) []? 199703191630
  The load timer has been activated.
```

deactivate

スケジュールされたロードを取り消します。

例 1: 時刻によって起動されたロードの非活動化

```
Boot Config> timedload deactivate
Deactivate Load Timer Processing...

  Do you want to deactivate the load timer? (Yes, No, Quit) [No]? yes
  The load timer has been deactivated
```

view スケジュールされたロード情報を表示します。

例 1: ロード・イメージ・ソースがリモート・ホストの場合

```
Boot Config> timedload view
Time Activated Load Schedule Information...

  The router is scheduled to reload as follows.

  Date: March 19, 1997
  Time: 16:30
  Remote host IP address: 1.1.1.2
  Via gateway: 0.0.0.0
  Timeout in seconds: 10
  Filename: /tftpboot/vl3.cce
  Interface address: 0
  New address: 1.1.1.1
  Network mask for this interface: 255.255.255.0
  Config filename:  ibd/vl3.cfg
```

例 2： ロード・イメージ・ソースが IBD の場合

```
Boot Config> timedload view
Time Activated Load Schedule Information...

  The router is scheduled to reload as follows.

  Date: March 19, 1997
  Time: 16:30
  Filename: vl3.cce
  Config filename:  ibd/vl3.cfg
```

TFTP

TFTP コマンドは、リモート・ホストと装置の不揮発性構成メモリーまたは IBD の間で TFTP ファイル転送を開始するのに使用します。このコマンドにより、TFTP サーバーまたは IBD をもつルーターとの間でロード・イメージを保管/検索する機能が提供されます。

ルーターは TFTP クライアントとして動作します。リモート・ホストは、TFTP サーバー・ノードとして動作する、IP を実行している任意の装置 (たとえば、ルーター、ワークステーション、PC) です。ルーターは Config-only モードであってはなりません。

TFTP get および **put**コマンドを入力すると、この操作の間、CONFIG プロセスはロックされます。 TFTP 操作時には、次の 2 つのキーボード文字の組み合わせが認識されます。

Ctrl-P OPCON プロンプト (*) を表示します。

Ctrl-C TFTP 操作を取り消します。

注: ルーターが **TFTP get** 操作を実行中は、リセット・ボタンを押さないでください。リセット・ボタンを押すとルーターの電源が切れます。この場合、宛先の構成メモリーは矛盾した (無効な) 状態になります。すなわち、構成またはロードの一部分しか持っていないことになりますが、これが有効であるように見えます。

構文:

tftp get
put

get *CONFIG address-remote-server path/filename*
サーバーから 装置へ ファイルを転送するために、TFTP サーバーへの要求を開始します。サーバーはデータ・パケットを送信し、クライアントはデータ

の受信を確認します。このサイクルは、転送が完了し、次のようなメッセージがコンソールに表示されるまで続きます。 `TFTP transfer complete, Status: OK`

TFTP 転送が失敗すると、詳細なエラー・メッセージが画面に表示されます。ファイルを CONFIG に転送している間、次のようなメッセージがコンソールに表示されます。 `Updating Config: Do Not Interrupt`

IBD にファイルを転送しようとしたときに、IBD 内に十分なメモリーがない場合には、次のようなメッセージがコンソールに表示されます。

```
No Free IBD Bank
```

重要： 構成メモリーの更新が進行中に、ルーターをリセットしたり、電源を切ったりしてはなりません。そうすると、構成メモリー内のデータが破壊され、ルーターを再構成しなければならなくなります。

例:

```
tftp get
local filename [CONFIG]?
remote host [0.0.0.0]? 128.185.163.1
host filename [0A019947.cfg]? configs/vl-28.cfg
TFTP transfer complete, status:  OK
```

Local filename

ローカル装置に転送された後のファイル名を指定します。ファイルを IBD に転送する場合は、ファイル名を入力するときに、必ず**完全**なパス名を指定してください。デフォルトは CONFIG です。

Remote Host

転送したいファイルが入っているホストのアドレスを指定します。ファイルに保管されているマジック・ナンバーが、静的 RAM 内の番号と比較されます。こうすることによって、ルーターのタイプ間で、不揮発性メモリーを取り違えてロードするのを防止することができます。

Host filename

ホスト上の転送したいファイルの名前を指定します。必ず、**完全**なパス名を指定してください。デフォルト値は、ホストの IP アドレス (16 進数) の 1 つを ASCII 表示したものです。これによって、ファイルは固有の名前を持ちます。

ホスト名は、保存ファイル内のホスト名と一致していなければなりません。ホスト名は大文字・小文字を区別します。

put *CONFIG address-remote-server path/filename*

ルーターから サーバーへ ファイルを転送するために、TFTP サーバーへの要求を開始します。サーバーは要求に対して確認応答し、クライアントはファイルを転送します。このサイクルは、転送が完了し、次のようなメッセージがコンソールに表示されるまで続きます。

```
TFTP transfer complete, Status: OK
```

注: TFTP put コマンドを用いて、別の装置の構成メモリーまたは IBD にファイルを入れることはできません。そのようにしたい場合は、該当の装置にログインし、**TFTP get** コマンドを使用する必要があります。

コンソールの表示は **TFTP get** コマンドの場合と同じです。

例:

```
tftp put
Local filename [CONFIG]?
Remote host [0.0.0.0]? 128.185.163.1
Host filename [0A019947.cfg]?
TFTP transfer complete, status:  Timeout
```

local filename?

CONFIG が、装置の不揮発性メモリーを参照するファイル名です。

remote Host?

CONFIG をリモート・ホストに保管するために使用する、リモート・ホストの IP アドレスとファイル名を指定する必要があります。

host filename?

ホスト上の転送したいファイルの名前を指定します。必ず、完全なパス名を指定してください。デフォルト値は、ホストの IP アドレス (16 進数) の 1 つを ASCII 表示したものです。これによって、ファイルは固有の名前を持ちます。ホスト名は、保存ファイル内のホスト名と一致していなければなりません。ホスト名は大文字・小文字を区別します。

例:

```
tftp put IBD/r151.ldc
Remote host [0.0.0.0]? 140.187.2.100
Host filename [80B9D626.cfg]? vl605.ldc
TFTP transfer complete, status:  OK
```

TFTP トランザクションを中断する場合は、**Ctrl-C** を押します。 `Are you sure (yes or no):` に対して **yes** と応答します。

TFTP コマンドは、以下のエラー・メッセージを生成します。

エラー・メッセージ	意味
Unknown Error	プロトコル障害
File Not Found	指定したホスト・ファイルが存在しない。
Access Violation	ファイル保護エラー
Disk Full	書き込み中にファイル・システムがいっぱいになった。
Illegal Operation	未定義の TFTP 操作が要求された
Unknown TID	予期しない TFTP パケットを受信した。
File Already Exists	ファイルはすでに存在している。
No Such User	TFTP がホストでサポートされていない。

第9章 ブート・オプション

この章では、使用可能なブート・オプションについて説明します。通常、装置は統合ブート装置 (IBD) からブートします。本章が必要となるのは、保守または診断操作のため、あるいはソフトウェア・アップグレードの場合のみです。

ブート・オプションにより、以下の方式によって 2210をブートすることができます。

表 14. ブート方式の説明

ブート方式	説明
IBD	照会を使用して IBD からブートする。 2210 は異なるブート方式に構成されているが、それに代えて IBD から 2210 をブートしたい場合に、この方式を使用します。
TFTP ホスト・サーバー	TFTP ホスト・サーバー上のロード・イメージ・ファイルからブートする。別のルーターが TFTP ホスト・サーバーとして動作することができます。
BOOTP	ブートストラップ・プロトコルを用いて LAN ポートを介してブートする。

ブート・モニター・プロンプトから使用可能なその他のオプションを使用して、診断の実行、構成情報の表示、ネットワーク上のホストからまたはサービス・ポートを介した構成メモリーのロード、SRAM 内の構成の消去、およびサービス・ポートを介したルーター・コードのダウンロードとアップロードを実行することができます。

この章には、以下の節が含まれています。

始める前に

2210 をブートする前に、以下のことに注意してください。

- この章の手順を使用するためには、2210 に直接接続された端末が必要です (端末の接続方法については、*IBM 2210 Nways マルチプロトコル・ルーター 計画とセットアップの手引き* を参照してください)。
- 2210 は、ブート・ファイル (IBD に保管されている) を添えて出荷されます。
- 2210を ISDN インターフェースを介してブートすることはできません。
- トークンリング・インターフェースを介してブートしている場合、アクティブのトークンリング・リンクがない場合には、次のメッセージを受け取ります。 `lobe media test failed: function failure.`

注: 2210 のブートを停止する場合は、端末のキーボードで **Ctrl-C** を押します。

コンソール端末を使用した統合ブート装置からのブート

コンソール端末を使用した IBD ブートの例は、この手順の最後に示します。このブート方式は、IBD にロード・イメージが保管されている場合に使用します。

1. 次のような著作権情報がコンソールの画面に表示されていなければなりません。必要な場合は、**Reset** ボタンを押してから **Ctrl-C** を押して、この情報を表示させてください。

```
            Bootstrap Monitor V1.0
          (c) Copyright IBM Corp. 1994, 1997
```

2. **bm** と入力すると、次の情報と最初のブート・プロンプトがコンソールに表示されます。

```
PROM Load/Dump Program * Revision: 1.0 *
Copyright IBM Corp. 1994, 1997

IBD has load(s) load image names

Device Slot Number or IBD Load Name:
```

3. ロード・イメージ名を入力します。 IBD ロード名は、大文字・小文字を区別します。 **Return** を押してください。次のメッセージが表示されれば、ソフトウェアのロードが進行しています。

```
Loading using IBD Load Image "ibmMRNS.ldc"
```

コンソール端末を使用した BOOTP

BOOTPは、最初に自己テストが正常に行われたカードから始めて、すべての可能なハードウェア構成を使用して、すべての導入済みインターフェースを介してブートを試みます。通常は、イーサネット、次にトークンリングの順で行われます。 BOOTP に関する詳しい情報は、第7章 ブート CONFIG プロセス を参照してください。

コンソールに次の情報が表示されれば、BOOTP ブートが成功したことを示します。

```
PROM Load/Dump Program * Revision: 1.0 *
Copyright IBM Corp. 1994, 1997

BOOTP Using interface name at (CSR address, vector address)

Trying connector
Doing BOOTP
Trying host IP address
    file name
loading
Copyright IBM Corp. 1994, 1997
Config Only Mode - Switch Selected
*
```

* は、ロード・イメージのロードが終了したこと示します。

BOOTP の失敗

BOOTP は、次の条件下では正常に行われません。

- サーバーが 2210 について知らない場合。コンソールには次の情報が表示されます。

```
PROM Load/Dump Program * Revision: 1.0 *
Copyright IBM Corp. 1994, 1997

BOOTP Using interface at (CSR address, vector address)

Trying connector
Doing BOOTP         BOOTP timeout
Auto BOOTP failed
```

コンソールには、手動ブートを行うように指示するプロンプトが出ます。これらのプロンプトについての説明は、121ページの表16 に示してあります。

- サーバーは 2210 について知っていても、ロード・ファイルが存在しない場合、コンソールには次のような情報が表示されます。

```
PROM Load/Dump Program * Revision: 1.0 *
Copyright IBM Corp. 1994, 1997

BOOTP Using interface at (CSR address, vector address)

Trying connector
Doing BOOTP
BOOTP got reply but server sent no filename
Manual BOOTP failed - Enter @ at prompt BOOTP again
```

@ を入力して、BOOTP を再度試行してください。再試行も失敗した場合は、別の方法を使用して 2210 をブートします。

コンソール端末を使用した TFTP ホスト・サーバーからのブート

TFTP ホスト・サーバー上のロード・イメージ・ファイルを使用して、2210 をブートすることができます。別のルーターが TFTP ホスト・サーバーとして動作することができます。 TFTP ブートの例を、以下に示します。

1. ブート・モニター・プロンプト (>) で **bm** と入力して、次のような情報と最初のブート・プロンプトを表示します。

```
PROM Load/Dump Program * Revision: 1.0 *
Copyright IBM Corp. 1994, 1997

Device Types available:

                IBD
                Token Ring
                WAN
```

2. 表示されるプロンプトは、ブートに使用するインターフェースのタイプによって異なります。イーサネット、トークンリング、または WAN ポートのブートについての詳細は、123ページの『BM (コンソール照会を使用したブート)』 を参照してください。これらのプロンプトについての説明は、121ページの表16 に示してあります。

使用可能なブート・オプション

120ページの表15 に、使用可能なブート・オプションのリストを示してあります。表の後に、ブート・プロセスおよびシステム・プロンプトの詳しい説明があります。

ブート・オプションへのアクセス

1. ロード手順を開始するために、装置の電源を入れるか、または OPCON (*) プロンプトで **reload** と入力し、 **Enter** キーを押します。
2. ブート・モニター・プロンプト (>) を表示するために、ロード手順中に **Ctrl-C** を押します。
3. ブート・プロンプト (>) で **?** と入力すると、ブート・オプションが表示されます。 120ページの表15 は、これらのオプションについて説明しています。

表 15. ブート・オプション

オプション	名前	説明
B	保管済み構成を使用したブート	TFTP または IBD 内に保管されている構成を使用して自動的にブートします。
BC	コンソール照会を使用した Config-only モードへのブート	2210 を手動でブートするためのプロンプトを表示し、Config-only モードに入ります。 2210 の構成を開始することができます。
BM	コンソール照会を使用したブート	2210 を手動でブートするためのプロンプトを表示します。これらのプロンプトについての説明は、121ページの表16 に示してあります。
BN	コンソール照会を使用したブート (実行禁止)	デバッグのためにサービス技術員が使用します。ブートしてブートストラップ・モニターへ戻ります。ただし、ロードは開始しません。
BP	BOOTP を使用したブート	ブートストラップ・プロトコルを使用してブートするためのプロンプトを表示します。
D	保管済み構成を使用したダンプ	この機能は現在 2210 上では利用できません。
DIAG	IBM 拡張診断の開始	内部テストを開始します。内部テストが完了したら、システム拡張チェックアウト (内部テストと外部テスト)、WAN/LAN 折り返しテスト・メニュー、または診断ユーティリティーを使用して、テストを継続するかどうかの選択ができます。いつでも終了して再ブートすることができます。
DM	コンソール照会を使用したダンプ	この機能は現在 2210 上では利用できません。
UB	ブート構成の表示	静的 RAM の TFTP ブートストラップ構成を表示します。
UC	ハードウェア構成の表示	ハードウェア構成に関する情報を表示します。これには装置タイプ、ボー・レート、記憶域サイズ、基本 MAC アドレス、部品番号、製造番号、および改訂レベルが含まれます。
UG	RAM 内のアドレスへの移動と実行	このオプションはサービス技術員が使用します。
LC	構成メモリーのロード	ネットワークに接続するホストから構成メモリーをロードします。
CC	構成メモリーの消去	SRAM 内の構成を消去します。
ZB	ZModem ブート	サービス・ポートを通してルーター・コードをダウンロードおよびアップロードします。
ZC	ZModem 構成メモリーのロード	サービス・ポートを通して構成メモリーをロードします。

ブート・オプション・プロンプト

以下では、各ブート・オプションについて詳しく説明します。

表16 では、2210 がブートされたときに表示されるプロンプトについて説明しています。これらのプロンプトは、ハードウェア構成および 2210 にロードされているソフトウェアによって異なります。

表 16. ブート・オプション・プロンプト

プロンプト	説明
Device Type	2210 のブートを行う装置タイプ。IBD、トークンリング、あるいはイーサネット・インターフェース
IBD Loadname	IBD ロード名。最大 79 の文字、数字、記号を含めることができ、大文字・小文字を区別します。初期導入時に、リリース情報 (バックアップ・ソフトウェア・ディスケット上のファイル README.NTS) にファイル名を入力します。
Interface IP Address	ブートに使用する 2210 インターフェースの IP アドレス。
IP Mask	IP ネットワーク・アドレスを他の IP アドレス・フィールドから分離する 16 進値。ネットワークとサブネットの部分のビットはすべて 1 でなければなりません。
Boot From Host	ブート元のホストの IP アドレス
Via gateway	ブート元のホストが別の (サブ) ネットワークにある場合、中間ルーターが存在します。その中間ルーターの IP アドレスを入力します。
Load Image Name	初期導入の場合、リリース情報 (バックアップ・ソフトウェア・ディスケット上のファイル README.NTS) に記載されているロード・イメージ名を入力します。
Boot File Name	ホスト・サーバーに常駐するロード・イメージ・ファイルのフル・パス名。たとえば、/usr/local/ibm2210.ldc (UNIX の例)。
イーサネット・プロンプト	
Connector Type (AUI/RJ45)	以下のいずれかを入力して、このポートに接続されるケーブル・タイプを指定します。 **AUI** Thick/AUI (10BASE5) **RJ45** シールドなし対より線 (10BASE-T) **AUTOCONFIG** ケーブル・タイプを自動的に検知します。
トークンリング・プロンプト	
Speed (4/16) Mb	**4** または **16** を入力して、トークンリング媒体の転送速度を Mbps 単位で指定します。 **注:** 入力する値は、リングの速度と一致していなければなりません。
Media (UTP/STP)	以下のいずれかを入力して、このインターフェースに接続されるケーブル・タイプを指定します。 **UTP** シールドなし対より線 **STP** シールド付き対より線
WAN プロンプト	
WAN port	2210 をブートするのに使用する WAN ポート。**1** または **2**。

表 16. ブート・オプション・プロンプト (続き)

プロンプト	説明
Timeout (secs)	インターフェースがネットワークを介してブートを試みる時間の長さ (秒)。タイムアウトは 5 秒より大きくなければなりません。
Clock Source (INT/EXT)	接続によって、次のようになります。 • モデムまたは DSU に接続している場合、外部刻時を指定する **EXT** を入力します。 • DTE 装置に接続し、DCE ケーブルを使用している場合は、内部刻時を指定する **INT** を入力します。
Internal Clock Speed	このプロンプトは、Clock Source として **INT** を入力した場合にのみ表示されます。範囲は 1 ～ 10 000 000 です。
Cable Type (X21/Other)	X.21 ケーブルをこのポートに入力する場合は、**X21** を入力します。他のケーブル・タイプをこのポートに接続する場合は、**other** を入力します。

B (ブート)

構成メモリーに保管されている構成を使用して、ルーターを自動的にブートします。構成が TFTP ホストに保管されていない限り、このオプションはルーターに IBD からブートさせます。

BC (Config-only モードでのブート)

2210 をブートし、ただちに Config-only モードに入ります。以下の例は、IBD、トークンリング、イーサネット、および WAN インターフェースを介して 2210 をブートする方法を示しています。ユーザーの入力は太字体で示されています。大括弧内に示されているデフォルト値を受け入れる場合は、**Enter** を押します。

注: 以下のインターフェース・ダイアログの例では、装置のインターフェース・タイプは、`Device Types` リストおよび `Device Type` プロンプトには、トークンリングまたはイーサネットのいずれかとして示されています。

ブート・プロンプト (>) で **bc** と入力します。ソフトウェアは、次のルーター情報の入力を求めます。

```
Device Types available:

          IBD
          Token Ring/Ethernet
          WAN
          Device Type [WAN]: IBD
```

- **IBD** を入力すると、以下が表示されます。

  ```
  IBD has load(s) loadname
  IBD Load Name:  loadname
  ```

  現行構成を再ロードする場合は、**Enter** を押します。

  ```
  Loading using IBD Load Image "load name"
  ```

  正しくないか、あるいは存在しないロード名を指定すると、システムはメッセージ `No such load` を出して、IBD Load Name のプロンプトに戻ります。
- **Token Ring** と入力すると、以下が表示されます。

```
      Media (UTP/STP) [UTP]:
      Speed (4/16)Mb [16Mb]:
      Interface IP address: 123.175.23.119
      IP Mask (FFFFFF00):
      Boot from host: 123.175.68.190
      Via gateway: 123.175.23.213
      Boot file name: ibmMRNS.ldc

  Using Token Ring at (6000000, 0).
  Trying host 123.175.68.190 via 123.175.23.213
  file ibmMRNS.ldc

  .loading
  ................................

  Starting at 1040010

  The Standalone Configuration Process.  You are here because
  the watchdog timer timed out and/or Autoboot not selected.

Config (only)>
```

トークンリング・リンクが活動状態でない場合、次のメッセージを受け取ります。

```
lobe media test failed: function failure
```

- **Ethernet** を入力すると、以下が表示されます。

```
      Connector Type (AUI/RJ45) [AUTO_CONFIG]:
      Interface IP Address: 123.175.56.119
      IP Mask (FFFFFF00):
      Boot from host: 123.175.68.213
      Via Gateway: 123.175.56.190
      Boot File Name: ibmMRNS.ldc

  Using Ethernet at (6000000, 0)
  Trying host 123.175.68.213 via 123.175.56.190
  file ibmMRNS.ldc

  .loading
  ................................

  Starting at 1040010

  The Standalone Configuration Process.  You are here because
  the watchdog timer timed out and/or Autoboot not selected.

  Config (only)>
```

- WAN を介したブート

  指定された WAN ポート上で活動状態となっている CTS 信号が存在しない場合には、 `CTS not active on WAN port #` というメッセージを受け取ります。

  注: PPP プロトコルは、WAN インターフェースを介してブートするときに使用可能な、現在では唯一のデータ・リンク・レイヤー・プロトコルです。

BM (コンソール照会を使用したブート)

コンソール照会を使用してブートを実行します。以下の例は、 IBD を介して、またトークンリング、イーサネット、および WAN インターフェースを介して 2210 をブートする方法を示しています。ユーザーの入力は太字体で示されています。大括弧内に示されているデフォルト値を受け入れる場合は、**Enter** を押します。

このオプションを使用して TFTP ホスト・サーバー上のロード・イメージ・ファイルからブートすることもできます。

注: 以下に示すインターフェース・ダイアログの例では、2210 特定のインターフェース・タイプは、Device Types のリストおよび Device Type のプロンプトに、トークンリングまたはイーサネットのいずれかとして示されています。

ブート・プロンプト (>) で **bm** と入力します。ソフトウェアは、次のルーター情報の入力を求めます。

```
Device Types available:

    IBD
    Token Ring/Ethernet
    WAN

    Device Type [Token Ring/Ethernet]: IBD
```

- **IBD** を入力すると、以下が表示されます。

  ```
  IBD has load(s) load image name
  IBD Load Name: load image name
  ```

  現行構成を再ロードする場合は、**Enter** を押します。別の構成をロードする場合は、プロンプトにロード名を入力します。

  ```
  Loading using IBD Load Image "load name"
  ```

  正しくないか、あるいは存在しないロード名を入力すると、システムは No such load というメッセージを出して、IBD Load Name のプロンプトに戻ります。

- **Token Ring** を入力すると、コンソールに次のような構成ダイアログが表示されます。

  注: 指定されたホストにルーターが直接アクセスできない場合、ゲートウェイの IP アドレスを入力するよう指示されます。このプロンプトは、下の例では括弧で囲んで示されています。

  ```
    Media (UTP/STP) [UTP]:
    Speed (4/16)Mb [16Mb]:
    Interface IP address: 123.175.56.119
    IP Mask (FFFFFF00):
    Boot from host: 123.175.68.213
    Via Gateway: 123.175.56.190
    Boot File Name: ibmMRNS.ldc

  Using Token Ring at (6000000, 0).
  Interface configured for 16Mbps & UTP
  Trying host 123.175.68.213 via 123.175.56.190
  file ibmMRNS.ldc
  loading
  ..................................................

  Starting at 1040000


  Copyright Notices:
  Copyright IBM Corp. 1994, 1997

  MOS Operator Control
  *
  ```

- **Ethernet** を入力すると、以下のように表示されます。

```
        Connector Type (AUI/RJ45)[AUTO_CONFIG]:
        Interface IP Address: 123.175.56.119
        IP Mask (FFFFFF00):
        Boot from host: 123.175.68.213
        Via Gateway: 123.175.56.190
        Boot File Name: ibmMRNS.ldc

    Using Ethernet at (6000000, 0)
    Trying host 123.175.68.213 via 123.175.56.190
    file ibmMRNS.ldc

    .loading
    ................................

    Starting at 1040000

    Copyright Notices:
    Copyright IBM Corp. 1994, 1997

    MOS Operator Control
    *
```

- WAN を介したブート

  指定された WAN ポート上にアクティブの CTS 信号が存在しない場合には、 `CTS not active on WAN port #` というメッセージを受け取ります。

  注: PPP プロトコルは、WAN インターフェースを介してブートするときに使用可能な、現在では唯一のデータ・リンク・レイヤー・プロトコルです。

BN (コンソール照会を使用したブート、実行禁止)

このブート・オプションは使用しないでください。このオプションはサービス技術員だけが使用します。

BP (BootP を使用したブート)

ブートストラップ・プロトコルを使用してブートします。以下の例は、2210 のブート方法を示しています。ユーザーの入力は太字体で示されています。大括弧内に示されているデフォルト値を受け入れる場合は、**Enter** を押します。

注: 以下のインターフェース・ダイアログの例では、装置のインターフェース・タイプは、`Device Types` リストおよび `Device Type` プロンプトには、トークンリングまたはイーサネットのいずれかとして示されています。

ブート・プロンプト (>) で **bp** と入力します。ソフトウェアは、次のルーター情報の入力を求めます。

```
Device Types available:

          Token Ring/Ethernet
          Device type (for BOOTP) [Token Ring]:
```

- **Token Ring** を入力すると、以下のように表示されます。

```
        Media (UTP/STP) [UTP]:
        Speed (4/16)Mb [16Mb]:

    BOOTP Using Token Ring at (6000000, 0).
    Doing BOOTP o
    Interface configured for 16Mbps & UTP
```

```
Trying host 123.175.68.213 via 123.175.56.190
 file load image name
.loading
.................................................

Copyright Notices:
Copyright IBM Corp. 1994, 1997

MOS Operator Control
*
```

- **Ethernet** を入力すると、以下のように表示されます。

```
      Connector Type (AUI/RJ45)[AUTO_CONFIG]:

BootP Using Ethernet at (6000000, 0)
Doing BootP o o o o
Trying host 123.175.68.213 via 123.175.56.190
 file load image name
.loading
...................

Copyright Notices:
Copyright IBM Corp. 1994, 1997

MOS Operator Control
*
```

端末に OPCON (*) プロンプトが表示されれば、BOOTP ブートは成功したことになります。

BOOTP の失敗

BOOTP ブートが失敗するのは、サーバーがダウン状態の場合、サーバーが指定されたファイルを見つけられない場合、あるいは TFTP が失敗した場合です。 BOOTP が失敗しすると、端末に次のメッセージが表示されます。

```
Manual BOOTP failed - enter "@" at prompt to BOOTP again.
```

@ を入力して、BOOTP を再試行してください。再試行も失敗した場合は、別の方法を使用して 2210 をブートします。

D (保管済み構成を使用したダンプ)

システム障害が発生すると、システム・メモリーの内容をファイルに書き込みます。固有命名が使用可能にされている場合、ルーターは自動的にダンプ・ファイル名に文字列を付加します。このコマンドを使用すると、既存のダンプ・ファイルが後続のダンプによって上書きされるのを防止することができます。固有命名を使用可能にする方法については、106ページを参照してください。

ブート・プロンプト (>) で **d** と入力します。画面に次のような情報が表示されます。

```
PROM Load/Dump Program * Revision 1.0
Copyright IBM Corp. 1994, 1997
Host 325.321.62.763 loading


Using Token Ring/Ethernet  (00000, 0)
Trying host 235.211.62.243 via 123.192.23.243
   file load image name
```

```
loading

Starting at 1040000
```

ダンプが失敗した場合、**Dump failed** (ダンプ失敗) というメッセージが、障害の原因の簡単な説明とともに表示されます。

DIAG (IBM 拡張診断プログラムの実行)

内部自己テストを開始します。内部自己テストが完了すると、提供された拡張診断ユーティリティーを選択することができます。拡張診断テストを実行するためには、拡張診断サービス・キット (機構コード 2532) が必要です。このキットには、LAN、シリアル、およびサービスの各ポートに必要なすべての折り返しプラグが入っています。

1. ブート・プロンプト (>) に **diag** と入力して、内部自己テストを実行します。画面に次のようなメッセージが表示されます。

   ```
   Starting at 1FF00

   Starting Hardware Diagnostics
           Version:  XXXXXX  XXXXXX

   Testing System Internal

   System Checkout:  All Systems Pass

   Press space to continue.....
   ```

2. スペース・バーを押して、診断テストの次のレベルに入ります。これらのテストを実行するには、ネットワークからケーブルを取り外して、該当する折り返しプラグを接続することが必要です。折り返しプラグの取り付けは、拡張診断サービス・キットに入っている説明書に従ってください。

   折り返しプラグを取り付けずに、これらのテストのいずれかを実行しようとすると、次のメッセージが出ます。

   ```
   You have selected a test that requires external wrap
   plugs to be present.  Remove the cable(s) from the
   network, and attach the appropriate wrap plug(s).
   ```

3. スペース・バーを押して使用可能な診断オプションの 1 つを選択し、拡張診断サービス・キットに入っている説明書に下がってください。

   ```
   Diagnostic Main Menu (c) 1994

   1) System Checkout (Internal Tests)
   2) System Extended Checkout (Internal and External Tests)
   3) WAN/LAN Wrap Menu
   4) Diagnostic Utilities

   x) Exit (and Reboot)
   ```

DM (コンソール照会を使用したダンプ)

手動でネットワーク・ダンプ情報を構成するためのプロンプトを表示します。

ブート・プロンプト (>) で **dm** と入力します。

画面に次のような情報が表示されます。

```
PROM Load/Dump Program * Revision 1.0
Copyright IBM Corp. 1994, 1997
Host  ??? loading


Using Token Ring/Ethernet  (00000, 0)
Trying host 0.0.0.0 via 0.0.0.0
   file load image name

loading

Starting at 1040000
```

ダンプが失敗した場合、**Dump failed** (ダンプ失敗) というメッセージが、障害の原因の簡単な説明とともに表示されます。

UB (TFTP ブート構成の表示)

以下の情報を含む、静的 RAM の TFTP ブートストラップ構成を表示します。

- ホスト名
- ダンプが使用可能か使用不可か
- 固有命名が使用可能か使用不可か
- インターフェース IP アドレス、インターフェースのタイプ、およびマスク
- ブート・ファイル名
- ホストの IP アドレス
- ゲートウェイの IP アドレス

ダンプ・ファイルが作成されている場合、UB はダンプ・ファイル名とダンプ・ファイルが存在するホストの IP アドレス、および中間ゲートウェイの IP アドレス (該当する場合) も表示します。

この情報を表示するには、ブート・プロンプト (>) の後に **ub** と入力します。画面に次の例と同様の情報が表示されます。

```
TFTP bootstrap configuration:
    Host ibmMRNSV1 - .191, Dumping disabled, Unique dump naming off
Interface Addresses:
    1: 128.196.145.191 on port 0 (Token Ring/Ethernet), mask FFFFF00
Boot Files
    1: ibmMRNS.ldc on 123.175.68.213 via 123.175.56.190 for 20 secs
    2: r15.1.ldc on 123.175.68.213 via 123.175.56.190 for 20 secs
    3: ibmMRNS-univ.ldc on 123.175.68.213 via 123.175.56.190 for 20 secs
Dump Files:
    1: "gw/ibmMRNS.dmp" on 123.175.68.213 via 123.175.56.190 for 20 secs
>
```

UC (ハードウェア構成の表示)

次の情報を表示します。

- 使用可能な装置タイプ
- コンソールのボー・レート
- 主メモリーと IBD のサイズ (MB 単位)
- 基本 MAC アドレス
- ルーターの製造番号

- システム・カードの製造番号
- モデム番号
- システム・カードの部品番号
- システム・カードの改訂 (ECO) レベル
- プラットフォームの改訂

注: 各 2210 は、イーサネットの配列の基本 MAC アドレスを使用して、工場でプログラムされています。トークンリング装置を使用している場合、2210 はアドレスをトークンリングの配列に変換しますが、 **uc** コマンドは、アドレスをイーサネット配列で表示します。

ブート・プロンプト (>) で **uc** と入力します。画面に以下のような情報が表示されます。

```
Boot device types available:
          IBD
          Token Ring
          WAN

Console Baud Rate:        9600 (Autobaud)
Main Memory size:         8 MB
IBD (flash Memory) size:  4 MB
Base MAC Address:         000093808068
System Part Number        04H7063
System Serial Number      55554000008
System EC Level           D50514
System Card Part Number   13H7771
System Card Serial Number 110653
System EC Level           C99200B
```

UG (RAM 内アドレスでの実行)

このオプションはサービス技術員だけが使用します。

LC (構成メモリーのロード)

ネットワークに接続するホストから構成メモリーをロードします。このオプションを使用する場合は、以下を実行します。

ブート・プロンプト (>) で **lc** と入力します。画面に以下のような情報が表示されます。

```
Device Types available:

          IBD
          Token Ring/Ethernet
          WAN

          Device type [Token Ring]:
```

- **Token Ring** を入力すると、次のように表示されます。

```
Media (UTP/STP) [UTP]:
Speed (4/16)Mb [16Mb]:
Interface IP address: 123.175.56.119
IP Mask (FFFFFF00):
Load Cfg from host: 123.175.68.213
Via gateway: 123.175.56.190
Config File Name: ibmMRNS.cfg
```

```
Using Token Ring at (6000000, 0).
Trying host 123.175.68.213 via 123.175.56.190
file ibmMRNS.cfg

.loading
Receiving config memory image
.................................................

Starting at 1040000

Copyright Notices:
Copyright IBM Corp. 1994, 1997

MOS Operator Control
*
```

- **Ethernet** を入力すると、次のように表示されます。

```
     Connector Type (AUI/RJ45)[AUTO_CONFIG]:
     Interface IP address: 123.175.56.119
     IP mask (FFFFFF00):
     Load Cfg from host: 123.175.68.219
     Via gateway: 123.175.56.190
     Config file name: ibmMRNS.cfg

Using Ethernet at (6000000, 0).
Trying host 123.175.68.219 via 123.175.56.190
file ibmMRNS.cfg

.loading
Receiving config memory image
.................................

Starting at 1040000

Copyright Notices:
Copyright IBM Corp. 1994, 1997

MOS Operator Control
*
```

- **WAN** を入力すると、次のように表示されます。

```
     WAN port [2]:
     Timeout (secs) [20] ?
     Clock Source (INT/EXT) [INT]:
     Internal Clock Speed 1
     Interface IP address: 123.175.56.119
     IP mask [FFFFFF00]:
     Load Cfg from host: 123.175.68.219
     Via gateway: 123.175.56.190
     Config file name: ibmMRNS.cfg

Using Serial Line at ( 0, 0).
Trying host 123.175.68.219 via 123.175.56.190
file ibmMRNS.cfg

.loading
Receiving config memory image
.................................
Starting at 1040000

Copyright Notices:
Copyright IBM Corp. 1994, 1997

MOS Operator Control
*
```

CC (構成メモリーの消去)

重要 : このコマンドを出すと、すべての構成情報が失われます。

このコマンドはメモリー内の構成を消去します。ブート・プロンプト (>) で **cc** と入力します。ソフトウェアは、次のような消去の確認を求めるプロンプトを出します。

```
Are you sure you want to clear config memory?
```

ZB (ZModem ブート)

コンソール・ポートを介して、ルーター・コードをダウンロードおよびアップロードします。

1. ブート・プロンプト (>) で **ZB** と入力すると、コンソールに次のような表示が出ます。

   ```
   Are you sure you want to load via the console?
   ```

2. **y** を入力すると、コンソールに次のメッセージが表示されます。

   ```
   Okay, GO!!
   ```

3. **Return** を押すと、操作が開始されます。システム・プロンプト (>) が画面に表示されれば、操作は完了です。

注: コンソール端末で使用する ZModem コマンドについては、ZModem ソフトウェアに付属の資料を参照してください。

ZC (ZModem 構成メモリーのロード)

コンソール・ポートを通して構成メモリーをロードします。

注: このオプションを使用するためには、リモート・ブート・サーバーが ZModem ソフトウェアをサポートしていることが必要です。

1. ブート・プロンプト (>) で **ZC** と入力します。コンソールに次のようなプロンプトが表示されます。

   ```
   Are you sure you want to load config memory via the console?
   ```

2. **y** を押します。コンソールに次のようなメッセージが表示されます。

   ```
   Okay, GO!!
   ```

3. **Return** を押すと、操作が開始されます。ブート・プロンプトが画面に表示されれば、この操作は完了です。
4. **n** を入力して、OPCON プロンプトに戻ります。

注: コンソール端末で使用する ZModem コマンドについては、ZModem ソフトウェアに付属の資料を参照してください。

2210 の構成

2210 のブート後、これを構成することができます。以下では、**ASCII 端末**を使用している場合に利用できる構成プロセスを簡単に説明します。

注: IBM Nways マルチプロトコル・ルーティング・サービス構成プログラム (構成プログラム) を使用して 2210 を構成することもできます。構成プログラムは、**スタンドアロン・ワークステーション**で実行し、グラフィカル・ユーザー・インターフェースを備えています。事前構成またはクイック構成を行っておけば、構成プログラムを使用して 2210 を完全に構成することができます。

構成プロセスを開始するには、以下の手順で行います。

1. * プロンプトで **status** と入力すると、構成 (Config) の PID (プロセス ID) が表示されます。

```
Pid  Name      Status TTY  Comments
1    COpCN1    RDY    TTY0
2    Monitr    DET     --
3    Tasker    RDY     --
4    MOSDDT    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ROpCN1    IDL    TTY1 128.185.133.2
8    ROpCN2    RDY    TTY2 128.185.134.50
```

2. **talk** と PID を入力します。 132ページのステップ 1 の出力から、次のように入力します。

```
* talk 6
```

   Return を押します。次のような情報が表示されます。

```
Gateway user configuration
Config>
```

3. これで、以下のプロセスの 1 つを使用して、インターフェース、ブート・レコード、ブリッジング、およびルーティング・プロトコルを構成することができます。

   - **クイック構成プロセス**を使用すると、クイック構成プロンプトに応答しながら、選択された装置、ブリッジング・プロトコル、およびルーティング・プロトコルを構成することができます。最小構成を作成した後、TFTP を使用して完全な構成を 2210 に転送する必要があります。

     Config> プロンプトで **qc** と入力して、クイック構成プロセスを開始します。

   - **CONFIG プロセス**を使用すると、Config> プロンプトでコマンドを入力することにより、すべてのブリッジングおよびルーティング・プロトコル、インターフェース、およびブート・レコードを構成することができます。

     CONFIG プロセスを使用してプロトコルを構成する場合は、 *プロトコルの構成と監視 解説書* の該当するプロトコルの章を参照してください。また、インターフェースやブート・レコードを含めたその他のパラメーターの構成については、この資料の該当する構成の章を参照してください。

第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド

この章では GWCON プロセスについて説明し、以下の節が含まれています。

GWCON とは

ゲートウェイ・コンソール (監視) プロセス GWCON (CGWCON とも言います) は、ルーター・ユーザー・インターフェースの第 2 レベルのプロセスです。

GWCON コマンドを使用して、次のことが行えます。

- ルーターに現在構成されているプロトコルおよびインターフェースをリストする。
- メモリーおよびネットワークの統計を表示する。
- 現行のイベント・ログ・システム (ELS) パラメーターを設定する。
- 指定されたネットワーク・インターフェースをテストする。
- 第 3 レベルのプロセス (プロトコル環境を含む) と通信する。
- インターフェースを使用可能および使用不可にする。

GWCON コマンド・インターフェースは、いくつかのレベル (モードと呼ばれる) で構成されています。各モードには、それぞれ独自のプロンプトがあります。たとえば、IP プロトコルのプロンプトは `IP>` です。

自分が通信しているプロセスおよびモードを知りたい場合は、**Return** キーを押すと、プロンプトが表示されます。この章で説明する一部のコマンド (**network** や **protocol** など) では、GWCON の種々のレベルにアクセスすることができます。

GWCON の出入り

OPCON から GWCON コマンド環境に入り、GWCON プロンプトを表示するには、**talk 5** と入力します。

```
* talk 5
```

コンソールに GWCON プロンプト (+) が表示されます。このプロンプトが表示されない場合は、**Return** キーを押します。ここで GWCON コマンドを入力することができます。

OPCON に戻るには、OPCON インターセプト文字を入力します。 (デフォルトは **Ctrl-P** です。)

GWCON コマンド

この節には GWCON コマンドを記載します。各コマンドごとに、説明、構文の要件、および例を示します。 GWCON コマンドの要約を 表17 に示します。

GWCON コマンドを使用するには、**talk 5** と入力して GWCON プロセスにアクセスし、(+) プロンプトで GWCON コマンドを入力します。

表 17. GWCON コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Activate	新たに構成された予備インターフェースを使用可能にします。
Boot	装置が最後にブートされたときのブート方法についての情報を表示します。
Buffer	各インターフェースに割り当てられたパケット・バッファーに関する情報を表示します。
Clear	ネットワーク統計を消去します。
Configuration	現行のプロトコルおよびインターフェースの状態をリストします。
Disable	指定されたインターフェースをオフラインにします。
Environment	環境システム・コンソールに入ります。現在の温度を表示し、温度限界値 (上限または下限) を外れると警報を出します。
Error	誤りの件数を表示します。
Event	イベント・ログ・システム環境に入ります。
Fault	前回のシステム障害に関する情報を表示します。
Feature	通常のプロトコルおよびネットワーク・インターフェースのコンソール・プロセスの外部の、独立したルーター機能のコンソール・コマンドへのアクセスを提供します。
Interface	ネットワークのハードウェア統計または指定されたインターフェースの統計を表示します。
Log	イベント・ログ・システムに含まれていないイベントのログ・レベルを設定または表示します。
Memory	メモリー、バッファー、およびパケット・データを表示します。
Network	指定されたネットワークのコンソール環境に入ります。
Performance	基本プロセッサーの使用状況の統計のスナップショットを提供します。
Protocol	指定されたプロトコルのコマンド環境に入ります。
Queue	指定されたインターフェースのバッファー統計を表示します。
Reset	指定されたインターフェースを使用不可にした後で、新しいインターフェース、プロトコル、および機能構成パラメーターを使用して、再びインターフェースを使用可能にします。
Statistics	指定されたインターフェースの統計を表示します。
Test	使用不可にされているインターフェースを使用可能にするか、または指定されたインターフェースをテストします。
Uptime	ルーターの時間に関する統計を表示します。

Activate

activate コマンドは、この装置上の予備インターフェースを使用可能にするのに使用します。詳細については、49ページの『予備インターフェースの構成』 を参照してください。

構文:

activate *interface#*

Boot

boot コマンドは、この装置に関するブート情報を表示するのに使用します。

構文:

boot

例 1:

```
boot
Booted using Ethernet, line 0 at (80740000, 4) as 128.185.227.220
Filename vl.ldc
Host 128.185.122.17, Gateway 128.185.227.15
```

この最初の例では、ルーターはイーサネットを介して TFTP を使用してブートされました。メッセージは、ブートの方式、回線番号、CSR (コマンドおよび状況レジスター) アドレス、IP アドレス、ファイル名、ホスト、およびゲートウェイを示しています。 *line number* は、複数ポート・ボード上の個々のポートを区別します。 *CSR address* (括弧内の 2 つの値のうちの最初の値) は、ルーターをブートするために使用されたインターフェース・ボードのスロットを識別します。

『as』 の後にリストされている *IP アドレス* (この例では、128.185.227.220) は、ルーターが自分自身の IP アドレスとして使用した IP アドレスを示します。 *Filename* は、ロード・イメージが入っているファイルの名前です。 *Host* の後にリストされている IP アドレスは、ファイルが保管されているサーバーの IP アドレスです。 *Gateway* (リストされている場合) は、サーバーとブートするルーターとの間での要求と応答をルーティングするルーターです。

例 2:

```
boot
Manual Booted using Integrated Boot Device Loadname vl.ver1
```

2 番目の例では、ルーターは統合ブート装置 (IBD) を使用してブートされました。 *Manual* は、ブートするときにブート情報が手動で入力されたことを示しています。

Buffer

buffer コマンドは、各インターフェースまたは一定範囲のインターフェースに割り当てられたパケット・バッファーに関する情報を表示するのに使用します。

注: 1 つの装置上の各バッファーは同じサイズで、動的に作成されます。バッファーのサイズは装置によって異なります。

1 つのインターフェースだけの情報を表示する場合は、そのインターフェースまたはネットワークの番号を、コマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

構文:

buffer [*network#* または *range_of_network#*]

複数のインターフェースに関する情報を表示するには、range_of_network# (または、*network#* と *range_of_network#* の組み合わせ) を指定します。たとえば、**buffer 0 3 25-50** と指定すると、ネット 0、3、および 25 ～ 50 の情報が表示されます。

例:

```
buffer
                Input  Buffers:       Buffer sizes:
Nt  Interface   Req  Alloc   Low Curr  Hdr  Wrap  Data  Trail Total   Bytes Alloc
0   TKR/0        20    20     7    0  109   92    2052    7   2260   45200
1   PPP/0        20    20     7   20  109   92    2052    7   2260   45200
2   PPP/1        10    10     4    0  108   92    2048    0   2248   22480
```

Nt ソフトウェアに対応するネットワーク・インターフェース番号

Interface
インターフェースのタイプ

Input Buffers:

Req 要求されたバッファー数

Alloc 割り振られたバッファー数

Low 最低水準点 (フロー制御)

Curr この装置の現行のバッファー数。装置が使用不可にされている場合は、この値は 0 になります。パケットを受信したときに、*Curr* の値が *Low* より下である場合、そのパケットはフロー制御可能です。 (条件については、**queue** を参照してください。)

Buffer Sizes:

Hdr 最大ハードウェア、MAC、およびデータ・リンク・ヘッダー数の合計

Wrap プロトコル折り返しのために MAC、LLC、またはネットワーク・レイヤー・ヘッダーに与えられる許容範囲

Data 最大データ・リンク・レイヤー・パケット・サイズ

Trail 最大 MAC およびハードウェア・トレーラー数の合計

Total 各パケット・バッファーの合計サイズ

Bytes Alloc
この装置のバッファー・メモリーの量。この値は、*Alloc x Total* の乗算値によって決まります。

Clear

clear コマンドは、ルーターのネットワーク・インターフェースの 1 つまたはすべての統計情報を削除するのに使用します。このコマンドは、大容量カウンター内の変更を追跡するのに便利です。このコマンドを使用しても、スペースの節約やルーターの高速化にはつながりません。

インターフェース (または、ネットワーク) 番号を、コマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

構文:

clear *interface#*or *range_of_interface#*

複数のインターフェースに関する情報を消去するには、range_of_network# (または *interface#* と *range_of_interface#* の組み合わせ) を指定します。たとえば、**clear 0 3 25-50** と指定すると、ネット 0、3、および 25 ～ 50 の情報が消去されます。

Configuration

configuration コマンドは、プロトコルまたはネットワーク・インターフェースに関する情報を表示するのに使用します。出力は 3 つのセクションに分けて表示されます。最初のセクションには、ルーターの識別、ソフトウェア・バージョン、ブート ROM バージョン、および自動ブート・スイッチの状態がリストされます。 2 番目と 3 番目のセクションには、プロトコルおよびインターフェースの情報がリストされます。

構文:

configuration

複数のインターフェースに関する情報を表示するには、range_of_network# (または、*network#* と *range_of_network#* の組み合わせ) を指定します。たとえば、**configuration 0 3 25-50** と指定すると、ネット 0、3、および 25 ～ 50 の情報が表示されます。

例:

```
configuration

Multiprotocol Routing Services


5765-C90 Feature 5047 V1 R2.0 PTF 0 RPQ 0
Boot ROM version  1.20     Watchdog timer enabled  Auto-boot enabled
Time: 15:46:12    Friday     September 20, 1996  Console baud rate: 9600

Num Name  Protocol
0   IP    DOD-IP
3   ARP   Address Resolution
11  SNMP  Simple Network Management Protocol
12  OSPF  Open SPF-Based Routing Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
26  DLS   Data Link Switching

Num Name  Feature
2   MCF   MAC Filtering

3 Networks:
Net Interface  MAC/Data-Link         Hardware          State
0   TKR/0   Token-Ring/802.5         Token-Ring         Up
1   Eth/0   Ethernet/IEEE 802.3      Ethernet/802.3     Up
2   PPP/0   Point to Point           SCC Serial Line    Up
```

- 最初の行は、プロダクト名を示しています。
- 2 行目には、プログラム/プロダクト番号、機構番号、バージョン、リリース、PTF、および RPQ 情報がリストされます。
- 3 行目は、現在ルーター内に導入されているブート PROM (プログラム式読み取り専用メモリー) のバージョンと、見張りタイマーおよび自動ブート・スイッチの現行設定を表示します。
- 4 行目は、日付と時刻、および DTE と DCE の現行コンソール・ボー・レート設定を表示します。

- 残りの行は、構成済みのプロトコルをリストし、その後に構成済みの機能をリストしています。

プロトコルに関する以下の情報が表示されます。

Num プロトコルに対応する番号

Name プロトコルの簡略名

Protocol
プロトコルのフルネーム

機能に関する以下の情報が表示されます。

Num 機能に対応する番号

Name 機能の簡略名

Feature
機能のフルネーム

ネットワークに関する以下の情報が表示されます。

Net ソフトウェアがインターフェースに割り当てるネットワーク番号。ネットワークには 0 から始まる番号が付けられます。これらの番号は、CONFIG プロセスの項で説明したインターフェース番号に対応しています。

Interface
インターフェースの名前とこのタイプのインターフェースのインスタンス

MAC/Data Link
インターフェースに構成された MAC/データ・リンクのタイプ

Hardware
ハードウェア・タイプで表された特定の種類のインターフェース

State ネットワーク・インターフェースの現在の状態

Testing
インターフェースが自己テスト中であることを示します。自己テストが行われるのは、ルーターが最初にスタートしたとき、インターフェースで問題が検出されたとき、または **test command** が使用されたときです。

インターフェースが動作可能のときは、インターフェースは定期的に保守パケットを送り出すか、ポートまたは伝送路の物理的状態をチェックする (あるいは、その両方を行う) ことによって、インターフェースがまだ正常に機能していることを確認します。この保守で障害が生じた場合、インターフェースはダウンとして宣言され、5 秒後に自己テストを実行するようにスケジュールされています。自己テストに失敗した場合、インターフェースはダウン状態に変換され、次回の自己テストまでの期間が、最大 2 分まで増やされます。自己テストが正常に行われた場合は、ネットワークはアップとして宣言されます。

Up インターフェースが動作可能であることを示します。

Down インターフェースが動作不能であり、自己テストに失敗したことを

示します。ネットワークは定期的に testing 状態になり、インターフェースが再び動作可能になったかどうかを調べます。

Disabled

インターフェースが使用不可にされていることを示します。インターフェースは、次の方法で使用不可にすることができます。

- CONFIG **disable** コマンドを使用して、インターフェースを使用不可として構成する。ルーターを再初期化するたびに、インターフェースの初期状態は使用不可になります。使用可能にする処置を取るまでは、使用不可の状態のままです。
- GWCON **disable** コマンドを使用して、インターフェースを使用不可にする。この方法は一時的なもので、ルーターを再初期化すると、インターフェースは構成された状態 (使用可能または使用不可) に戻ります。
- ネットワーク・マネージャーが SNMP を使用してインターフェースを使用不可にする。この方法は一時的なもので、ルーターを再初期化すると、インターフェースは構成された状態 (使用可能または使用不可) に戻ります。

インターフェースが使用不可にされている場合、次の方法の 1 つを使用して使用可能にするまでは、使用不可のままです。

- GWCON **test** コマンドを使用して、インターフェースの自己テストを開始する。
- ネットワーク・マネージャーが SNMP を使用して自己テストを開始する。

WAN 再ルートを使用して、使用不可にされたインターフェースの状態を変更することもできます。インターフェースが WAN 再ルートの代替インターフェースとして構成されており、構成された状態が使用不可である場合、WAN 再ルートは、1 次インターフェースがダウンするとインターフェースの自己テストを開始します。 1 次インターフェースが再び動作可能になり安定すると、WAN 再ルートは代替インターフェースを構成された状態に戻します。詳細については、787ページの『第59章 WAN 再ルート機能』 を参照してください。

Available

インターフェースは 2 次 WAN 復元インターフェースとして構成されており、1 次インターフェースのバックアップとして利用可能であることを示します。

Not Present

インターフェースのアダプターのプラグが差し込まれていないことを示します。

Not Present は、空の装置の状態を示すのにも使用されます。予備インターフェースは、起動されるまでは空の装置として表示されます。

HW Mismatch

構成されたアダプター・タイプが、実際にスロット内に存在するアダプターのタイプと一致していないことを示します。

Disable

disable コマンドは、ネットワーク・インターフェースをオフラインにし、そのインターフェースを利用不能にするのに使用します。 このコマンドは、インターフェースを即時に使用不可にします。確認を求めるプロンプトは出ず、検証メッセージも表示されません。このコマンドを用いてインターフェース を使用不可にした場合、GWCON **test** コマンドまたは OPCON **restart** コマンドを用いて使用可能にするまで、インターフェースは使用不可のままです。

インターフェースまたはネットワーク番号を、コマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

注: 使用不可にしようとしているインターフェースが代替 WAN 再ルートとして構成されている場合、この代替インターフェースを含む WAN 再ルート 1 次/代替の組みを使用不可にするかどうかを尋ねられます。 *yes* と応答すると、インターフェースは使用不可にされ、1 次インターフェースのバックアップとして利用できなくなります。 *no* と応答すると、代替インターフェースは使用不可にされますが、対応する 1 次インターフェースがダウンした場合には、WAN 再ルートはこれの起動を試みます。 詳細については、787ページの『第59章 WAN 再ルート機能』、 763ページの『第57章 WAN 復元の使用』、および 769ページの『第58章 WAN 復元の構成および監視』 を参照してください。

構文:

disable *interface#*

Environment

注: このコマンドを呼び出すのは、サービス・ポートが 2 つあるルーターの場合***だけ***です。

ENV> プロンプトを表示します。ここで使用可能なコマンドは 3 つあります。すなわち、**list**、**reset-max-min**、および **exit** です。 **exit** を入力すると、+ プロンプトに戻ります。

厳しい温度条件下では、温度チップがルーターをリセット状態に保持し、動作を停止させます。温度条件下でのルーターの正常な動作を保証するために、温度チップはルーターを -55°C ～ 85°C の範囲で動作するようにします。これは動作可能な範囲ではありません。

85°C 以上になると、温度チップはルーターを遮断し、温度が 80°C 以下になるまで、ルーターは再稼働しません。チップに影響を与えるのは高温だけです。低温条件はルーターのリセットの原因になりません。マイナス 55°C (-67°F) が、チップが記録できる最低温度です。

構文:

environment

list コマンドは、現在の温度、連続的な温度読み取り間隔、前回のリセット/クリア以降に記録された最高温度と最低温度を表示し、温度限界値 (上限または下限) を超えている場合は警報を出し、合わせてヒステリシス値も表示します。

例:

```
ENV>list

   Time: 14:23:12    Sunday, January 09 2011

   Current Ambient Temperature: 44C (111F)

   Recalculate temperature approx. every 60 seconds.

   Maximum:  48C (118F) at 11:47:32   Friday,     January 07 2011
   Minimum:  40C (104F) at 15:24:21   Saturday,   January 08 2011
   Last Max/Min Reset:     09:21:17   Thursday,   January 06 2011

   High Temperature Alarm Threshold:  85C (185F)
   Low Temperature Alarm Threshold:   -55C (-67F)
    (Hysteresis value: +/- 5C))
```

reset-max-min コマンドは、最後に記録された最高温度と最低温度の値を、現在の温度に設定します。これは標準的な温度計のリセットに似ています。

例

```
reset-max-min

Maximum and Minimum Temperature reset to current ambient temperature: 44C (111F)
```

Error

error コマンドは、ネットワークの誤りの統計を表示するのに使用します。このコマンドは、誤りカウンターのグループを表示します。

構文:

error [*network#* or *range_of_network#*]

複数のインターフェースに関する情報を表示するには、range_of_network# (または、*network#* と *range_of_network#* の組み合わせ) を指定します。たとえば、**error 0 3 25-50** と指定すると、ネット 0、3、および 25 ～ 50 の情報が表示されます。

例:

```
error

                  Input   Input      Input      Input     Output  Output
Nt  Interface  Discards  Errors  Unk Proto  Flow Drop   Discards  Errors
0   TKR/0             0       0          0          0          0         0
1   PPP/0             0       0          0          0          0         0
2   PPP/1             0       0          0          0          0         0
```

Nt ソフトウェアに対応するネットワーク・インターフェース番号

Interface
インターフェースのタイプ

Input Discards
誤りは検出されなかったが、高位レイヤー・プロトコルに送達される可能性を防止するために廃棄された着信パケットの数。これらのパケットは、バッファー・スペースを空けるために廃棄された可能性もあります。

Input Errors
データ・リンクで欠陥が見つかったパケットの数

Input Unk Proto
確認不能のプロトコルの受信パケットの数

Input Flow Drop
出力時にフロー制御された受信パケットの数

Output Discards
ルーターがフロー制御のために転送せずに廃棄することを選択したパケットの数

Output Errors
ダウンしているネットワークや、転送中にダウンしたネットワーク上で送信を試みるといった出力誤りの数

注: 廃棄された出力パケットの合計は、すべてのネットワーク上の入力フロー除去数と同じではありません。廃棄された出力には、ローカルで発信されたパケットが含まれていることもあります。

Event

event コマンドは、イベント・ログ・システム (ELS) コンソール環境にアクセスするのに使用します。この環境は、トラブルシューティングのために一時的にメッセージ・フィルターを設定するのに使用されます。 ELS コンソール環境で行われたすべての変更は即時に有効になりますが、ルーターが再初期化されると無効になります。イベント・ログ・システムとそのコマンドについては、153ページの『第12章 イベント・ログ・システム (ELS) の使用』 を参照してください。 GWCON プロセスに戻るには **exit** コマンドを使用します。

構文:

event

Fault

fault コマンドは、最後のシステム障害に関する情報を表示するのに使用します。この診断情報は、サービス技術員が繰り返し発生するシステム・エラーをトレースする場合に役立ちます。生成される出力は、サービス技術員だけが使用するためのものです。

構文:

fault

Feature

feature コマンドは、プロトコルおよびネットワーク・インターフェースのコンソール・プロセスの外部の、特定 2210 機能のコンソール・コマンドにアクセスするのに使用します。

使用しているソフトウェア・リリースで利用可能な機能のリストを入手するには、**feature** コマンドの後に疑問符を入力します。

その機能のコンソール・プロンプトにアクセスするには、GWCON プロンプトで **feature** コマンドを入力し、その後に続けて機能番号または短縮名を入力します。72ページの表8 に、利用可能な機能番号と短縮名をリストしてあります。

機能のプロンプトにアクセスしたら、その機能を監視するための特定のコマンドの入力を開始することができます。 GWCON プロンプトに戻るには、機能のコンソール・プロンプトで **exit** コマンドを入力します。

構文:

feature *feature#* or *feature-short-name*

Interface

interface コマンドは、ネットワーク・インターフェース (たとえば、イーサネットまたはトークンリング) に関する統計情報を表示するのに使用します。 このコマンドは、クォリファイアーを付けずに使用して、すべてのインターフェースの要約 (下記の出力に表示) を示したり、クォリファイアーを付けて、1 つの特定インターフェースの詳しい情報を表示したりすることができます。

各タイプのインターフェースの詳細な出力についての説明は、本書の中の特定インターフェースの*監視* の項に記載されています。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

構文:

interface [*interface#* or *range_of_interface#*]

複数のインターフェースに関する情報を表示するには、range_of_network# (または *interface#* と *range_of_interface#* の組み合わせ) を指定します。たとえば、**interface 0 3 25-50** と指定すると、ネット 0、3、および 25 ～ 50 の情報が表示されます。

例: interface

```
                                    Self-Test  Self-Test  Maintenance
 Nt Nt' Interface      CSR  Vec      Passed     Failed       Failed
 0  0   Eth/0        81600   5E           1          0            0
 1  1   PPP/0        81620   5D           0         31            0
 2  2   PPP/1        81640   5C           0         31            0
```

注: 表示は装置に応じて異なります。

Nt グローバル・インターフェース番号

Nt' ダイヤル回線用に予約済み。ダイヤル回線が使用する物理ネットワーク・インターフェースのインターフェース番号

Interface
インターフェース名

CSR コマンドおよび状況レジスター・アドレス

Vec 割り込みベクトル

Self-Test Passed
自己テストが正常に行われた回数 (インターフェースがダウンからアップに変わった状態)

Self-Test Failed
自己テストが正常に行われなかった回数 (インターフェースがアップからダウンに変わった状態)

Maintenance Failed
保守障害の数

Log

log コマンドは、イベント・ログ・システムに含まれていないメッセージの現在のログ・レベルを表示したり、一時的に変更したりするのに使用します。このコマンドは一時的で、ルーターが再初期設定されると無効になります。

現在のログ・レベルを表示する場合、8 進数を含めずにコマンドを入力します。ログ・レベルを変更する場合は、新しいログ・レベルを表す 8 進数をコマンドの一部として入力します。デフォルトのログ・レベルは 76 (8 進数) です。

注: 初期ログ・レベル (つまり、ルーターが開始時に使用するレベル) を変更する場合は、CONFIG **set logging level** コマンドを使用します。 (このコマンドについての詳細は、43ページの『第5章 構成 (CONFIG) プロセスおよびコマンド (Talk 6)』を参照してください。)

構文:

log [*octal_#*]

Memory

memory コマンドは、現行の CPU メモリー使用量 (バイト)、バッファーの数、およびパケット・サイズを表示するのに使用します。

このコマンドを使用するためには、空きメモリーが利用可能であることが必要です。空きパケット・バッファー数がゼロまで低下し、一部の着信パケットが失われる結果を招くことがありますが、それによってルーターの動作に悪影響を与えることはありません。ルーターのアイドル時には、空きバッファー数は一定に保たれていなければなりません。一定に保たれていない場合は、サービス技術員に連絡してください。

構文:

memory

例:

```
memory
                 Total  Reserve    Never      Perm     Temp     Prev
                                   Alloc     Alloc    Alloc    Alloc

Heap memory    5463895   201824  5065383    328344   375856    22656
```

```
Number of global buffers:  Total = 294, Free = 287, Fair = 57, Low = 58
Global buff size:  Data = 4478, Header = 128, Wrap = 92, Trailer = 19
Total = 4700
```

Heap memory:
データ構造を動的に割り振るのに使用されたメモリーの量

Total メモリーの割り振りに使用できるスペースの合計量

Reserve
現在構成済みのプロトコルおよび機能が必要とするメモリーの最少量

Never Alloc
割り振られたことがないメモリー

Perm Alloc
ルーター・タスクによって永続的に要求されているメモリー

Temp Alloc
ルーター・タスクに一時的に割り振られるメモリー

Prev Alloc
一時的に割り振られ、返却されるメモリー

Number of global buffers: グローバル・バッファーの数

Total システム内のグローバル・バッファーの合計数

Free 使用可能なグローバル・バッファーの数

Fair 各インターフェースの妥当なバッファー数 (『Low』 の項を参照)

Low バッファーを保存するように割り振り方式が変更される基準となる空きバッファー数。 *Free* の値が *Low* を下回った場合、*Fair* 値を上回るバッファー数が入っている待ち行列には、バッファーは割り振られなくなります。

Global buff size:
グローバル・バッファー・サイズ

Data インターフェースの最大データ・リンク・パケット・サイズ

Header
最大ハードウェア、MAC、およびデータ・リンク・ヘッダー数の合計

Wrap プロトコル折り返しのために MAC、LLC、またはネットワーク・レイヤー・ヘッダーに認められる許容範囲

Trailer
最大 MAC およびハードウェア・トレーラー数の合計

Total 各パケット・バッファーの全体サイズ

Network

network コマンドは、サポートされるネットワーク (X.25 ネットワークなど) のコンソール環境に入るのに使用します。このコマンドを実行すると、指定したインターフェースのコンソール・プロンプトが表示されます。このプロンプトから、統計情報 (トークンリング・ネットワークのルーティング情報フィールドなど) を表示することができます。

構文:

network *interface#*

GWCON プロンプト (+) で **configuration** コマンドを入力すると、ルーターに構成されているプロトコルとネットワークを見ることができます。構成コマンドについての詳細は、137ページの『Configuration』 を参照してください。

ルーターが構成されているネットワークを表示するには、+ プロンプトで **interface** と入力します。

GWCON **network** コマンドと監視または変更するインターフェースの番号を入力します。たとえば、次のように入力します。

```
+network 3
X.25>
```

この例では X.25> プロンプトが表示されます。そこで X.25 動作コマンドを入力すれば、X.25 インターフェースに関する情報を表示することができます。

監視するインターフェースのインターフェース番号を識別した後、インターフェース特有の情報が必要な場合は、本書の中の指定のネットワークまたはリンク・レイヤー・インターフェースの監視の項を参照してください。以下のネットワークおよびリンク・レイヤー・インターフェースには、コンソール・サポートが提供されています。

- イーサネット
- フレーム・リレー
- PPP
- SDLC
- SDLC リレー (SRLY)
- トークンリング
- V.25bis
- X.25
- ATM
- ISDN
- V.34
- ダイヤルイン
- ダイヤルアウト
- マルチリンク PPP (MP)

Performance

性能に関する監視環境に入るには、Config> プロンプトで **performance** コマンドを使用します。詳細については、221ページの『第14章 性能の構成および監視』を参照してください。

Protocol

protocol コマンドは、ルーターに導入されているネットワーク・プロトコルを実現しているルーター・ソフトウェアと通信するのに使用します。プロトコルのコマンド環境にアクセスするには **protocol** コマンドを使用します。 このコマンドを入力すると、指定したプロトコルのプロンプトが表示されます。このプロトコルから、そのプロトコルに特有のコマンドを入力することができます。

構文:

protocol *prot#*

プロトコルの番号または短縮名を、コマンドの一部として入力します。プロトコルの番号または短縮名を入手するには、 CONFIG コマンド環境 (Config>) に入り、**list configuration** コマンドを入力します。 Config> にアクセスする方法については、16ページの『構成プロセスへのアクセス、CONFIG (Talk 6)』を参照してください。 GWCON に戻るには、**exit** と入力します。

特定のプロトコルのコンソール・コマンドについては、本書または *Protocol Configuration and Monitoring Reference* の該当する監視の項を参照してください。

Queue

queue コマンドは、指定したインターフェース上の入出力待ち行列の長さに関する統計を表示するのに使用します。 queue コマンドによって提供される入出力待ち行列に関する情報には、以下のものが含まれます。

- 割り振られたバッファーの合計数
- 最低水準バッファー値
- インターフェース上の現在アクティブのバッファーの数

構文:

queue *interface#*or *range_of_interface#*

複数のインターフェースに関する情報を表示するには、range_of_network# (または *interface#* と *range_of_interface#* の組み合わせ) を指定します。たとえば、**queue 0 3 25-50** と指定すると、ネット 0、3、および 25 〜 50 の情報が表示されます。

1 つのインターフェースだけの情報を表示する場合は、そのインターフェースまたはネットワークの番号を、コマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

例:

```
queue
                Input Queue       Output Queue
Nt Interface  Alloc Low Curr    Fair Curr
0  Eth/0         30  10   30      30    1
1  PPP/0         24   4   24       4    0
2  FR/0          24   4   24       5    0
```

Nt ソフトウェアに対応するネットワーク・インターフェース番号

Interface
インターフェースのタイプ

Input Queue:

Alloc この装置に割り振られたバッファーの数

Low この装置上のフロー制御に関する最低水準点

Curr この装置の現行のバッファー数。装置が使用不可にされている場合は、この値は 0 になります。

Output Queue:

Fair この装置上の出力待ち行列の長さに関する妥当なレベル

Curr この装置上で現在送信されるのを待っているパケットの数。ローカル発信パケットの場合、適格性廃棄は **memory** コマンドで説明されているグローバル最低水準点によって異なります。

ルーターは、少なくとも Low 値のパケット数を、インターフェースを介して受信できるように維持しようとします。パケットを受信し、その Curr 値が Low より小さい場合、そのパケットはフロー制御の対象になります。フロー制御の対象のバッファーがこの装置上で待ち行列化されることになった場合、Curr レベルが Fair より大きければ、そのバッファーは待ち行列化されずに廃棄されます。廃棄されたバッファーは、**error** コマンドの Output Discards 欄に表示されます。また、ELS イベント GW.036 または GW.057 も生成されます。

ルーターのスケジューリング・アルゴリズムが原因で、Curr (特に、Input Queue Curr) の動的な数が、パケット転送中の標準的な値を十分に表していないことがあります。コンソール・コードは、入力待ち行列が空になったときにのみ実行されます。したがって、Input Queue Curr が非ゼロになるのは、通常、パケットが低速の送信待ち行列上で待っているときだけということになります。

Reset

reset コマンドは、指定したインターフェースを使用不可にした後で、新しいインターフェース、プロトコル、および機能構成パラメーターを使用して、再びインターフェースを使用可能にするのに使用します。詳細については、52ページの『インターフェースのリセット』を参照してください。

構文:

reset *interface#*

Statistics

statistics コマンドは、ネットワーク・ソフトウェアに関する統計情報 (ルーター内のネットワークの構成など) を表示するのに使用します。

構文:

statistics *interface#*or *range_of_interface#*

複数のインターフェースに関する情報を表示するには、range_of_network# (または *interface#* と *range_of_interface#* の組み合わせ) を指定します。たとえば、**statistics 0 3 25-50** と指定すると、ネット 0、3、および 25 ～ 50 の情報が表示されます。

1 つのインターフェースだけの情報を表示する場合は、そのインターフェースまたはネットワークの番号を、コマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。

例:

```
statistics
                Unicast  Multicast      Bytes    Packets      Bytes
 Nt Interface  Pkts Rcv   Pkts Rcv   Received      Trans      Trans
 0  Eth/0           137          1       8832       1068      65297
 1  PPP/0             0          0          0          0          0
 2  PPP/1             0          0          0          0          0
```

Nt
ソフトウェアに対応するネットワーク・インターフェース番号

Interface
インターフェースのタイプ

Unicast Pkts Rcv
MAC レイヤーの非マルチキャスト、非ブロードキャストの、特別にアドレス指定されたパケットの数

Multicast Pkts Rcv
受信されたマルチキャストまたはブロードキャスト・パケットの数

Bytes Received
MAC レイヤーのこのインターフェースで受信されたバイト数

Packets Trans
送信されたユニキャスト、マルチキャスト、またはブロードキャスト・タイプのパケットの数

Bytes Trans
MAC レイヤーで送信されたバイト数

Test

test コマンドは、インターフェースの状態を検証するため、または以前に **disable** コマンドによって使用不可にされたインターフェースを使用可能にするために使用します。インターフェースが使用可能で、通信が行われている場合、**test** コマンドを使用すると、インターフェースはネットワークから除去され、インターフェース上で自己診断テストが実行されることになります。

構文:

test *interface#*

注: このコマンドが機能するためには、コマンドの**完全な** 名前に続けて、インターフェース番号を入力する必要があります。

インターフェースまたはネットワークの番号をコマンドの一部として入力します。インターフェース番号を入手するには、GWCON **configuration** コマンドを使用します。たとえば、テストが開始されると、コンソールに次のようなメッセージが表示されます。

```
Testing net 0 TKR/0...
```

テストが完了するか、失敗するか、あるいは GWCON がタイムアウトになると (30 秒後)、次のようなメッセージが表示される可能性があります。

```
Testing net 0 Eth/0 ...successful
Testing net 0 Eth/0 ...failed
Testing net 0 Eth/0 ...still testing
```

インターフェースによっては、テストが完了するまでに 30 秒以上かかる場合があります。

注: テストしているインターフェースが代替 WAN 再ルート・インターフェースとして構成されている場合、次のことを尋ねるプロンプトが出ます。

- 現在 WAN 再ルートの代替インターフェースが使用不可にされている場合、インターフェースの 1 次/代替の組みを使用可能にするかどうか。

  yes と応答した場合は、**t 5 enable alternate-circuit** WAN 復元コマンド (これについては、769ページの『第58章 WAN 復元の構成および監視』で説明しています) を入力した場合と同じ処置が取られます。

- インターフェースをテストしたいかどうか。

  通常、WAN 再ルート・インターフェースは、対応する 1 次インターフェースをバックアップする必要が生じるまで、使用不可にされています。 *yes* と応答すると、インターフェースの自己テストが開始します。 *no* と応答すると、自己テストは行われません。

詳細については、787ページの『第59章 WAN 再ルート機能』、 763ページの『第57章 WAN 復元の使用』、および 769ページの『第58章 WAN 復元の構成および監視』 を参照してください。

Uptime

uptime コマンドは、ルーターの時間に関する統計を表示するのに使用します。以下のものが表示されます。

- リスタートの回数
- 認知されたクラッシュの数
- 前回はルーターは再ロードされたのか、リスタートされたのか
- 前回の再ロードからの経過時間
- 前回のリスタートからの経過時間

構文:

uptime

第11章 メッセージ処理 (MONITR - Talk 2) プロセス

この章では、メッセージを収集および表示する方法について説明します。 (ELS およびメッセージのフォーマットについての詳細は、153ページの『第12章 イベント・ログ・システム (ELS) の使用』を参照してください。) 各メッセージの説明は、*IBM Nways イベント・ログ・システム メッセージの手引き*を参照してください。本章には、以下の節が含まれています。

- 『メッセージ処理 (MONITR) とは』
- 『メッセージ処理に影響を与えるコマンド』
- 『メッセージ処理 (MONITR) プロセスへの出入り』
- 152ページの『メッセージの受信』

メッセージ処理 (MONITR) とは

MONITR プロセスでは、ルーターおよびネットワークの内部の活動を表示して見ることができます。 MONITR は、ソフトウェアからのログに記録されたメッセージも表示します。

メッセージ処理に影響を与えるコマンド

以下のコマンドは、メッセージ処理プロセスに影響します。

- OPCON コマンド:
  - **divert** は、一時的に出力を別の装置に転送します。
  - **flush** は、ソフトウェアが収集したメッセージを廃棄させます。
  - **halt** は、divert コマンドの処置を取り消します。
  - **talk** は、メッセージ出力を表示します。
- CONFIG **set logging disposition** コマンドは、ソフトウェアがその出力を送信する最初の装置を設定します。

メッセージ処理 (MONITR) プロセスへの出入り

OPCON からメッセージ処理プロセスに入るには、**talk 2** コマンドを入力します。

ソフトウェアが収集したメッセージがコンソールに表示されます。

メッセージ処理を終了して OPCON に戻るには、OPCON インターセプト文字 (デフォルトは **Ctrl-P**) を入力します。

メッセージの受信

コンソールでメッセージを受信するには、前の節で説明したようにして、メッセージ処理プロセスに入ります。ソフトウェアは、前回に呼び出された以降に記録したすべてのメッセージを表示します。メッセージ処理プロセスに接続されている間、到着するすべてのメッセージが表示されます。

OPCON **divert** および **halt** コマンドを使用すれば、ルーターで何か別のことを行いながら、software メッセージを見ることができます。許可された装置は、出力を TTY0 (ローカル・コンソール)、TTY1、または TTY2 (リモート・コンソール) に着信転送します。

MONITR のデフォルト装置を指定するには、CONFIG **set logging disposition** コマンドを使用して、静的 RAM に装置を定義します。印刷用にセットアップされた端末がある場合は、デフォルト装置を指定しておくと便利です。

第12章 イベント・ログ・システム (ELS) の使用

この章では、イベント・ログ・システム (ELS) とその構成について説明します。 ELS は、すべてのイベントを継続的にログに記録し、それらをユーザーが選択したパラメーターに従ってフィルター処理します。動作カウンターと ELS の組み合わせにより、システムの正常な動作と活動を監視するのに必要な情報が提供されます。この章は、以下の節に分けて説明します。

- 『ELS とは』
- 154ページの『ELS 構成環境への出入り』
- 154ページの『イベント・ログの概念』
- 173ページの『ELS 構成コマンド』

ELS とは

ELS は監視システムで、ルーター・オペレーティング・システムの一部です。 ELS では、ルーター活動の結果としてログに記録されたメッセージを管理します。 ELS コマンドを使用すれば、ユーザーにとって重要なメッセージだけをえり分けるように構成を設定できます。そのメッセージは、コンソール端末画面に表示したり、リモート・ワークステーションのログに記録したり、あるいはシンプル・ネットワーク・マネージメント・プロトコル (SNMP) トラップを使用してネットワーク管理ステーションに送信したりすることができます。

ELS システムと動作カウンターは、ルーターに生じた問題を分離するための最良のトラブルシューティング・ツールです。イベント・メッセージにざっと目を通せば、ルーターに問題が生じているかどうかを知り、問題の解明をどこから始めればよいかというような基本的なことが分かります。

ELS 構成環境では、コマンドを使用してデフォルト構成を設定します。このデフォルト構成は、ルーターが初期化されるまでは有効になりません。

ときには、ELS 構成環境で設定したもの以外のメッセージを一時的に表示して見ることが必要になりますが、その場合はルーターを再初期化する必要はありません。 ELS 動作および監視環境は、以下の目的で使用します。

- デフォルトの ELS 表示設定値を一時的に変更する。
  - ELS コンソール環境で行った変更は、即時に有効になります。
  - コンソール・コマンドを使用して行った変更は、不揮発性構成記憶域には保管されません。
- ELS による動的 RAM の使用に関する統計情報を表示する。

注: 特定の ELS メッセージについては、 *IBM Nways イベント・ログ・システム・メッセージの手引き* で説明しています。

ELS は、OPCON プロセスからアクセスするサブプロセスです。

ELS 構成環境への出入り

ELS 構成環境 (CONFIG プロセスからアクセス可能) は、ELS Config> プロンプトによって示されます。このプロンプトで入力されたコマンドは、ELS のデフォルト状態を作成します。これはルーターのリスタート後に有効になります。これらのコマンドについては、この章の後半で詳しく説明します。

サブシステム、グループ、またはイベントをパラメーターとする構成コマンドは、次の順序で実行されます。

- サブシステム
- グループ
- イベント

基本 ELS 構成を設定するには、ELS Config> プロンプトで **display subsystem all standard** コマンドを入力します。このコマンドは、STANDARD ログ・レベル (つまり、すべての誤りと異常通知コメント) を持つすべてのサブシステムからのメッセージを表示するように、ELS を構成します。

注: ルーターには、デフォルトの ELS 構成はありません。ユーザーが ELS 構成環境に入り、デフォルト状態を設定する必要があります。

OPCON から ELS 構成環境に入るには、次のようにします。

1. **talk 6** コマンドを入力する。コンソールに CONFIG プロンプト (Config>) が表示されます。最初に CONFIG に入ったときにこのプロンプトが表示されない場合は、**Return** を押してください。
2. CONFIG プロンプトで、次のコマンドを入力して ELS にアクセスする。

   ```
   Config> eve
   ```

   コンソールに ELS 構成プロンプト (ELS config>) が表示されます。これで、ELS 構成コマンドを入力できます。

ELS 構成環境を終了するには、**exit** コマンドを入力します。

イベント・ログの概念

この節では、イベントをログに記録する方法およびメッセージの解釈方法について説明します。また、サブシステム、イベント番号、およびログ・レベルの概念についても説明します。大部分の ELS 機能は、サブシステム、イベント番号、およびログ・レベルをパラメーターとして取るコマンドが基本になっています。

イベントの原因

イベントは、ルーターが動作している間、連続的に発生します。以下の理由のいずれも、その原因になります。

- システム活動
- 状態の変更
- サービス要求

- データの送受信
- データ誤りおよび内部誤り

イベントが発生すると、ELS はその発生源とイベントの性質を識別するデータを、システムから受け取ります。 ELS は、受信したデータをその一部として使用してメッセージを生成します。

メッセージの解釈

この節では、ELS によって生成されるメッセージの解釈方法について説明します。 図4 に、メッセージの内容を示します。

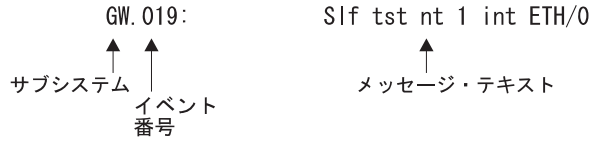


図4. イベントによって生成されるメッセージ

図4 に示されている情報、および **list subsystem** コマンドによって表示される ELS ログ・レベル情報について、以下で説明します。

サブシステム

サブシステム とは、ルーターのコンポーネント (プロトコルやインターフェースなど) を表す、事前定義された短縮名です。 図4 では、**GW** がこのイベントを発生したサブシステムを識別しています。

その他のサブシステムの例としては、IP、TKR、および X25 があります。特定のルーター上に実際に存在するサブシステムは、そのルーターに構成されているハードウェアおよびソフトウェアによって異なります。この章で後述する **list subsystem** コマンドを使用すれば、ルーター上のサブシステムのリストを表示して見ることができます。

ELS コマンドの影響がサブシステム全体に及ぶようにしたい場合は、そのサブシステムをコマンドのパラメーターとして入力します。たとえば、ELS コマンド **display subsystem GW** は、GW サブシステム全体で発生するすべてのイベント ('debug' ログ・レベルのイベントを除く) を表示します。

イベント番号

イベント番号 は、サブシステム内の各メッセージに割り当てられる、事前定義された固有の任意の番号です。 図4 では、**19** が GW サブシステム内のイベント番号です。**list subsystem** コマンドを使用すれば、サブシステム内のすべてのイベントのリストを表示することができます (ただし、*subsystem* はそのサブシステムの短縮名)。

イベント番号は、常にサブシステムと共に表示され、サブシステムとの間をピリオドで区切られています。たとえば、**GW.019** のように表示されます。サブシステムとイベント番号の組み合わせで、*個々の* イベントを識別します。これらは、ELS コマ

ンドのパラメーターとして入力されます。コマンドの影響が指定のイベントだけに及ぶようにしたい場合は、サブシステムとイベント番号をその ELS コマンドのパラメーターとして入力します。

ログ・レベル

ログ・レベル は、各メッセージをその生成の原因となったイベントのタイプによって分類する、事前定義された設定値です。この設定値は、**list subsystem** ELS コンソール・コマンドを使用すると表示されます。 表18 は、ログ・レベルとタイプをリストしています。

表 18. ログ・レベル

ログ・レベル	タイプ
UI ERROR	異常な内部誤り
CI ERROR	一般的な内部誤り
UE ERROR	異常な外部誤り
CE ERROR	一般的な外部誤り
ERROR	上記のすべての誤りレベルが含まれる
UINFO	異常な通知コメント
CINFO	一般的な通知コメント
INFO	上記のすべてのコメント・レベルが含まれる
STANDARD	すべての誤りレベルとすべての通知コメント・レベルが含まれる (デフォルト)
PTRACE	パケット単位のトレース
UTRACE	異常な動作トレース・メッセージ
CTRACE	一般的な動作トレース・メッセージ
TRACE	上記のすべてのトレース・レベルが含まれる
DEBUG	デバッグ用のメッセージ
ALL	すべてのログ・レベルが含まれる

表18 で、ERROR、INFO、TRACE、STANDARD、および ALL は、他のログ・レベル・タイプを集合したものです。 STANDARD が推奨されるデフォルト値です。

ログ・レベルの設定値は、以下のコマンドの動作に影響を与えます。

- **Display subsystem**
- **Nodisplay subsystem**
- **Trap subsystem**
- **Notrap subsystem**
- **Remote subsystem**
- **Noremote subsystem**

ログ・レベルは、上記のコマンドの 1 つのパラメーターとして指定すると、その特定コマンドに対して設定されます。たとえば、次のように入力します。

```
display subsystem TKR ERROR
```

このログ・レベルをコマンド行に含めると、**display** コマンドが変更されて、UI-ERROR または CI-ERROR のログ・レベルをもつイベントがサブシステム TKR で発生するたびに、その結果のメッセージがコンソールに表示されるようになります。

グループまたはイベントに影響を与える動作に対してログ・レベルを指定することはできません。

メッセージ・テキスト

メッセージ・テキスト は短縮形で表示されます。 155ページの図4 で、`Slf tst nt 1 int ETH/0` は、このイベントによって生成されたメッセージです。変数 (*source_address* や *network* など) は、メッセージがコンソールに表示されるときに実際のデータで置き換えられます。

一部のイベント・ログ・システム・メッセージ記述では、変数 *error_code* が参照されます (通常は、その前に rsn (reason 理由) が付いています)。これらは、検出されたパケット誤りのタイプを示しています。 表19 は、誤り符号、つまりパケット完了符号を記述しています。パケット完了符号は、ルーターに到着したパケットの後処理を示します。

表 19. パケット完了符号 (誤り符号)

符号	意味
0	パケットは出力のために正常に待ち行列に入れられました。
1	ランダムの未識別の誤り
2	パケットは、フロー制御が理由で、出力のために待ち行列に入れられませんでした。
3	パケットは、ネットワークのダウンにより、待ち行列に入れられませんでした。
4	パケットは、ループまたは不正なブロードキャストを避けるため、待ち行列に入れられませんでした。
5	パケットは、宛先ホストのダウンのため (これを検出できるネットワーク上のみ)、待ち行列に入れられませんでした。

ELS はネットワーク情報を、次のように表示します。

`nt 1 int Eth/0` (または) `network 1, interface Eth/0,`

ただし、

- 1 はネットワーク番号 (ルーター上の各ネットワークには、ゼロから順に番号が付けられています)
- 0 は、装置番号 (各ハードウェア・タイプのインターフェースには、ゼロから順に番号が付けられています)

イーサネットおよび 802.5 ハードウェア・アドレスは、長い 16 進数として表示されます。

IP (インターネット・プロトコル) アドレスは、ピリオドで区切られた 4 つの 10 進バイト (たとえば、18.123.0.16) として表示されます。

グループ

グループ は、名前が付けられた (グループ名) ユーザー定義のイベントの集合です。サブシステム、サブシステムとイベント番号、およびログ・レベルと同様に、グループ名も ELS コマンドのパラメーターとして使用することができます。ただし、事

前定義されたグループ名はありません。グループを作成してからでないと、その名前をコマンド行で指定することができません。

グループを作成するには、この章で説明する **add** 構成コマンドを使用し、グループの呼び名を指定し、次にそのグループに含めるイベントを指定します。グループに追加するイベントは、サブシステムおよびログ・レベルが異なっていても構いません。

グループを作成した後は、そのグループ名を使用して、グループ内のイベント全体をまとめて操作することができます。たとえば、grouptwo という名前のグループに追加されたイベントからのすべてのメッセージの表示をオフにするには、次のように、コマンド行にグループ名を含めます。

```
nodisplay group grouptwo
```

グループを削除するときは、**delete** コマンドを使用します。

ELS の使用

ELS を効果的に使用するために、以下のステップを実行することを推奨します。

- ELS システムを使用する前に、何が見たいかをはっきり知っておく。 MONITR プロセスを使用する前に、表示して見たい問題またはイベントを明確に定義しておきます。
- コマンド **nodisplay subsystem all all** を実行して、すべての ELS メッセージをオフにする。
- 直面している問題に関連したメッセージだけをオンにする。
- *IBM Nways イベント・ログ・システム メッセージの手引き* を使用して、表示されているどのメッセージが正常かを判別する。

MONITR プロセスから初めて ELS を表示したときは、かなりの量の情報が表示されます。中度から重度の負荷時には、ルーターはすべてのパケットをバッファーして表示することはできないので、バッファーはフラッシュされます。この状態が起こると、次のようなメッセージが表示されます。

```
xx messages flushed
```

ルーターは、これらのメッセージを保管しません。このメッセージが表示されたときは、監視している現行タスクにとって重要な情報だけを表示するように、ELS 出力を調整することができます。

ELS メッセージの回転の管理

ELS メッセージはルーターのバッファーを連続して回転していることに注意することも大切です。 ELS メッセージの表示の停止およびリスタートには、以下のキーの組み合わせを使用します。

Ctrl-S スクロールを一時停止する場合

Ctrl-Q スクロールを再開する場合

Ctrl-P 直前のプロセスに戻る場合

ELS 出力をファイルに取り込むこともできます。これは、ルーターに Telnet 接続しているときに、自分の場所からスクリプト・ファイルまたはログ・ファイルを開始して行うことができます。あるいは、PC をルーターのコンソール・ポートに接続し、端末エミュレーション・パッケージ内からログ・ファイルを開始して行うこともできます。この情報は、カストマー・サービスによる問題の診断に役立てるために必要です。

UNIX ホスト上の Telnet 接続を使用した ELS 出力の取り込み

AIX または UNIX ホスト上の Telnet 接続を使用して、画面上の ELS メッセージをホスト上のファイルに取り込むことができます。始める前に、173ページの『第13章 イベント・ログ・システム (ELS) の構成および監視』 の ELS コンソール・コマンドを使用して、取り込みたいメッセージ用に ELS を設定します。

AIX または UNIX ホスト上のファイルに ELS 出力を取り込む場合は、以下のステップに従います。

1. ホストから **telnet** *router_ip_addr* **| tee** *local_file_name* と入力する。

   router_ip_addr は、ルーターの IP アドレスです。

   local_file_name は、ELS メッセージを保管したいホスト上のファイルの名前です。

   tee コマンドは、ELS メッセージを画面に表示し、同時に、それをローカル・ファイルにコピーします。

2. OPCON プロンプト (*****) から **t 2** と入力する。これにより MONITR プロセスにアクセスしますが、これが ELS メッセージを画面に表示するプロセスです。構成した ELS メッセージに応じて、画面に ELS メッセージが表示されるはずです。

   MONITR プロセスにある限り、すべての ELS メッセージがローカル・ファイルに書き込まれます。 MONITR プロセスを終了する (**Ctrl-P** を入力して) か、Telnet セッションを終了すると、ローカル・ファイルへのメッセージのログは停止します。

UNIX ホスト上で ELS 出力を取り込む代わりに、リモート・ログ記録を使用することもできます。リモート・ログ記録についての詳細は、162ページの『ELS リモート・ログ記録の使用および構成』を参照してください。

イベント・メッセージを SNMP トラップで送信できるように ELS を構成

イベント・メッセージが SNMP エンタープライズ特定トラップでネットワーク管理ワークステーションに送信できるように、ELS を構成することができます。これらのトラップは、状態や診断結果を報告するのに便利で、2210 のリモート監視にしばしば使用されます。 ELS が適正に構成されていると、選択されたイベントが発生するたびに、SNMP トラップが生成されます。 SNMP の詳細については、*プロトコルの構成と監視 解説書* を参照してください。

特定のイベントを SNMP トラップとして送信するために起動する必要があることを ELS に通知するには、`ELS config>` プロンプトまたは `ELS>` プロンプトで、たとえば IP を使用して、次のように入力します。

```
trap event ip.007
```

ELS の使用

注: ELS config> プロンプトを使用する場合は、リブートする必要があります。

ELS エンタープライズ特定トラップを使用可能にするには、以下のステップに従います。

1. SNMP config> プロンプトで、たとえば **public** を使用して、次のように入力する。

   ```
   SNMP config> add address public <network manager IP address>
   SNMP config> enable trap enterprise public
   SNMP config> set community access read_trap public
   ```

   注: これらの変更をアクティブするためには、リブートする必要があります。
2. ネットワーク管理ステーションがエンタープライズ特定トラップを受信し、正しく表示できるようにする。

上記のステップに従って、グループ、サブシステム、およびイベントをトラップすることができます。

ELS を使用してのトラブルシューティング

イベントは、ルーターが動作している間、連続的に発生します。以下の理由のいずれも、その原因になります。

- システム活動
- 状態の変更
- サービス要求
- データの送受信
- データ誤りおよび内部誤り

イベントが発生すると、ELS はその発生源とイベントの性質を識別するデータを、システムから受け取ります。 ELS は、受信したデータをその一部として使用してメッセージを生成します。

特定の問題のトラブルシューティングを行うときは、その問題に関連するメッセージを表示します。たとえば、ブリッジングの問題が起きているときは、ブリッジング・メッセージを表示します。

display subsystem srt all

display subsystem br all

画面上のメッセージのスクロールする速度が速いので、当初は、表示された番号をメモしておき、後でそれを資料で調べても構いません。特定プロトコルについて表示される種々のタイプのメッセージに慣れてきたら、トラブルシューティングに必要な情報が含まれているメッセージだけをオン、オフにすることができるようになります。以下に、特定の ELS の例を示します。問題の種類によって必要なステップが異なることに注意してください。

ELS 例 1

トークンリング・インターフェース上のポーリングの頻度を調べ、ポーリングが正常に行われているかどうかを知りたい場合

```
ELS> nodisplay subsystem all all
ELS> display subsystem tkr all
Ctrl-P
* t 2
```

メッセージがスクロールし始めたら、ELS メッセージ tkr.031 を探します。

ELS 例 2

SRB ブリッジングが動作していない場合

1. 構成をチェックする。
2. GWCON ブリッジング・コンソールを使用して、ブリッジング・インターフェースが使用可能になっているかどうかを検査する。
3. 次のように入力する。

   ```
   * t 6
   config> event
   ELS config> nodisplay subsystem all all
   ELS config> display subsystem srb all
   ELS config> exit
   config> Ctrl-P
   ```
4. ルーティング・サブシステムをリスタートする。サブシステムがリスタートしたら、次のように入力する。

   ```
   * t 2
   ```

ELS 例 3

ルーターがイーサネット上の IPX と通信できない場合

1. **talk** コマンドと GWCON の PID を入力する。

   ```
   * talk 5
   ```

   コンソールに GWCON プロンプト (+) が表示されます。最初に GWCON に入ったときにこのプロンプトが表示されない場合は、**Return** を押してください。
2. GWCON プロンプト (+) で **IPX** と入力し、IPX コンソール・プロンプト (IPX>) にアクセスする。
3. IPX コンソール・プロンプトで **slist** コマンドを入力して、そのサーバーがリストされているかどうかを検査する。 (slist コマンドについては、*プロトコルの構成と監視 解説書* の IPX の監視に関する項を参照してください。)
4. IPX 構成をチェックする。
5. 次のように入力する。

   ```
   * t 5
   + event
   ELS> nodisplay subsystem all all
   ELS> display subsystem IPX all
   ELS> display subsystem eth all
   ```

```
ELS> Ctrl-P
* t 2
```

メッセージがスクロールし始めたら、ELS メッセージ eth.001 を探します。これは、サーバーのイーサネット・タイプ・フィールドが正しくないことを示します。

ELS リモート・ログ記録の使用および構成

リモート・ログに記録された ELS メッセージには、モニター待ち行列内の ELS メッセージ (talk 2 で表示) の他に、図5 に示すような追加情報が含まれています。

```
Date/Time         IP address      Sequence Number      Local Name      ELS Subsystem Name, &
                  assigned        used for detecting   assigned        Formatted message
                  by the user     missing messages     by the user

Nov 20 12:13:47   5.1.1.1         Msg [0444] from      ** IBM/2210 **  :els: ARP.011 Del ent ...
```

図5. Syslog メッセージ記述

リモート・ログ表示には、以下のような相違点があります。

- 時刻として、時間に加えて月と日が常に表示されます。
- IP アドレスは、ユーザー指定の発信元 IP アドレスです。 DNS サーバーが発信元 IP アドレスをホスト名に変換した場合、そのホスト名が IP アドレスの代わりに表示されます。
- 発信元の装置によってシーケンス番号がメッセージに付加されるので、廃棄されたメッセージを検出するのに役立ちます。廃棄メッセージについての説明は、166 ページの『リモート・ログ記録の出力』を参照してください。メッセージのシーケンス番号が 9999 に達すると、その次のシーケンス番号は 0001 になります。
- 発信元ルーターの 『ローカル名』 は、複数のソースからのメッセージを区別するのに役立ちます。ローカル名を構成しなかった場合、このフィールドはブランクになります。

Syslog ファシリティーとレベル

リモート・ログ ELS メッセージは、UDP パケットに入れてネットワーク上で転送されます。UDP ヘッダー内の宛先ポート番号は、常に 514 (syslog ポート) です。 UDP パケットを受信して処理するためには、ELS メッセージを受信してログに記録するリモート・ワークステーションで *syslog* デーモン (syslogd) が実行されていることが必要です。詳細については、163ページの『リモート・ワークステーションの構成』を参照してください。

リモート・ログ ELS メッセージには表示されませんが、UDP パケットに入れてネットワーク上で送信される各 ELS メッセージには、*syslog_facility* と *syslog_level* を割り当てる必要があります。 syslog デーモンは、ファシリティーとレベルの組み合わせを使用して、メッセージの送信先を判別します。通常は、ELS メッセージはリモート・ホストの 1 つまたは複数のファイルに書き込まれます。その他のオプションとし

ては、メッセージをコンソールに表示する、メッセージを 1 人または複数のユーザーに送信する、あるいはメッセージを別のワークステーションに送信するといったことが可能です。

syslog_facility と *syslog_level* の値を指定するのに使用するコマンド、およびその他のリモート・ログ関連のコンソール・コマンドについては、194ページの『ELS 監視コマンド』 および 173ページの『ELS 構成コマンド』で説明しています。次の節に進む前に、これらのコマンドについて理解しておいてください。

リモート・ワークステーションの構成

以下に示す構成では、単一の 2210 が単一のリモート・ワークステーションにリモート・ログ記録するものと想定しています。複数の 2210 が同一のリモート・ワークステーションにリモート・ログ記録するように構成することも可能です。ただし、ある特定の 2210 は 1 つだけのリモート・ワークステーションのログにしか記録できません。この例で使用しているオペレーティング・システムは AIX 4.2 です。ユーザーの環境とは、いくぶん異なっている可能性があります。 syslog についての詳細は、ご使用のオペレーティング・システムの資料を参照してください。

AIX ワークステーションで構成を実行するためには、**ルート** としてログインする必要があります。ワークステーションの構成は、以下の手順で行います。

1. syslog.conf ファイルを作成または編集して、特定の*syslog_facility* 値と *syslog_level* 値をもつ ELS メッセージを書き込む場所を指定する。メッセージの宛先を指定する方法の例は、164ページの図6 の最下部を見てください。ログ・ファイルは、完全なパス名を指定する必要があることに注意してください。 syslog 構成ファイルのデフォルトの場所は、/etc/syslog.conf です。
2. syslog.conf ファイルに指定した syslog メッセージをログ記録するためのファイルを作成する。
3. **syslogd** と入力して、syslog デーモンを開始する。 SRC (システム・リソース・コントローラー) から syslog デーモンを開始するときは、**startsrc -s syslogd** と入力します。構成ファイルのパス名が /etc/syslog.conf ではないときは、**syslogd -f** *pathname* を入力します。デバッグ・モードで syslog デーモンを開始するときは、**syslogd -d** と入力します。

   注: syslog デーモンの複数インスタンスを実行することは、サポートされません。
4. syslog.conf ファイルを作成または変更したときに、すでに syslog デーモンが実行されていた場合は、デーモンをリスタートして、syslog.conf. からデーモンを再初期化する必要があります。
5. 次のように **logger** コマンドを使用して、設定を確認する。

   ```
   logger -p user.alert  THIS IS A TEST MESSAGE (user.alert)
   logger -p news.info  THIS IS A TEST MESSAGE (news.info)
   ```

   設定が正しければ、syslog.conf で指定したファイルに `THIS IS A TEST MESSAGE...` が書き込まれます。

```
# @(#)34       1.9 src/bos/etc/syslog/syslog.conf, cmdnet, bos411, 9428A410j 6/13/93 14:52:39
#
# COMPONENT_NAME: (CMDNET) Network commands.
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1988, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# /etc/syslog.conf - control output of syslogd
#
# Each line must consist of two parts:-
#
# 1) A selector to determine the message priorities to which the
#    line applies
# 2) An action.
#
# The two fields must be separated by one or more tabs or spaces.
#
# format:
#
# <msg_src_list>               <destination>
#
# where <msg_src_list> is a semicolon separated list of <facility>.<priority>
# where:
#
# <facility> is:
#      * - all (except mark)
#      kern,user,mail,daemon, auth, syslog, lpr, news, uucp, cron, authpriv, local0 - local7
#
# <priority or level> is one of (from high to low):
#      emerg,alert,crit,err(or),warn(ing),notice,info,debug
#      (meaning all messages of this priority or higher)
#
# <destination> is:
#      /filename - log to this file
#      username[,username2...] - write to user(s)
#      @hostname - send to syslogd on this machine
#      * - send to all logged in users
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
#  mail.debug          /usr/spool/mqueue/syslog
#  *.debug             /dev/console
#  *.crit                      *

#   syslog messages with facilty / priority values of LOG_USER,   LOG_ALERT
user.alert            /tmp/syslog_user_alert

#   syslog messages with facilty / priority values of LOG_NEWS,  LOG_INFO
news.info           /tmp/syslog_news_info
```

図 6. syslog.conf 構成ファイル

リモート・ログ記録用の 2210 の構成

2210 の構成は、以下の手順で行います。

1. talk 6 で、165ページの図7 に示すように、リモート・ログ・ファシリティーを構成する。 *source-ip-addr* として指定する IP アドレスは、リモート・ログ ELS メッセージに表示された IP アドレスまたはホスト名を識別しやすくするために、2210 に構成された IP アドレスを使用することが必要です。また、この IP アドレスは、ネーム・サーバーが速やかにホスト名に変換できること、あるいは少な

くともネーム・サーバーが速やかに 『address not found』を応答できるものであることを確認する必要があります。これを調べるには、ワークステーション上で次のような **host** コマンドを出します。

```
workstation>
host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

応答に 1 秒以上かかる場合は、もっと迅速に解決できる IP アドレスを選択してください。

2. talk 6 で、166ページの図8 に示すように、リモート・ログ記録用のイベントおよびサブシステムを構成する。
3. 2210 をリスタートする。

```
ELS config>set remote source-ip-addr 5.1.1.1
Source IP Addr = 5.1.1.1

ELS config>set remote remote-ip-addr 192.9.200.1
Remote Log IP Addr = 192.9.200.1

ELS config>set remote local-id ** IBM/2210 **
Remote Log Local ID = ** IBM/2210 **

ELS config>set remote no-msgs-in-buffer 100
Number of messages in Remote Log Buffer must be 100-512
Number of Messages in Remote Buffer = 100

ELS config><B>set remote facility log_news
Default Syslog Facility = LOG_NEWS

ELS config>set remote level log_info
Default Syslog Level = LOG_INFO

ELS config>set remote on
Remote Logging is ON

ELS config>list remote

------------------   Remote Log Status  -----------------

Remote Logging is ON
Source IP Address = 5.1.1.1
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_NEWS
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log = 100
Remote Logging Local ID = ** IBM / 2210 **
ELS config>
```

図 7. リモート・ログ記録用の 2210 の構成

```
ELS config>display sub snmp all
ELS config>remote sub snmp all log_news log_info

ELS config>display event srt.017
ELS config>remote event srt.017 log_news log_info

ELS config>display event stp.016
ELS config>remote event stp.016 log_user log_info

ELS config>display event stp.026
ELS config>remote event stp.026 log_news log_info

ELS config>display event stp.024
ELS config>remote event stp.024 log_news log_info

ELS config>display event ip.068
ELS config>remote event ip.068 log_news log_info

ELS config>display event ip.058
ELS config>remote event ip.058 log_news log_info

ELS config>display event ip.022
ELS config>remote event ip.022 log_news log_info

ELS config>display event gw.022
ELS config>remote event gw.22 log_news log_info

ELS config>display event arp.011
ELS config>remote event arp.011 log_user log_alert

ELS config>display event arp.002
ELS config>remote event arp.022 log_user log_alert

ELS config>list status
Subsystem:    SNMP
Disp levels:  ERROR INFO TRACE
Trap levels:  none
Trace levels: none
Remote levels:  ERROR INFO TRACE
        Syslog Facility/Level: LOG_NEWS LOG_INFO

Event     Display Trap    Trace     Remote
SRT.017   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.016   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.026   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.024   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.068    On      Unset   Unset
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.058    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.022    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
GW.022    On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
ARP.011   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_USER LOG_ALERT
ARP.002   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_USER LOG_ALERT
```

図 8. リモート・ログ記録用のサブシステムおよびイベントの構成

リモート・ログ記録の出力

167ページの図9 は、/tmp/syslog_news_info ファイルからの出力の例を示しています。最初のメッセージはシーケンス番号 310 であることに注意してください。これは、最初の 309 ELS メッセージは、発信元の 2210 から送られなかったことを意味しています。これには、いくつかの理由があります。

- メッセージが最初に ELS に渡されたときに、リモート・ログ・ファシリティーの初期化が完了していなかった。
- 発信元 2210 からリモート・ワークステーションへのルートが、ルーティング・テーブルになかった。
- ELS メッセージが入っている発信 UDP パケット用のインターフェースが 『Up』 状態でなかった。

1 では、メッセージ 311-313 がリモート・ログに記録されなかったことに注意してください。これは、ARP 要求がアウトスタンディングであったためであり、ARP レスポンスを受信するまでは、最初のパケットを除く発信元 2210 内のすべてのパケットが廃棄されます。また、ARP キャッシュは、ユーザーが構成したリフレッシュ速度で消去され、新規の ARP 要求が出されます。この状態が起きているかどうかを調べるために、対象となる ELS イベントに加えて、イベント ARP.002 と ARP.011 もリモート・ログに記録してみることができます。 169ページの図11 は、*syslog_user_alert* ファイルに記録された ARP イベントを示しています。ここにはイベント 445 と 446 が記録されており、これらは 図9 には脱落として示されています。

```
Nov 20 12:03:16 workstа01 root:  THIS IS A TEST MESSAGE  (news.info)
Nov 20 12:08:48 5.1.1.1 Msg [0310] from ** IBM / 2210 **: els:  IP.022: add nt 192.9.200.0 int 192.9.200.20
nt 0 int Eth/0

1 ( messages 311, 312, and 313 did not get remote-logged due to ARP request outstanding - see
  explanation in the text)

2 (messages 314 and 315 were logged to a separate
file - see explanation in the text)

Nov 20 12:08:48 5.1.1.1 Msg [0316] from ** IBM / 2210 **: els:  IP.068: routing cache cleared
Nov 20 12:08:48 5.1.1.1 Msg [0317] from ** IBM / 2210 **: els:  IP.022: add nt 5.0.0.0 int 5.1.1.1 nt 5 int Eth/4
Nov 20 12:08:48 5.1.1.1 Msg [0318] from ** IBM / 2210 **: els: SRT.017: Enabling SRT on port 5 nt 5 int Eth/4


(message 319 was logged to a separate file)

Nov 20 12:08:48 5.1.1.1 Msg [0320] from ** IBM / 2210 **: els:  IP.068: routing cache cleared

(120 messages not shown)

Nov 20 12:13:33 5.1.1.1 Msg [0441] from ** IBM / 2210 **: els:  GW.022: Nt fld slf tst nt 3 int Eth/3
Nov 20 12:13:33 5.1.1.1 Msg [0442] from ** IBM / 2210 **: els:  GW.022: Nt fld slf tst nt 6 int Eth/5
Nov 20 12:13:38 5.1.1.1 Msg [0443] from ** IBM / 2210 **: els:  GW.022: Nt fld slf tst nt 11 int ISDN/0


(messages 444 and 447 were logged to a separate file)


(messages 445 and 446 did not get remote-logged due to ARP request outstanding)

Nov 20 12:13:50 5.1.1.1 Msg [0448] from ** IBM / 2210 **: els:  GW.022: Nt fld slf tst nt 4 int ATM/0
Nov 20 12:13:50 5.1.1.1 Msg [0449] from ** IBM / 2210 **: els:  IP.068: routing cache cleared
Nov 20 12:13:50 5.1.1.1 Msg [0450] from ** IBM / 2210 **: els:  IP.058: del nt 4.0.0.0 rt via 0.0.0.4 nt 4 int ATM/0
```

図 9. Syslog News Info ファイルの内容の例

ブート中およびブート直後に生成される初期 ELS メッセージに特に関心がある場合は、これらのメッセージもモニター待ち行列に表示することをお勧めします。これは talk 2 で表示されます。 168ページの図10 は、リモート・ログに記録されなかった初期メッセージが含まれている talk 2 出力を示しています。 talk 2 出力には、リモート・ログ・ファシリティーが使用可能であることを示すメッセージがあることに注意してください。これは、リモート・ワークステーションへのルートが存在することを示しているのでもなく、関連のインターフェースが 『Up』 状態にあることを示しているのでもありません。これは単に、それ以前はメッセージを正常にリモート・ログに記録できないことを示す参照点として示されています。

また、talk 2 出力には、脱落していたメッセージ (167ページの図9 に **2** で示されている) も記録されていることに注意してください。

```
12:08:17 SNMP.024: generic trc (P2) at snmp_mg.c(766): Now 0 trap destinations
12:08:17 SNMP.012: comm public added
12:08:17 SNMP.012: comm public added
12:08:17 SNMP.024: generic trc (P2) at lesConf.cpp(1491): Set  DEFAULT_ATMDEVNUM
= 4, DEFAULT_ATM_LINE_SPEED = 155
12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_router_if_info(): sr
rdrec failed

12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_router_if_info(): sr
rdrec failed

12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:27 DOLOG: Found an ISDN interface record for ifn=0
12:08:27 DOLOG: ***************In config_mem_init
12:08:27  DOLOG: .....Remote Logging Facility is now available.....
12:08:28   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:28   IP.022: add nt 4.0.0.0 int 4.1.1.1 nt 4 int ATM/0



     ( 297 messages not shown )                                          Corresponding Sequence
                                                                         Numbers in
12:08:43   GW.022: Nt fld slf tst nt 12 int PPP/2                        Remote-Logging Files :
12:08:43   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:48   IP.022: add nt 192.9.200.0 int 192.9.200.20 nt 0 int Eth/0    [0310] first message logged
12:08:48  SRT.017: Enabling SRT on port 1 nt 0 int Eth/0                 -- not logged (ARP request) --
12:08:48  STP.016: Select as root TB-1, det topol chg                    -- not logged (ARP request)--
12:08:48  STP.026: Root TB-1, strt hello tmr                             -- not logged (ARP request)--
12:08:48  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0                         [0314]
12:08:48  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                         [0315]
12:08:48   IP.068: routing cache cleared                                 [0316]


     ( 126 messages not shown )

12:13:38   GW.022: Nt fld slf tst nt 11 int ISDN/0                       [0443]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                            [0444]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                            -- not logged (ARP request) --
12:13:47  ARP.002: Pkt in 1 1 800 nt 5 int Eth/4                         -- not logged (ARP request)--
12:13:47  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                         [0447]
12:13:50   GW.022: Nt fld slf tst nt 4 int ATM/0                         [0448]
```

図 10. Talk 2 からの出力

タイム・スタンプを使用して (これは、リモート・ログ出力ファイルと talk 2 出力の両方に表示されます)、最初の ELS メッセージが正常にリモート・ログに記録された時刻を調べることができます。この目的のためにタイム・スタンプを使用するには、ELS を構成して、モニター待ち行列内のタイム・スタンプが時刻を表示するようにします。

167ページの図9 では、メッセージ 311-313 がリモート・ログに記録されなかったことにも注意してください。これは ARP 要求がアウトスタンディングであったためであり、ARP レスポンスを受信するまでは、最初のパケットを除く発信元 IBM 2210 内のすべてのパケットが廃棄されます。 ARP キャッシュは、ユーザーが構成したリフレッシュ速度で消去され、装置は新規の ARP 要求を出します。 ARP 要求が出されているかどうかを調べるために、対象となる ELS イベントに加えて、イベント

ARP.002 と ARP.011 もリモート・ログに記録してみることができます。 図11 は、*syslog_user_alert* ファイルに記録された ARP イベントを示しています。ここにはイベント 445 と 446 が記録されており、これらは 167ページの図9 には脱落として示されています。

```
Nov 20 12:02:53 workstа01 root: THIS IS A TEST MESSAGE (user.alert)
Nov 20 12:08:48 5.1.1.1 Msg [0314] from ** IBM / 2210 **: els:  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0315] from ** IBM / 2210 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0319] from ** IBM / 2210 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0444] from ** IBM / 2210 **: els:  ARP.011: Del ent 1 3 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0447] from ** IBM / 2210 **: els:  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
```

図 11. Syslog_user_alert ファイルの内容の例

IP アドレスと MAC アドレスの間に静的な関係を設定しておくことによって、このARP シーケンスが原因で生じる ELS メッセージの損失を防止することができます。基本的なステップを以下に示し、その例を 170ページの図12 に示します。

1. talk 5 で、リモート・ワークステーションの IP アドレスを 『ping』 する。
2. talk 5 で、メッセージをリモート・ワークステーションの IP アドレスに送信するのに使用するインターフェース (ネット) 番号を調べる。
3. 前のステップからのネット番号を使用して、対応する MAC アドレスを調べる。
4. talk 6 で、ARP 項目を追加して、IP アドレスと MAC アドレスの静的な関係を設定する。

```
*t 5
+p ip

IP>ping 192.9.200.1
PING 192.9.200.20 -> 192.9.200.1: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.9.200.1: icmp_seq=0. ttl=64. time=0. ms
----192.9.200.1 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms

IP>dump

  Type   Dest net            Mask          Cost    Age       Next hop(s)
.
   Dir*  192.9.200.0         FFFFFF00      1       102305    Eth/0
.
IP>exit
+int
                                                    Self-Test  Self-Test   Maintenance
Net   Net'   Interface  Slot-Port                   Passed     Failed      Failed
0     0      Eth/0      Slot: 1   Port: 1               1          0           0
.
+p arp
ARP>dump
Network number to dump [0]? 0
Hardware Address        IP Address        Refresh
02-60-8C-2D-69-5D       192.9.200.1       2

Ctrl-P
*t 6
config>p arp
ARP config>add entry
Interface Number [0]? 0
Protocol [IP]? IP
IP Address [0.0.0.0]? 192.9.200.1
Mac Address []? 02608C2D695D
ARP config> list entry

Mac address translation configuration

IF #      Prot #  Protocol -> Mac address
   0           0  192.9.200.1 -> 02608C2D695D
ARP config>exit
Config>

Ctrl-P

*restart
Are you sure you want to reload the gateway? (Yes or [No]): Yes

 (after reload, static ARP entry is active)
```

図 12. 静的 ARP 項目の設定例

その他の考慮事項

IP アドレスを含む ELS メッセージ

リモート・ワークステーションの IP アドレスに一致する IP アドレスを含んでいる ELS メッセージは、たとえリモート・ログ記録用に構成されていても、リモート・ログには記録されず、talk 2 のもとで表示されます。このようなメッセージは、過度の UDP パケットがネットワーク上で送信されるのを防止するために、リモート・ログに記録されずに、廃棄されます。

重複ログ

syslog.conf 内でファシリティー値が繰り返されている場合、たとえば、

```
user.debug        /tmp/syslog_user_debug
user.alert        /tmp/syslog_user_alert
```

syslog デーモンは、*user.debug* メッセージは */tmp/syslog_user_debug* ファイルにのみ記録し、一方の user.alert メッセージは */tmp/syslog_user_debug*ファイルと */tmp/syslog_user_alert* ファイルの両方に記録します。これは、重大な状態は複数の場所に記録するという syslog 設計に従うものです。

この重複ログを防止するために、*syslog.conf* ファイルには、異なるファシリティー値を指定することをお勧めします。合計 19 のファシリティー値を使用できます。

Syslog 出力ファイル内の反復シーケンス番号

ネットワークの構成によっては、ELS メッセージが入った重複する UDP パケットが、リモート・ホストに到着する可能性があります。また、パケットが送信された順序とは異なる順序で到着する可能性もあります。この現象の例を 図13 に示します。シーケンス番号が 628 ～ 633 のメッセージが 2 度記録されていることに注意してください。また、最初のシーケンス番号 0630 の後に、シーケンス番号 0629 が再び記録され、その後に 2 度目の 0630 があることにも注目してください。

```
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
```

図 13. Syslog 出力内の反復シーケンス番号の例

Syslog と UDP はどちらも重複シーケンスまたはシーケンス誤りパケットを処理する能力を備えていないので、重複シーケンス番号が発生する可能性があることを認識しておくことが重要です。

第13章 イベント・ログ・システム (ELS) の構成および監視

この章では、ELS によってログに記録されるイベントの構成方法および ELS コマンドの使用法について説明します。この章には、以下の節が含まれています。

- 『ELS 構成環境へのアクセス』
- 『ELS 構成コマンド』
- 194ページの『ELS 動作環境への出入り』
- 194ページの『ELS 監視コマンド』

イベント・ログ・システムについての詳細、および ELS イベント・メッセージの解釈の仕方については、153ページの『第12章 イベント・ログ・システム (ELS) の使用』を参照してください。

ELS 構成環境へのアクセス

ELS 構成環境は、ELS config> プロンプトによって示されます。このプロンプトで入力できるコマンドについては、『第13章 イベント・ログ・システム (ELS) の構成および監視』で説明しています。

ELS 構成環境に入るには、次のようにします。

1. **talk 6** と入力する。

   ディスプレイに Config> プロンプトが表示されますこのプロンプトが表示されない場合は、**Return** キーを押します。
2. Config> プロンプトで、次のコマンドを入力して ELS にアクセスする。

   ```
   event
   ```

   ディスプレイに ELS 構成プロンプト (ELS config>) が表示されます。これで、ELS 構成コマンドを入力できます。

ELS 構成環境を終了するには、**exit** コマンドを入力します。

ELS 構成コマンド

表20 は、ELS 構成コマンドを要約しています。この節の残りの部分で、各コマンドについて詳しく説明します。 ELS 構成環境にアクセスした後、ELS Config> プロンプトから ELS 構成コマンドを入力することができます。

表 20. ELS 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	イベントを既存のグループに追加するか、または新しいグループを作成します。
Clear	すべての ELS 構成情報を消去します。

表 20. ELS 構成コマンドの要約 (続き)

コマンド	機能
Default	イベント、グループ、またはサブシステムの表示またはトラップ設定値をリセットします。
Delete	イベント番号を既存のグループから削除するか、またはグループ全体を削除します。
Display	コンソール・モニター上のメッセージの表示を使用可能にします。
Filter	ネット番号に基づいて ELS メッセージをフィルターに掛けます。
List	ELS 設定値およびメッセージに関する情報をリストします。
Nodisplay	コンソール上のメッセージの表示を使用不可にします。
Noremote	リモート・ワークステーションへのリモート・ログ記録を使用不可にします。
Notrace	パケット・トレース・イベントの使用不可化を制御します。
Notrap	メッセージが SNMP トラップで送信されないようにします。
Remote	メッセージがリモート・ワークステーションのログに記録されるようにします。
Set	ピン・パラメーター、タイム・スタンプ機能、および ATM パケット・トレース・オプションを設定します。
Trace	パケット・トレース・イベントの使用可能化を制御します。
Trap	メッセージが SNMP トラップでネットワーク管理ステーションに送信されるようにします。
View	トレースされたパケットを表示できるようにします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、個々のイベントを既存のグループに追加したり、新しいグループを作成したりするのに使用します。グループ名は英字で始める必要があり、大文字小文字を区別します。サブシステム全体をグループに追加することはできません。

構文:

add *group_name subsystem.event_number*

注: 指定されたグループが存在しない場合は、次のようなプロンプトが出され、新しいグループの作成を確認するように求められます。

```
Group not found. Create new group? (yes or no)
```

Clear

clear コマンドは、すべての ELS 構成情報を消去するのに使用します。

構文:

clear

例:

```
clear

You are about to clear all ELS configuration information
Are you sure you want to do this (Yes or No):
```

Default

イベント、グループ、またはサブシステムの表示またはトラップ設定値をリセットして、使用不可の状態に戻します。

構文:

default display
trap
remote

display *event* **OR** *group* **OR** *subsystem*
モニターへのメッセージの表示の出力を制御します。

trap *event* **OR** *group* **OR** *subsystem*
ネットワーク管理ステーションへのトラップの生成を制御します。

remote *event* **OR** *group* **OR** *subsystem*
リモート端末へのトラップの生成を制御します。

Delete

delete コマンドは、既存のグループからイベント番号を削除したり、グループ全体を削除したりするのに使用します。指定したイベントがグループ内で削除される最後のイベントのときは、ユーザーに通知されます。 *subsystem.event_number* ではなく*all* を指定した場合は、グループ全体の削除を確認するように求めるプロンプトが出ます。

構文:

delete *group_name subsystem.event_number*

Display

display コマンドは、特定のイベント、サブシステムの一定範囲のイベント、グループ、またはサブシステムについて、モニター上のメッセージの表示を使用可能にするのに使用します。

構文:

display event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
指定されたイベント (*subsystem.event#*) のメッセージを表示します。

group *groupname*
指定されたグループ (*groupname*) のメッセージを表示します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージを表示します。

例:

```
display range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 を表示します。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージを表示します。ルーター上でサポートされるサブシステムのリストを、以下に示します。ルーター上にあるサブシステムを調べたい場合は、**list subsystems** を入力します。

注: ELS はこれらのサブシステムをすべてサポートしますが、すべての装置がすべてのサブシステムをサポートしているとは限りません。サポートされるサブシステムの最新リストは、 *ELS Messages* を参照してください。

サブシステム	説明
AI	自動装置導入
All	全サブシステム **注:** ルーターがライブ・プロトコル・トラフィックを転送しているときは、長時間にわたって全サブシステムを表示しないようにしてください。ルーターがモニターとの通信に過剰な時間を費やすことになるからです。リモート・モニターを介してルーターと通信しているときは、絶対に全サブシステムを表示しないでください。ルーターは時間のほとんどをリモート・モニターとの通信に費やすことになります。
AP2	AppleTalk フェーズ 2
ARP	アドレス解決プロトコル
APPN	拡張対等通信ネットワーキング機能
ATM	非同期転送モード
BAN	境界アクセス・ノード
BGP	ボーダー・ゲートウェイ・プロトコル
BR	ブリッジング/ルーティング
BRS	帯域幅予約
BTP	BOOTP リレー・エージェント
CLNP	ISO 8473 - CLNP
COMP	データ圧縮
DIAL	ダイヤル回線
DLS	データ・リンク交換

DN	DECnet
DOUT	DIAL サーバー・ダイヤルアウト
DNAV	DNA フェーズ V
DVM	DVMRP マルチキャスト・ルーティング・プロトコル
ENCR	データ暗号化
ESIS	ISO 9542 - ESIS プロトコル
ETH	イーサネット・ハンドラー
EZ	EasyStart
FLT	フィルター・ライブラリー
FRL	フレーム・リレー
GW	ルーター・ベースおよびネットワーク・ライブラリー
ICMP	インターネット制御メッセージ・プロトコル
ILMI	中間ローカル管理インターフェース
IP	インターネット・プロトコル
IPPN	IP プロトコル・ネット
IPX	インターネットワーク・パケット交換
ISDN	サービス総合ディジタル網
ISIS	ISO 10589 - ISIS プロトコル
ILMI	ATM 中間ローカル管理インターフェース
LCS	論理チャネル・ステーション
LEC	ATM LAN エミュレーション・クライアント
LECS	LAN エミュレーション構成サーバー
LES	LAN エミュレーション・サーバー
LLC	論理リンク制御
LSA	リンク・サービス・アーキテクチャー
LSI	LAN スイッチ統合
LNM	LAN ネットワーク・マネージャー
MCF	MAC フィルター
MPC	マルチパス・チャネル
MSPF	OSPF マルチキャスト拡張
NBS	NetBIOS サポート・サブシステム
NOT	非サポート・プロトコル転送機能
OSPF	SPF (最短パス最優先) オープン・ベースのルーティング・プロトコル
PPP	ポイント・ポイント・プロトコル
RIP	IP ルーティング情報プロトコル

R2MP	AppleTalk フェーズ 2 ルーティング・テーブル管理プロトコル
SAAL	シグナル ATM アダプテーション・レイヤー
SDLC	IBM SDLC
SL	シリアル・ライン・ハンドラー
SNMP	シンプル・ネットワーク管理プロトコル
SRLY	SDLC リレー
SRT	ソース・ルーティング透過ブリッジ
STP	スパンニング・ツリー・プロトコル
SVC	スイッチド・バーチャル・コネクション
TCP	トランスポート制御プロトコル
TFTP	トリビアル・ファイル転送プロトコル
TKR	トークンリング・ハンドラー
UDP	ユーザー・データグラム・プロトコル
VIN	Banyan VINES
V25B	CCITT/ITU V.25bis
WRS	WAN 復元/再ルート
XN	XNS/IPX/DDS 共通処理
XNS	Xerox ネットワーク・システム・プロトコル
X25	X.25 プロトコル
X251	X.25 物理レイヤー
X252	X.25 フレーム・レイヤー
X253	X.25 パケット・レイヤー
XTP	X.25 トランスポート・プロトコル
ZIP2	AppleTalk フェーズ 2 ゾーン情報プロトコル

Filter

filter コマンドは、フィルター構成コマンド環境にアクセスするのに使用します。このコマンドについての詳細は、191ページの『ELS ネット・フィルター構成コマンド』を参照してください。

構文:

filter net

List

list コマンドは、ELS 設定値の更新情報および選択されたメッセージのリストを入手するのに使用します。

構文:

list
- all
- filter-status
- groups
- pin
- remote-log status
- status
- subsystem . . .
- subsystems all
- trace-status

all すべての **list** カテゴリーの情報をリストします。

filter-status
ELS ネット番号フィルターをリストします。

groups
ユーザー定義のグループ名と内容をリストします。

pin SNMP トラップで送信される ELS イベント・メッセージの現在数 (1 秒当り) をリストします。

remote-log status
リモート・ログ記録オプションの現行値をリストします。

例:

```
list r

Remote Logging is ON
Source IP Address = 192.67.38.2
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_DAEMON
Default Syslog Priority Level = LOG_CRIT
Number of Messages in Remote Log = 256
Remote Logging Local ID = MYHOSTNAME
```

status **display**、**nodisplay**、**trap**、および **notrap**、**trace**、**notrace**、**remote**、および **noremote** コマンドによって変更されたサブシステム、グループ、およびイベントをリストします。

例:

```
list status

Subsystem:             TKR
Disp Levels:           STANDARD
Trap levels:           none
Trace levels:          none
Remote levels:         ERROR INFO TRACE
Syslog Facility/Level: LOG_USER LOG_INFO

Group        Disp     Trap    Trace  Remote
Mygroup     Unset    Unset    Unset    On
                                       Syslog Facilty/Level: LOG_DAEMON LOG_CRIT

Event        Disp     Trap    Trace  Remote
IP.007      Unset    Unset    Unset    On
                                       Syslog Facility/Level: LOG_CRON LOG_NOTICE
```

注: ディスプレイには、リモート・ログ記録が使用可能であることだけでなく、各サブシステム、グループ、およびイベントの Syslog Facility/Level 値も表示されます。イベントの範囲は、個々のイベントとしてリストされます。

subsystem
すべてのサブシステムの名前、イベント、および記述をリストします。

(**list subsystem** コマンドの出力例は、198ページに記載してあります。)

subsystem *subsystem*
指定されたサブシステム内のすべてのイベントをリストします。

例:

```
list subsystem gw


Event      Level      Message

GW.001     ALWAYS   Copyright 1984 Mass Institute of Technology
GW.002     ALWAYS   Portable CGW %s Rel %s strtd
GW.003     ALWAYS   Unus pkt len %d nt %d int %s/%d
GW.004     ALWAYS   Sys %s q adv alloc %d excd %d
GW.005     ALWAYS   Bffrs: %d avail %d idle   fair %d low %d
GW.006     C-INFO    Pkt frm nt %d int %s/%d for uninit prt, disc
GW.007     C-INFO    Ip err %x nt %d int %s/%d
GW.008     U-INFO    Ip ovfl nt %d int %s/%d, disc
GW.009     UI-ERROR  Nt dwn ip rstrt nt %d int %s/%d
GW.010     UI-ERROR  Ip q len %d no ip buf nt %d int %s/%d
GW.011     U-INFO    Op err %x hst %wo nt %d int %s/%d
GW.012     U-INFO    Op err cnt excd hst %wo nt %d int %s/%d
GW.013     U-INFO    Rtrns cnt excd hst %wo nt %d int %s/%d
GW.014     UI-ERROR  Nt dwn op rstrt nt %d int %s/%d
GW.015     UI-ERROR  Nt dwn to hst %wo nt %d int %s/%d
GW.016     U-INFO    Op ovfl to hst %wo nt %d int %s/%d
GW.017     UE-ERROR  Intfc hdw mssng nt %d int %s/%d
GW.018     U-TRACE   Strt nt slf tst nt %d int %s/%d
GW.019     C-INFO    Slf tst nt %d int %s/%d
GW.020     U-TRACE   Nt pss slf tst nt %d int %s/%d
GW.021     UE-ERROR  Nt up nt %d int %s/%d
GW.022     U-TRACE   Nt fld slf tst nt %d int %s/%d
```

subsystems all
すべてのサブシステム内のすべてのイベントをリストします。

trace-status
構成および実行時情報を含めて、パケット・トレースの状況に関する情報を表示します。

例:

```
list trace-status

------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
```

Nodisplay

nodisplay コマンドは、コンソール上のメッセージ表示を選択して、オフにするのに使用します。

構文:

nodisplay event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*
指定されたイベント (*subsystem.event#*) の表示を抑制します。

group *groupname*
指定されたグループ (*groupname*) に以前に追加されたメッセージの表示を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージを表示を抑制します。

例:

```
nodisplay range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 の表示を抑制します。

subsystem *subsystemname*
指定されたサブシステムに関連するメッセージの表示を抑制します。

Noremote

noremote コマンドは、イベント番号、グループ、イベントの範囲、またはサブシステムに基づくリモート・ワークステーションへのイベント・ログ記録を抑制するのに使用します。

注: 通常、**noremote** コマンドでは、**remote** コマンドの場合のように、*syslog_facility* と *syslog_level* を指定する必要はありません。ただし、**noremote subsystem** コマンドには、すべてをオフにする代わりに、特定のメッセージ・レベルを選択して (たとえば、『error』 のみ、あるいは 『trace』 のみ) それだけを抑制するオプションがあります。 (特定のメッセージ・レベルを指定しなかった場合は、『all』が想定されます。) さらに、**noremote subsystem** コマンドは、オフにしなかった残りのメッセージ・レベルに対して *syslog_facility* と *syslog_level* を設定することも可能です。

構文:

noremote event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*
指定されたイベントのメッセージのリモート・ログ記録を抑制します。

group *group.name*
以前に指定されたグループ (*group.name*) に追加されたメッセージのリモート・ログ記録を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージのリモート・ログ記録を抑制します。

例:

```
noremote range gw 19 22
```

イベント gw.019, gw.020, gw.021, および gw.022 のリモート・ログ記録を抑制します。

subsystem *subsystem.name [syslog_facility syslog_level]*

指定されたサブシステム (*subsystem.name*) に関連するメッセージのリモート・ログ記録を抑制します。

例 1:

```
noremote subsystem tkr
```

すべての 『tkr』 メッセージのリモート・ログ記録を抑制します。

例 2:

```
ELS config> noremote subsystem tkr info
ELS config> SYSLOG FACILITY[LOG_USER]?
ELS config> SYSLOG LEVEL[LOG_INFO]?
```

この例で、『LOG_USER』 と 『LOG_INFO』 は、サブシステム TKR に対して最後に指定された値です。指定されたコマンドは、『info』 用に生成されたメッセージについてのみ、サブシステム TKR のリモート・ログ記録を抑制します。 *syslog_facility* と *syslog_level* が指定されていないので、ソフトウェアは *syslog_facility* と *syslog_level* を求めるプロンプトを出します。プロンプトに対して別8の値を入力すると、*syslog_facility* と *syslog_level* はその値で置き換えられ、TKR サブシステムの残りのリモート・ログ・メッセージに適用されます。

list all または **list status** コマンドを使用すれば、**noremote** および **remote** コマンドで行った設定を表示することができます。

syslog_facility および *syslog_level* についての詳細は、184ページの『Remote』を参照してください。

Notrace

指定されたイベント/範囲/サブシステム/グループのトレースを使用不可にします。

構文:

notrace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
指定された event# のパケット・トレース・データの送信を抑制します。

group *groupname*
指定されたグループ (groupname) に以前に追加されたパケット・トレース・データの送信を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージのパケット・トレース・データの送信を使用不可にします。

例:

```
trace range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のパケット・トレース・データの送信を抑制します。

subsystem *subsystemname*
指定されたサブシステム (subsystemname) のパケット・トレース・データの送信を抑制します。

Notrap

notrap コマンドは、メッセージを選択してオフにし、SNMP トラップでネットワーク管理ステーションに送信されないようにするのに使用します。

構文:

notrap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
指定されたメッセージの SNMP トラップでの送信 (*subsystem.event#*) を抑制します。

group *groupname*
指定されたグループ (*groupname*) に以前に追加されたメッセージの SNMP トラップでの送信を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のイベントのメッセージの SNMP トラップでの送信を抑制します。

例:

```
notrap range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のメッセージの SNMP トラップでの送信を抑制します。

subsystem *subsystemname*
指定されたサブシステムに関連するメッセージの SNMP トラップでの送信を抑制します。

Remote

remote コマンドは、イベント番号、イベントの範囲、グループ、またはサブシステムに基づいて、リモート・ワークステーションにログ記録するイベントを選択するのに使用します。

構文:

remote event . . .
range . . .
group . . .
subsystem . . .

event *subsystem.event# syslog_facility syslog_level*
指定されたイベントをリモート・ログに記録します。

リモート・ワークステーションの syslog デーモンは、Syslog ファシリティー値とレベル値を使用して、メッセージを記録する場所を判別します。この値は、**set facility** および **set level** コマンドを使用して設定したデフォルト値をオーバーライドします。

syslog_facility

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level

log_emerg
log_alert
log_crit

log_err
log_warning
log_notice
log_info
log_debug

これらの値は、IBM 2210 上のデーモンと特別な関連はありません。リモート・ワークステーション上の syslog デーモンによって使用される識別子にすぎません。

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のイベントが、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログに記録されます。 184ページの『remote event コマンド』 を参照してください。

例:

```
remote range gw 19 22 log_user log_info
```

イベント gw.19、gw.20、gw.21、および gw.22 が、log_user の *syslog_facility* 値と log_info の *syslog_level* 値に基づいて、リモート・ログに記録されます。

group *group.name syslog_facility syslog_level*

指定されたグループに属するイベントを、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログに記録することができます。 184ページの『remote event コマンド』 を参照してください。

subsystem *subsystem.name message_level syslog_facility syslog_level*

ここで、*subsystem.name* はサブシステムの名前、*message_level* は、サブシステム内の選択されたメッセージのレベルです。

指定された *subsystem.name* の中の、*message_level* が指定の *message_level* に一致するイベントが、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログ・ファイルに記録されます。 184ページの『remote event コマンド』を参照してください。

Message_level の値は、『ALL』、『ERROR』、『INFO』、または『TRACE』 です。 156ページの『ログ・レベル』を参照してください。 **remote** コマンドで指定された値は、サブシステム内の特定のイベントにコーディングされた値と一致していなければなりません。そうでない場合、サブシステム内のそのイベントはリモート・ログに記録されません。

例:

```
remote subsystem TKR all log_user log_info
```

上の例では、サブシステム TKR 内のすべてのメッセージ (『all』には、『error』、『info』、または 『trace』 として符号化されているメッセージがすべて含まれます) が、log_user 値と log_info の値に基づいて、リモート・ホストのログに記録されます。

list all または **list status** コマンドを使用すれば、**noremote** および **remote** コマンドで行った設定を表示することができます。

Set

set コマンドは、1 秒当りの最大トラップ数の設定、タイム・スタンプ機能の設定、または ATM 装置のトレース・オプションの設定を行うのに使用します。

構文:

set pin . . .
remote-logging . . .
timestamp . . .
trace . . .

pin *max_traps*
ピン・パラメーターを秒単位で送信できるトラップの最大数に設定するのには、**set pin** コマンドを使用します。内部で、ピンは 10 分の 1 秒ごとにリセットされます。 (10 分の 1 の数 (*max_traps*) が、10 分の 1 秒ごとに送信されます。)

remote-logging
set remote-logging コマンドは、リモート・ログ記録オプションを構成するのに使用します。これらのオプションを監視環境から構成した場合、変更は即時に有効になり、装置がリブートされると以前に構成された設定値に戻ります。

構文:

set remote-logging on
off
facility . . .
level . . .
no-msgs
remote_ip_addr . . .
source_ip_addr ...
local_id

on リモート・ログ記録をオンにします。これでリモート・ログ記録が使用可能になり、**remote** コマンドで選択したメッセージを記録することができます。

off リモート・ログ記録をオフにします。 'remote' コマンドによって選択されたすべてのメッセージがログに記録されなくなります。

facility
リモート・ワークステーションの syslog デーモンが、メッセージを記録する場所を判別するために、*level* 値と組み合わせて使用する値を指定します。 **remote** コマンドを使用して、特定の ELS イベント、

範囲、グループ、またはサブシステムに対して異なる値を指定しない限り、この値がすべてのリモート・ログ記録 ELS メッセージに適用されます。

すべての可能な syslog ファシリティー値は、次のとおりです。

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

level リモート・ワークステーションの syslog デーモンが、メッセージを記録する場所を判別するために、*facility* 値と合わせて使用する値を指定します。 **remote** コマンドを使用して、特定の ELS イベント、範囲、グループ、またはサブシステムに対して異なる値を指定しない限り、この値がすべてのリモート・ログ記録 ELS メッセージに適用されます。

すべての可能な syslog レベル値は、次のとおりです。

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

no-msgs
ログが循環する前の、リモート・ログ用のバッファー内のメッセージの数を指定します。

remote_ip_addr
これは xxx.xxx.xxx.xxx 形式の IP アドレスです。ただし、xxx は 0 ～ 255 の任意の整数です。これは、ログ・ファイルが存在するリモート・ホストの IP アドレスです。

source_ip_addr
これは xxx.xxx.xxx.xxx 形式の IP アドレスです。ただし、xxx は 0 ～ 255 の任意の整数です。

リモート・ログ ELS メッセージに示された IP アドレスまたはホスト名を識別しやすくするために、2210 に構成された IP アドレスを使用することが必要です。また、この IP アドレスは、ネーム・サーバーが速やかにホスト名に変換できること、あるいは少なくともネーム・サーバーが速やかに 『address not found』を応答できるものであることを確認する必要があります。

IP アドレスの解決が適切に行われるかどうかを調べるには、ユーザーのワークステーションで、次のような **host** コマンドを入力してみます。

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

応答に 1 秒以上かかる場合は、もっと迅速に解決できる IP アドレスを選択してください。

local_id

これは、リモート・ログ・ファイルに記録されたメッセージに含まれ、そのメッセージを記録したマシンを識別するのに役立つ、最高 32 文字までの任意の文字列です。

timestamp [timeofday or uptime or off]

メッセージ・タイム・スタンプをオンにして、時刻またはアップタイム (日付はなく、ルーターの最後の初期化以降の時間、分、および秒数) が、各メッセージの横に表示されます。 Set timestamp をオフにすることもできます。

set timestamp コマンドを使用して、以下のタイム・スタンプ・オプションの 1 つを使用可能にします。

timeofday

1 日 24 時間での発生時刻を示す HH:MM:SS プレフィックスを、各メッセージに追加します。

uptime

100 時間周期における発生時刻を示す HH:MM:SS プレフィックスを、各メッセージに追加します。アップタイム 100 時間後に、アップタイム・カウンターはゼロに戻り、別の 100 時間周期を開始します

off ELS タイム・スタンプ・プレフィックスをオフにします。

trace ATM 装置のトレース・オプションを構成するには、**set trace** コマンドを使用します。トレース・オプションを監視環境から構成した場合、変更は即時に有効になり、装置がリブートされると以前に構成された設定値に戻ります。

注: トレースは、熟練したサポート技術員の指示の下でのみ使用してください。トレースは、特にシャドー・ディスクを使用可能にして使用する場合、装置の資源を使用するので、全体的な性能およびスループットに影響を与える可能性があります。

構文:

set trace decode

default-bytes-per-pkt

max-bytes-per-pkt

off

on

reset

wrap-mode

decode *off/on*
パケットの復号をオンまたはオフにします。パケット復号は、すべてのコンポーネントによってサポートされているとは限りません。

default-bytes-per-pkt *bytes*
デフォルトのトレースされるバイト数を設定します。トレースを行うコンポーネントによって値が指定されない場合、この値が使用されます。

max-bytes-per-pkt *bytes*
各パケットごとに、トレースされる最大バイト数を設定します。

off パケット・トレースを使用不可にします。

on パケット・トレースを使用可能にします。

reset トレース・バッファーをクリアし、すべての関連のカウンターをリセットします。

wrap-mode [off or on]
トレース・バッファー折り返しモードをオフにします。折り返しモードがオンで、トレース・バッファーが満杯の場合は、トレースを継続する必要に応じて、前のトレース・レコードに新しいトレース・レコードが上書きされます。

Trace

指定されたイベント/範囲/サブシステム/グループのトレースを使用可能にします。**trace** コマンドを `ELS Config>` プロンプトから使用した場合、変更は構成の一部になり、その変更をアクティブにするためにはリブートが必要です。

構文:

trace event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*
指定されたトレース・イベント (*subsystem.event#*) をシステム・モニターに表示します。

group *groupname*
指定されたグループに以前に追加されたトレース・イベントを、ルーター・モニターに表示できるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のトレース・イベントを、システム・モニターに表示します。

例:

```
trace range gw 19 22
```

トレース・イベント gw.19、gw.20、gw.21、および gw.22 を、システム・モニターに表示します。

subsystem *subsystemname*

指定されたサブシステムに関連するトレース・イベントを、ルーター・モニターに表示できるようにします。

Trap

trap コマンドは、リモート SNMP ネットワーク管理ワークステーションに送信するメッセージを選択するのに使用します。リモート SNMP ネットワーク管理ワークステーションは、SNMP マネージャーとして働くネットワーク内の IP ホストです。

構文:

trap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*

指定されたメッセージ (*subsystem.event#*) が SNMP でネットワーク管理ワークステーションに送信されるようにします。

group *groupname*

指定されたグループに以前に追加されたメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

例:

```
trap range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 内のメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

subsystem *subsystemname*

指定されたサブシステムに関連するメッセージが、SNMP トラップで管理ステーションに送信されるようにします。

注: IP、ICMP、ARP、および UDP サブシステムのメッセージは、SNMP トラップで送信することはできません。これらの区域は SNMP トラップを送信する過程で使用されているか、使用される可能性があるからです。これはトラフィックの無限のループを招いて、ルーターに不当な負担をかけることになります。

ELS ネット・フィルター構成コマンド

ELS ネット・フィルターは、特定のネット番号をもつ ELS メッセージのみを見つけ、その他の ELS メッセージは廃棄する機能を提供します。

フィルターを作成するときには、そのフィルターを適用するサブシステム、イベント、またはイベントの範囲を指定します。待ち行列も指定します (たとえば、『DISPLAY』、『TRAP』、『TRACE』、または 『REMOTE-LOGGING』)。最後に、フィルターに掛けるネット番号 (または、ネット番号の範囲) を指定します。

フィルターを使用可能にすると、ELS コマンドによってオンにされたメッセージがフィルターに掛けられます。フィルターは、指定されたネット番号をもつメッセージのみを通過させます。指定されたネット番号を含まないメッセージは、装置に廃棄させます。

送信される ELS メッセージの数を減らすことによって、対象のインターフェースに関するメッセージを見つけやすくなります。

この節では、ELS ネット・フィルターを構成するためのコマンドについて説明します。これらのフィルターを構成するには、ELS> プロンプトで **filter net** コマンドを入力します。次に、`ELS Filter net>` プロンプトで構成コマンドを入力します。

表 21. ELS ネット・フィルター構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Create	フィルターを作成し、それに番号を割り当てます。最大 64 のフィルターを作成できます。
Delete	指定されたフィルター番号またはすべてのフィルターを削除します。
Disable	指定されたフィルター番号またはすべてのフィルターを使用不可にします。
Enable	指定されたフィルター番号またはすべてのフィルターを使用可能にします。
List	指定されたフィルター番号またはすべてのフィルターをリストにします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Create

create コマンドは、ELS ネット・フィルターを作成するのに使用します。

構文:

create ***queue***

event *event_name net#_start net#_end*

range *event_range net#_start net#_end*

subsystem *subsystem_name net#_start net#_end*

queue フィルターを設定する待ち行列。有効な待ち行列は、次のとおりです。

Display

Trace

Trap

Remote

event *event_name net#_start net#_end*

フィルターに掛けるイベントとネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1 つのネット番号をフィルターに掛けることになります。

コマンド **create trap event GW.009 2 10** は、ネット番号 2 〜 10 のメッセージ GW.009 のトラップをフィルターに掛けます。

range *event_range net#_start net#_end*

フィルターに掛ける ELS メッセージの範囲とネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1 つのネット番号をフィルターに掛けることになります。

コマンド **create remote range ipx 19 22 3 6** は、リモート・ログ記録用の、ネット番号 3 〜 6 の IPX.019 で始まり IPX.022 で終わるすべての IPX メッセージをフィルターに掛けます。

subsystem *subsystem_name net#_start net#_end*

フィルターに掛けるサブシステムとネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1 つのネット番号をフィルターに掛けることになります。

コマンド **create display subsys ip 1 1**, は、ディスプレイへの、ネット番号 1 を含む IP サブシステムのすべての ELS メッセージをフィルターに掛けます。その他の IP サブシステム・メッセージはすべて廃棄します。

Delete

delete コマンドは、特定の ELS フィルターまたはすべての ELS フィルターを削除するのに使用します。

構文:

delete

all

filter *filter#*

all 現在構成されているすべてのフィルターを削除します。

filter *filter#*
filter# によって指定されたフィルターを削除します。削除したいフィルターの番号を入手するには、**list** コマンドを使用します。

Disable

disable コマンドは、特定の ELS フィルターまたはすべての ELS フィルターを使用不可にするのに使用します。

構文:

disable all
filter *filter#*

all 現在構成されているすべてのフィルターを使用不可にします。

filter *filter#*
filter# によって指定されたフィルターを使用不可にします。使用不可にしたいフィルターの番号を入手するには、**list** コマンドを使用します。

Enable

enable コマンドは、特定の ELS フィルターまたはすべての ELS フィルターを使用可能にするのに使用します。

構文:

enable all
filter *filter#*

all 現在構成されているすべてのフィルターを使用可能にします。

filter *filter#*
filter# によって指定されたフィルターを使用可能にします。使用可能にしたいフィルターの番号を入手するには、**list** コマンドを使用します。

List

list コマンドは、特定の ELS フィルターまたはすべての ELS フィルターをリストするのに使用します。

構文:

list all
filter *filter#*

all 現在構成されているすべてのフィルターをリストします。

filter *filter#* によって指定されたフィルターをリストします。

ELS 動作環境への出入り

ELS 監視環境 (GWCON プロセスからアクセス可能) は、ELS> プロンプトによって示されます。このプロンプトで入力されるコマンドは、現行の ELS パラメーターの設定値を変更します。これらのコマンドについては、173ページの『第13章 イベント・ログ・システム (ELS) の構成および監視』 で説明します。

OPCON から ELS 監視環境に入るには、次のようにします。

1. **talk 5** コマンドを入力する。

   ```
   * talk 5
   ```

   モニターに GWCON プロンプト (+) が表示されます。最初に GWCON に入ったときにこのプロンプトが表示されない場合は、**Return** を押してください。
2. GWCON プロンプトで、次のコマンドを入力して ELS にアクセスする。

   ```
   + event
   ```

   モニターに ELS 監視プロンプト (ELS>) が表示されます。これで、ELS 監視コマンドを入力できます。

ELS 監視環境を終了するには、**exit** コマンドを入力します。

ELS 監視コマンド

この節では、すべての ELS 監視コマンドの要約を示し、個々のコマンドについて説明します。 ELS 監視環境にアクセスした後、ELS> プロンプトから ELS 監視コマンドを入力することができます。

表 22. ELS 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Clear	指定されたイベント、グループ、またはサブシステムに関連したメッセージのカウントをゼロにリセットします。
Display	コンソール上のメッセージの表示を使用可能にします。
Exit	ELS コンソール・プロセスを終了し、ユーザーを GWCON に戻します。
Filter	ネット番号に基づいて ELS メッセージをフィルターに掛けます。
List	ELS 設定値およびメッセージに関する情報をリストします。
Nodisplay	コンソール上のメッセージの表示を使用不可にします。
Noremote	リモート・ワークステーションのファイルへのリモート・ログ記録を使用不可にします。
Notrace	コンソール上のトレース・イベントの表示を使用不可にします。
Notrap	メッセージが SNMP トラップでネットワーク管理ワークステーションに送信されないようにします。
Packet-trace	アクティブ・パケット・トレース・パラメーターを設定およびリストするための拡張集中環境を提供します。
Remote	メッセージがリモート・ワークステーション上のファイルに記録されるようにします。
Remove	保管されている情報を消去して、メモリーを解放します。

表 22. ELS 監視コマンドの要約 (続き)

コマンド	機能
Restore	現行の設定値をクリアして、初期 ELS 構成を再ロードします。
Retrieve	保管されている ELS 構成を再ロードします。
Save	現行構成を保管します。
Set	ピン・パラメーターおよびタイム・スタンプ機能を設定します。
Statistics	使用可能なサブシステムと関連の統計を表示します。
Trace	コンソール上のトレース・イベントの表示を使用可能にします。
Trap	メッセージが SNMP トラップでネットワーク管理ステーションに送信されるようにします。
View	トレースされたパケットを表示できるようにします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Clear

clear コマンドは、特定のイベント、グループ、またはサブシステムに関連した display、trace、trap、または remote コマンドのカウントをゼロにリセットするのに使用します。

構文:

clear event . . .
group . . .
subsystem . . .

event *subsystem. event#*
指定されたイベント (*subsystem.event#*) の表示、トラップ、トレース、またはリモート・ログ記録用のイベントのカウントをゼロにリセットします。

group *group.name*
指定されたグループ (*group.name*) の表示、トラップ、トレース、またはリモート・ログ記録用のイベントのカウントをゼロにリセットします。

subsystem *subsystem.name*
指定されたサブシステム (*subsystem.name*) の表示、トラップ、トレース、またはリモート・ログ記録用のイベントのカウントをゼロにリセットします。

Display

display コマンドは、特定のイベントについて、監視モニター上のメッセージの表示を使用可能にするのに使用します。

構文:

display event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
指定されたイベント (subsystem.event#) に関するメッセージを表示します。

group *groupname*
指定されたグループ (*groupname*) のメッセージを表示します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージを表示します。

例:

```
display range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 を表示します。

subsystem *subsystem.name*
指定されたサブシステム (*logging level*) に関連するメッセージを表示します。ログ・レベルを指定しないと、そのサブシステムのすべてのメッセージがオンになります。

Files

files コマンドは、TFTP を使用してネットワーク上の別のホストにトレース・ファイルを転送するのに使用します。

構文:

files trace tftp *host_IP_addr filename*

host_IP_addr
ファイルの転送先のホストの IP アドレスです。

filename
ターゲット・ファイル名です。 TFTP の場合、ファイル名には完全なパスを指定し、そのファイル名がすでにターゲット・ホストに存在している必要があります。

Filter

filter コマンドは、フィルター構成コマンド環境にアクセスするのに使用します。このコマンドについての詳細は、216ページの『ELS ネット・フィルター監視コマンド』を参照してください。

構文:

filter net

List

list コマンドは、ELS 設定値の更新情報や、選択されたメッセージのリストを入手するのに使用します。

構文:

list all

active . . .

event . . .

filter-status

groups . . .

pin

remote-log status

subsystems . . .

trace-status

all すべてのサブシステム、定義されたグループ、使用可能にされたサブシステム、使用可能にされたイベント、およびピンをリストします。

active *subsystem.name*
特定のサブシステムのアクティブのイベント、およびメッセージの発生カウントを表示します。

例:

```
list active ip

EventActiveCount
IP.00789354
ETH.009D10
Subsystem X25: no event active
```

リモート・ログ記録がオンになっている場合、サブシステムについてアクティブとして表示されているイベントは、その名前の横に 『R』が表示されます。

event *subsystem.event#*
指定されたイベントのログ・レベル、メッセージ、およびカウントを表示します。

例:

```
list event ip.007

Level: p-TRACE
Message: source_ip_address -> destination_ip_address
Active:  Count: 84182
```

このイベントに対してリモート・ログ記録がアクティブにされており、*syslog_facility* と *syslog_level* の値が、それぞれ log_daemon と log_crit である場合、最後の行は次のようになります。

```
Active:  R count:84182
Syslog Facility: log_daemon   Syslog Level: log_crit
```

filter-status
ELS ネット番号フィルターをリストします。

groups *group.name*
ユーザー定義のグループ名を表示します。

pin SNMP トラップで送信される ELS イベント・メッセージの現在数 (1 秒当り) をリストします。これは、SNMP トラップ・トラフィックの量を減らすために使用できる限界値です。

例:

```
list pin

Pin: 100 events/second
```

remote-log status

set remote-logging コマンドで設定されたリモート・ログ記録オプションの現行値をリストします。

例:

```
list r

Remote Logging is On
Source Ip Address = 192.9.200.8
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_USER
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log = 256
Remote Logging Local ID =  SPHINX
```

subsystem *subsystem.name*

イベント名、発生したイベントの合計数、およびその記述を表示します。

注: ELS はこれらのサブシステムをすべてサポートしますが、すべての装置がすべてのサブシステムをサポートしているとは限りません。サポートされるサブシステムの最新リストは、 *ELS Messages* を参照してください。

例:

```
list subsystem

Name      Events  Description

ALL               All subsystems
GW           101  Router base and network library
FLT            7  Filter Library
BRS            5  Bandwidth  Reservation
ARP          142  Address Resolution Protocol
IP           100  Internet Protocol
ICMP          21  Internet Control Message Protocol
TCP           57  TCP
UDP            6  User Datagram Protocol
BTP           13  BOOTP relay agent
RIP           22  IP Routing Information Protocol
OSPF          73  Open SPF-Based Routing Protocol
MSPF          17  OSPF Multicast extensions
TFTP          29  TFTP Protocol
SNMP          28  Simple Network Management Protocol
DVM           21  DVMRP Multicast Routing Protocol
DN           115  DECnet
XN            21  XNS/IPX/DDS common processing
IPX          110  Internetwork Packet Exchange Protocol
CLNP          58  ISO 8473 - CLNP
ESIS          24  ISO 9542 - ESIS Protocol
ISIS          58  ISO 10589 - ISIS Protocol
DNAV          26  DNA Phase V
AP2           70  AppleTalk Phase 2
ZIP2          51  AppleTalk Phase 2 Zone Information Protocol
R2MP          38  AppleTalk Phase 2 Routing Table Management Protocol
VIN           79  Banyan VINES
SRT           94  Source Routing Transparent Bridge
STP           32  Spanning Tree Protocol
BR            30  Bridge/Routing
SRLY          28  SDLC Relay
ETH           47  Ethernet Handler
SL            35  Serial Line Handler
TKR           45  Token Ring Handler
X25           53  X.25 Protocols
FDDI          27  FDDI Handler
SDLC          95  IBM SDLC
FRL           97  Frame Relay
PPP          186  Point-to-Point
X251          16  X.25-Physical-Layer
X252          34  X.25-Frame-Layer
X253          42  X.25-Packet-Layer
ISDN          43  Integrated Services Digital Network
IPPN           4  IP Protocol Net
WRS           33  WAN Restoral
LNM           60  LNM
```

```
LLC       168     Logical Link Control
BGP        74     Border Gateway Protocol
MCF         9     MAC Filtering
DLS       497     Data Link Switching
V25B       28     CCITT/ITU V.25bis
BAN        29     Boundary Access Node
COMP       26     Data Compression Engines
NBS        50     NetBIOS Support Subsystem
ATM       216     Asynchronous Transfer Mode
LEC       174     ATM LAN Emulation Client
APPN       28     Advanced Peer-to-Peer Networking
ILMI       23     ATM Interim Local Management Interface
SAAL       26     ATM Signalling ATM Adaptation Layer
SVC        26     ATM Signalling
LES       361     LAN Emulation Services
LECS      145     LAN Emulation Configuration Server
EVLOG       1     EventLog() error logging system
NOT        15     Forwarder messages not loaded
NHRP      211     Next Hop Resolution Protocol
XTP        58     X.25 Transport


LCS        22     LCS Handler
LSA        61     LSA Handler
MPC        30     MPC Handler
SCSP       34     Server Cache Synchronization Protocol
ALLC       36     ATM LLC (RFC1483)
NDR        38     Network Dispatcher Router Feature
MLP        93     Multilink-PPP
SEC        30     Security Protocols
ENCR        4     Data Encryption Engines
PM          6     Presence Manager
DGW         9     Default Gateway
QLLC       54     QLLC-Packet-LayerName  Events  Description
VLAN       20     Virtual LAN
```

subsystem *subsystem.name*

指定されたサブシステムに関するすべてのイベント、ログ・レベル、およびメッセージを表示します。

例:

```
list subsystem eth

Event      Level      Message
ETH.001    P-TRACE    brd rcv unkwn type packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.002    UE-ERROR   rcv unkwn typ packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.010    C-INFO     LLC unk SAP DSAP source_Ethernet_address ->
                      destination_Ethernet_address nt network
```

subsystems all

すべてのイベント、ログ・レベル、およびルーター上で発生した各イベントのすべてのメッセージをリストします。

trace-status

構成および実行時情報を含めて、ATM パケット・トレースの状態に関する情報を表示します。

例:

```
list trace-status

------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:OFF  HD Shadowing:OFF
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Default Packet Bytes Traced:100  Max Packet Bytes Traced:256
----------------------- Run-time Status ---------------------------
Packets in RAM Trace Buffer:535   Free Trace Buffer Memory:180
Trace Errors:22  First Packet:23  Last Packet:557
Trace Buffers Shadowed to HD:0  Trace Buffer File Size:0
```

- STOP-ON-EVENT アクションが発生すると、LIST TRACE-STATUS 画面の『Trace Status』 は OFF を示します。

- STOP-ON-EVENT アクションが発生するか、タイム・リミットを超過すると、LIST TRACE-STATUS 画面の 『HD Shadowing』 は OFF を示します。
- トレース・ファイルで折り返しが行われると、『Trace Buffer File Size』 は 『<wrapped>』 を表示します。
- シャドー・ディスクのタイム・リミットを超過したが、時間が満了した以降はトレース・レコードが書き込まれていない場合には、『 HD-Shadowing Time Exceeded? NO <Next trace will turn it OFF>』 が表示されます。次のトレース・レコードが書き込まれると、『HD-Shadowing Time Exceeded? YES』 が表示されます。

talk 6 の下の ELS Config>**LIST TRACE** コマンドは、次のような情報を表示します。

```
------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
```

Nodisplay

nodisplay コマンドは、コンソール上のメッセージ表示を選択して、オフにするのに使用します。

構文:

nodisplay event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
指定されたイベントに関するメッセージの表示を抑制します。

group *group.name*
指定されたグループ (*group.name*) に以前に追加されたメッセージの表示を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージを表示を抑制します。

例:

```
nodisplay range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 の表示を抑制します。

subsystem *subsystem.name*
指定されたサブシステム (*logging level*) に関連するメッセージの表示を抑制します。

Noremote

noremote コマンドは、リモート・ワークステーションへのログを選択し、それをオフにするのに使用します。

構文:

noremote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
指定されたイベントのメッセージのリモート・ログ記録を抑制します。

group *group.name*
以前に指定されたグループ (*group.name*) に追加されたメッセージのリモート・ログ記録を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージのリモート・ログ記録を抑制します。

例:

```
noremote range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のリモート・ログ記録を抑制します。

subsystem *subsystem.name*
指定されたサブシステム (*logging level*) に関連するメッセージのリモート・ログ記録を抑制します。

例:

```
noremote subsystem tkr
```

注: Noremote では、Remote の場合のように、Syslog ファシリティー値とレベル値を指定する必要はありません。

remote および **noremote** コマンドを使用して設定した内容を確認する場合は、**list event** および **list active** コマンドを使用します。

Notrace

notrace コマンドは、選択されたトレース・イベントのモニターの表示を停止するのに使用します。

構文:

notrace event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*
指定されたトレース・イベントの表示を抑制します。

group *groupname*
指定されたグループ (*groupname*) に関連するトレース・イベントの表示を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの一定範囲のメッセージのパケット・トレース・データの送信を使用不可にします。

例:

```
notrace range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のパケット・トレース・データの送信を抑制します。

subsystem *subsystemname [logging-level]*
指定されたサブシステムとログ・レベルに関連したトレース・イベントの表示を抑制します。 *logging-level* を指定しないと、そのサブシステムのすべてのログ・レベルのトレースが抑制されます。

例:

```
notrace subsystem atm error
notrace subsystem atm
```

Notrap

notrap コマンドは、メッセージを選択してオフにし、SNMP トラップでネットワーク管理ステーションに送信されないようにするのに使用します。

構文:

notrap event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*
指定されたメッセージの SNMP トラップでの送信 (*subsystem.event#*) を抑制します。

group *groupname*
指定されたグループ (*groupname*) に以前に追加されたメッセージの SNMP トラップでの送信を抑制します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のイベントのメッセージの SNMP トラップでの送信を抑制します。

例:

```
notrap range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 のメッセージの SNMP トラップでの送信を抑制します。

subsystem *subsystemname [logging-level]*

指定されたサブシステムとログ・レベルに関連したメッセージの SNMP トラップでの送信を抑制します。 *logging-level* を指定しないと、そのサブシステムのすべてのログ・レベルのトラップが抑制されます。

例:

```
notrap subsystem tkr error
```

Packet Trace

packet-trace コマンドは、種々のサブシステムに関するパケット・トレース情報を表示/使用可能/使用不可にするのに使用します。このコマンドは **Trace** コマンドに似た機能を提供します。

構文:

packet-trace

Packet Trace の使用を終了するときは、**Exit** コマンドを使用します。

コマンドについての詳しい説明は、213ページの『パケット・トレース監視コマンド』を参照してください。

Remote

remote コマンドは、イベント番号、イベントの範囲、グループ、またはサブシステムに基づいて、リモート・ログ・ファイルに記録するイベントを選択するのに使用します。

構文:

remote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event# syslog_facility syslog_level*

指定されたイベントをリモート・ログに記録します。

リモート・ワークステーションの syslog デーモンは、Syslog ファシリティー値とレベル値を使用して、メッセージを記録する場所を判別します。この値は、**set facility** および **set level** コマンドを使用して設定したデフォルト値をオーバーライドします。

syslog_facility

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

これらの値は、IBM 2210 上のデーモンと特別な関連はありません。リモート・ワークステーション上の syslog デーモンによって使用される識別子にすぎません。

例:

```
remote event gw.019 log_user log_info
```

group *group.name syslog_facility syslog_level*
指定されたグループに属するイベントを、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログに記録することができます。203ページの『remote event コマンド』を参照してください。

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のイベントを、*syslog_facility* と *syslog_level* に基づいて、リモート・ログに記録します。 203ページの『remote event コマンド』を参照してください。

例:

```
remote range gw 19 22 log_user log_info
```

イベント gw.19、gw.20、gw.21、および gw.22 が、log_user の *syslog_facility* 値と log_info の *syslog_level* 値によって指定されたリモート・ログ・ファイルに記録されます。

subsystem *subsystem.name message_level syslog_facility syslog_level*

ここで、*subsystem.name* はサブシステムの名前、*message_level* は、サブシステム内の選択されたメッセージのレベルです。

指定された *subsystem.name* の中の、*message_level* が指定の *message_level* に一致するイベントが、*syslog_facility* 値と *syslog_level* 値に基づいて、リモート・ログ記録されます。 203ページの『remote event コマンド』を参照してください。

Message_level の値は、『ALL』、『ERROR』、『INFO』、または『TRACE』 です。 156ページの『ログ・レベル』を参照してください。 **remote** コマンドで指定された値は、サブシステム内の特定のイベントにコーディングされた値と一致していなければなりません。そうでない場合、サブシステム内のそのイベントはリモート・ログに記録されません。

例:

```
remote subsystem TKR all log_user log_info
```

上の例では、サブシステム TKR 内のすべてのメッセージ (『all』には、『error』、『info』、または 『trace』 として符号化されているメッセージがすべて含まれます) が、log_user 値と log_info の値に基づいて、リモート・ホストのログに記録されます。

remote および **noremote** コマンドを使用して設定した内容を確認する場合は、**list event** および **list active** コマンドを使用します。

Remove

remove コマンドは、保管されている情報を消去して、メモリーを解放するのに使用します。以前に **save** コマンドを使用して現行構成を保管した場合、remove を使用すると、保管した構成を消去することができます。

構文:

remove

Restore

restore コマンドは、すべての現行設定値 (カウンターを除く) をクリアし、初期 ELS 構成を再ロードするのに使用します。現行設定値を保存する場合は、初期構成に復元する前に **save** コマンドを使用します。

構文:

restore

Retrieve

retrieve コマンドは、保管された ELS 構成を再ロードするのに使用します。以前に **save** コマンドを使用して現行構成を保管した場合、**retrieve** を使用してそれを再ロードします。 **Retrieve** を実行しても、保管された構成は消去されません。保管された構成を消去するには、**remove** コマンドを使用します。

構文:

retrieve

Save

save コマンドは、現行構成 (カウンターを除く) を保管するのに使用します。 **Save** は、デフォルト構成 (構成コマンドを用いて設定した構成) には影響を与えません。監視コマンドを用いて構成を変更した後に **save** を使用するのは、リスタート後もこの構成を保存したい場合です。保管された構成は、一度に 1 つしか存在できません。保管された構成を再ロードするには、**retrieve** コマンドを使用します。

構文:

save

Set

set コマンドは、1 秒当りの最大トラップ数の設定、タイム・スタンプ機能の設定、またはトレース・オプションの設定に使用します。

構文:

set pin . . .
remote-logging . . .
timestamp . . .
trace . . .

pin ピン・パラメーターを秒単位で送信できるトラップの最大数に設定するのには、**set pin** コマンドを使用します。内部で、ピンは 10 分の 1 秒ごとにリセットされます。 (10 分の 1 の数 (*max_traps*) が、10 分の 1 秒ごとに送信されます。)

remote-logging

set remote-logging コマンドは、リモート・ログ記録オプションを構成するのに使用します。これらのオプションを監視環境から構成した場合、変更は即時に有効になり、装置がリブートされると以前に構成された設定値に戻ります。

構文:

set remote-logging on

off
facility . . .
level . . .
local_id
remote_ip_addr . . .
source_ip_addr ...

on リモート・ログ記録をオンにします。これでリモート・ログ記録が使用可能になり、**remote** コマンドで選択したメッセージを記録することができます。

off リモート・ログ記録をオフにします。 **remote** コマンドによって選択されたすべてのメッセージがログに記録されなくなります。

facility
リモート・ワークステーションの syslog デーモンが、メッセージを記録する場所を判別するために、*level* 値と組み合わせて使用する値を指定します。 **remote** コマンドを使用して、特定の ELS イベント、範囲、グループ、またはサブシステムに対して異なる値を指定しない限り、この値がすべてのリモート・ログ記録 ELS メッセージに適用されます。

すべての可能な syslog ファシリティー値は、次のとおりです。

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

level リモート・ワークステーションの syslog デーモンが、メッセージを記録する場所を判別するために、*facility* 値と合わせて使用する値を指定します。 **remote** コマンドを使用して、特定の ELS イベント、範囲、グループ、またはサブシステムに対して異なる値を指定しない限り、この値がすべてのリモート・ログ記録 ELS メッセージに適用されます。

すべての可能な syslog レベル値は、次のとおりです。

log_emerg
log_alert
log_crit

log_err

log_warning

log_notice

log_info

log_debug

local_id

リモート・ログ・メッセージに表示され、特定のメッセージを記録したマシンを識別するのに役立つ、1 ～ 32 文字の識別子を指定します。

remote_ip_addr

これは、ログ・ファイルが存在するリモート・ホストの IP アドレスです。

source_ip_addr

リモート・ログ記録するメッセージを発信したマシンの IP アドレスを指定します。

リモート・ログ ELS メッセージに示された IP アドレスまたはホスト名を識別しやすくするために、2210 に構成された IP アドレスを使用することが必要です。また、この IP アドレスは、ネーム・サーバーが速やかにホスト名に変換できること、あるいは少なくともネーム・サーバーが速やかに 『address not found』を応答できるものであることを確認する必要があります。

IP アドレスの解決が適切に行われるかどうかを調べるには、ユーザーのワークステーションで、次のような **host** コマンドを入力してみます。

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

応答に 1 秒以上かかる場合は、もっと迅速に解決できる IP アドレスを選択してください。

timestamp

メッセージ・タイム・スタンプをオンにして、時刻またはアップタイム (日付はなく、ルーターの最後の初期化以降の時間、分、および秒数) が、各メッセージの横に表示したり、あるいはメッセージ・タイム・スタンプをオフにしたりすることができます。

注: タイム・スタンプをオンにする場合は、CONFIG プロセスに戻り、time コマンドを使用してルーターの日付と時刻を設定することを忘れないようにしてください。そうしないと、すべてのメッセージに 00:00:00 が表示されるか、時間、分、または秒数 (あるいは、その全部) に負数が表示される (たとえば、00:-4:-5) ことになります。

set timestamp コマンドを使用して、以下のタイム・スタンプ・オプションの 1 つを使用可能にします。

timeofday

1 日 24 時間での発生時刻を示す HH:MM:SS プレフィックスを、各メッセージに追加します。

uptime
ルーターのアップタイムの 100 時間周期における発生時刻を示す HH:MM:SS プレフィックスを、各メッセージに追加します。アップタイム 100 時間後に、アップタイム・カウンターはゼロに戻り、別の 100 時間周期を開始します

off ELS タイム・スタンプ・プレフィックスをオフにします。

構文:

set timestamp [timeofday or uptime or off]

trace トレース・オプションを構成するのには、**set trace** コマンドを使用します。トレース・オプションを監視環境から構成した場合、変更は即時に有効になり、装置がリブートされると以前に構成された設定値に戻ります。

構文:

set trace decode . . .
default-bytes-per-pkt . . .
max-bytes-per-pkt . . .
off
on
reset
wrap-mode . . .

decode [off or on]
パケットの復号をオンまたはオフにします。パケット復号は、すべてのコンポーネントによってサポートされているとは限りません。

default-bytes-per-pkt *bytes*
デフォルトのトレースされるバイト数を設定します。トレースを行うコンポーネントによって値が指定されない場合、この値が使用されます。

max-bytes-per-pkt *bytes*
各パケットごとに、トレースされる最大バイト数を設定します。

off パケット・トレースを使用不可にします。

on パケット・トレースを使用可能にします。

reset トレース・バッファーをクリアし、すべての関連のカウンターをリセットします。

wrap-mode *off/on*
トレース・バッファー折り返しモードをオフにします。折り返しモードが使用可能のときにトレース・バッファーが満杯の場合、トレースを継続するのに必要なため、前のトレース・レコードが新しいトレース・レコードによって上書きされます。

Statistics

statistics コマンドは、すべての利用可能なサブシステムとその統計のリストを表示するのに使用します。

注: 以下の例は、ご使用のディスプレイとは正確に一致しない場合があります。コマンドの出力は、導入されているソフトウェアのバージョンおよびリリースによって異なります。

構文:

statistics

例:

```
statistics

Subsys  Vector  Exist   String  Active    Heap

  GW     105     101      3411     0         0
 FLT      20       7       184     0         0
 BRS      50       5       201     0         0
 ARP     150     142      7030     0         0
  IP     100     100      2463     2        20
ICMP      30      21       529     0         0
 TCP      60      57      2420     0         0
 UDP      10       6       179     0         0
 BTP      40      13       695     0         0
 RIP      30      22       474     0         0
OSPF      80      73      2859     0         0
MSPF      40      17       593     0         0
TFTP      35      29       819     0         0
SNMP      30      28       821     0         0
 DVM      30      21       589     0         0
  DN     140     115      5842     0         0
  XN      35      21       780     0         0
 IPX     110     110      4705     0         0
CLNP      80      58      1763     0         0
ESIS      40      24       716     0         0
ISIS      80      58      2422     0         0
DNAV      50      26      1314     0         0
 AP2      80      70      1755     0         0
ZIP2      60      51      1859     0         0
R2MP      50      38      1185     0         0
 VIN      90      79      3159     0         0
 SRT     120      94      5040     0         0
 STP      60      32      1590     0         0
  BR      50      30      1616     0         0
SRLY      30      28      1409     0         0
 ETH      60      47      1098     0         0
  SL      50      35       584     0         0
 TKR      60      45      2031     0         0
 X25      70      53      1909     0         0
FDDI      30      27      1155     0         0
SDLC     100      95      4263     0         0
 FRL     130      97      6068     0         0
 PPP     190     186      6394     0         0
X251      50      16       546     0         0
X252      50      34       996     0         0
X253      50      42      1649     0         0
ISDN      50      43      1994     0         0
IPPN      20       4       132     0         0
 WRS      40      33      1938     0         0
 LNM      70      60      3137     0         0
 LLC     170     168      9840     0         0
 BGP      80      74      2477     0         0
 MCF      15       9       244     0         0
 DLS     500     497     24340     0         0
 V25B     30      28      1058     0         0
 BAN      30      29      1223     0         0
 COMP     80      26      1050     0         0
 NBS     100      50      3029     0         0
 ATM     300     216     10808     0         0
 LEC     200     174      7258     0         0
```

```
APPN     100      28       467     0         0
ILMI     150      23       487     0         0
SAAL      30      26       621     0         0
 SVC      30      26       465     0         0
 LES     400     361     22333     0         0
LECS     150     145      5666     0         0

EVLOG      1       1       105     0         0
 NOT      25      15       508     0         0
NHRP     250     211      8193     0         0
 XTP      64      58      2271     0         0
 ESC     150      67      3122     0         0
 LCS      40      22       858     0         0
 LSA      70      61      3506     0         0
 MPC     130      30      1677     3        44
SCSP      40      34      1234     0         0
ALLC      50      36      1842     0         0
 NDR      50      38      1150     0         0
 MLP     100      93      4006     0         0
 SEC      50      30       688     0         0
ENCR     100       4       194     0         0
  PM      25       6       120     0         0
 DGW      20       9       238     0         0
QLLC      55      54      2411     0         0

Total   6490    4942    215805     5        64

Maximum:7976 vector, 155 subsystem
Memory:71784/620 vector+ 81256/217714 data+ 64 heap=371438Subsys
```

Subsys
サブシステムの名前

Vector
サブシステムの最大サイズ

Exist このサブシステム内で定義されているイベントの数

String このサブシステム内でメッセージの記憶に使用されるバイト数

Active サブシステム内の活動 (表示されるか、トラップされるか、またはカウントされた) イベントの数

Heap サブシステムにより使用中の動的メモリー

Trace

trace コマンドは、システム・モニターに表示するトレース・イベントを選択するのに使用します。このコマンドは、213ページの『パケット・トレース監視コマンド』に説明されている **packet trace** コマンドに似た機能を提供します。

構文:

trace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
指定されたトレース・イベント (*subsystem.event#*) をシステム・モニターに表示します。

group *groupname*
指定されたグループに以前に追加されたトレース・イベントを、ルーター・モニターに表示します。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のトレース・イベントを、システム・モニターに表示します。

例:

```
trace range gw 19 22
```

トレース・イベント gw.19、gw.20、gw.21、および gw.22 を、システム・モニターに表示します。

subsystem *subsystemname*
指定されたサブシステムに関連するトレース・イベントを、ルーター・モニターに表示できるようにします。

Trap

trap コマンドは、リモート SNMP ネットワーク管理ワークステーションに送信するメッセージを選択するのに使用します。リモート SNMP ネットワーク管理ワークステーションは、SNMP マネージャーとして働くネットワーク内の IP ホストです。

構文:

trap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
指定されたメッセージ (*subsystem.event#*) が SNMP でネットワーク管理ワークステーションに送信されるようにします。

group *groupname*
指定されたグループに以前に追加されたメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

range *subsystemname first_event_number last_event_number*

ここで、*first_event_number* は指定されたイベント範囲の最初のイベントの番号で、*last_event_number* は指定されたイベント範囲の最後のイベントの番号です。

指定されたサブシステムの指定された範囲のメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

例:

```
trap range gw 19 22
```

イベント gw.19、gw.20、gw.21、および gw.22 内のメッセージが、SNMP トラップでネットワーク管理ワークステーションに送信されるようにします。

subsystem *subsystemname*
指定されたサブシステムに関連するメッセージが、SNMP トラップで管理ステーションに送信されるようにします。

注: IP、ICMP、ARP、および UDP サブシステムのメッセージは、SNMP トラップで送信することはできません。これらの区域は SNMP トラップを送信する過程で使用されているか、使用される可能性があるからです。これはトラフィックの無限のループを招いて、ルーターに不当な負担をかけることになります。

View

view コマンドは、トレース・パケットを表示するのに使用します。

構文:

view current
first
jump
last
next
prev
search ...

current
現行のトレース・パケットを表示します。現行パケットが無効の場合は、トレース・バッファー内の最初のパケットが表示されます。

first トレース・バッファー内の最初のトレース・パケットを表示します。

jump *n*
現行パケットから *n* パケット前または後のトレース・パケットを表示します。

last トレース・バッファー内の最後のトレース・パケットを表示します。

next 次のトレース・パケットを表示します。

prev 直前のトレース・パケットを表示します。

search *hexstring*
指定された 16 進ストリングが入っている、次のトレース・パケットを表示します。

パケット・トレース監視コマンド

この節では、Packet-trace 監視コマンドについて説明します。 Packet-trace 監視環境にアクセスした後、`ELS Packet Trace>` プロンプトから Packet-trace 監視コマンドを入力することができます。

表 23. パケット・トレース監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Off	パケット・トレースを使用不可にします。
On	パケット・トレースを使用可能にします。メモリー・トレース・バッファー・サイズの入力を求めるプロンプトが出ます (前に設定されていない場合)。
Reset	トレース・バッファーをクリアし、すべての関連カウンターをリセットします。
Set	トレース・オプションを構成します。
Subsystems	ATM サブシステムのトレースを起動するか、または要約を表示します。
Trace-status	構成および実行時情報を含めて、ATM パケット・トレースの状態に関する情報を表示します。
View	取り込まれたパケット・トレース・バッファーをコンソールに表示する機能を提供します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Off

off コマンドは、パケット・トレースを使用不可にするのに使用します。

構文:

off

On

on コマンドは、パケット・トレースを使用可能にするのに使用します。

構文:

on

Reset

reset コマンドは、トレース・バッファーをクリアし、すべての関連カウンターをリセットするのに使用します。

構文:

reset

Set

set コマンドは、トレース・オプションを構成するのに使用します。

構文:

set decode
default-bytes-per-pkt
disk-shadowing

max-bytes-per-pkt

memory-trace-buffer-size

stop-event

wrap-mode

exit

set コマンドの説明は、206ページの『Set』 を参照してください。

Subsystems

subsystems コマンドは、ATM サブシステムのトレースを起動するか、または要約を表示するのに使用します。

構文:

subsystems atm

lec

summary

例:

```
subsystems atm
Network number? 0
ATM Interface is selected
on | off | list [list]? on
Note that SVC  uses VPI = 0, VCI = 5
and ILMI uses VPI = 0, VCI = 16
Beginning of VPI range [0]?
End of VPI range [0]?
Beginning of VCI range [0]? 16
End of VCI range [0]? 16
Tracing event ATM.88: ATM frames
```

例:

```
subsystems lec
Network number? 1
ATM Emulated LAN is selected
on | off | list [list]? on
Trace which types of frames (data, control, both) [both]?
Tracing event LEC.11: data frames over ATM Forum LEC: interface 1
Tracing event LEC.12: control frames over ATM Forum LEC: interface 1
Note that if the user DISABLEs and TESTs this LEC interface,
the LEC trace settings from Talk 6 Config will take effect.
```

例:

```
subsystems summary
Subsystems Being Traced

ATM        net number = 0, VPI Range:     0 -     0
                           VCI Range:    16 -    16
LEC        net number = 1
```

Trace-Status

trace-status コマンドは、パケット・トレースに関する更新情報を入手するのに使用します。

構文:

trace-status

例:

```
trace-status
------------------------- Configuration -----------------------------
Trace Status:OFF  Wrap Mode:OFF  Decode Packets:OFF  HD Shadowing:OFF
RAM Trace Buffer Size:0  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: None
Maximum Hours to HD Shadow:  24
----------------------- Run-time Status ---------------------------
Packets in RAM Trace Buffer:0   Free Trace Buffer Memory:0
Trace Errors:0  First Packet:0  Last Packet:0
Trace Records Stored on HD:0  Trace Buffer File Size:0
HD-Shadowing Time Exceeded? NO
Has Stop Trace Event Occurred? NO
```

View

view コマンドは、取り込まれたパケット・トレース・バッファーをモニターに表示する環境に入るのに使用します。

view コマンドの説明は、213ページの『View』 を参照してください。

構文:

view	current
	first
	jump
	last
	next
	prev
	search *hexstring*
	exit

ELS ネット・フィルター監視コマンド

この節では、ELS ネット・フィルターを操作するためのコマンドについて説明します。フィルター環境に入るには、ELS> プロンプトで **filter net** コマンドを入力します。次に、ELS Filter net> プロンプトで監視コマンドを入力します。

表 24. ELS ネット・フィルター監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Create	フィルターを作成し、それに番号を割り当てます。最大 64 のフィルターを作成できます。
Delete	指定されたフィルター番号またはすべてのフィルターを削除します。
Disable	指定されたフィルター番号またはすべてのフィルターを使用不可にします。
Enable	指定されたフィルター番号またはすべてのフィルターを使用可能にします。

表 24. ELS ネット・フィルター監視コマンド (続き)

コマンド	機能
List	指定されたフィルター番号またはすべてのフィルターをリストにします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Create

create コマンドは、ELS ネット・フィルターを作成するのに使用します。

構文:

create *queue* event *event_name net#_start net#_end*

range *event_range net#_start net#_end*

subsystem *subsystem_name net#_start net#_end*

queue フィルターを設定する待ち行列。有効な待ち行列は、次のとおりです。

Display

Trace

Trap

Remote

event *event_name net#_start net#_end*

フィルターに掛けるイベントとネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1 つのネット番号をフィルターに掛けることになります。

コマンド **create trap event GW.009 2 10** は、ネット番号 2 〜 10 のメッセージ GW.009 のトラップをフィルターに掛けます。

range *event_range net#_start net#_end*

フィルターに掛ける ELS メッセージの範囲とネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1 つのネット番号をフィルターに掛けることになります。

コマンド **create remote range ipx 19 22 3 6** は、リモート・ログ記録用の、ネット番号 3 〜 6 の IPX.019 で始まり IPX.022 で終わるすべての IPX メッセージをフィルターに掛けます。

subsystem *subsystem_name net#_start net#_end*

フィルターに掛けるサブシステムとネット番号を指定します。

net#_start と *net#_end* を同じ番号として指定した場合、1 つのネット番号をフィルターに掛けることになります。

コマンド **create display subsys ip 1 1**, は、ディスプレイへの、ネット番号 1 を含む IP サブシステムのすべての ELS メッセージをフィルターに掛けます。その他の IP サブシステム・メッセージはすべて廃棄します。

Delete

delete コマンドは、特定の ELS フィルターまたはすべての ELS フィルターを削除するのに使用します。

構文:

delete all
filter *filter#*

all 現在構成されているすべてのフィルターを削除します。

filter *filter#*
filter# によって指定されたフィルターを削除します。削除したいフィルターの番号を入手するには、**list** コマンドを使用します。

Disable

disable コマンドは、特定の ELS フィルターまたはすべての ELS フィルターを使用不可にするのに使用します。

構文:

disable all
filter *filter#*

all 現在構成されているすべてのフィルターを使用不可にします。

filter *filter#*
filter# によって指定されたフィルターを使用不可にします。使用不可にしたいフィルターの番号を入手するには、**list** コマンドを使用します。

Enable

enable コマンドは、特定の ELS フィルターまたはすべての ELS フィルターを使用可能にするのに使用します。

構文:

enable all
filter *filter#*

all 現在構成されているすべてのフィルターを使用可能にします。

filter *filter#*
filter# によって指定されたフィルターを使用可能にします。使用可能にしたいフィルターの番号を入手するには、**list** コマンドを使用します。

List

list コマンドは、特定の ELS フィルターまたはすべての ELS フィルターをリストするのに使用します。

構文:

list all
filter *filter#*

all 現在構成されているすべてのフィルターをリストします。

filter *filter#*

filter# によって指定されたフィルターをリストします。

第14章 性能の構成および監視

この章では、性能監視の構成コマンドと動作コマンドについて説明します。本章には、以下の節が含まれています。

- 『性能構成環境へのアクセス』
- 『性能構成コマンド』
- 222ページの『性能監視環境へのアクセス』
- 223ページの『性能監視コマンド』

性能構成環境へのアクセス

性能監視構成プロセスにアクセスするには、以下の手順で行います。

1. OPCON プロンプトで、**talk 6** と入力する。 (このコマンドの詳細については、ソフトウェア使用者の手引きの*OPCON プロセスおよびコマンド*の章を参照してください。) たとえば、次のように入力します。

   ```
   * talk 6
   Config>
   ```

   talk 6 コマンドを入力すると、CONFIG プロンプト (Config>) が端末に表示されます。最初に構成に入ったときにプロンプトが表示されない場合は **Return** をもう一度押してください。
2. CONFIG プロンプトで **perf** コマンドを入力して、PERF Config> プロンプトを表示する。

性能構成コマンド

性能を構成するには、PERF Config> プロンプトでコマンドを入力します。

表 25. PERF 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Disable	CPU 使用率統計の収集または Talk 2 ELS モニター出力を使用不可にします。
Enable	CPU 使用率統計の収集または Talk 2 ELS モニター出力を使用可能にします。
List	構成をリストします。
Set	報告期間を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Disable

disable コマンドは、CPU 使用率統計の収集および talk 2 ELS モニター出力を使用不可にするのに使用します。

性能構成コマンド (Talk 6)

構文:

disable cpu statistics

t2 output

Enable

enable コマンドは、CPU 使用率統計の収集および `talk 2` ELS モニター出力を使用可能にするのに使用します。

構文:

enable cpu statistics

t2 output

List

list コマンドは、性能監視構成を表示するのに使用します。

構文:

list

Set

set コマンドは、報告期間を設定するのに使用します。

構文:

set *time*

time ショート・ウィンドウ・タイムを指定します。

有効値: 2 ～ 30 秒

デフォルト値: 2

性能監視環境へのアクセス

性能監視コマンドにアクセスするには、以下の手順で行います。このプロセスにより、性能監視 プロセスにアクセスできます。

1. OPCON プロンプトで、**talk 5** と入力する。 (このコマンドの詳細については、ソフトウェア使用者の手引きの*OPCON プロセスおよびコマンド*の章を参照してください。) たとえば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、GWCON プロンプト (+) が端末に表示されます。最初に構成に入ったときにプロンプトが表示されない場合は **Return** をもう一度押してください。

2. + プロンプトで **perf** コマンドを入力して、`PERF Console>` プロンプトを表示する。

   例:

```
+ perf
PERF Console>
```

性能監視コマンド

この節では、性能監視コマンドについて説明します。

表 26. PERF 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Clear	CPU 使用率高基準統計をクリアし、報告期間をリセットして新しいサイクルにします。
Disable	CPU 使用率統計の収集または Talk 2 ELS モニター出力を使用不可にします。
Enable	CPU 使用率統計の収集または Talk 2 ELS モニター出力を使用可能にします。
List	構成をリストします。
Report	性能統計の報告を表示します。
Set	報告期間を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Disable

disable コマンドは、CPU 使用率統計の収集および talk 2 ELS モニター出力を使用不可にするのに使用します。

構文:

disable cpu statistics

t2 output

Enable

enable コマンドは、CPU 使用率統計の収集および talk 2 ELS モニター出力を使用可能にするのに使用します。

構文:

enable cpu statistics

t2 output

List

list コマンドは、性能監視構成を表示するのに使用します。

構文:

list

Report

report コマンドは、性能監視統計を表示するのに使用します。

構文:

report

例:

```
PERF Console>report
------------------------------------------------------------
KEY:  SW = Short Window = 9 seconds
KEY:  LW = Long Window =  9.0 minutes  (60 x SW)

  CPU UTIL :   Most recent SW                     = 38%
               Most recent LW                     = 33%
               Highest for all SW's               = 92%
               Highest for all LW's               = 52%
               % of time cpu util (SW) was > 60%  = 16%
               % of time cpu util (SW) was > 70%  = 15%
               % of time cpu util (SW) was > 80%  = 1%
               % of time cpu util (SW) was > 90%  = 0%
               % of time cpu util (SW) was > 95%  = 0%
------------------------------------------------------------
```

Set

set コマンドは、報告期間を設定するのに使用します。

構文:

set *time*

time ショート・ウィンドウ・タイムを指定します。

有効値: 2 ～ 30 秒

デフォルト値: 2

第3部 インターフェースの概要、構成、および動作

第15章 ネットワーク・インターフェースの開始

この章では、ルーターによってサポートされるネットワーク・インターフェースおよびリンク・レイヤー・プロトコルの構成と監視の方法について説明します。この章の目的は、いくつかの基本的な構成と監視に関するガイドラインを示すことです。また、GWCON **interface** コマンドを用いてインターフェースを監視するのに必要な基本的な手順および情報も提供します。本章には、以下の節が含まれています。

- 『先に進む前に』
- 『ネットワーク・インターフェースと GWCON インターフェース・コマンド』
- 『ネットワーク・インターフェースの構成プロセスおよびコンソール・プロセスへのアクセス』
- 228ページの『リンク・レイヤー・プロトコルの構成プロセスおよびコンソール・プロセスへのアクセス』
- 228ページの『予備インターフェースの定義』

先に進む前に

先に進む前に、ネットワーク・インターフェース構成プロセスにアクセスするのに必要な手順を十分に理解しておいてください。

これらの手順についての詳しい情報は、本章の以下の節を参照してください。

ネットワーク・インターフェースと GWCON インターフェース・コマンド

ネットワーク・インターフェースの構成時に、特定のインターフェースについての特定の情報を表示することが必要になる場合があります。一部のインターフェースは、それぞれ独自の監視用コンソール・プロセスを備えていますが、GWCON 環境から **interface** コマンドを使用すると、ルーターはすべての 導入済みのネットワーク・インターフェースの統計を表示します。 (143ページの『Interface』 を参照してください。)

ネットワーク・インターフェースの構成プロセスおよびコンソール・プロセスへのアクセス

以下に示す参照個所には、背景情報と、インターフェースの構成プロンプトおよびコンソール・プロンプトにアクセスする方法の例が示されています。

インターフェースの構成プロセスおよびコンソール・プロセスへのアクセスに関する詳しい情報は、18ページの『ネットワーク・インターフェースの構成プロセスと動作プロセスへのアクセス』、18ページの『ネットワーク・インターフェース構成プロセスへのアクセス』、および 21ページの『ネットワーク・インターフェース・コンソール・プロセスへのアクセス』 を参照してください。これらのプロセスにアクセ

スすると、ルーターで使用されているネットワーク・インターフェースのソフトウェア構成可能パラメーターの変更や監視を行うことができます。

リンク・レイヤー・プロトコルの構成プロセスおよびコンソール・プロセスへのアクセス

プロトコルの構成プロセスおよびコンソール・プロセスへのアクセスについての詳しい情報は、3ページの『第1章 開始』 を参照してください。これらのプロセスにアクセスすると、ルーターによってサポートされているリンク・レイヤー・プロトコルの構成可能パラメーターの変更や監視を行うことができます。

予備インターフェースの定義

装置上に現在は存在していないインターフェースを定義することが必要になる場合があります。装置のこの***動的再構成*** は、装置を構成する際に予備インターフェースを定義しておき、装置が存在するようになったときに、コンソール・プロセスを使用して起動する方法で行います。詳しくは、49ページの『予備インターフェースの構成』 および 134ページの『Activate』 を参照してください。

第16章 IEEE 802.5 トークンリング・ネットワーク・インターフェースの構成

この章では、トークンリング・インターフェースの構成コマンドと動作コマンドについて説明します。本章には、以下の節が含まれています。

トークンリング・インターフェース構成プロセスへのアクセス

TKR config> プロンプトを表示するには、network コマンドに続けて、トークンリング・インターフェースのインターフェース番号を入力します。たとえば、次のように入力します。

```
Config>network 0
Token-Ring interface configuration
TKR Config>
```

Config> プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。

注: パラメーターを変更した場合は、必ずルーターをリスタートして、その変更を有効にする必要があります。

トークンリング構成コマンド

この節では、トークンリング構成コマンドについて説明します。コマンドは TKR config> プロンプトで入力します。 表27 は、トークンリング構成コマンドをリストしています。

表 27. トークンリング構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	選択されたトークンリング・インターフェース構成を表示します。
LLC	LLC 構成環境およびサブコマンドにアクセスします。
Media	媒体タイプを shielded (シールド付き) または unshielded (シールドなし) として設定します。
Packet-size	すべてのトークンリング・ネットワークのパケット・サイズのデフォルト値を変更します。
Set	RIF キャッシュの経時タイマーおよび物理 (MAC) アドレスを設定します。
Source-routing	インターフェース上の送信ルーティングを使用可能または使用不可にします。
Speed	インターフェースの速度を Mbps 単位で設定します。

表 27. トークンリング構成コマンドの要約 (続き)

コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、トークンリングの現行構成を表示するのに使用します。

注: MAC アドレスが 0 のときは、デフォルトの端末アドレスが使用されます。

構文:

list

例:

```
list
Token-Ring configuration:

    Packet size (INFO field): 2052
Speed:                    16 Mb/sec
Media:                    Shielded

RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
```

Packet size
トークンリング・パケットのサイズ

Speed ネットワークの速度

Media ネットワークが使用する媒体のタイプ（シールドまたは非シールド)

RIF Aging Timer
ルーティング情報フィールド (RIF) に入っている情報をルーターが保持する時間の長さ

Source Routing
ソース・ルーティング機能の状態（使用可能または使用不可)。

MAC Address
set physical-address コマンドを用いて設定した、構成済みの MAC アドレス。オール 0 が表示された場合、その MAC アドレスはデフォルト・アドレスです。

LLC

LLC コマンドは、LLC 構成環境にアクセスするのに使用します。各コマンドについての説明は、241ページの『LLC 構成コマンド』 を参照してください。

構文:

llc

注: ルーター・ソフトウェア・ロードに APPN が含まれていない場合、このコマンドを使用しようとすると、次のようなメッセージを受け取ります。

```
LLC configuration is not available for this network.
```

LLC 構成環境は、ソフトウェア・ロードに APPN が含まれている場合にのみ利用可能です。

Media

media コマンドは、ネットワークの媒体タイプを変更するのに使用します。デフォルトの媒体タイプは STP ケーブルです。有効な媒体タイプ値は、シールド付き (shielded) とシールドなし (unshielded) です。 media コマンドの後に *media-type* を入力します。

構文:

media *media-type*

例:

```
media unshielded
```

Packet-Size

packet-size コマンドは、すべてのトークンリング・ネットワークの最大パケット・サイズを変更するのに使用します。 **packet-size** コマンドの後に、必要なバイト数を入力します。

構文:

packet-size *bytes*

表 28. トークンリング 4/16 の有効なパケット・サイズ

ネットワーク・データ速度	値 (バイト数)
4 Mbps	516 ～ 4498 **注:** 4 Mb TR に対して 4498 より大きい値が定義されている場合、ソフトウェアはそれを 4498 に設定します。ユーザーが値を指定しない場合は、デフォルト値の 2052 になります。
16 Mbps	516 ～ 18144 **注:** 値を指定しない場合は、デフォルト値の 2052 になります。

注: パケット・サイズが大きくなると、バッファーのメモリー所要量が増えます。

Set

set コマンドは、ルーティング情報フィールド (RIF) タイマーおよび物理 (MAC) アドレスを設定するのに使用します。

構文:

set physical-address

rif-timer

physical-address

トークンリング・インターフェースの MAC サブレイヤー・アドレスにローカル管理アドレスを定義するか、あるいは工場出荷時のデフォルトの端末ア

ドレス (オール 0 で示される) を使用するかを指示します。 MAC サブレイヤー・アドレスは、トークンリング・インターフェースがフレームの送受信に使用するアドレスです。

注: **Return** を押すと、値はそのままです。 **0** を入力して **Return** を押すと、ルーターは工場出荷時の端末アドレスを使用します。デフォルトでは、工場出荷時の端末アドレスを使用します。

有効値: 任意の 12 桁の 16 進アドレス

デフォルト値: 刻印されたアドレス (オール 0 で示されます)

例:

```
set physical-address
MAC address in 00:00:00:00:00:00 form []?
```

rif-timer

RIF 内の情報が更新される前に維持されている最大時間 (秒数) を設定します。デフォルト値は 120 です。

例:

```
set rif-timer
RIF aging timer value [120]?  120
```

Source-routing

source-routing コマンドは、端末ステーションのソース・ルーティングを使用可能または使用不可にするのに使用します。送信ルーティングというのは、エンド・ステーションがソース・ルーティング・ブリッジを経由するのに使用するソース・ルートを決めるプロセスです。ソース・ルーティングにより、IP、IPX、および AppleTalk フェーズ 2 プロトコルは、ソース・ルーティング・ブリッジの反対側のノードに到達することが可能になります。

このスイッチは完全に独立しており、このインターフェースが SRT 転送機能を介してソース・ルーティングを提供しているかどうかとは無関係です。デフォルトの設定値は「使用可能」です。

一部のステーションでは、ソース・ルーティング RIF をもつフレームを正常に受信できません。これは特に NetWare ドライバーに共通に見られる特徴です。この状態のときは、ソース・ルーティングを使用不可にすれば、これらのステーションと通信できるようになります。

IP、IPX、および AppleTalk フェーズ 2 パケットを通過させたいソース・ルーティング・ブリッジがこのリング上に存在する場合だけ、ソース・ルーティングを使用可能にします。また、LLC テスト応答メッセージを戻すようにしたい場合にも、ソース・ルーティングを使用可能にする必要があります。

構文:

source-routing enable

disable

speed

speed コマンドは、データ速度を変更するのに使用します。デフォルトの速度は 4 Mbps です。 **speed** コマンドの後に速度値 (Mbps 単位) を入力します。

構文:

speed *speed-value*

例: `speed 16`

インターフェース監視プロセスへのアクセス

トークンリング監視プロンプト (TKR>) を表示するには、network コマンドに続けて、トークンリング・インターフェースのインターフェース番号を入力します。たとえば、次のように入力します。

```
+network 0
TKR>
```

Config> プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。

18ページの『ネットワーク・インターフェース構成プロセスへのアクセス』 で説明されている手順に従って、本章で説明するインターフェースのインターフェース監視プロセスにアクセスします。必要なインターフェース監視プロセスにアクセスしたら、監視コマンドの入力を開始することができます。

トークンリング・インターフェース監視コマンド

この節では、トークンリング監視コマンドの要約を示します。コマンドは TKR> 監視プロンプトで入力します。 表29 は、監視コマンドをリストしています。

表 29. トークンリング監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Dump	RIF キャッシュのダンプを表示します。
LLC	LLC 監視プロンプトを表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Dump

tkr config> プロセスでソース・ルーティングが使用可能にされている場合、**dump** コマンドを使用して、RIF キャッシュの内容のダンプを要求することができます。

構文:

dump

例:

```
dump
MAC address    State     Usage   RIF
0000C90B1A57   ON_RING   Yes     0220
```

MAC address
トークンリングの MAC アドレスを表示します。

State インターフェースの状態の 1 つを表示します。

On_ring - そのリング上のノードの RIF が見つかったことを示します。

Have_route - リモート・リング上のノードの RIF が見つかったことを示しています。

No_route - 探索フレームが送信され、ルーターが戻りを待っている間、短時間表示されます。

Discovering - RIF を再発見するためにルーターが探索フレームを送信したことを示しています。

St_route - スパンニング・ツリー探索からルートが得られたことを示します。

Usage パケット内で RIF が使用されたことを示します。番号は任意で、機能上の意味はありません。

RIF RIF を示すコードを 16 進数で表示します。

注: RIF は、トークンリング・インターフェース上でソース・ルート・ブリッジングが使用可能にされている場合にのみ表示されます。

- NetBIOS RIF データは、次のコマンド・シーケンスを使用して表示することができます: **talk 5, protocol ASRT, name-caching, list cache rifs。**
- データ・リンク交換 RIF データは、次のコマンド・シーケンスを使用して表示することができます: **talk 5, protocol dlsw, list llc2 session all。**

LLC

LLC コマンドは、LLC 監視プロンプトにアクセスするのに使用します。 LLC コマンドは、この新たに表示されたプロンプトで入力します。各コマンドについての説明は、245ページの『LLC 監視コマンド』 を参照してください。

構文:

llc

トークンリング・インターフェースと GWCON インターフェース・コマンド

トークンリング・インターフェースには独自の監視用コンソール・プロセスがありますが、GWCON 環境から **interface** コマンドを使用すると、ルーターも導入済みのネットワーク・インターフェースの統計を表示します。

802.5 トークンリング・インターフェースについて表示される統計

GWCON 環境からトークンリング・インターフェースに対して **interface *<net#>*** コマンドを入力すると、以下の統計が表示されます。

```
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed

0  0   TKR/0      6000000   1C          1          0            0
Token-Ring/802.5  MAC/data-link on IBM Token-Ring interface
Microcode version: 000VL00A0 (050394)

Physical address        000C90820C7
Network speed           16 Mbps
Max packet size (INFO)  2052
Handler state           Ring open
Ring status             SERR | CO
Interface Restarts      0

# times Signal lost     0          # times Beaconing  0
Hard errors             0          Lobe wire faults   0
Auto-removal errors     0          Removes received   0
Ring recovery actions   0

Line errors             0          Burst errors       0
ARI/FCI errors          0          Inputs dropped     0
Frame copy errors       0          Token errors       0
Lost frames             0
```

以下では、一般的なインターフェース統計について説明します。

Nt グローバル・インターフェース番号

Nt' ダイヤル回線にのみ適用されます。

Interface
タイプ 『intrfc』 のインターフェース内のこのインターフェースのインターフェース名と番号

CSR COMM および状況レジスター・アドレス

Vec 割り込みベクトル

Self-Test: Pass
成功した自己テストの回数

Self-Test: Fail
失敗した自己テストの回数

Maint: Fail
保守障害の数

以下では、トークンリング・インターフェースに特有の統計を説明します。

input overflows
入力バッファー・サイズより大きかった受信フレームの数を指定します。大きすぎて 1 つの入力バッファーに収まらないフレームは廃棄されます。

Physical address
トークンリング・インターフェースの物理アドレスを指定します。

Network speed
インターフェースに接続しているトークンリング・ネットワークの速度を指定します。ネットワーク速度カウンターは、インターフェースが毎秒通過させることができるパケット数を表示します。

Max packet size (info)
そのインターフェースに構成された最大パケット・サイズを表示します。最大パケット・サイズ・カウンターは、インターフェースが送信または受信できるパケットの最大長さ (バイト数) を表示します。このカウンターは、ユーザーが定義します。

Handler state
トークンリング・ハンドラーの現行状態を表示します。ハンドラー状態カウンターは、自己テストの実行後のハンドラーの状態を示します。

Ring status
トークンリング・インターフェースの最後のリング状態

SIGL SIGNAL_LOSS　インターフェースはリング上で信号の損失を検出しました。

HERR HARD_ERROR　インターフェースは現在リング上でビーコン・フレームを送信または受信中です。

SERR SOFT_ERROR　インターフェースは報告誤り MAC フレームを転送しました。

BEAC TRANSMIT_BEACON　インターフェースはリングへ (または、リングからの) ビーコン・フレームを転送中です。

LWF LOBE_WIRE_FAULT　インターフェースは、インターフェースと集線装置の間のケーブルで回線の開きまたは短絡を検出しました。インターフェースはクローズされ、初期化後の状態になっています。

ARMV AUTO_REMOVAL_ERROR　インターフェースは、ローブ折り返しテストに失敗し (ビーコン自動除去プロセスの結果として)、自動的にリングから除去されました。インターフェースはクローズされ、初期化後の状態になっています。

RMVD REMOVED_RECEIVED　インターフェースはリング・ステーション除去 MAC フレーム要求を受信し、自動的にリングから除去されました。インターフェースはクローズされ、初期化後の状態になっています。

CO COUNTER_OVERFLOW　次の誤りカウンターの 1 つが 254 から 255 に増分されました: Line, ARI/FCI, Frame Copy, Lost Frames, Burst, Lobe wire faults, Removes received。このディスプレイは、これらの誤りカウンターを表示します。

SSTA SINGLE_STATION　インターフェースは、それがリング上の唯一のステーションであることを検出しました。

RR RING_RECOVERY　インターフェースは、リング上でトークン請求 MAC フレームを監視します。インターフェースはトークン請求フレームを送信している可能性があります。この状態は、インターフェースがリング除去フレームを送信するまで残ります。

Interface Restarts
トークンリング・チップ・タイムアウトの回数、またはトークンリング・ドライバーがハンドラーから無効コマンドを受信した回数を指定します。リスタートが行われた理由についての情報は、 イベン

*ト・ログ・システム メッセージの手引き*に記載されているメッセージ TKR.37、TKR.38、TKR.39、TKR.40、および TKR.41 を参照してください。

# of times signal lost
信号の損失のためにルーターがパケットを転送できなかった合計回数を指定します。

Hard errors
インターフェースがネットワークからビーコン・フレームを送受した回数を表示します。

Auto-removal errors
ビーコン自動除去プロセスが原因で、インターフェースがローブ折り返しテストに失敗し、自動的にネットワークから除去された回数を表示します。

Ring recovery actions
インターフェースがネットワークでトークン請求媒体アクセス制御（MAC）フレームを検出した回数を表示します。

Line errors
フレームが反復またはコピーされ、着信フレームのエラー検出標識 (EDI) がゼロのときに増分されます。

さらに、以下の条件の 1 つも存在している必要があります。

- コード違反のトークンが存在する。
- フレームの開始区切り文字と終了区切り文字の間にコード違反がある。
- フレーム検査シーケンス (FCS) 誤りが発生している。

ARI/FCI errors
ARI/FCI (アドレス認知標識/フレーム複写標識) 誤りカウンターは、インターフェースが次のいずれかを受信すると増分します。

ARI/FCI ビットがゼロに等しいアクティブ・モニター・プレゼント (AMP) MAC フレームと、ARI/FCI ビットがゼロに等しい待機モニター・プレゼント (SMP) MAC フレーム。

AMP MAC フレームが介在しない、ARI/FCI ビットがゼロに等しい複数の SMP MAC フレーム。

この誤りは、アップストリーム近隣がフレームをコピーしたが、ARI/FCI ビットをセットできないことを示しています。

Frame copy errors
受信/反復モードのインターフェースが特定のアドレスにアドレス指定されたフレームを認識したが、そのアドレス認識標識 (ARI) ビットがゼロでないことを発見した回数を表示します。この誤りは、回線ヒットまたは重複アドレスの可能性を示します。

Lost frames
インターフェースが送信モード (除去) にあり、送信フレームの終了を受信できなかった回数を表示します。

 # times beaconing
インターフェースがビーコン・フレームをネットワークに送信した回数を表示します。

Lobe wire faults
インターフェースが、インターフェースと集線装置の間のケーブルに回線の開きまたは短絡を検出した回数を表示します。

Removes received
インターフェースがリング・ステーション除去 MAC フレーム要求を受信し、自動的にネットワークから除去された回数を表示します。

Burst errors
インターフェースが、開始区切り文字 (SDEL) と終了区切り文字 (EDEL) の間、あるいは EDEL と SDEL の間で、5 回の半ビット期間に変換がなかったことを検出した回数を表示します。

Inputs dropped
反復モードにあるインターフェースが、自身のアドレス宛てのフレームを認知したが、利用可能なバッファー・スペースがないためにフレームをコピーできなかった回数を表示します。

Token errors
トークン・エラー・カウンターは、アクティブ・モニターが以下のいずれかの誤りをもつトークン・プロトコルを検出すると増分されます。

非ゼロの優先順位をもつトークンの MONITOR_COUNT ビットが 1 に等しい。

フレームの MONITOR_COUNT ビットが 1 に等しい。 10-ms ウィンドウ以内にトークンまたはフレームを受信していません。

開始区切り文字/トークンのシーケンスの、コード違反が存在してはならない区域にコード違反がある。

第17章 LLC インターフェースの使用

この章では、ルーター内の論理リンク制御 (LLC) インターフェースのソフトウェア構成可能情報を設定する方法について説明します。

論理リンク制御は 『サブプロトコル』 と考えることができます。 Talk 6 (構成) または Talk 5 (コンソール) 環境から直接アクセスすることはできません。代わりに、**LLC** コマンドを入力して、トークンリング、ポイント・ポイント (PPP)、またはフレーム・リレー・プロトコルからアクセスします。

第18章 LLC インターフェースの構成および監視

この章では、インターフェース・コマンドまたは GWCON インターフェース・コマンドを使用して、ルーター内の特定の LLC インターフェースを構成する方法について説明します。

論理リンク・レベルは 『サブプロトコル』 と考えることができます。 Talk 6 (構成) または Talk 5 (監視) 環境から直接アクセスすることはできません。代わりに、**LLC** コマンドを入力して、トークンリング、ポイント・ポイント (PPP)、またはフレーム・リレー・プロトコルからアクセスします。

本章には、以下の節が含まれています。

インターフェース構成プロセスへのアクセス

LLC を介して構成するプロトコルの構成コマンドにアクセスするには、次のようにします。

- トークンリングの場合は、229ページの『第16章 IEEE 802.5 トークンリング・ネットワーク・インターフェースの構成』の説明に従います。
- ポイント・ポイントの場合は、467ページの『第33章 ポイント・ポイント・プロトコル・インターフェースの使用』の説明に従います。
- フレーム・リレーの場合は、409ページの『第31章 フレーム・リレー・インターフェースの使用』の説明に従います。

これらのプロンプト・レベルのそれぞれに LLC コマンドがあります。 **LLC** と入力して LLC 構成コマンドにアクセスし、LLC を構成します。終了したら、**Exit** と入力して、構成しているプロトコルのプロンプト・レベルに戻ります。

LLC 構成コマンド

SNA ネットワークを介してパケットを渡す必要がある場合、LLC の構成が必要です。これらのコマンドを入力するには、最初に LLC 構成環境に入る必要があります (229ページの『トークンリング・インターフェース構成プロセスへのアクセス』 を参照してください。)

この節では、すべての LLC 構成コマンドの要約を示し、その後で個々のコマンドについて説明します。これらのコマンド (242ページの表30) を使用すると、SNA ネットワークを介してパケットを渡す必要がある場合に、LLC を構成することができます。

表 30. LLC 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	選択された LLC 構成を表示します。
Set	LLC に関連したタイマーと、送信および受信ウィンドウのサイズを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、LLC の現行構成を表示するのに使用します。

構文:

list

例:

```
list
Reply Timer (T1):                 1 seconds
Receive ACK Timer (T2):           100 milliseconds
Inactivity Timer (Ti):            30 seconds
Max Retry value (N2):             8
Rcvd I-frames before ACK (N3):    1
Transmit Window (Tw):             2
Receive Window (Rw):              2
Acks needed to increment Ww (Nw): 1
```

Reply Timer (T1)
このタイマーは、LLC が相手側の LLC ステーションから必要な確認またはレスポンスを受信できないと満了します。

Receive ACK Timer (T2)
このタイマーは、受信 I フォーマット・フレームの確認の送信を遅らせるのに使用します。

Inactivity Timer (Ti)
このタイマーは、指定された期間に LLC がフレームを受信しないと満了します。このタイマーが満了すると、相手側の LLC が応答するか、N2 再試行カウントを超えるまで、LLC は RR を送信します。デフォルト値は 30 秒。

Max Retry value (N2)
LLC プロトコルによる最大再試行数。デフォルト値は 8。

Rcvd I-frames before ACK (N3)
この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは、指定された値にセットされ、I フレームを受信するたびに減分されます。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。デフォルト値は 1。

Receive Window (Rw)
LLC がリモート・ホストから受信できる、未確認のシーケンス番号付き I フレームの最大数を示します。

Transmit Window (Tw)
RR を受信する前に送信できる I フレームの最大数を示します。

Acks needed to increment Ww (Nw)
このフィールドは、デフォルト値の 1 に設定します。

Set

set コマンドは、LLC を構成するのに使用します。

重要： LLC パラメーターをデフォルト値から変更すると、LLC プロトコルの動作方法に影響を与える可能性があります。

構文:

set
- n2-max-retry *count*
- n3-frames-rcvd-before-ack *count*
- nw-acks-to-inc-window *count*
- rw-receive-window *count*
- t1-reply-timer *seconds*
- t2-receive-ack-timer *seconds*
- ti-inactivity-timer *seconds*
- tw-transmit-window *count*

n2-max-retry
LLC プロトコルによる再試行の最大数。たとえば、N2 は、非活動タイマーが満了したときに、LLC が確認応答を受信せずに RR を送信する最大回数です。デフォルト値は 8。最小値は 1。最大値は 127。

例:

```
set n2-max-retry
Max Retry value (N2) [8]?
```

n3-frames_rcvd-before-ack
この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは、指定された値に設定します。 I フレームを受信するたびに、この値が減分します。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。デフォルト値は 1。最小値は 1。最大値は 255。

例:

```
set n3-frames_rcvd-before-ack
Number I-frames received before sending ACK(N3) [1]?
```

rw-receive-window
LLC がリモート LLC 同位から受信できる未確認のシーケンス番号付き I フレームの最大数を示します。この値は 127 以下でなければなりません。

例:

```
set rw-receive-window
Receive Window (Rw), 127 Max. [2]?
```

nw-acks-to-inc-ww

このフィールドは、デフォルト値の 1 に設定します。

t1-reply-timer

このタイマーは、LLC が相手側の LLC ステーションから必要な確認またはレスポンスを受信できないと満了します。このタイマーが満了すると、ポーリング・ビットをセットして RR が送信され、T1 が再びスタートします。LLC が構成された再試行最大数 (N2) の後もレスポンスを受信しない場合、基礎リンクは動作不能として宣言されます。デフォルト値は 1。最小値は 1。最大値は 256。

例:

```
set t1-reply-timer
Reply Timer (T1) in sec. [1]?
```

t2-receive-ack-timer

このタイマーは、受信 I フォーマット・フレームの確認の送信を遅らせるのに使用します。このタイマーは、I フレームを受信するスタートします。確認が送信されると、タイマーはリセットされます。このタイマーが満了すると、LLC2 はできるだけ速やかに確認を送信します。この値は、T1 の値より小さくなるように設定します。これにより、T1 タイマーが満了する前に、リモート LLC2 同位が遅らせた確認を確実に受信できるようになります。デフォルト値は 1 (100 ミリ秒)。最小値は 1。最大値は 2560。

例:

```
set t2-receive-ack-timer
Receive Ack timer (T2) in 100 millisec. [1]?
```

注: このタイマーが 1 (デフォルト値) に設定されている場合、タイマーは動作しません (たとえば、**n3-frames_rcvd-before-ack=1**)。

ti-inactivity-timer

このタイマーは、指定された期間に LLC がフレームを受信しないと満了します。このタイマーが満了すると、相手側の LLC が応答するか、N2 再試行カウントを超えるまで、LLC は RR を送信します。デフォルト値は 30 秒。最小値は 1 秒。最大値は 256 秒。

例:

```
set ti-inactivity-timer
Inactivity Timer (Ti) in sec. [30]?
```

tw-transmit-window

RR を受信する前に送信できる I フレームの最大数を示します。相手側の LLC セッションが実際にこの数の連続 I フレームを受信することが可能であり、しかもルーターに確認を受信するまでこれらのフレームのコピーを保持できる十分なヒープ・メモリーがあると仮定した場合、この値を大きくすると、スループットが向上します。デフォルト値は 2。最小値は 1。最大値は 127。

例:

```
set tw-transmit-window
Transmit Window (Tw), 127 Max. [2]?
```

インターフェース監視プロセスへのアクセス

LLC を介して監視するプロトコルの監視コマンドにアクセスするには、次のようにします。

- トークンリングの場合は、229ページの『第16章 IEEE 802.5 トークンリング・ネットワーク・インターフェースの構成』の説明に従います。
- ポイント・ポイント場合は、483ページの『第34章 ポイント・ポイント・プロトコル・インターフェースの構成および監視』 の説明に従います。
- フレーム・リレー場合は、429ページの『第32章 フレーム・リレー・インターフェースの構成および監視』 の説明に従います。

これらのプロンプト・レベルのそれぞれに LLC コマンドがあります。 **LLC** と入力して、LLC を監視するための LLC 監視コマンドにアクセスします。終了したら、**Exit** と入力して、監視しているプロトコルのプロンプト・レベルに戻ります。

LLC 監視コマンド

この節では、すべての LLC 監視コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドを使用すると、SNA ネットワークを介してパケットを渡している間 LLC を監視することができます。

表 31. LLC 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Clear-counters	すべての統計カウンターを消去します。
List	インターフェース、SAP、およびセッション情報を表示します。
Set	セッションの存続期間中だけ有効な LLC パラメーターを動的に構成することができます。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Clear-Counters

clear-counters コマンドは、すべての LLC 統計カウンターをクリアするのに使用します。

構文:

clear-counters

List

list コマンドは、インターフェース、サービス・アクセス・ポイント (SAP)、およびセッション情報を表示するのに使用します。

構文:

list interface

sap . . .

session

interface

このインターフェース上のすべてのオープンしている SAP を表示します。

例:

```
list interface
SAP      Number of Sessions
F4       1
```

sap sap_number

そのインターフェース上の指定された SAP の情報を表示します。

例:

```
list sap
SAP value in hex (0FE) [1]? F4

Interface                      0, TKR/0
Reply Timer(T1)                1 sec
Receive ACK Timer (T2)         100 millisec
Inactivity Timer (Ti)          30 sec
MAX Retry Value (N2)           8
MAX I-field Size (N1)          2052
Rcvd I-frames before ACK (N3)  1
Transmit Window Size (Tw)      2
Acks Needed to Inc Ww (Nw)     1

Frame                          Xmt   Rcvd
UI-frames                      4     5
TEST-frames                    0     1
XID-frames                     0     0
I-frames                       291   26
RR-frames                      81    291
RNR-frames                     0     0
REJ-frames                     0     0
SABME-frames                   1     0
UA-frames                      0     1
DISC-frames                    0     0
DM-frames                      0     0
FRMR-frames                    0     0
I-frames discarded by LLC            0
I-frames Refused by LLC user         0

Cumulative number of sessions        1
Number of active sessions            1

Session ID                                          Remote
(int-sap-id)   Local MAC          Remote MAC          SAP   State
00F40000     00:00:C9:08:41:DB   10:00:5A:F1:02:37   F4    OPENED
```

SAP value in hex (0FE)

そのセッションの SAP 値

Interface

セッションが使用するインターフェースの番号とタイプ

Reply Timer (T1)

LLC が他の LLC ステーションから確認応答またはレスポンスを受信しなかった場合、このタイマーが満了するまでにかかる時間を示します。

Receive ACK Timer (T2)

LLC が受信した I フレームに対する確認応答を送信する前に使用する時間遅延を示します。

Inactivity Timer (Ti)

RR を出す前の非アクティブ時に LLC が待機する時間を示します。

MAX Retry Value (N2)
LLC プロトコルによる最大再試行数

MAX I-field Size (N1)
LLC2 フレームの I フィールドに入れられるデータの最大量 (バイト数)

Rcvd I-frame before ACK (N3)
受信した I フレームに対する確認応答トラフィックを減らすために、T2 タイマーとともに使用される値を示します。

Transmit Window Size (Tw)
RR を受信する前に送信できる I フレームの最大数を示します。

Acks Needed to Inc Ww (Nw)
このフィールドは、デフォルト値の 1 に設定します。

Frames Xmt and Rcvd
転送された (Xmt) および (Rcvd) フレーム・タイプの合計数を表示するカウンター

I-frames discarded by LLC
LLC によって廃棄された (通常は、シーケンス番号が順序通りでないという理由で) I フレームの合計数を表示するカウンター

I-frames refused by LLC user
LLC の上位ソフトウェアによって廃棄された I フレーム数を示すカウンター。たとえば、DLSw (データ・リンク交換)

Cumulative number of sessions
この SAP を介してオープンされたセッションの合計数

Number of active sessions
インターフェース上で実行されている現在アクティブのセッションの合計数

Session ID (int-sap-id)
監視しているインターフェースのセッション ID

Local MAC
ルーターの LLC MAC アドレス

Remote MAC
リモート LLC の MAC アドレス

Remote SAP
LLC 接続のリモート SAP

Remote State
LLC 同位間の相互動作の結果としての有限状態。以下に説明する 21 の状態があります。

Link_Closed
リモート LLC 同位がローカル LLC 同位に認知されず、存在しないものと見なされます。

Disconnected
ローカル LLC 同位は、相手側に認知されています。この LLC 同位は、

XID、TEST、SABME、および DISC コマンド、XID TEST、UA、および DM レスポンスを送受信することができます。

Link_Opening
受信した SABME に応答して SABME または UA を送信した後のローカル LLC 同位の状態

Disconnecting
DISC コマンドをリモート LLC 同位に送信した後のローカル LLC の状態

FRMR_Sent
ローカル LLC 同位は、フレーム・リジェクト例外状態に入り、リンクを介して FRMR レスポンスを送信しました。

Link_Opened
ローカル LLC 同位は、データ転送フェーズにあります。

Local_Busy
ローカル LLC 同位は、追加の I フレームを受信できません。

Rejection
ローカル LLC 同位が、1 つまたは複数のシーケンス誤り I フレームを受信しました。

Checkpointing
ローカル LLC 同位は、リモート LLC 同位にポーリングを送信し、適切なレスポンスを待っています。

CKPT_LB
checkpointing 状態と local busy 状態の組み合わせ

CKPT_REJ
checkpointing 状態と rejection 状態の組み合わせ

Resetting
ローカル LLC 同位は SABME を受信し、リンクを再確立中です。

Remote_Busy
リモート LLC 同位から RNR を受信したときに生じる状態

LB_RB
local_busy 状態と remote_busy 状態の組み合わせ

REJ_LB
rejection 状態と local_busy 状態の組み合わせ

REJ_RB
rejection 状態と remote_busy 状態の組み合わせ

CKPT_REJ_LB
checkpointing、rejection、および local_busy 状態の組み合わせ

CKPT_CLR
LLC 同位が CKPT_LB の間に local_busy 状態が終了した結果生じた組み合わせ状態

CKPT_REJ_CLR
リンク・ステーションが CKPT_REJ_LB 状態にあるときに未確認ローカル・ビジー・クリアが転送された結果生じた組み合わせ状態

REJ_LB_RB

rejection、local_busy、および remote_busy 状態の組み合わせ

FRMR_Received

ローカル LLC 同位は、リモート LLC 同位から FRMR レスポンスを受信しました。

Session

インターフェース上でオープンしている指定の LLC セッションに関する情報を表示します。

例:

```
list session
Session Id: [0]? 00-F4-0000

Interface0,                     TKR/0
Remote MAC addr                 10:00:5A:F1:02:37
Source MAC addr                 00:00:C9:08:35:47
Remote SAP                      F4
Local SAP                       F4
RIF                             (089E 0101 0022 0010)
Access Priority                 0
State                           LINK_OPENED
Replay Timer                    1 sec
Receive ACK Timer (T2)          100 millisec
Inactivity Timer (Ti)           30 sec
MAX I-field Size (N1)           2052
MAX Retry Value (N2)            8
Rcvd I-frames before ACK (N3)   1
Transmit Window Size (Tw)       2
Working Transmit Size (Ww)      2
Acks Needed to Inc Ww (Nw)      1
Current Send Seq (Vs)           9
Current Rcv Seq (Vr)            7
Last ACK'd sent frame (Va)      9
No. of frames in ACK pend q     0
No. of frames in Tx pend q      0
Local Busy                      NO
Remote Busy                     NO
Poll Retry count                8
Appl output flow stopped        NO
Send process running            YES

Frame                            Xmt   Rcvd
I-frames                         1456  2678
RR-frames                        502   403
RNR-frames                       0     0
REJ-frames                       0     0
I-frames discarded by LLC              0
I-frames Refused by LLC user           0
```

Session Id

セッション ID 番号を示します。

Interface

このセッションを実行しているインターフェースの番号を示します。

Remote MAC addr

リモート LLC 同位の MAC アドレスを示します。

Source MAC addr

ローカル LLC の MAC アドレスを示します。

Remote SAP

LLC 接続のリモート側 SAP

Local SAP

LLC 接続のローカル側 SAP

RIF フレームの実際の RIF

Access Priority
パケットの優先順位。高位レイヤー制御の場合は 07

State LLC 同位間の相互動作の結果としての有限状態。詳細については、246ページの **list sap** コマンドの項を参照してください。

Receive ACK timer (T2)
LLC が受信した I フレームに対する確認応答を送信する前に使用する時間遅延を示します。

Inactivity timer (Ti)
RR を出す前の非アクティブ時に LLC が待機する時間を示します。

MAX I-field size (N1)
フレームのデータ・フィールドの最大サイズ (バイト数)。デフォルト値は、インターフェースのサイズです。

MAX Retry Value (N2)
LLC が確認応答を受信せずに RR を送信する最大回数

Rcvd I-frames before ACK (N3)
受信 I フレームに対する確認応答トラフィックを減らすために T2 タイマーと共に使用される値を示します。

Transmit window size (Tw)
RR を受信する前に送信できる I フレームの最大数を示します。

Working transmit size (Ww)
RR を受信する前に送信できる I フレームの最大数

Acks Needed to Inc Ww (Nw)
このフィールドは、デフォルト値の 1 に設定します。

Current send seq (Vs)
送信状態変数 (転送される次の I フレームの Ns 値)

Current Rcv seq (Vr)
受信状態変数 (受け付ける次の in-sequence Ns)

Last ACK'd sent frame (Va)
確認応答された状態変数 (受信した最後の有効な Nr)

No. of frames in ACK pend q
確認応答を待機中の送信済み I フレーム数

No. of frames in transmit pend q
送信されるのを待っているフレーム数

Local Busy
LLC 接続のローカル側が RNR を送信中

Remote Busy
LLC 接続のリモート側が RNR を受信中

Poll Retry count
LLC プロトコル内のカウンターの再試行の現行値 (カウントダウン) を示します。

Appl output flow stopped
LLC がアプリケーションに対して発信データ・フレームの供給停止を指示しました。

Send process running
このプロセスは、その他のフレーム・アクションと並行して実行され、 I フレームを送信待ち行列に入れて送信します。

Frames Xmt and Rcvd
転送されたフレーム・タイプ (Xmt) および (Rcvd) の総数を表示します。

I-frames discarded by LLC
LLC によって廃棄された (通常は、シーケンス番号が順序通りでないという理由で) I フレームの合計数を表示するカウンター

I-frames refused by LLC user
LLC の上位ソフトウェアによって廃棄された I フレーム数を示すカウンター。たとえば、DLSw (データ・リンク交換)

Set

set コマンドは現行 LLC セッションに関する LLC パラメーターを動的に構成するのに使用します。パラメーターに加えた変更は、セッションの存続期間中だけ有効です。これらのパラメーターは、243ページの『Set』 にリストされているものと同一です。

考慮事項: LLC パラメーターをデフォルト値から変更すると、LLC プロトコルの動作方法に影響を与える可能性があります。

構文:

set n2-max_retry *count*
n3-frames-rcvd-before-ack *count*
nw-acks-to-inc-ww *count*
t1-reply-timer *seconds*
t2-receive-ack-timer *seconds*
ti-inactivity-timer *seconds*
tw-transmit-window *seconds*

n2-max_retry
LLC プロトコルによる再試行の最大数。たとえば、N2 は、非活動タイマーが満了したときに、LLC が確認応答を受信せずに RR を送信する最大回数です。デフォルト値は 8。最小値は 1。最大値は 127。

n3-frames-rcvd-before-ack
この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは、指定された値に設定します。 I フレームを受信するたびに、この値が減分します。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。デフォルト値は 1。デフォルト値は 1。最小値は 255。

nw-acks-to-inc-ww

このフィールドは、デフォルト値の 1 に設定します。

t1-reply-timer

このタイマーは、LLC が相手側の LLC ステーションから必要な確認またはレスポンスを受信できないと満了します。このタイマーが満了すると、ポーリング・ビットをセットして RR が送信され、T1 が再びスタートします。LLC が構成された再試行最大数 (N2) の後もレスポンスを受信しない場合、基礎リンクは動作不能として宣言されます。デフォルト値は 1。デフォルト値は 1。最小値は 256。

t2-receive-ack-timer

このタイマーは、受信 I フォーマット・フレームの確認の送信を遅らせるのに使用します。このタイマーは、I フレームを受信するとスタートし、確認を送信するととリセットされます。このタイマーが満了すると、LLC2 はできるだけ速やかに確認を送信します。この値は、T1 の値より小さくなるように設定します。これにより、T1 タイマーが満了する前に、リモート LLC2 同位が遅らせた確認を確実に受信できるようになります。デフォルト値は 1 (100 ミリ秒)。最小値は 1。最大値は 2560。

注: このタイマーが 1 (デフォルト値) に設定されている場合、タイマーは動作しません (たとえば、**n3-frames_rcvd-before-ack=1**)。

ti-inactivity-timer

このタイマーは、指定された期間に LLC がフレームを受信しないと満了します。このタイマーが満了すると、相手側の LLC が応答するか、N2 タイマーが満了するまで、LLC は RR を送信します。デフォルト値は 30 秒。最小値は 1 秒。最大値は 256 秒。

tw-transmit-window

RR を受信する前に送信できる I フレームの最大数を示します。相手側の LLC セッションが実際にこの数の連続 I フレームを受信することが可能であり、しかもルーターに確認を受信するまでこれらのフレームのコピーを保持できる十分なヒープ・メモリーがあると仮定した場合、この値を大きくすると、スループットが向上します。デフォルト値は 2。最小値は 1。最大値は 127。

第19章 イーサネット・ネットワーク・インターフェースの使用

この章では、イーサネット・インターフェースの使用法について説明します。本章には、以下の節が含まれています。

インターフェース・コマンドによるイーサネット統計の表示

GWCON 環境から **interface** コマンドを使用して、以下の統計を表示することもできます。

```
+ interface 0
                              Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
0  0   Eth/0        81600   5E          1          1            0
Ethernet/IEEE 802.3 MAC/data-link on SCC Ethernet interface

Physical address         000093808000
RISC Microcode Revision:            1
PROM address             000093808000

Input statistics:
  failed, frame too long          0   failed, FCS error           0
  failed, alignment error         0   failed, FIFO overrun        0
  internal MAC rcv error          0   packets missed              0

Output statistics:
  deferred transmission           6   single collision            2
  multiple collisions             0   total collisions            2
  failed, excess collisions       0   failed, FIFO underrun       0
  failed, carrier sense err       0   SQE test error              0
  late collision                  0   internal MAC trans errors   0
```

これらの統計は、次のような意味を持っています。

Nt グローバル・ネットワーク番号

Nt' このフィールドは、シリアル・インターフェース・カード用です。出力とは無関係です。

Interface
インターフェース名とそのインスタンス番号

CSR コマンドおよび状況レジスター・アドレス

Vec 割り込みベクトル

Self-Test: Passed
成功した自己テストの回数

Self-Test: Failed
失敗した自己テストの回数

Maintenance: Failed
保守障害の数

Physical address
現在使用している装置のイーサネット・アドレス。これは PROM アドレス、あるいは他のプロトコルによって上書きされたアドレスです。

PROM address
このイーサネット・インターフェースの PROM 内の永続的な固有のイーサネット・アドレス。

Interface restarts
イーサネット・チップ・タイムアウトの回数、またはイーサネット・ドライバーがハンドラーから無効なコマンドを受信した回数。リスタートが行われた理由についての詳細は、 *IBM Nways イベント・ログ・システム メッセージの手引き* の中のメッセージ Eth.043 および Eth.044 を参照してください。

Interface type
これは、コネクター・タイプを AUI または RJ45 として指定します。

Input statistics:

failed, packet too long or failed, frame too long
「障害、パケットが長過ぎる」カウンターは、インターフェースが、イーサネット・フレームの最大サイズである 1518 バイトより大きいパケットを受信すると増分します。このデータは SNMP を介して dot3StatsFrameTooLongs カウンターとしてエクスポートされます。

failed, CRC error or failed, FCS (Frame Check Sequence) error
「障害、CRC (巡回冗長検査) 誤り」カウンターは、インターフェースが CRC 誤りを含むパケットを受信すると増分します。このデータは SNMP を介して dd3StatsFCSErrors カウンターとしてエクスポートされます。

failed, framing error or failed, alignment error
「障害、フレーム誤り」カウンターは、インターフェースが、長さ (ビット数) が 8 の倍数でないパケットを受信すると増分します。

failed, FIFO over-run or failed, FIFO overrun
「障害、FIFO (先入れ先出し) オーバーラン」カウンターは、イーサネット・チップ・セットが、線路から送り出される速度に見合う速度で、ローカル・パケット・バッファーにバイトを保管できない場合に増分します。

collision in packet
このカウンターは、インターフェースがパケットを受信しようとしたがローカル・パケット・バッファーがいっぱいで、パケットが衝突すると増分します。この誤りは、インターフェースの処理能力を超えるトラフィックがネットワーク上に存在することを示しています。

short frame
このカウンターは、インターフェースが短いフレームのパケットを受信すると増分します。

buffer full warnings
「バッファー満ぱい警告」カウンターは、ローカル・パケット・バッファーがいっぱいになるたびに増分します。

packets missed
「パケット紛失」カウンターは、インターフェースがパケットを受信しよう

としたが、ローカル・パケット・バッファーが満ぱいであるときに増分します。この誤りは、インターフェースの処理能力を超える通信量がネットワーク上に存在することを示しています。

internal mac rcv errors
遅延、過剰、またはキャリア・チェック衝突以外の受信誤り。このデータは SNMP を介して dot3StatsInternalMacReceiveErrors カウンターとしてエクスポートされます。この統計は FIFO オーバーランの合計値です。

Output statistics:

initially deferred or deferred transmission
「初期遅延」カウンターは、キャリア・センス機構がインターフェースの転送を遅らせるようなライン・アクティビティーを検出すると増分します。このデータは SNMP を介して dot3StatsDeferredTransmissions カウンターとしてエクスポートされます。

single collision
「単一衝突」カウンターは、初回の転送試行でパケットが衝突した後、2 回目の転送試行でパケットを正常に送信できた場合に増分します。このデータは SNMP を介して dot3StatsSingleCollisionFrames カウンターとしてエクスポートされます。

multiple collisions
「複数衝突」カウンターは、パケットが正常に転送されるまでに複数回の衝突が生じた場合に増分します。このデータは SNMP を介して dot3MultipleCollisionFrames カウンターとしてエクスポートされます。

total collisions
「合計衝突数」カウンターは、パケットに発生した衝突の数だけ増分されます。

failed, excess collisions
「障害、超過衝突」カウンターは、16 回の連続衝突によりパケット転送が失敗すると増分します。この誤りは、ネットワーク通信量が多いか、ネットワークにハードウェア問題があることを示しています。このデータは SNMP を介して dot3StatsExcessiveCollisions カウンターとしてエクスポートされます。

failed, FIFO underrun
「障害、FIFO アンダーラン」カウンターは、インターフェースがネットワーク上の転送に対応できる速度でローカル・パケット・バッファーからパケットを取り出せないためにパケットの転送に失敗すると増分します。

failed, carrier check or failed, carrier sense error
「障害、キャリア・チェック」カウンターは、キャリア・センスが使用不可にされているためにパケットが衝突すると増分します。この誤りは、インターフェースとそのイーサネット・トランシーバー間に問題があることを示しています。このデータは SNMP を介して dot3StatsCarrierSenseErrors カウンターとしてエクスポートされます。

CD heartbeat error or SQE test error
「CD (衝突検出) ハートビート誤り」または「SQE (信号品質誤り)」カウンターは、インターフェースがパケットを送信したが、トランシーバーがハートビートを生成しないことを検出すると増分します。トランシーバーによっ

てはハートビートを生成しないものがあるので、このパケットは正常に転送されたものとして扱われます。このデータは SNMP を介して dot3StatsSQETestErrors カウンターとしてエクスポートされます。

out of window collisions or late collisions
「ウィンドウ外衝突」カウンターは、少なくとも 512 ビット転送した後でパケットが衝突した場合に増分します。この誤りは、ネットワーク上のインターフェースによる遅延に失敗したか、ネットワーク上のステーション数が多過ぎることを示しています。

internal mac tx errors or internal MAC trans errors
遅延、過剰、またはキャリア・チェック衝突以外の送信誤り。このデータは SNMP を介して dot3StatsInternalMacTransmitErrors カウンターとしてエクスポートされます。この統計は FIFO アンダーランの合計値です。

RISC Microcode Version:
これは、通信プロセッサー・モジュールの RISC 制御装置内で実行されているマイクロコードのバージョンを示します。

第20章 イーサネット・ネットワーク・インターフェースの構成および監視

この章では、イーサネット・インターフェースの構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

イーサネット・インターフェース構成プロセスへのアクセス

構成プロセスにアクセスするには、以下の手順を使用します。このプロセスにより、イーサネット・インターフェースの構成 プロセスにアクセスできます。

1. OPCON プロンプトで **talk 6** と入力する。(このコマンドの詳細については、29ページの『第3章 OPCON プロセスおよびコマンド』 を参照してください。) たとえば、次のように入力します。

   ```
   * talk 6
   Config>
   ```

   コンソールに CONFIG プロンプト (Config>) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は **Return** をもう一度押してください。

2. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。 たとえば、次のように入力します。

   ```
   Config> list devices

   Ifc 0 Ethernet                      CSR  81600, CSR2  80C00, vector 94
   Ifc 1 WAN X.25                      CSR  81620, CSR2  80D00, vector 93
   Ifc 2 WAN X.25                      CSR  81640, CSR2  80E00, vector 92
   Ifc 3 WAN PPP                       CSR 381620, CSR2 380D00, vector 125
   Ifc 4 WAN Frame Relay               CSR 381640, CSR2 380E00, vector 124
   Ifc 5 Token Ring                    CSR 600000, vector 95
   ```

3. インターフェース番号を記録する。
4. **network** コマンドと、構成するイーサネット・インターフェースの番号を入力する。 たとえば、次のように入力します。

   ```
   Config> network 0
   ETH Config>
   ```

   イーサネット構成プロンプト (ETH Config>) が表示されます。

イーサネット構成コマンド

この節では、イーサネット構成コマンドの要約を示し、個々のコマンドについて説明します。コマンドは ETH config> プロンプトで入力します。

表 32. イーサネット構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Connector-Type	コネクター・タイプを設定します。
IP-Encapsulation	IP カプセル化を、イーサネット (タイプ X'0800') または IEEE (SNAP 付き 802.3) として設定します。
List	現行のコネクター・タイプ、NetWare IPX カプセル化、および IP カプセル化を表示します。
Physical-Address	物理 MAC アドレスを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Connector-Type

connector-type コマンドは、コネクター・タイプを設定するのに使用します。 2210 は、AUI (10BASE5) および RJ-45 (10BASE-T) コネクターと、自動構成 (auto-config) オプションをサポートします。

構文:

connector-type *name*

IP-Encapsulation

IP-encapsulation コマンドは、イーサネット (イーサネット・タイプ X'0800') または IEEE 802.3 (SNAP を備えたイーサネット 802.3) を選択するのに使用します。 **e** または **i** を入力します。

構文:

ip-encapsulation *type*

List

list コマンドは、コネクター・タイプ、IPX カプセル化タイプ、および IP カプセル化タイプを含めて、イーサネット・インターフェースの現行構成を表示するのに使用します。

構文:

list all

例: `list all`

```
Connector type:          AUI (10BASE5)
MAC Address:             12:15:00:FA:00:FE
```

Physical-Address

physical-address コマンドは、物理 (MAC) アドレスを設定するのに使用します。

physical-address

このコマンドでは、イーサネット・インターフェースの MAC サブレイヤー・アドレスにローカル管理アドレスを定義するのか、あるいはデフォルトの刻印されたアドレス (オール 0 で示される) を使用するのかを指示することができます。 MAC サブレイヤー・アドレスは、イーサネット・インターフェースがフレームの送受信に使用するアドレスです。

注: **Enter** を押すと、値はそのままになります。 **0** を入力すると、ルーターは刻印されたアドレスを使用します。デフォルトでは、刻印されたアドレスを使用します。

有効値: 任意の 12 桁の 16 進アドレス

デフォルト値: 刻印されたアドレス (オール 0 で示されます)

例:

```
set physical-address

MAC address in 00:00:00:00:00:00 form []? 12:15:00:FA:00:FE
```

イーサネット・インターフェース動作プロセスへのアクセス

イーサネット・ネットワーク・インターフェースに関連する情報を監視するには、以下の手順を使用して、インターフェース監視プロセスにアクセスします。

1. OPCON プロンプトで **talk 5** と入力する。たとえば、次のように入力します。

   ```
   * talk 5
   ```

   GWCON プロンプト (+) がコンソールに表示されます。最初に GWCON に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

   ```
   + configuration
   ```

   (**configuration** コマンドの出力例については、137ページの『Configuration』を参照してください。)

3. **network** コマンドとイーサネット・インターフェースの番号を入力する。この例では、次のように入力します。

   ```
   + network 0
   ETH>
   ```

   イーサネット監視プロンプトが表示されます。これで、監視コマンドを入力すれば、イーサネット・インターフェースに関する情報を見ることができます。

イーサネット・インターフェース監視コマンド

この節では、イーサネット監視コマンドの要約を示し、個々のコマンドについて説明します。コマンドは ETH> プロンプトで入力します。 表33 は、監視コマンドをリストしています。

表 33. イーサネット構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Collisions	指定されたイーサネット・インターフェースの衝突統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Collisions

このコマンドは、正常に転送される前に衝突を起こしたパケットの転送数を示します。カウンターは、15 回の衝突の後に送信された、衝突 XXXXx パケットの後に送信されたパケット数を示します。衝突を伴って転送されたパケット数が増えること、およびパケット当たりの衝突回数が増えることは、ビジー状態のイーサネットに転送されていることを示しています。

これらのカウンターは、OPCON **clear** コマンドによってクリアされます。このデータは SNMP を介して dot3CollTable カウンターとしてエクスポートされます。

構文:

collisions

例:

```
Eth> coll
Transmitted with  1 collisions:0
Transmitted with  2 collisions:0
Transmitted with  3 collisions:0
Transmitted with  4 collisions:0
Transmitted with  5 collisions:0
Transmitted with  6 collisions:0
Transmitted with  7 collisions:0
Transmitted with  8 collisions:0
Transmitted with  9 collisions:0
Transmitted with 10 collisions:0
Transmitted with 11 collisions:0
Transmitted with 12 collisions:0
Transmitted with 13 collisions:0
Transmitted with 14 collisions:0
Transmitted with 15 collisions:0
```

第21章 LAN エミュレーションの概説

注: 本章で使用されている頭字語および用語の定義については、用語集を参照してください。

ルーターは、複数のベンダーの複数のプロトコルの相互接続性のための業界標準として広く受け入れられている *LAN Emulation Over ATM: Version 1.0 Specification*を実現しています。この章では、MSS 実現のコンテキストの中で LAN エミュレーション (LE) の基本概念を紹介します。 最初に、エミュレートされた LAN (ELAN) を導入する動機について検討します。

LAN エミュレーションの利点

LAN エミュレーション・プロトコルは、ATM ネットワークをイーサネット LAN またはトークンリング LAN のように見せることができます。 LAN エミュレーションは、ATM の利点のすべてを活用できるわけではありませんが、 ATM 技術への移行やネットワーク管理コストの削減に役立ちます。高速 ATM リンクを利用できる上に、ソフトウェアとハードウェアの投資の保護を図れます。

ソフトウェア投資を保護できるのは、アプリケーション・インターフェースが変更されないからです (LAN エミュレーションは、エンド・ステーションのデバイス・ドライバー・インターフェースの下にあるデータ・リンク制御レイヤー内で実現されます)。ハードウェア投資を保護できるのは、転送装置本体が LAN ネットワークや ATM ネットワークをブリッジするので、既存のアダプターや配線を引き続き使用できるからです。

LAN エミュレーションを使用すれば、高帯域幅をもつステーション (たとえば、サーバー、技術ワークステーション、マルチメディア・ワークステーション) に ATM アダプターを徐々に増設していくことができます。単純な LAN エミュレーションの例の物理図と論理図を 図14 に示します。

単純な LAN エミュレーション・ネットワーク

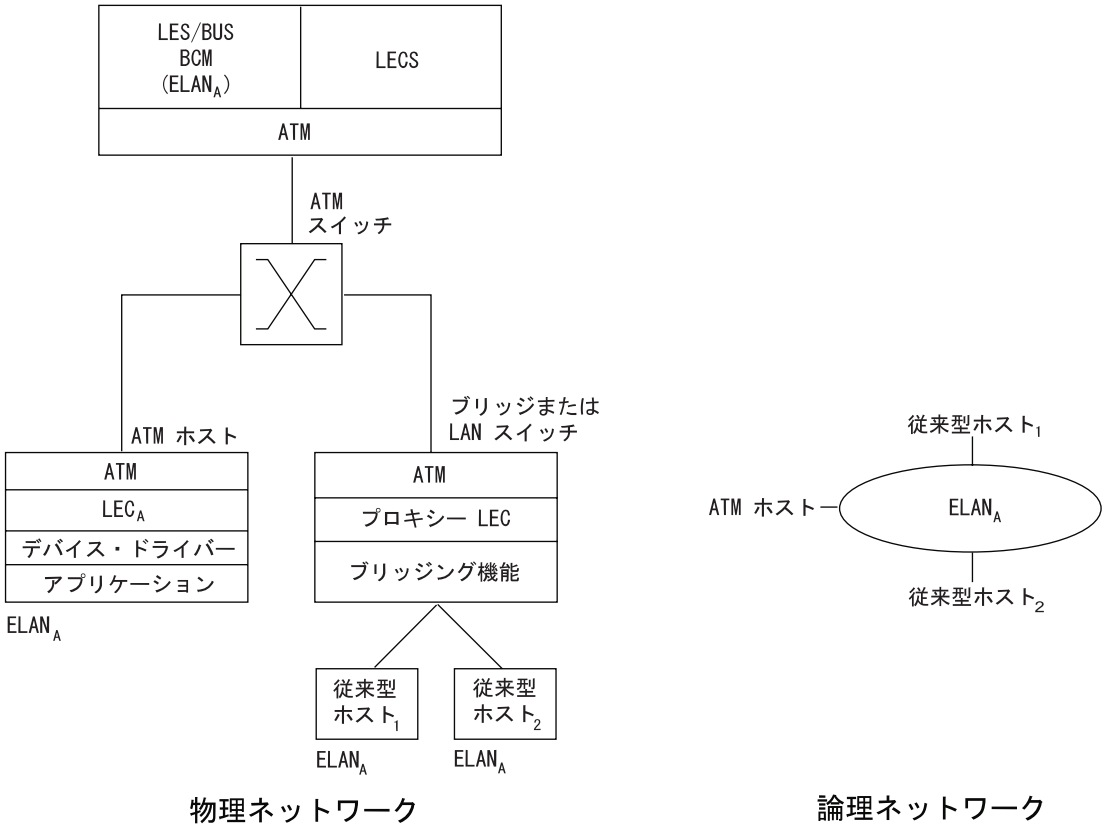


図 14. 単純な LAN エミュレーション・ネットワークの物理図と論理図

エミュレートされた LAN (ELAN) のネットワーク管理上の利点は、移動、追加、および変更が柔軟になることから得られます。 ELAN のメンバーシップは物理的な場所に基づくのではなく、論理的に関連したステーションがグループ化されて、1 つの ELAN を形成します (ステーションは複数の ELAN のメンバーになることも可能です)。

ELAN メンバーシップが保持されている限り、ステーションが物理的に別の場所に移動しても、再構成の必要はありません。同様に、ステーションをある ELAN から別の ELAN に移動しても、配線を変える必要はありません。

LAN エミュレーションのコンポーネント

以下のコンポーネントによって ELAN が実現します。

LAN エミュレーション (LE) クライアント (LEC)
エミュレートされた LAN のユーザーを表す LAN エミュレーションのコンポーネント

LE 構成サーバー (LECS)
構成データを中央に集めて広く配布する LAN エミュレーション・サービス・コンポーネント

LE サーバー (LES)
LAN 着信先を ATM アドレスに変換する LAN エミュレーション・サービス・コンポーネント

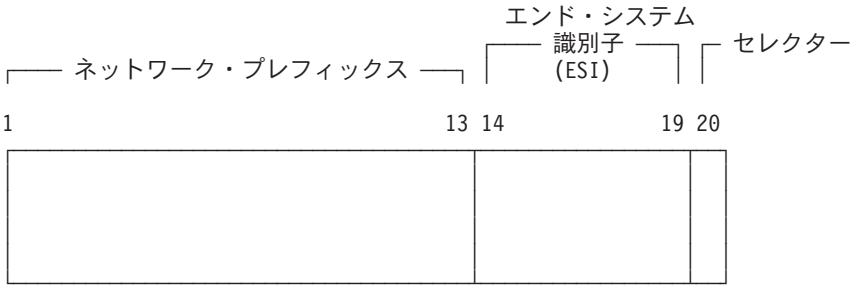
ブロードキャストおよび不明サーバー (BUS)
マルチキャスト・フレームおよび不明ユニキャスト・フレームの送達を担当する LAN エミュレーション・サービス・コンポーネント

LES、BUS、および LECS をまとめて LE サービス・コンポーネントと呼んでいます。各 ELAN には専用の LES および BUS があります。 LE クライアントは、エンド・システム内 (ATM 接続ホスト内、あるいはブリッジまたは LAN スイッチ内のいずれか) に存在します。ブリッジまたは LAN スイッチは、イーサネットLAN またはトークンリング LAN に接続されているホストを表します。 LE クライアントは、MAC レベルのサービスを高位レベル・ソフトウェアに提供します。イーサネット IEEE 802.3 または IEEE 802.5 トークンリング LAN をエミュレートすることができますが、ELAN 上のすべてのステーションが同じタイプであることが必要です。

トークンリングまたはイーサネット LAN セグメントと ELAN 間をブリッジする機能は、プロキシー LEC と呼ばれます。 LAN をエミュレートする場合は、LE クライアントは LECS、LES、および BUS からのサービスを要求します。以下の節では、ATM アドレッシングおよび関連の中間ローカル管理インターフェース (ILMI) 機能について簡単に説明します。これらの概念を理解しておかないと、ネットワーク内の LE コンポーネントの機能は理解できません。

ATM でのアドレッシング

ATM では 20 バイトの階層型アドレッシングを使用します。



ATM アドレスの最初の 13 オクテットはネットワーク・プレフィックスです。 ATM ネットワーク内の各スイッチは、固有のネットワーク・プレフィックスをもっていることが必要です。 ATM スイッチは、ネットワーク・プレフィックスを使用して、VCC 設定要求を着信側 ATM スイッチにルーティングします。エンド・システム (このルーターのような) は、起動したときに、ATM スイッチからネットワーク・プレフィックスを取り出します。

ATM アドレスのオクテット 14-19 は、エンド・システム識別子 (ESI) です。同じスイッチに接続されている各エンド・システムは、別々の ESI セットを使用しなければなりません。エンド・システムが起動すると、中間ローカル管理インターフェース (ILMI) を使用して、その ESI を ATM スイッチに登録しようと試みます。

ILMI は、エンド・システムと ATM スイッチ間のインターフェースを管理するのに使用される 1 組の SNMP ベースの手順を定義します。エンド・システムは ILMI を使用して、以下のことを行います。

- スイッチからネットワーク・プレフィックスを入手する。
- ESI をスイッチに登録する。
- ATM スイッチの UNI バージョンを動的に判別する。
- LEC はスイッチから LECS アドレスのリスト入手できるようになる。

スイッチは、すべての登録済み ESI が固有になるようにします。

ATM アドレスのオクテット 20 はセレクターです。

エンド・ステーションは、スイッチからネットワーク・プレフィックスを入手し、ESI とセレクターを追加して、独自のアドレスを形成します。こうして作成されたアドレスがスイッチに登録されますが、ATM アドレスが固有でない場合、スイッチは登録を拒否します。

ESI

ルーター上の各 ATM インターフェースは、汎用管理または出荷時設定 MAC アドレスをもっています。この MAC アドレスを、ルーターの ATM アドレスの一部または全部の ESI として使用することができます。あるいは、各インターフェースに最大 64 個のローカル管理アドレスを定義することもできます。すべてのエンド・システムが汎用管理 MAC アドレスを ESI として使用すれば、ATM アドレスが固有であることが保証されます。こうすれば、構成の負担が軽くなります。ただし、ローカル管理 ESI を使用すると、問題判別が容易になる場合もあります。ユーザーは、汎用管理 ESI とローカル管理 ESI を任意に組み合わせて使用することができます。

固有の ATM アドレスを得る 1 つの方法として、出荷時設定 IEEE MAC アドレスを ESI として使用し、固有のセレクターをローカルで選択するという方法もあります。デフォルトでは、ルーターは ATM インターフェースの MAC アドレスを、その ATM アドレス内の ESI として使用します。各 ATM インターフェースに追加 ESI を構成できます。

各 ESI は最大 255 個の対応するセレクター (0x00 ～ 0xff) をもつことができます。セレクターの範囲は、構成されるセレクター範囲と自動的に割り当てられるセレクター範囲の 2 つに区分されています。構成されるセレクター範囲の上限は、ATM インターフェース・パラメーター max-configured-selector で定めます。

ルーター上の ATM コンポーネントは、さまざまな方法でセレクターを選択します。あるコンポーネントの場合は、構成されたセレクター範囲から、ユーザーが明示的にセレクターを構成する必要があります。このようなコンポーネントの例としては、LES/BUS があります。別のコンポーネント (クラシカル IP クライアントなど) は、実行時に自動的にセレクターを割り当てることができます。ユーザーはセレクターを選択する必要はなく、ルーターが起動時にこれを選択します。このセレクターは、ルーターのリスタートのたびに一貫しているとは保証されません。自動的なセレクターの割り当ては、ネットワーク上の他の装置があらかじめその ATM アドレスを知っていなくても構わない ATM コンポーネントの場合にのみ便利です。

ATM の構成は、エミュレートされた LAN、ブリッジング、またはルーティングを構成する前に行う必要があります。

LAN エミュレーション・コンポーネントの ATM アドレス

一般的には、ATM アドレスは LAN エミュレーション・コンポーネント間で固有であることが必要です。唯一の例外として、同じ ELAN にサービスする LES と BUS は ATM アドレスを共用できます (ルーターはこれに相当します)。

LAN エミュレーション・コンポーネントは、特定の ATM インターフェースに対して構成されます。コンポーネントの ATM アドレスの ESI 部分として出荷時設定 MAC アドレスの使用することに決めても構いませんし、その ATM インターフェースに対して定義されたローカル管理 ESI の 1 つを選択することもできます。セレクターが固有であれば、複数の LE コンポーネントが同じ ESI を共用することも可能です。デフォルトでは、構成インターフェースが各 ESI コンポーネントごとに、構成済み ESI に対して固有のセレクター値を割り当てます。ただし、この割り当てをオーバーライドして、明示的に特定のセレクター値を構成することも可能です。

ATM インターフェース・パラメーターを用いて、明示的な割り当て用として予約される ESI 当たりのセレクター数を定めます。残りは、実行時に ATM インターフェースが動的に割り当てるのに利用できます。 LE コンポーネントは、明示的な割り当て用に予約されたセレクターのみを使用します。デフォルトでは、ESI 当たり可能な 256 個のセレクターのうちの 200 個が、明示的割り当て用として予約されます。実行時のセレクター割り当てが有利なのは、割り当てられたセレクターを制御する必要がない場合です。たとえば、ARP サーバーと対をなしていないクラシカル IP 内のクライアントを構成する場合などです。

LE コンポーネント間では ATM アドレスは固有でなければなりませんが、LE コンポーネントは、クラシカル IP サーバー機能のような非 LE コンポーネントとは同じ ATM アドレスを使用しても構いません。

関連 ILMI 機能の概説

ILMI は、エンド・システムと ATM スイッチの間のユーザー・ネットワーク・インターフェース (UNI) を管理するのに使用される 1 組の SNMP ベースの手順を定義します。特に LAN エミュレーションに関係のある ILMI 機能には、次の 3 つがあります。

1. ATM アドレス登録 (263ページの『ATM でのアドレッシング』 で説明)
2. スイッチで実行中の信号バージョンの動的な判別
3. LECS ATM アドレスの獲得

263ページの『ATM でのアドレッシング』 で説明しているように、ATM アドレス登録は、ATM エンド・システムとスイッチの間で共同で行われる作業です。あらかじめスイッチに ATM アドレスを登録しておかないと、呼を送信または受信することはできません。

デフォルトでは、ルーターの ATM インターフェースは ILMI 手順を使用してスイッチ MIB を照会し、スイッチで実行されている信号バージョンの判別 (UNI 3.0 また

は 3.1) を試みます。照会が正常に行われた場合、ATM インターフェースはスイッチと同じ UNI バージョンを実行します。照会が正常に行われなかった場合は、ATM インターフェースは UNI 3.0 を実行します。あるいは、デフォルトをオーバーライドして、ATM インターフェースで実行される UNI バージョンを明示的に構成することもできます。

信号バージョンの手動による構成

ATM スイッチが UNI 3.1 を実行しており、UNI バージョン MIB 変数がない場合は、信号バージョンを手動で構成する必要があります。この場合、ATM インターフェースは UNI バージョンを動的に判別することはできません。ルーターの ATM インターフェースは、デフォルトでは UNI 3.0 を使用するので、ユーザーは ATM インターフェースが UNI 3.1 を使用するように手動で構成する必要があります。

ILMI の使用による LECS の探索

ILMI は、LECS を見つける方法として特にすぐれています。 ATM スイッチの ILMI MIB には、LE クライアントが検索できる LECS ATM アドレスのリストが入っています。この方式が便利な理由は、LECS ATM アドレスを構成する必要があるのは ATM スイッチだけで、LE クライアントはその必要がなく、しかもスイッチの数は LE クライアントの数より少ないことにあります。クライアントは、このリストの最初の LECS への接続を試みます。接続に失敗すると、クライアントは接続が確立されるまで、順番に次の LECS アドレスへの接続を試みます。

LECS 機能の概説

LE クライアントは、LECS の使用が推奨されますが、必ず使用しなければならないわけではありません。 LECS を使用しない場合は、各 LE クライアントで、ELAN にサービスする LES の ATM アドレスを構成することが必要です。 LECS は、構成データの中央リポジトリーとして機能することによりネットワーク管理の負担を減らし、LE クライアントの構成を最小限に抑えます。

注: 各ルーターに構成できる LECS は最高で 1 つです。

クライアントは、事前定義された手順を使用して LECS に接続します。 LECS へのバーチャル・チャネル・コネクション（VCC）が確立されるまで、クライアントは以下の手順を試みます。

1. 構成された LECS アドレス情報があれば (LE クライアントでの LECS ATM アドレスの構成はオプションであり、推奨されて***いません***)、それを使用して LECS に接続する。
2. ILMI を使用して LECS のリストを入手し、VCC が確立されるまで、リストの各 LECS への接続を順番に試みる。
3. ATM フォーラムで定義されている事前割り当て LECS ATM アドレスへの VCC を確立する。

前述のとおり、LE クライアントが LECS を見つける方法としては、ILMI が優先されます。一部のスイッチは ILMI 方式をサポートしないので、事前割り当て LECS アドレスが必要になります。 LE クライアントで LECS アドレスを構成するのは、ス

イッチが ILMI 方式をサポートせず、LE サービスが事前割り当て LECS アドレスをサポートしない場合に***限る*** ことが必要です。

ルーターと IBM ATM スイッチは、3 つの方式、つまり、事前割り当て LECS アドレス、ILMI 接続、および事前割り当て LECS ATM アドレスをすべてサポートします。

LECS は、初期構成データを LE クライアントに提供する必要があります。最も重要なデータは、LES の ATM アドレスです。この情報を LE クライアントに提供するためには、LECS が LE クライアントを識別し、その LE クライアントの正しい LES を判別できることが必要です。 LECS は、LE クライアントによって送信される LE_CONFIGURATION_REQUEST フレーム内の情報を使用して、LE クライアントを識別します。この構成要求には、LE クライアントが加入を求めている ELAN を識別するための情報も含まれています。構成要求には、以下の情報を含めることができます。

1. LE クライアントの 1 次 ATM アドレス

   このフィールドは必須であり、LE クライアントを固有に識別します。

2. LAN クライアントに対応する LAN 着信先

   このフィールドには、LE クライアントを固有に識別する MAC アドレスまたはルート記述子を入れてもよいし、指定しないでおくこともできます。

3. ELAN ネーム

   このフィールドには、要求される ELAN または要求する LE クライアントを識別する名前を入れることができます。ルーターの実現では、ELAN ネームは標準 ASCII ストリングです。 ELAN ネームは、要求の中で指定しなくても構いません。

4. ELAN タイプ

   このフィールドでは、LE クライアントがイーサネットまたはトークンリングに属することを指定できますが、指定しなくても構いません。 LE クライアントが ELAN のタイプを指定している場合、LECS はそのクライアントに異なるタイプの ELAN を割り当てることはできません。

5. LE クライアントによってサポートされる最大フレーム・サイズ

   このフィールドでは、LE クライアントが処理できるデータ・フレームのサイズの上限を指定できますが、指定しなくても構いません。 LECS はクライアントを、そのクライアントが指定したより**大きい** 最大フレーム・サイズをもつ ELAN に割り当てることはできません。 ELAN が使用するフレームが大きすぎてクライアントが処理できない場合、クライアントはその ELAN 上では機能できません。

この情報に基づいて、LECS は LE クライアントを LES に割り当てます。これは、ポリシーとポリシー値を使用して行います。ポリシーとは、LECS が LE クライアントの LES への割り当てを決めるときに使用する基準のことです。 ポリシー値とは、指定の値を指定の LES に割り当てることを指示する値の組み合わせ (値、LES) です。たとえば、ポリシーは LE クライアントの MAC アドレスとし、ポリシー値は (MAC ADDR_A, LES_1) というように指定します。 MAC ADDR_A の LE クライアントが、LES_1 に割り当てられることになります (その LE クライアントが、ポリシーの優先順位が上位のために、すでに別の LES に割り当てられていない場合)。 1 組のポリシーとポリシー値が、すべての ELAN に適用されます。

ATM フォーラムの LE サービス MIB 仕様に準拠して、6 つのポリシーが定義されています。

1. ATM アドレス
2. MAC アドレス
3. ルート記述子
4. ELAN タイプ
5. 最大フレーム・サイズ
6. ELAN ネーム

ポリシーには優先順位もあります。 LECS は優先順にポリシーを調べます。優先順位フィールドの値が小さいポリシーが、優先順位フィールドの値が大きいポリシーより先に考慮されます。優先順位フィールドの値が等しいポリシーは、同時に考慮されて *AND (論理積)* が取られます。

LECS は、現行の優先順位のポリシーがすべて満たされ、しかも一致している場合に、LE クライアントを LES に割り当てます。ポリシーが満たされるのは、現行の優先順位の各ポリシーの構成要求の対応するフィールドと一致するポリシー値が存在する場合です。ポリシーが一致するのは、すべてのポリシーに共通の LES が一致の集合に含まれている場合です。これらの条件に適合しない場合は、LECS は次の優先順位のポリシーを考慮します。 LECS がどの優先順位でも LES を見つけられなかった場合、構成不成功のレスポンスが LE クライアントに戻されます。

ポリシーの一致の意味を理解するために、一致していないポリシーの例を考えてみましょう。優先順位 1 のポリシーが、MAC アドレスと ELAN ネームであるとします。ポリシー値の 1 つは (X'400000121225', LES_A) で、1 つは (ELAN 1, LES_B) とします。 LE クライアントが LAN 着信先 X'400000121225' を提供した場合は、MAC アドレス・ポリシーは満たされています。 LE クライアントが ELAN ネーム *ELAN 1* を提供した場合は、ELAN ネーム・ポリシーも満たされています。この場合、優先順位 1 のポリシーはそれぞれ異なる LES を参照しているので、一致**していません**。この例の場合は、LECS は次の優先順位のポリシーを調べることになります。

LE クライアントの正しい LES が決まると、LECS は次の情報が入っている構成応答を LE クライアントに戻します。すなわち、LES ATM アドレス、ELAN タイプ、最大フレーム・サイズ、および ELAN ネームです。構成応答には。タイプ/長さ/値 (TLV) パラメーターを含めることもできます。 TLV は、オプションまたはユーザー定義パラメーターを LE クライアントにダウンロードする手段を提供します。

LECS 割り当てポリシーの使用例

この節では、各種の LECS 割り当てポリシーの例を示します。

ATM アドレス・ポリシー

LECS は、2 つのタイプの ATM アドレス・ポリシー値を使用することができます。最初のタイプは、可変長 ATM アドレス・プレフィックスです。たとえば、ポリシー値 (399999999999900000102, LES_A) は、ATM アドレスが 399999999999900000102 で始まるすべての LE クライアントを LES_A に割り当てることを意味しています。

2 番目のタイプの ATM アドレス・ポリシー値は、ATM アドレスの ESI とセレクターです。たとえば、ポリシー値 (10002345003281, LES_A) は、ESI が 100023450032 で、セレクターが 81 の LE クライアントを、LES A に割り当てることを意味しています。

LE クライアントの ATM アドレスが与えられると、LECS は最初に ESI とセレクターが一致するものを探します。一致が戻されなかった場合、LECS は、一致するプレフィックスが最も長い ATM アドレス・プレフィックス・ポリシー値を探します。したがって、上記の例のポリシーは、ポリシー値 (399999999999990000, LES_B) より優先されます。

ATM アドレス ESI とセレクター・ポリシー値を使用すると、LE クライアントの物理的な場所から独立した形で、クライアントを LES に割り当てることができます (ESI とセレクターは、ローカルでクライアントに定義されます)。 ATM アドレス・プレフィックスが、地理情報を示す唯一のポリシー値です。

LAN 着信先ポリシー

MAC アドレスまたはルート記述子に基づいて、LE クライアントを LES に割り当てることができます。 LAN 着信先は、地理的な場所から独立した形で LE を固有に識別するので、このポリシーは、LE クライアントを物理的な場所とは関係なく (たとえば、ワークステーションをあるスイッチから別のスイッチに移動するときに、そのメンバーシップを保持したままで) 正しい ELAN に確実に割り当てることができるので便利です。

ELAN ネーム・ポリシー

ELAN ネームは、おそらく最も柔軟な割り当て基準です。以下に、ELAN ネーム・ポリシー値を使用できる方法をいくつか挙げます。

- ELAN の実名の使用

  LES_A が Elan 1 にサービスする場合は、ポリシー値 (Elan 1, LES_A) を作成します。この場合、構成要求で Elan 1 を指定している LE が、LES_A に割り当てられます。

- ELAN の別名の使用

  たとえば、経理部に属するすべての LE クライアントは ELAN ネーム *Accounting* を使用し、技術部に属するすべての LE クライアントは ELAN ネーム *Engineering* を使用するように構成することができます。 ELAN 上の LE クライアントの数に応じて、これらの名前を同じ ELAN に割り当てる場合は、ポリシー値を次のように構成します。

  ```
  (Accounting, LES_A)
  (Engineering, LES_A)
  ```

  あるいは、異なる ELAN に割り当てる場合は、ポリシー値を次のように構成します。

  ```
  (Accounting, LES_A)
  (Engineering, LES_B)
  ```

  この設定の場合は、LE クライアントに正しい ELAN ネームを構成することが必要です。

- LE クライアントの名前の使用

  各 LE クライアントに独自の名前を与えることができます。たとえば、ポリシー値 (Joe, LES_A) と (Mary, LES_A) を作成できます。この場合、これらの名前を構成された LE クライアントは、同じ LES に割り当てられることになります。この方法では、個々の LE クライアントと LECS で、ELAN ネームを構成する必要があります。ただし、Joe と Mary はクライアントを新しい場所に移動することができます。移動によって、クライアントは新しい ATM アドレスまたは MAC アドレスを持つことになりますが、新しい LE クライアントを同じ ELAN ネームで構成する限り、元の ELAN のメンバーシップが保持されます。各 LE クライアントの名前をパスワードとみなせば、この方式は適度のセキュリティーも提供することになります。

ELAN タイプ・ポリシー

ELAN タイプ・ポリシー値は、デフォルト ELAN を提供する場合に非常に便利です。たとえば、次のポリシー値は、個々の LE クライアントが確実に LES の 1 つに割り当てられます。

```
(Token-ring ELAN Type,  LES_A)
(Ethernet ELAN Type,    LES_B)
(Unspecified ELAN Type, LES_C)
```

一般的には、デフォルト ELAN 割り当てを提供するポリシーには低い優先順位を与え、特定的なポリシーが先に考慮されるようにすべきです。

最大フレーム・サイズ・ポリシー

最大フレーム・サイズ・ポリシーも、デフォルト ELAN 割り当てを提供するのに使用できます。

重複ポリシー値

特定のポリシーの複数の LES に対して同じポリシー値が対応している場合に、重複が起こります。 ELAN タイプ・ポリシーと最大フレーム・サイズ・ポリシーでは、重複ポリシー値は許容されますが、その他のポリシーでは認められません。重複値が便利なのは、同じ優先順位の異なるポリシーと組み合わせる場合だけです。

たとえば、次のような 3 つの ELAN があるとします。最大フレーム・サイズが 4544 バイトのイーサネット ELAN、最大フレーム・サイズが 4544 バイトのトークンリング ELAN、および最大フレーム・サイズが 18190 バイトの別のトークンリング ELAN です。 ELAN タイプ・ポリシーと最大フレーム・サイズ・ポリシーを同じ優先順位に設定し、次のポリシー値を定義することにより、LE クライアントを該当する ELAN に割り当てることができます。

```
(Ethernet ELAN Type,     LES_1)     (Max Frame Size = 4544,   LES_1)
(Token-Ring ELAN Type,   LES_2)     (Max Frame Size = 4544,   LES_2)
(Token-Ring ELAN Type,   LES_2)     (Max Frame Size = 18190,  LES_2)
```

TLV に関するその他の情報

TLV は、ELAN ベースで定義されます。したがって、特定の ELAN に割り当てられるすべての LE クライアントに、同じ TLV セットが戻されます。構成応答に TLV が含まれている場合、LE クライアントは TLV に指定されている値を動作パラメー

ターとして使用することが***必要*** です (LE クライアントがその ELAN タイプを認識できる場合)。 TLV が有益と考えられる状況の例を、以下にいくつか挙げます。

- ELAN が地理的に大きな場所に広がっている場合は、LE クライアントのデフォルトのタイムアウト値では不十分な場合があります。すべての LE クライアントのタイムアウト値は、LECS で TLV にそれぞれの値を指定することによって制御できます。
- デフォルトでは、ELAN はベストエフォート接続を使用して BUS に接続します。BUS トラフィックが多い ELAN の場合、BUS への予約帯域幅接続を使用することにより、性能の向上を図ることができます。 LE クライアントと BUS 間のマルチキャスト・センド VCC の特性は、TLV を用いて制御することができます。
- TLV を使用して、ELAN セグメント番号をソース・ルート・ブリッジにダウンロードすることができます。

TLV は、構成の微調整に加えて、ELAN 上のすべてのクライアントが矛盾のないパラメーターで動作することを要求します。ルーターは、すべての ATM フォーラム定義の TLV、ならびに任意のユーザー定義の TLV をサポートします。

LES への接続

LES への ATM アドレスを入手した後、LE クライアントは LES へのコントロール・ダイレクト VCC を開始します。この VCC が確立されると、LE クライアントは LE_JOIN_REQUEST を LES に送信します。 LES は、LE クライアントを該当するポイント・マルチポイント間コントロール・ディストリビュート VCC に追加し、LE_JOIN_RESPONSE を戻して応答します。デフォルトでは、図15 に示すように、LES はプロキシー・クライアントと非プロキシー・クライアントを区分して、別々のコントロール・ディストリビュート VCC に割り当てますが、必要なポイント・マルチポイント VCC の数を減らすために、すべての LE クライアントに対して単一のコントロール・ディストリビュート VCC を使用するように構成することも可能です。VCC を区分すると、非プロキシー・クライアントに送信される妨害トラフィックが減るので、一般的には有用です。 272ページの『アドレス解決』 で説明するように、LE_ARP_REQUEST が非プロキシー LE クライアントに送信されることはありません。

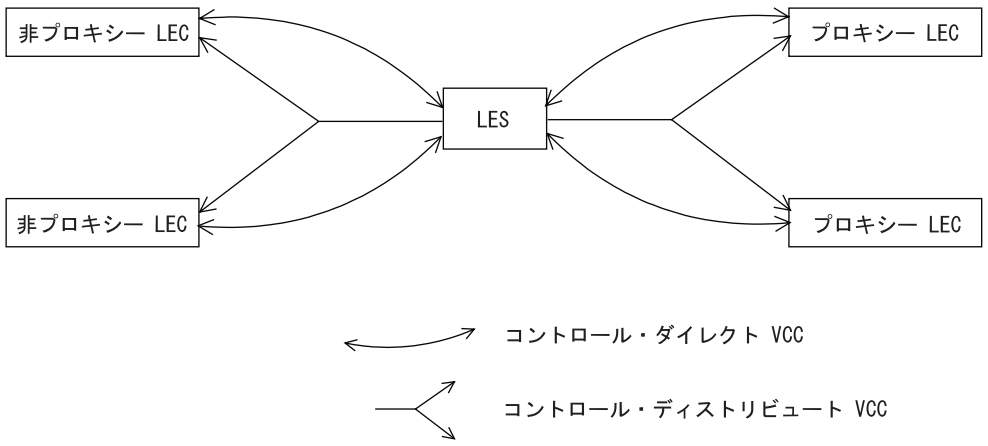


図 15. LE クライアントと LES 間のデフォルト接続

LE クライアントと LES 間に、以下の ATM 接続が確立されます。

コントロール・ダイレクト VCC (双方向、ポイント・ポイント)
LE クライアントから LES へ

コントロール・ディストリビュート VCC (ポイント・マルチポイント)
LES から LE クライアントへ

アドレス登録

LE クライアントは、LAN 着信先を LES に登録して固有性を確保し、LES が LE_ARP_REQUEST (LE クライアントが、特定の LAN 着信先に対応する ATM アドレスを確認するために出す) に応答できるようにします。登録するのは、LAN 着信先と、LE クライアントがその LAN 着信先に対応付ける ATM アドレスです。 LAN 着信先は、MAC アドレスまたはルート記述子のいずれでも構いません。

プロキシー LE クライアントは、それが ELAN にブリッジしている LAN セグメント上のステーションの MAC アドレスを登録しません。これに対して、非プロキシー LE クライアントは、それが表す LAN 着信先をすべて登録する必要があります。ルート記述子は、対応する LE クライアントがプロキシーであるか、非プロキシーであるかに関係なく、すべて登録する必要があります。ルート記述子を適用できるのは、ソース・ルート・ブリッジングを実行しているプロキシー LEC だけです。ルート記述子には、プロキシー LE クライアントのブリッジ番号と、LE クライアントがブリッジしている先のリンクのセグメント番号 (1 ホップの隔たりに相当する) が入っています。

アドレス解決

LAN 通信は、発信元と着信先の MAC アドレスが基礎になります。このような通信を ATM ネットワーク上で可能にするためには、MAC アドレスを ATM アドレス変換 (解決) することが必要です。 LE クライアントは、LE_ARP_REQUEST を LES に送信して、特定の LAN 着信先の ATM アドレスを確認します。 LAN 着信先が登録されている場合、LES はその LAN 着信先に対応する ATM アドレスで応答します。そうでない場合は、要求はコントロール・ディストリビュート VCC 上のすべてのプロキシー LE クライアントに転送されます。非プロキシー LEC は、それぞれの LAN 着信先がすべて登録されているので、要求を転送する必要はありません。ただし、LES が単一のコントロール・ディストリビュート VCC を使用するように構成されている場合には、プロキシーおよび非プロキシーの両方の LE クライアントが要求を受け取ることになります。コントロール・ディストリビュート VCC は、LES が複数の LE クライアントに制御フレームを配布するための効率的な手段を提供します。

プロキシー LE クライアントは、それが表す未登録 MAC アドレスに対する LE_ARP_REQUEST に応答します。 LE_ARP_RESPONSE は、コントロール・ダイレクト VCC で LES に送信され、LES は要求を出した LE クライアントに応答を転送します。

BUS への接続

LES に接続した後、LE クライアントはオール 1 の同報通信 MAC アドレスに対して LE_ARP_REQUEST を出します。 LES は、BUS の ATM アドレスで応答します。次に LE クライアントは、BUS へのマルチキャスト・センド VCC の確立を開始します。 BUS は、LE クライアントを該当するポイント・マルチポイント間マルチキャスト・フォワード VCC に追加することによって応答します。デフォルトでは、プロキシー・クライアントと非プロキシー・クライアントを区分して、別々のマルチキャスト・フォワード VCC に割り当てますが、コントロール・ディストリビュート VCC の場合と同様に、すべての LE クライアントに対して単一のマルチキャスト・フォワード VCC を使用するように BUS を構成することも可能です。 図16 は、分割されたマルチキャスト・フォワード VCC を示します。

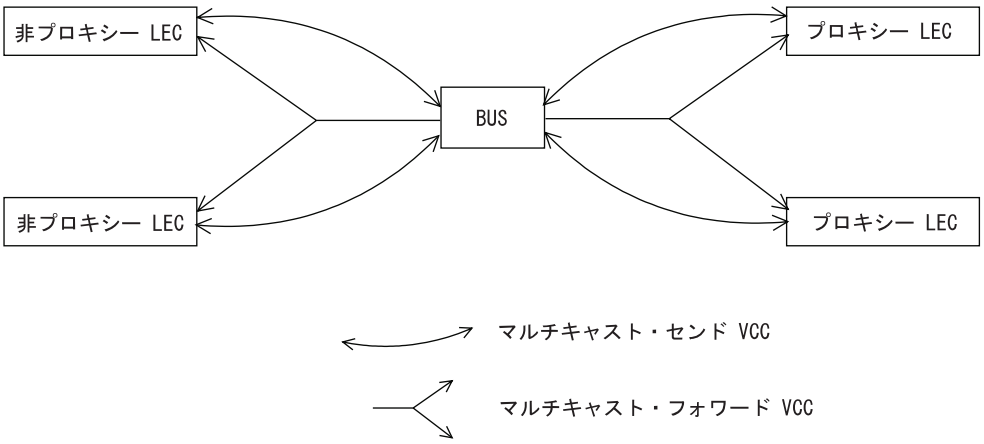


図 16. LE クライアント (LEC) と BUS 間のデフォルト接続

LE クライアントと BUS 間に確立される ATM 接続を明確にするために、次のリストを示します。

マルチキャスト・センド VCC (双方向、ポイント・ポイント)
LE クライアントから BUS へ

マルチキャスト・フォワード VCC (ポイント・マルチポイント)
BUS から LE クライアントへ

BUS 機能

BUS には 2 つの基本機能があります。

1. マルチキャスト・フレームを ELAN 内のすべての LE クライアントに配布する。
2. ユニキャスト・フレームを該当する着信先に転送する。

LE クライアントがユニキャスト・フレームを BUS に送信するのは、着信先を表す LE クライアントへの直接接続がない場合です。 BUS にネックが生じるのを避けるために、LE クライアントが BUS にユニキャスト・フレームを送信できる速度には制限があります。

このルーターの実現では、BUS には 2 つの動作モードがあります。つまり、ユニキャスト・フレーム・ドメインの区分化と、ユニキャスト・フレーム・ドメインの非区分化です。ユニキャスト・フレーム・ドメインを区分化した場合、BUS は 2 つのマルチキャスト・フォワード VCC を使用します。そうでない場合、BUS は単一のマルチキャスト・フォワード VCC を使用します。

単一のマルチキャスト・フォワード VCC が使用される場合、BUS の動作は非常に単純です。受信したすべてのフレームがすべての LE クライアントに転送されるだけです。 2 つのマルチキャスト・フォワード VCC が使用される場合、BUS はユニキャスト・フレームをすべての LE クライアントに同報通信する必要はありません。代わりに、非プロキシー・クライアントあてのユニキャスト・フレームが、マルチキャスト・センド VCC で着信先 LE クライアントに直接転送され、それ以外のすべてのユニキャスト・フレームは、プロキシー・マルチキャスト・フォワード VCC を使用して、プロキシー LE クライアントにだけ転送されます。 2 つのマルチキャスト VCC が使用される場合、ルーターはインテリジェント BUS (IBUS) モードにあるものと見なされます。

IBUS では、妨害ユニキャスト・フレーム (クライアント宛てでないユニキャスト・フレーム) が減ります。プロキシー・クライアントは非プロキシー・クライアント宛てのユニキャスト・フレームは受信せず、非プロキシー・クライアントが妨害ユニキャスト・フレームを受信することは決してありません。妨害フレーム専用のネットワーク帯域幅も減ります。一方、BUS の処理の所要量は増え、マルチキャスト・フレームは 2 回 (各マルチキャスト・フォワード VCC ごとに 1 回) 転送する必要があります。一般的には IBUS 動作が推奨されますが、非プロキシーとして ELAN に加入するソース・ルート・ブリッジをもつ構成では、このオプションを使用不可にする必要があります。

データ・ダイレクト VCC の確立

データ・ダイレクト VCC は、2 つの LE クライアントを接続し、BUS が介在せずにユニキャスト・フレームを交換するのに使用されます。 LE クライアントは、アドレス解決手順を使用して、必要な LAN 着信先に対応する ATM アドレスを判別します。 LE クライアントがすでにその ATM アドレスへのデータ・ダイレクト VCC を持っている場合 (おそらく、そのターゲット LE クライアントによって表される別の LAN 着信先への)、以降のユニキャスト・フレームは既存の VCC 上で伝送されます。そうでない場合は、LE クライアントは信号プロトコルを起動して、新しい VCC を確立します。

LE クライアントは、LAN 着信先と ATM アドレスのマッピングが入っている LE_ARP キャッシュを維持します。このキャッシュのエントリーはエージング (経時処理) されるので、定期的に更新する必要あります。 LAN 着信先からデータ・フレームを受信すると、エントリーは更新されます。データ・トラフィックがないときでも、LE クライアントはエントリーの更新を試みます。

また、データ・ダイレクト VCC の使用状況が監視され、VCC タイムアウト期間 (これは構成可能) にトラフィックがないと、VCC は解放されます。利用可能な資源が不十分なために新規データ・ダイレクト VCC を正常に確立できない場合も、LRU 方式で (最も古くに使用されたものから順に) データ・ダイレクト VCC が解放されます。

LAN エミュレーションの拡張機能の概説

IBM では、ルーター上で利用可能な ATM フォーラム LAN エミュレーションを機能強化して付加価値を付けました。これらの機能強化により、性能、信頼性、セキュリティー、および管理性の向上が図られています。

ブロードキャスト・マネージャー (BCM)
この機能は、ELAN の同報通信を減らすことにより、ネットワーク全体の性能を向上させます。

冗長度 冗長機構は、1 次サーバーに障害が生じたときにバックアップ・サーバーに引き継ぐことを可能にし、信頼性を高めます。

セキュリティー
LECS に ELAN メンバーシップを制御させることにより、セキュリティーが向上します。

BUS モニター
この機能は、BUS の上位ユーザーを識別することにより、管理を強化します。

以下の各節では、これらの拡張機能のそれぞれについて説明します。

ブロードキャスト・マネージャー

ブロードキャスト・マネージャー (BCM) は、IBM による LAN エミュレーション BUS 拡張機能からなる LAN エミュレーションの拡張です。 BCM がないと、以下の事象が起こります。

- BUS に送信されたマルチキャスト・フレームが、ELAN 上のすべての LE クライアントに転送される。
- ブリッジング・サポートを提供するためにプロキシー機能が組み込まれている LE クライアントは、ブロードキャスト・フレームを他の LAN セグメントに転送する。
- すべてのエンド・ステーションが、すべてのブロードキャスト・フレームを受信して処理する。

BCM は、個々の ELAN 上で次のプロトコルに対して使用可能にすることができます。

IP

IPX

NetBIOS

BCM が使用可能の場合、BUS に送信される特定タイプのブロードキャスト・フレームの最少量のレイヤー 2 およびレイヤー 3 情報が復号されます。可能な場合はいつでも、BCM はブロードキャスト・フレームをユニキャスト・フレームに変換し、それを関係のある LE クライアントとエンド・ステーションにのみ送信します。 BCM は、妨害ブロードキャスト・フレームをフィルターすることにより、ネットワーク上の通信量および関連のエンド・ステーションの両方のオーバーヘッドを減らします。これらの機能により、システム全体の性能を高め、より大規模な ELAN の実用化を可能にします。

IP の BCM サポート

IP に対して使用可能にすると、BCM はすべての IP ARP 要求と応答をスキャンし、この ELAN を含む IP サブネット内の IP アドレスのロケーションを確認します。その目的は、BCM が各ブロードキャスト ARP 要求フレームを受け取り、それをユニキャスト・フレームとして直接、ターゲット IP ステーションを表す LE クライアントに転送することです。要求は、マルチキャスト・フォワード VCC を通してすべての LE クライアントに同報通信されるのではなく、マルチキャスト・センド VCC で該当する LE クライアントに直接転送されるので、ネットワークの通信量とエンド・ステーションの処理の両方が削減されます。着信先ステーションがブリッジ機能の背後にある場合は、その着信先ステーションが属する LAN も、同報通信の通信量の削減の恩恵を受けることになります。

IPX の BCM サポート

IPX の場合、BCM は公示やその他の同報通信要求の範囲を制限します。 IPX ルーターとサーバーは、それぞれが知っているネットワーク情報およびサービス情報を定期的に同報通信します。 IPX クライアントは、同報通信要求を送信して、特定のサービスまたはルーターを見つけます。一般的には、これらの同報通信 (ルーティング情報プロトコル (RIP) およびサービス公示プロトコル (SAP) パケットと呼ばれます) は、他の IPX ルーターおよびサーバーのみが受信する必要があるものです。

IPX に対して使用可能にされている場合、BCM は伝送された公示に基づいて IPX ルーターとサーバーの集合を動的に識別し、RIP および SAP 公示およびその他の同報通信要求を、他の IPX ルーターおよびサーバーにのみ転送します。 BCM IPX によって管理されるブロードキャスト・フレームは、一連のユニキャスト・フレームとして、動的に確認された IPX ルーターとサーバーの組み合わせに送られます。

「BCM IPX サーバー・ファーム検出」が使用可能のとき、BCM IPX は指定の LEC の背後で見つかった IPX ルーターとサーバーの数が、構成可能な限界値 (*BCM IPX サーバー・ファーム限界値*) を超えると、IPX サーバー・ファームを検出します。サーバー・ファームが検出されると、BCM IPX はサーバー・ファーム内の各ダウンストリーム IPX ルーターとサーバーに個別に複数のユニキャスト・フレームを転送するのではなく、そのサーバー・ファームを代表する各 LEC に対して管理フレームを同報通信します。このように BCM IPX は、ネットワークの望まれる分野で、うまく同報通信メカニズムを活用できるようになりました。

BCM IPX BCM を使用可能にした場合は、IPX 公示を受信する必要があるクァイエット装置 (つまり、IPX 公示を転送しない装置) を BCM 静的ターゲットとして構成する必要があります。このような装置の例としては、IPX 公示を監視することにより IPX ネットワーク・トポロジーを検出するソフトウェアを実行するステーションがあります。

BCM IPX サーバー・ファーム検出が使用可能のときに、特定の LEC が BCM IPX によってサーバー・ファームとして扱われるのを防止したい場合には、その LEC の ATM アドレスと MAC アドレスを 00.00.00.00.00.00. と指定して BCM 静的ターゲットを構成します。これにより、たとえ検出されたルーターとサーバーの数が *BCM IPX サーバー・ファーム限界値* を超えても、強制的に BCM IPX はこの LEC の背

後で検出された各ダウンストリーム IPX ルーターとサーバーに対して、BCM が管理するフレームを複数のユニキャスト・フレームとして送信するようにされます。

NetBIOS の BCM サポート

NetBIOS はブロードキャストを多用するプロトコルと見なされているので、BCM には最適な用途です。 NetBIOS 通信は名前に基づいて行われます。送信側ステーションは、照会を同報通信するか、フレームを NetBIOS 機能アドレスにマルチキャストすることによって、特定の着信名に対応する MAC アドレスを確認することができます。後者の場合、ネットワーク上のすべての NetBIOS 装置がフレームを受信し、フレームの着信名が自身に該当するかどうかを判別する必要があります。さらに悪いことに、NetBIOS 装置は特定タイプのフレームの転送を 10 回も繰り返す傾向があります。従来、これはネットワークの輻輳 (ふくそう) がひどい場合に、すべての装置が確実にフレームを受信できるようにするために取られた処置です。

BCM ストラテジーは、BUS に送信された NetBIOS フレームから名前を確認して、固有の NetBIOS 名を MAC アドレスと LE クライアントに対応付けます。固有の NetBIOS 名が確認された後は、その名前あての後続の NetBIOS ブロードキャスト・フレームは、単一の LE クライアントにユニキャスト・フレームとして転送されます。また、BCM は、繰り返し同報通信される特定の NetBIOS フレームをフィルターに掛けます。

BCM は、NetBIOS ネーム・シェアリングに対するサポートを提供します。すなわち、BCM NetBIOS は、同じ NETBIOS 名を共用する複数の LAN アダプターを持つ OS/2 LANServer ステーションを扱うことができます。

ソース・ルート・ブリッジングの BCM サポート

ソース・ルート・マネージメント (SRM) は、802.5 ELAN 用に構成できる追加 BCM 機能です。使用可能の場合、この機能は BCM IP または BCM NetBIOS によって管理されたフレームをさらに処理し、可能な場合はいつでも、全ルート探索 (ARE) またはスパニング・ツリー探索 (STE) フレームを特別ルート・フレーム (SRF) に変換します。フレームを SRF に変換すれば、そのフレームはブリッジ・ネットワークの各リングに転送する必要がなくなります。

各 LE クライアントの背後のトークンリング・トポロジーは、BUS が受信したフレームのルーティング情報フィールド (RIF) を記録することによって確認されます。SRM はトークンリング・トポロジー情報を動的に確認するので、エージング (経年処理) 機構を使用して、最近更新されていない情報を除去します。

BCM または SRM (あるいは、その両方) を使用可能にするかどうかを決める際は、ネットワーク・システム全体の利益と、BCM または SRM を使用可能にした場合に避けられないパケット転送速度の低下とを比較検討する必要があります。

注: ブロードキャスト・マネージャーおよびソース・ルート・マネージメント機能は、**bus-mode** が *adapter* に設定されている場合は利用できず、使用可能にすることはできません。

LAN エミュレーションの信頼性

確実性の欠如が、これまでの LAN エミュレーションに対する最も大きな批判の 1 つでした。 ATM フォーラムでは、LE サービス配布の仕様を用いてこの問題の解決に取り組んでいますが、ルーターはその中間解答の 1 つを提供するものです。 図17は、MSS 冗長問題の解決の枠組みを示しています。『構成』 の章を参照してください。

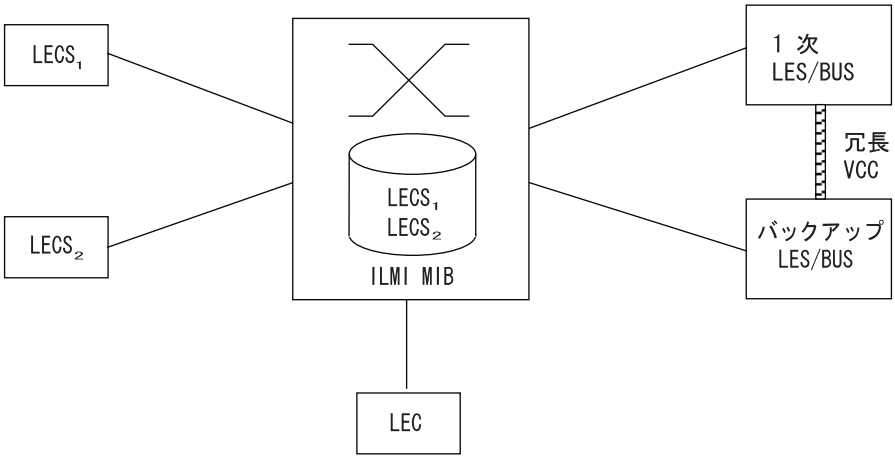


図 17. LAN エミュレーションの冗長度

各 LES/BUS を独立して構成することにより、冗長度をもたせることができます (デフォルトでは冗長度なし)。冗長度が使用可能の場合、LES/BUS は 1 次またはバックアップの役割を担うように構成されます。冗長 LES/BUS として構成されていない場合は、LES/BUS は 1 次です。通常は、LE クライアントから見える LES/BUS は、1 次 LES/BUS だけです。これがバックアップ LES への冗長 VCC の設定と維持の責任を持ちます。この VCC が存在することは、1 次 LES/BUS が運用可であることを示しています。冗長 VCC が確立されている間は、バックアップ LES はコントロール・ダイレクト VCC を受け入れませんが、冗長 VCC が存在**しない** 場合は、バックアップ LES/BUS は通常どおりに ELAN 要求にサービスします。

冗長プロトコルが有効であるためには、LE クライアントは 1 次 LES/BUS を検出し、バックアップに接続しなければなりません。 LE クライアントは VCC の解放によってサーバーの障害を検出します。バックアップ LES/BUS への接続は、LECS を介して行われます。

LE_CONFIGURE_REQUEST を受信すると、LECS は LE クライアントを該当する LES および ELAN に割り当てます。この LES にバックアップが構成されていない場合、LECS は LES の ATM アドレスを戻します。 LES にバックアップ LES が構成されている場合には、LECS は 1 次またはバックアップ LES アドレスを戻します。

LECS がバックアップ LES アドレスを戻すのは、バックアップ LES が LECS と同じ MSS サーバー上に存在し、現在 ELAN として機能している場合、1 次 LES が LECS と同じ MSS サーバー上に存在し、現在 ELAN として機能していない場合、あるいはどちらの LES も LECS と同じ MSS サーバー上に存在せず、クライアントが 1 次 LES に割り当てられた最後のクライアントである場合 (過去 5 分以内) です。それ以外の場合は、1 次 LES アドレスが LE クライアントに戻されます。

LECS は、すべてのクライアント割り当ての短期メモリーを保存し、 LE クライアントの割り当てを 1 次とバックアップ LES の間で交代できるようにしています。この単純な手法は、実質的に無障害で正しい割り当てを行い、自動修正します。最悪の場合でも、この手法は、LE クライアントを ELAN に加入させる構成フェーズを繰り返すだけです。

LECS 確実性は、複数のプラットフォームに重複 LECS を設定し、それらの ATM アドレスを ILMI データベースに含めることによって達成できます。これで、1 次 LECS が利用不能の場合に、LE クライアントはバックアップ LECS に接続するようになります。

LAN エミュレーションのセキュリティー

従来型の LAN では、物理接続により、2 つのステーションが同じ LAN 上にあることが暗黙に示されるので、その意味ではセキュリティーが提供されています。複数のエミュレートされた LAN が単一の ATM ネットワーク上に存在できるので、ELAN 上に存在しないステーションが ELAN 上のステーションに物理的に接続することが可能です。このような状態では、不許可ステーションが LES に接続し、そのサービスの使用を試みることができるので、セキュリティー上の危険が生じます。

ELAN メンバーシップを制御するために、LECS で LE_JOIN_REQUEST を検証するように MSS LES を構成することができます。このモードでは、LES は LE_JOIN_REQUEST からの情報を使用して、LE クライアントに代わって、LE_CONFIGURE_REQUEST を作成します。これらの LE_CONFIGURE_REQUEST には、IBM セキュリティー TLV とともに、発信元 LAN 着信先、発信元 ATM アドレス、ELAN タイプ、最大フレーム・サイズ、LE_JOIN_REQUEST からの ELAN ネームが入っています。セキュリティー要求は、LECS インターフェースと呼ばれる多重化コンポーネントによって LECS に転送され、LECS はその要求を ELAN 割り当てデータベースを用いて検証してからでないと、LE クライアントは ELAN への加入を認められません。

LECS インターフェースは ATM インターフェースに対応しており、ATM インターフェース上に構成されたすべての LES が同じ LECS インターフェースを使用します。 LECS インターフェースは、複数の LES からのセキュリティー要求を多重化して単一の VCC で LECS に送ることにより、VCC 資源を節約します。 LECS インターフェースは、ILMI および事前割り当て LECS アドレス機構を使用して、LECS を動的に見つけます。 LECS への VCC を確立した後、LECS インターフェースはローカル照会を出して、LECS が同じルーター上にあるかどうかを調べます。 LECS が同じルーター上にある場合は、ATM 網上に要求を転送しないで、ローカル・インターフェースを使用して、加入の要求を確認します。

LECS インターフェースを使用すると、ルーターは、LECS が結合を承認した場合にのみ LE クライアントは ELAN に結合されることを保証することができます。これにより、セキュリティーの責任が LES から LECS に移ります。しかし残念ながら、LECS も安全ではありません。 LECS は、任意のステーションからの接続や照会を、検証せずに受け入れます。侵入したステーションが LECS に接続して、繰り返し各種の構成を照会する可能性があります。また、侵入したステーションが他のステーションを装って、別のステーションの構成をダウンロードする可能性もあります。

LECS アクセス制御は、ユーザーが LECS 構成データベースへのアクセスを許可しない ATM アドレス・プレフィックスのリストを構成できるようにします。リストに一致する ATM アドレスからのすべての LECS 接続の試みと LE_CONFIGURE_REQUEST が自動的に拒否されます。 LECS インターフェースと合わせて使用すれば、安全な LANE 環境を提供することができます。

ELAN のセキュリティーを最大化するために、以下のステップを実行することをお勧めします。

1. LECS で、ATM アドレスを使用して、クライアントを LES に割り当てる。詳細については、266ページの『LECS 機能の概説』 を参照してください。
2. ルーター上の LECS インターフェースを起動する。
3. LES のセキュリティー・オプションを起動する。
4. LECS へのアクセスを認めない ATM アドレス・プレフィックスに対して、LECS アクセス制御をアクティブにする。
5. ATM スイッチで *アドレス・スクリーニング* を使用する。このオプションにより、スイッチは起呼端末が呼設定で実際の ATM アドレスを使用しているかどうかを検証します。これにより、ステーションは他のステーションを偽装することはできません。

これらのステップにより、ステーションが正しく識別され、許可されたステーションのみが ELAN に加入することが保証されます。

BUS モニター

BUS モニターは、BUS を過剰に使用する可能性のあるエンド・ユーザーを特定する手段を提供します。使用可能の場合、BUS モニターは、特定の ELAN 上の BUS に送信されるトラフィックを定期的にサンプリングします。各サンプル間隔の終了時に、BUS モニターは BUS の上位ユーザーを識別し、その発信元 MAC アドレス、LE クライアント ATM アドレス、およびそれぞれが BUS に送信したフレーム数を示します。 BUS モニターには、以下のパラメーターを構成できます。

- 上位ユーザーとして記録する MAC アドレス (ホスト) の数
- 各サンプル期間の秒数
- サンプル率。サンプル率は、受信した全フレーム数の分数として表します。たとえば、100 フレームごとに 1 つ、10 フレームごとに 1 つ、または各フレームごとに 1 つといった具合です。
- サンプル期間の相互間の間隔 (分)

LAN エミュレーションの主要な構成パラメーター

この節では、ルーターの LAN エミュレーション・コンポーネントの必須構成パラメーターについて、簡単に説明します。 LAN エミュレーション・コンポーネントの ATM インターフェースを定義してからでないと、コンポーネントを作成することはできません。

1. **LEC**:

LE クライアントを作成するには、ELAN タイプを指定するだけです。 1 つの ATM インターフェース上に 2 つの LE クライアントを定義し、それらを一緒にブリッジする場合には、LE クライアントの 1 つはデフォルト以外の MAC アドレスを使用することが必要です。デフォルトでは、LE クライアントは ATM インターフェースの出荷時設定 MAC アドレスを使用します。デフォルトの最大フレーム・サイズは、イーサネット LE クライアントの場合は 1516 バイトで、トークンリング LE クライアントの場合は 4544 バイトです。

2. **LES/BUS**:

   LES/BUS の必須パラメーターは、ELAN ネーム、ELAN タイプ、および ESI (出荷時設定 MAC アドレスと ATM インターフェースに定義されている任意のローカル管理値が入っているリストから選択します) です。他のパラメーターには、デフォルト値が提供されています。

   デフォルトの最大フレーム・サイズは、イーサネット ELAN クライアントの場合は 1516 バイトで、トークンリング ELAN クライアントの場合は 4544 バイトです。最大フレーム・サイズが ELAN の最大フレーム・サイズより小さい LE クライアントは、ELAN に加入することはできません。最大フレーム・サイズが ELAN の最大フレーム・サイズより大きい LE クライアントは、ELAN に加入することはできますが、加入時の LES とのネゴシエーションの結果として、ELAN の最大フレーム・サイズを使用することになります。

3. **LECS**:

   最小限として、LECS ESI を選択し、デフォルト ELAN 割り当てポリシーを構成することが必要です。詳細については、266ページの『LECS 機能の概説』 を参照してください。

第22章 ATM の使用

この章では、ATM インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『ATM および LAN エミュレーション』
- 『アドレスを入力する方法』
- 284ページの『ATM-LLC 多重化』
- 284ページの『ATM バーチャル・インターフェースの概念』

ATM および LAN エミュレーション

LAN エミュレーションは、ATM ネットワークを介するバーチャル・トークンリングおよびイーサネット LAN に対するサポートを提供します。 ATM アドレッシングについては、『アドレスを入力する方法』 を参照してください。

アドレスを入力する方法

アドレスを入力する方法は、アドレスが (1) IP アドレスであるか、あるいは (2) ATM アドレス、MAC アドレス、またはルート記述子であるかによって、2 通りの方法があります。

1. IP アドレス

   IP アドレスは、小数点付き 10 進数で入力し、4 バイト・フィールドに 4 つの 10 進数 (0 ～ 255) をピリオド (.) で区切って指定します。

   IP アドレスの例

   ```
   01.255.01.00
   ```

2. ATM アドレス、 MAC アドレス、またはルート記述子

   ATM アドレス、MAC アドレス、およびルート記述子は、16 進文字列として入力し、バイト間の区切り文字を使用するかしないかは任意選択です、有効な区切り文字は、ダッシュ (-)、ピリオド (.)、またはコロン (:) です。

   ATM アドレス、MAC アドレス、またはルート記述子の例

   ```
   A1FF01020304
       または
   A1-FF-01-02-03-04
       または
   A1.FF.01.02.03.04
       または
   39.84.0F.00.00.00.00.00.00.00.00.00.03.10.00.5A.00.DE.AD.08
       または
   A1:FF:01:02:03:04
       または
   A1-FF.01:0203:04
   ```

   各タイプのアドレスに必要な 16 進文字数は、それぞれ異なります。

   ATM 40

   MAC 12

   ESI 12

ルート記述子
4

この情報は、ATM、LAN エミュレーション、ATM を介するクラシカル IP と ARP、および ATM を介する IPX と ARP に対して入力するアドレスに適用されます。

ATM-LLC 多重化

ATM インターフェースを介して固有に実行されるプロトコルは、ATM-LLC 多重化を使用して、ATM アドレスと SVC および PVC の両方のチャネルを、ユーザー間で共用することができます。 ATM-LLC は、プロトコルを構成するときに暗黙に構成され、**t 5** から `ATM Config+` コマンド・プロンプトを使用して監視することができます。ATM-LLC 多重化機能の明示的な構成オプションはありません。たとえば、ATM-LLC 多重化を使用する 2 つのプロトコルが同じローカル ATM アドレス (ローカル・エンドポイント) を使用するように構成されている場合、これは暗黙に、両方のプロトコルが同じ共用 ATM アドレスを使用するように構成していることになります。

詳細については、301ページの『ATM-LLC 監視コマンド』 を参照してください。

ATM-LLC 多重化機能を使用するプロトコルと ATM-LLC 多重化機能を使用しないプロトコル (クラシカル IP など) の間で、ATM アドレスまたは SVC/PVC チャネルを共用することはできません。現在、ATM-LLC 多重化機能を使用できるプロトコルは、サーバー・キャッシュ同期プロトコル (SCSP) と APPN の 2 つだけです。

ATM バーチャル・インターフェースの概念

ATM バーチャル・インターフェース (AVI) は、実際には 1 つの物理インターフェースしか存在しないのに、複数の ATM インターフェースがあるような様相を呈します。ルーター上の各物理 ATM インターフェースに対して、複数の AVI を構成することができます。 AVI には、次のような特性があります。

- 各 AVI は、1 つの (そして、1 つだけの) 物理 ATM インターフェースに定義することが必要です。以下では、物理 ATM インターフェースを意味するものとして、ATM 実インターフェース (ARI) を使用します。
- ルーター上の各 ARI には、複数の AVI を構成することができます。
- 高位レイヤーのプロトコルは、ARI と AVI を同等に扱います。プロトコルは、ATM インターフェースの合計数を、ルーター上に構成された ARI と AVI の数の合計とみなします。
- プロトコルは、他のインターフェースからは独立して、各 ATM インターフェース (実または仮想) ごとに構成することができます。

  たとえば、インターフェース 0 (これは、実 ATM インターフェース) では IP アドレス 9.1.1.1 を用いて IP を構成し、インターフェース 1 (これは AVI) ではアドレス 9.2.1.1 を用いて IP を構成することができます。インターフェースが実 ATM インターフェースであるか、実インターフェースに構成されたバーチャル・インターフェースであるかは、プロトコル (たとえば、IP) にとっては違いはありま

せん。また、バーチャル・インターフェース 1 が、実 ATM インターフェース 0 上に構成されているのか、他の物理 ATM インターフェース上に構成されているのかも、プロトコルにとっては無関係です。

ATM バーチャル・インターフェースの使用による利点

ATM バーチャル・インターフェースを使用することによる主な利点は、次のとおりです。

- ATM バーチャル・インターフェース機構を使用すると、物理ATM インターフェースでサポートできるプロトコル・インスタンスが増えます。

  ARI 上に構成できる AVI の実際の数は、ルーター上で利用可能な物理資源 (メモリーなど) によって制限されます。作成できるインターフェースの合計数は、インターフェースのデータ・パケット・サイズによって異なりますが、最大数はルーター当り 253 に限定されています。

  AVI を使用すると、ATM インターフェース当たり 1 インスタンス (または、アドレス) に制限されているプロトコル (IPX など) の構成オプションが、大きく改善されます。適切な数の AVI を構成することによって、各物理 ATM インターフェースが複数の IPX アドレスをサポートできるようになります。

- ATM バーチャル・インターフェース機構は、ATM ネットワーク上のマルチキャスト・ルーティング・プロトコル (MOSPF など) をサポートするために欠かせないものです。

  マルチキャストが正しく動作するためには、各論理サブネットを異なるインターフェース上に構成する***必要*** があります。マルチキャスト・ルーティング・プロトコルは、通常、ルーター・インターフェースから来たパケットは、決して同じインターフェースを介して送信しないという方法で動作するかれです。つまり、あるインターフェースに 2 つ以上のサブネットが構成されており、あるサブネット内の発信元が、同じインターフェース上に定義された別のサブネット内のメンバーにマルチキャスト・パケットを送信する場合、このメンバーは決してそのパケットを受信することはありません。

  各サブネットに対して個別のバーチャル・インターフェースを作成することによって、パケットのマルチキャストを正常に実行することができます。通常は、ルーター上の ATM インターフェースの数が制限され、そのために、マルチキャスト動作用に正しく構成できるサブネットの数が制限されることになります。しかし、AVI を (ルーター上に構成する必要があるサブネットの数に応じて) 必要な数だけ作成すれば、物理 ATM インターフェースの数によって、ルーターに構成できるサブネットの数が制限されることはなくなり、正しいマルチキャスト動作を行えるようになります。

  たとえば、『one-armed』 ルーターは、AVI 機構がなければ、ELAN 以外のインターフェースを介したマルチキャスト・トラフィックをサポートできません。着信パケットは決して同じインターフェースから送信されることはなく、廃棄されてしまうからです。

- ARI 上に複数の AVI を作成し、同じ ARI 上の異なる AVI に異なるプロトコル・インスタンス (たとえば、各 IP サブネット) を構成することによって、性能の向上を図ることができます。

  たとえば、1 つの物理 ATM インターフェース上に複数のサブネットが構成されている場合は、インターフェースは、最大伝送単位または MTU (そのインターフェー

スを介して送信または受信できる最大パケット・サイズ) を、同じインターフェースを共用するすべてのサブネットのうちの最小の MTU に減らすことが必要になります。しかし、その ARI に複数の AVI が作成されており、各 IP サブネットが異なる AVI 上に構成されている場合には、各サブネットは、同じ物理 ATM インターフェース上に構成された他のサブネットを考慮せずに、既存の MTU サイズを使い続けることができます。これにより、MTU サイズの縮小によるパケットの分割と再組み立てが原因でのスループットの低下や遅延を回避することができます。

さらに、物理インターフェースに構成されたプロトコル・アドレスの数を、同じ物理インターフェースに構成された異なるバーチャル・インターフェースに分散させることによっても、性能の向上を図ることができます。インターフェース当たりのプロトコル・リストが短縮されるので、探索が速くなり、処理時間を削減できるからです。

ATM バーチャル・インターフェースの使用による不利益

ATM バーチャル・インターフェースを使用した場合の不利益としては、以下のものがあります。

- AVI は独自の物理資源をもっていないので、各バーチャル・インターフェースで確立できるバーチャル・コネクション (VC) の数は、1 つの物理インターフェースで確立できる数より少なくなります。利用可能な資源 (この場合は、VC) は、1 つの ARI 上に構成された異なるバーチャル・インターフェースと ARI 自体の間で区分されます。

  現行の実現では、資源の割り当てはオンデマンド 方式になっています。各物理 ATM インターフェースが資源をプールしており、これをすべての AVI と 1 つの ARI 自体が利用できるようになっています。

注: すべての資源が ARI とそのすべての AVI 間で共用されるので、ARI に追加された ESI は、自動的に ARI 上に構成されたすべての AVI で利用可能になります。同じ ARI を使用する 2 つの異なるプロトコル・クライアントに対しては、それらが異なるAVI 上に構成されていても、同じ ESI とセレクターの組み合わせを割り当てるべきではありません。

ARI と ARI 上に構成された AVI との間では、限定された PVC 共用が許されています。 PVC の共用は、異なるプロトコル・インスタンスとの間での共用のみに限定されています。同じプロトコルの複数のインスタンスが同じ PVC を共用することはできません。

第23章 ATM の構成および監視

この章では、ATM インターフェースの構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

ATM インターフェース構成プロセスへのアクセス

ATM キャリア・カードおよび 25 Mbps チャーム・アダプターを機構スロットに挿入してからでないと、ATM を構成することはできません。機構スロットに ATM キャリア・カード/25 Mbps チャーム・アダプターの組み合わせが正しく取り付けた後で、ルーターを再ロードする必要があります。

構成プロセスにアクセスするには、以下の手順を使用します。

1. OPCON プロンプトで **talk 6** と入力する。(このコマンドの詳細については、29ページの『第3章 OPCON プロセスおよびコマンド』 を参照してください。) たとえば、次のように入力します。

   ```
   * talk 6
     Config>
   ```

   コンソールに CONFIG プロンプト (`Config>`) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は **Return** をもう一度押してください。

2. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。
3. インターフェース番号を記録する。

   ATM がインターフェースとして指定されていない場合は、クイック構成プロセス *qconfig* を実行して、 ATM インターフェースを動的に追加します。
4. **network** コマンドと構成する ATM の番号を入力する。 たとえば、次のように入力します。

   ATM 構成プロンプト (`ATM Config>`) が表示されます。

ATM 構成コマンド

この節では、ATM 構成コマンドの要約を示します。コマンドは ATM config> プロンプトで入力します。

表 34. ATM 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
INTERFACE	ATM Interface Config> プロンプトを表示するので、ここから ATM インターフェースをリスト、変更、または構成することができます。 • ESI を追加する • 現行構成をリストする、または ESI をリストする • ESI を除去する • ATM ネットワークのパラメーターを設定する • ESI を使用可能または使用不可にする • 終了する
LE-CLIENT	LE Client Config> プロンプトを表示するので、303ページの『第24章 LAN エミュレーション・クライアントの使用』 で説明しているように、LAN エミュレーション・クライアント・インターフェースをリスト、変更、または構成することができます。 • トークンリングまたはイーサネットのエミュレートされた LAN に対して、LAN エミュレーション・クライアント (LEC) を追加する。 • ネットワーク # により LEC を構成する。このコマンドは LE Config> プロンプトを表示するので、ここから特定の LAN エミュレーション・クライアント (LEC) を構成することができます。 • LAN エミュレーション・クライアント (LEC) をリストする。 • LAN エミュレーション・クライアント (LEC) を除去する。
VIRTUAL ATM	ATM Virtual Interface Config> プロンプトを表示するので、296ページの『ATM バーチャル・インターフェース構成コマンド』 で説明しているように、ATM バーチャル・インターフェースをリスト、追加、または除去することができます。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

ATM インターフェース構成コマンド

この節では、特定の ATM インターフェースを構成するためのコマンドの要約を示し、個々のコマンドについて説明します。

コマンドは ATM INTERFACE> プロンプトで入力します。

表 35. ATM INTERFACE 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	ESI を追加します。
List	現行構成をリストするか、または ESI をリストします。
Qos	ATM I/F 0 QOS Config> プロンプトを表示するので、290ページの『QoS 構成』 で説明しているように、サービス品質 (QoS) を構成することができます。
Remove	ESI を除去します。
Set	ATM ネットワークのパラメーターを設定します。
Disable	ESI を使用不可にします。
Enable	ESI を使用可能にします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、ESI を ATM 構成に追加するのに使用します。

ATM アドレスのオクテット 14-19 は、エンド・システム識別子 (ESI) です。同じスイッチに接続されている各エンド・システムは、別々の ESI セットを使用しなければなりません。エンド・システムが起動すると、ILMI を使用して、その ESI を ATM スイッチに登録しようと試みます。スイッチは、すべての登録済み ESI が固有になるようにします。

構文:

add esi *esi-address*

esi *esi-address*

エンド・システム識別子のアドレス

Valid Values: 任意の 12 桁の 16 進数

デフォルト値: なし

List

list コマンドは、この ATM 装置の構成をリストしたり、あるいは構成された ESI の集合をリストするのに使用します。

構文:

list configuration

esi

configuration

ATM 装置構成をリストします。リストされたフィールドの説明は、290ページの『Set』 を参照してください。

例: `list con`

ATM インターフェース構成コマンド (Talk 6)

```
                              ATM Configuration

  Interface (net) number =     0
  Maximum VCC data rate Mbps   =      155
  Maximum frame size    = 9234
  Maximum number of callers =  209
  Maximum number of calls =  1024
  Maximum number of parties to a multipoint call =  512
  Maximum number of Selectors that can be configured  =  200
  UNI Version = UNI 3.0
  Packet trace = OFF
```

esi ATM 構成内の ESI をリストします。

例: `list esi`

```
ATM INTERFACE> list esi

        ESI                 Enabled
------------------------    -------
000000000009                   YES
000000000100                   YES
```

QoS 構成

qos-configuration コマンドを使用すると ATM I/F 0 QOS Config> プロンプトが表示されるので、『QoS 構成』 で説明しているように、サービス品質 (QoS) を構成することができます。

構文:

qos-configuration

Remove

remove コマンドは、ESI を ATM 構成から除去するのに使用します。この ESI を使用しているすべての ATM コンポーネントは、別の ESI を使用するように再構成する必要があります。除去された ESI を使おうとする ATM コンポーネントは、次回のルーターのリスタート時には起動されない可能性があります。

構文:

remove esi *esi-address*

esi *esi-address*
エンド・システム識別子のアドレス

有効値: 任意の 12 桁の 16 進数

デフォルト値: なし

Set

set コマンドは、ATM ネットワーク・パラメーターを指定するのに使用します。

構文:

set max-data-rate

max-frame

max-config-selectors

max-calls

max-callers

max-mp-parties

trace

uni-version

network-id

max-data-rate *speed*

ほとんどの LANE および CIP 接続の VCC トラフィック・パラメーターのデフォルト値および上限を設定します。たとえば、これは LE クライアントが開始するベストエフォート VCC のデフォルト PCR です。シグナルされた SCR 数および PCR 数は、この限界を超えることはできません。たいていの状況では、デフォルト値で十分です。この値を変更した方が有利な状況の一例として、大多数のステーションが 25-Mbps のアダプターを使用している場合があります。この場合は、VCC 上のデータ速度を 25 Mbps に制限して、低速のステーションがルーターからのフレームに圧倒されないようにします。このパラメーターの単位は Mbps です。

有効値:

25

100

155

デフォルト値:

25

例:

```
ATM INTERFACE> set speed 25
```

max-calls

この ATM 装置上に存在できるスイッチド・バーチャル・サーキット (SVC) の最大数を設定します。すべてのポイント・ポイントおよびポイント・マルチポイント SVC は、システム資源を使用します。このパラメーターは、信号接続および交換接続用に予約されるシステム資源を制限するのに役立ちます。このパラメーターを増やすと、同時伝送する SVC の数を増やすことができますが、これらの接続を管理するために必要なシステム・メモリーも増えることになります。

有効値:

64 ～ 10500 の範囲の整数

デフォルト値:

1024

例:

```
ATM INTERFACE> set max-calls 500
```

max-callers

ATM インターフェースを使用する、ルーター上のエンティティーの最大数を設定します。各 LEC、クラシカル IP クライアント、および 1483 ブリッジ・インターフェースは、ATM インターフェースのユーザーとしての資格があり

ます。このパラメーターを増やすと、インターフェースのユーザーの数を増やすことができますが、システム・メモリーの使用量も増えます。

有効値:

64 ～ 1024 の範囲の整数

デフォルト値:

209

例:

```
ATM INTERFACE> set max-callers 25
```

max-config-selectors

ユーザーの特定の制御下にあるセレクターの最大数を設定します。

セレクターは、同じエンド・システム上の異なるユーザーを区別するのに使用されます。 VCC 設定要求は、次のような階層方式でルート指定されます。つまり、ATM スイッチがネットワーク・プレフィックスを使用して着信先 ATM スイッチに転送します。着信先 ATM スイッチは、ESI を使用して着信先エンド・システムに転送します。そして、エンド・システムがセレクターに基づいて着信先ユーザーに通知します。

各 ESI は最大 255 個の対応するセレクター (0x00 ～ 0xff) をもつことができます。セレクターの範囲は、構成されるセレクター範囲と自動的に割り当てられるセレクター範囲の 2 つに区分されています。構成されるセレクター範囲の上限は、ATM インターフェース・パラメーター max-configured-selector で定めます。

ルーター上の ATM コンポーネントは、さまざまな方法でセレクターを選択します。あるコンポーネントの場合は、構成されたセレクター範囲から、ユーザーが明示的にセレクターを構成する必要があります。別のコンポーネント (クラシカル IP クライアントなど) は、実行時に自動的にセレクターを割り当てることができます。ユーザーはセレクターを選択する必要はなく、ルーターが起動時にこれを選択します。このセレクターは、ルーターのリスタートのたびに一貫しているとは保証されません。自動的なセレクターの割り当ては、ネットワーク上の他の装置があらかじめその ATM アドレスを知っていなくても構わない ATM コンポーネントの場合にのみ便利です。

セレクターの範囲の相対サイズは、ルーター上の ATM ユーザーのタイプと数に適合するように変更することができます。

有効値:

0 ～ 255 (0x00 ～ 0xFF)

デフォルト値:

200

注: セレクターは、20 バイトの ATM アドレスのバイト 20 です。

例:

```
ATM INTERFACE> set max-config-selectors 225
```

max-frame

ATM インターフェース上で送信または受信されるデータに許されるオクテットの最大数を設定します。このパラメーターに基づいて、システム・メモリ

ーが割り当てられます。 max-frame を増やすと、システム・メモリーの所要量がふえますが、より大きなフレームを処理できるようになります。

ATM インターフェースを使用するすべてのルーター・エンティティーは、ATM インターフェースの max-frame-size 以下の最大フレーム・サイズを使用する必要があります。これには、すべての LEC および 1483 ブリッジ・インターフェースが含まれます。

有効値:

16 ～ 32000 の範囲の整数

デフォルト値:

9234

例:

```
ATM INTERFACE> set max-frame 1000
```

max-mp-parties

ルーターが開始するポイント・マルチポイント接続上のリーフの最大数を設定します。このパラメーターは、システム・メモリーの割り当てに影響を与えます。ルーターが多数の着信先へのポイント・マルチポイント接続を設定する必要がある場合は、この値を増やすことが必要です。

有効値:

1 ～ 5000 の範囲の整数

デフォルト値:

512

例:

```
ATM INTERFACE> set max-mp-parties 300
```

trace

インターフェース上のパケット・トレース・パラメーターを設定します。パケット・トレースは、VPI/VCI 値の範囲で、使用可能または使用不可にすることができます。トレースの一般的な VPI/VCI 値は、次のとおりです。

- 信号パケットの場合は、0/5
- ILMI パケットの場合は、0/16

有効値:

ON または OFF

デフォルト値:

ON

トレースする VPI/VCI 範囲を入力するようにプロンプトで指示されます。

開始 VPI の有効値:

0 ～ 255

デフォルト値:

0

終了 VPI の有効値:

0 ～ 255

デフォルト値:

255

開始 VCI の有効値:

0 ～ 65535

デフォルト値:

0

終了 VCI の有効値:

0 ～ 65535

デフォルト値:

65535

例:

```
ATM INTERFACE> set trace on
beginning of VPI range [0]? 0
end of VPI range [255]? 0
beginning of VCI range [0]? 5
end of VCI range [65535]? 5
```

uni-version

ATM インターフェースが、接続された ATM スイッチと通信するのに使用する、ユーザー・ネットワーク・インターフェース (UNI) バージョンを設定します。 ATM スイッチおよび ATM 装置インターフェース上で、UNI バージョンが特定のバージョン (AUTO-DETECT ではなく) に構成されている場合は、その UNI バージョンと一致していることが必要です。

UNI バージョンが AUTO として構成されている場合、ATM 装置は使用する UNI バージョンをスイッチから確認しようと試みます。

UNI AUTO-DETECT モードでは、スイッチが UNI バージョンの照会に応答しない場合、デフォルトは UNI 3.0 になります。スイッチが UNI 3.0 または UNI 3.1 以外の値を応答した場合、デフォルトは UNI 3.1 になります。

有効値:

[UNI 3.0|UNI 3.1|AUTO-DETECT|None]

デフォルト値:

UNI 3.0

注: ATM スイッチと一致していることが必要です。

例:

```
ATM INTERFACE> set uni-version 3.0
```

network-id

ATM インターフェースのネットワーク ID を設定します。インターフェース間が ATM で接続されている場合は、複数の ATM インターフェースは同じネットワーク ID をもっていることが必要です。

有効値:

0 ～ 255

デフォルト値:

0

Enable

enable コマンドは、ATM 装置の構成内の ESI を使用可能にするのに使用します。ATM インターフェースは、起動されると、使用可能な ESI のみを登録しようと試みます。

構文:

enable esi *esi-address*

esi *esi-address*
エンド・システム識別子のアドレス

有効値:
任意の 12 桁の 16 進数

デフォルト値:
なし

例: enable esi

```
ATM INTERFACE> enable esi 00:00:00:00:00:09
```

Disable

disable コマンドは、構成内の ESI を使用不可にするのに使用します。使用不可にされた ESI を使用している ATM コンポーネントは、次回にルーターがリスタートされるときには、アクティブになりません。

構文: **disable** esi *esi-address*

esi *esi-address*
エンド・システム識別子のアドレス

有効値:
任意の 12 桁の 16 進数

デフォルト値:
なし

例: disable esi

```
ATM INTERFACE> disable esi 00:00:00:00:00:09
```

バーチャル ATM インターフェース構成プロセスへのアクセス

選択された実 ATM インターフェースの `ATM Config>` プロンプトから、**Virtual ATM** コマンドを使用して、バーチャル ATM 構成コマンド・モードに入ります。

ATM バーチャル・インターフェース構成コマンド

この節では、ATM バーチャル・インターフェース構成コマンドの要約を示します。コマンドは ATM virtual interface config> プロンプトで入力します。

表 36. ATM バーチャル・インターフェース構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	バーチャル ATM インターフェースを追加します。
List	現在構成されているバーチャル ATM インターフェースをリストします。
Remove	バーチャル ATM インターフェースを現行構成から除去します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、ATM バーチャル・インターフェースを追加するのに使用します。新規の ATM バーチャル・インターフェースが、対応する ATM 実インターフェース (この ATM バーチャル・インターフェースにアクセスするのに使用した構成メニュー) に追加されます。新たに作成された ATM バーチャル・インターフェースに割り当てられたネット/インターフェース番号が表示されます。

構文:

add

例:

```
ATM Virtual Interface config> add
Added ATM Virtual Interface Net as interface 5 on physical ATM interface 0
ATM Virtual Interface config>
```

List

list コマンドは、現行の実 ATM インターフェースに定義された構成済み ATM バーチャル・インターフェースをリストするのに使用します。

構文:

list

例:

```
ATM Virtual Interface config> list

                    ATM Virtual Interface Nets
------------------------------------------------------------------------
  ATM interface number = 0
  ATM Virtual Interface Net interface number = 5

ATM Virtual Interface config>
```

Remove

remove コマンドは、ATM バーチャル・インターフェースを除去するのに使用します。実 ATM インターフェース上の、指定されたインターフェース番号をもつバーチャル ATM インターフェースが、SRAM 構成レコードから除去されます。インターフェース番号を指定しなかった場合は、この実 ATM インターフェース上の最後の ATM バーチャル・インターフェースが削除されます。疑問符 (?) を入力すると、現行の実 ATM インターフェース上のすべての ATM バーチャル・インターフェースがリストされ、そのリストから削除したいインターフェースを選択することができます。

構文:

remove *n*

例: remove 5

```
Virtual ATM 5 deleted successfully.
ATM Virtual Interface config>
```

ATM 監視プロセスへのアクセス

構成プロセスにアクセスするには、以下の手順を使用します。このプロセスにより ATM の*監視* プロセスにアクセスできます。

1. OPCON プロンプトで **talk 5** と入力する。(このコマンドの詳細については、29ページの『第3章 OPCON プロセスおよびコマンド』 を参照してください。) たとえば、次のように入力します。

   ```
   * talk 5
   +
   ```

   GWCON プロンプト (+) がコンソールに表示されます。最初にコンソールに入ったときにプロンプトが表示されない場合は **Return** をもう一度押してください。

2. + プロンプトで **interface** と入力して、構成されたインターフェースのリストを表示する。
3. インターフェース番号を記録する。
4. **network** と入力し、続けて ATM インターフェースの番号を入力する。

   ```
   + network 5
   ATM+
   ```

   ATM 監視プロンプト (ATM+) が表示されます。

ATM 監視コマンド

この節では、ATM インターフェースを監視するための ATM コンソール・コマンドの要約を示します。コマンドは、ATM+ プロンプトで入力します。

表 37. ATM 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。

表 37. ATM 構成コマンドの要約 (続き)

コマンド	機能
Interface	ATM Interface+ プロンプトを表示するので、『ATM インターフェース監視コマンド (ATM INTERFACE+ プロンプト)』 で説明しているように、ATM インターフェースを監視することができます。
Atm-llc	ATM LLC+ プロンプトを表示するので、エンド・ポイント、一連のユーザー・クライアントおよび一連の ATM チャネルを監視することができます。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Interface

『ATM インターフェース監視コマンド (ATM INTERFACE+ プロンプト)』 で説明している ATM Interface+ プロンプトを表示します。

構文:

interface

ATM-LLC

301ページの『ATM-LLC 監視コマンド』 で説明している ATM-LLC+ プロンプトを表示します。

構文:

atm-llc

ATM インターフェース監視コマンド (ATM INTERFACE+ プロンプト)

この節では、特定の ATM インターフェースを監視するためのコマンドの要約を示し、個々のコマンドについて説明します。

コマンドは、ATM INTERFACE+ プロンプトで入力します。

表 38. ATM INTERFACE 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
List	ATM アドレスおよび VCC をリストします。
Trace	指定された VPI/VCI 範囲のパケット・トレースを開始/停止します。トレースは ELS によって表示できます。
Wrap	VCC 上のループバック・テストを開始/停止します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、さまざまなカテゴリーの ATM データをリストするのに使用します。

構文:

list addresses
all
circuit
vccs
reserved-bandwidth

addresses
装置上で使用されている ATM アドレスを、記述名とともにリストします。

例:

```
ATM INTERFACE+ list addresses

               ATM Address                                  Name
-----------------------------------------  -----------------------------------
39999999999999000099990200000041347391804  LEC 1 'eth1'
39999999999999000099990200000041347391802  LES/BUS 'eth1'
```

all 下に挙げるものがすべてリストされます。

- アドレス
- 回線統計
- VCC
- 予約帯域幅

circuit 特定の VCI-VPI 組みを指定することにより、特定の VCC の統計をリストします。コマンド行で回線を指定することもできます (たとえば、list circuit 33)。

例:

```
ATM INTERFACE+
list circuit
VPI [0]?
VCI [32]?33

     Frames transmitted   =         2  Bytes transmitted   =       216
     Frames received      =         2  Bytes received      =       216
```

vccs ルーターによって確立されたすべての VCC をリストします。 VCC は、パーマネント (PVC) またはスイッチ (SVC)、ポイント・ポイントまたはポイント・マルチポイントで、それぞれ固有の VPI/VCI によって識別されます。trace コマンドは、VCC の VPI/VCI 値を使用して、特定の VCC 上でパケット・トレースを実行します。

例:

P-P ポイント・ポイント VCC

P-MP ポイント・マルチポイント VCC

ILMI 中間ローカル管理インターフェース VCC

SAAL 信号 VCC

Bx-y VPI x、VCI y への内部結合 VCC

Sx-y VPI x、VCI y への内部スプライス VCC

reserved-bandwidth

ATM インターフェース上の予約帯域幅をリストします。

例:

```
ATM INTERFACE+ list reserved-bandwidth
Line Rate                    : 155000 Kbps
Peak Reserved Bandwidth      : None
Sustained Reserved Bandwidth : None
```

Trace

trace コマンドは、指定された範囲の VPI/VCI 値に対するパケット・トレースを起動するのに使用します。 213ページの『View』 で説明しているように、ELS を使用してトレース・データを表示することができます。

構文:

trace list
on
off

list ATM インターフェース上の現行のパケット・トレース・オプションを表示します。

例:

```
ATM Interface+ trace
on | off | list []? list
Packet trace is ON
Range of VPIs to be traced:       0 -       0
Range of VCIs to be traced:      32 -      39
```

on 指定された VPI/VCI 範囲内のすべてのアクティブ VCC 上のパケット・トレースを開始します。

例:

```
ATM Interface+ trace on
beginning of VPI range [0]?
end of VPI range [0]?
beginning of VCI range [32]?
end of VCI range [65535]? 39
```

off すべての VCC 上のパケット・トレースを停止します。

例:

```
ATM Interface+ trace off
ATM Interface+ trace list
Packet trace is OFF
```

Wrap

wrap コマンドは、アダプターの ATM インターフェース上でループバック・データ・テストを実行するのに使用します。 Wrap は、VPI-VCI の組を指定することにより、VC 単位で出すことができます。データは内部でループバックされます。

ラップの開始、ラップの停止、または現行ラップ設定値の表示を、選択的にスタートさせることができます。

ラップを停止または表示すると、以下の統計が表示されます。

- ラップ送信数
- ラップ受信数
- ラップ送信エラーの数
- ラップ受信エラーの数
- ラップ受信タイムアウト数

表示の場合は、現行ラップ統計が表示されます。

停止の場合は、最終ラップ統計が表示されます。

構文:

wrap display
start
stop

display
現行ラップ設定値を表示します。

start ラップ手順を開始し、パターンの VPI-VCI 長さとパターン自体を指定します。

例:

```
ATM Interface+ wrap start
VPI [0]?
VCI [32]?
wrap pattern length [32]?
Enter 32-byte wrap pattern: [ABCDEFGHIJKLMNOPQRSTUVWXYZ123456]?
```

stop ラップ手順を停止し、最終ラップ統計を表示します。

ATM-LLC 監視コマンド

この節では、ATM LLC 多重化のためのコマンドについて説明します。

コマンドは ATM-LLC+ プロンプトで入力します。

表 39. ATM LLC 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
List	各種のオプションをリストします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、さまざまなカテゴリーの ATM LLC 監視データをリストするのに使用します。

構文:

list endpoints

channels

endpoints

装置上の ATM-LLC 多重化機能を使用するプロトコルによって使用される ATM アドレスをリストします。エンドポイントは、エンド・システム識別子とセレクターとして表示されます。

例: `list endpoints`

```
ATM-LLC+ list endpoints
```

channels

装置上の ATM-LLC 多重化機能を使用するプロトコルによって使用されるチャネルをリストします。

例: `list channels`

```
ATM-LLC+ list channels
```

ATM バーチャル・インターフェース監視コマンド

ATM バーチャル・インターフェースの監視は、ATM LLC 監視コマンドを使用して行います。詳細については、301ページの『ATM-LLC 監視コマンド』を参照してください。

第24章 LAN エミュレーション・クライアントの使用

この章では LAN エミュレーション・クライアント (LEC) について説明します。本章には、以下の節が含まれています。

- 『LAN エミュレーション・クライアントの概要』

LAN エミュレーション・クライアントの概要

ルーター上の LEC は、従来のルーターおよびブリッジ上の 『プロンプト』 または『インターフェース』 の役目を果たします。ルーターは、LEC を介してトラフィックを送受信することによって、ポート間のトラフィックをブリッジおよびルート指定します。

LEC には、次の 2 つのプロンプト・レベルがあります。

1. `LE Client Config>` では、すべての LEC の環境を制御するコマンドを入力できます。このプロンプト・レベルのコマンドについては、305ページの『LAN エミュレーション・クライアントの構成』 で説明します。
2. コマンドの 1 つの **config** を使用すると、もう 1 つのプロンプト・レベルである `LEC Config>` にアクセスします。ここでは、特定の LEC を構成するためのコマンドを入力できます。

LAN エミュレーション・クライアントに関するコマンドについては、以下で説明します。

第25章 LAN エミュレーション・クライアントの構成および監視

この章では、LAN エミュレーション・クライアント (LEC) の構成方法について説明します。本章には、以下の節が含まれています。

- 『LAN エミュレーション・クライアントの構成』
- 307ページの『ATM フォーラム準拠 LE クライアントの構成』
- 322ページの『LEC 監視環境へのアクセス』
- 323ページの『LEC 監視コマンド』

LAN エミュレーション・クライアントの構成

この節では、特定の ATM インターフェース上の LE クライアントの集合を表示、変更、および使用するためのコマンドについて説明します。

`LE Client Config>` プロンプトにアクセスするには、 288ページの『ATM 構成コマンド』 で説明しているように、ATM Config> プロンプトで **le-c** と入力します。

コマンドは、288ページの『ATM 構成コマンド』 で説明しているように、`ATM Config>` プロンプトのもとの `LE Client Config>` プロンプトで入力します。

表 40. LAN EMULATION クライアント構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	以下のタイプの ATM フォーラム準拠のエミュレートされた LAN アーキテクチャーの LEC を追加します。 • イーサネット • トークンリング
Config	`LEC Config>` プロンプトを表示するので、ここから特定の LAN エミュレーション・クライアントを構成することができます。
List	LEC をリストします。
Remove	LEC を除去します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、トークンリングまたはイーサネット・エミュレート LAN の LEC を追加するのに使用します。

構文:

add Ethernet

Token Ring

token-ring

トークンリング・エミュレート LAN

LE Client Config>

例: add token ring

```
LE Client Config> add token-ring
Added Emulated LAN as interface 3
```

ethernet

イーサネット・エミュレート LAN

例: add ethernet

```
LE Client Config> add ethernet
Added Emulated LAN as interface 2
```

Config

config コマンドを使用すると、LEC Config> プロンプトが表示されるので、ここから特定の LAN エミュレーション・クライアントの詳細を構成することができます。

構文:

config interface#

interface#

LEC が構成に追加されたとき、ルーターによって割り当てられた整数の番号。 LEC に割り当てられているインターフェース番号を調べるときは、**list** コマンドを使用します。

例: config

```
LE Client Config> config 3
ATM LAN Emulation Client configuration
```

List

list コマンドは、LAN エミュレーション・クライアントをリストするのに使用します。

構文:

list

例: list

```
LE Client Config> list
                ATM Forum Compliant Emulated LANs
-----------------------------------------------------
  Physical ATM interface number = 0
  LEC interface number = 1
  Emulated LAN type    = Token Ring Forum Compliant
  Emulated LAN name    =
```

Remove

remove コマンドは、LEC を除去するのに使用します。 LEC が構成に追加されたときにルーターによって割り当てられたインターフェース番号を指定する必要があります。 LEC に割り当てられているインターフェース番号を調べるときは、**list** コマンドを使用します。

構文:

remove interface#

interface#
ルーターによって割り当てられた整数の番号

ATM フォーラム準拠 LE クライアントの構成

この節では、ATM フォーラム準拠 LAN エミュレーション・クライアントを構成するためのコマンドについて説明します。 Ethernet Forum Compliant LEC Config> プロンプトまたは Token Ring Forum Compliant LEC Config> プロンプトのいずれかで、該当するコマンドを入力します。下表のコマンドは、指摘されているものを除いて、トークンリング LEC およびイーサネット LEC の両方に適用されます。

コマンドは、LE Client Config>> プロンプトで **config** コマンドを入力した後、LEC Config>> プロンプトで入力します。

表 41. LAN エミュレーション・クライアントの構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
ARP-Configuration	ATM フォーラム準拠クライアントの LE-ARP 構成を構成することができます。
RIF-Timer	RIF 内の情報が更新される前に維持されている最大時間数を設定します。トークンリング LEC にのみ適用されます。
Source-routing	ソース・ルート・ブリッジングを使用可能または使用不可にするのに使用します。トークンリング LEC にのみ適用されます。
IP-Encapsulation	IP カプセル化を、イーサネット (タイプ X'0800') または IEEE (SNAP 付き 802.3) として設定します。イーサネット LEC にのみ適用されます。
List	LAN エミュレーション・クライアント構成をリストします。
QOS-Configuration	elan-x LEC QoS Config> プロンプトを表示するので、ここから、885ページの『LE クライアント QoS 構成コマンド』で説明しているように、サービス品質を構成することができます。
Set	LAN エミュレーション・クライアントのパラメーターを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

ARP Configuration

arp-configuration コマンドは、ATM フォーラム準拠 LAN エミュレーション・クライアントの静的 LE-ARP エントリーを構成するのに使用します。

構文:

arp-configuration

例:

```
Token Ring Forum Compliant LEC Config> arp-configuration
ATM LAN Emulation Clients ARP configuration
```

表 42. ATM LAN エミュレーション・クライアント ARP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	MAC またはルート記述子 ARP を使用して、LE-ARP キャッシュ・エントリーを追加します。
Config	キャッシュ・エントリー QoS パラメーター値を設定します。
List	構成された ARP キャッシュ・エントリーをリストします。
Remove	ARP キャッシュ・エントリーを除去します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、MAC アドレスまたはルート記述子を使用して ARP キャッシュ・エントリーを追加するのに使用します。

MAC アドレスおよびルート記述子は、16 進文字列として入力し、バイト間の区切り文字を使用するかしないかは任意選択です。有効な区切り文字は、ダッシュ (-)、ピリオド (.)、またはコロン (:) です。

構文:

add mac

route-descriptor

例 1:

```
ARP config for LEC>add mac
MAC address of LE ARP Entry []? 123456789098
ATM address in 00.00.00.00.00.00:... form []? 390f000000000000000000000000123456789098
Destination Type -  REMOTE or LOCAL [Remote]?
```

例 2:

```
ARP config for LEC>add route 12.34
ATM address in 00.00.00.00.00.00:... form []? 390f000000000000000000001234567890988888
ARP config for LEC>
```

Config

Config コマンドは、ARP フォーラム準拠 LAN エミュレーション・クライアントの固定 ARP キャッシュ・エントリー QOS パラメーターを構成するのに使用します。

構文:

config *arp-entry-number*

例:

```
ARP config for LEC> config
ARP entry number [1]
Configure LEC ARP entry
```

表 43. ATM LAN エミュレーション・クライアント ARP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Set	QoS パラメーター値を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Set:

Set コマンドは、ARP フォーラム準拠 LAN エミュレーション・クライアントの固定 ARP キャッシュ・エントリー QOS パラメーターを構成するのに使用します。

構文:

set max-reserved-bandwidth
traffic-type
peak-cell-rate
sustained-cell-rate
qos-class
max-burst-size

例:

```
ARP entry 'identifier' config> set ?
 MAX-RESERVED-BANDWIDTH
 TRAFFIC-TYPE
 PEAK-CELL-RATE
 SUSTAINED-CELL-RATE
 QOS-CLASS
 MAX-BURST-SIZE
```

QoS パラメーターについての詳細は、877ページの『第67章 サービス品質 (QoS) の使用』を参照してください。

List

list コマンドは、ARP 構成に関する情報を表示するのに使用します。

Remove

remove コマンドは、構成された MAC アドレスまたはルート記述子 LE-ARP エントリーを除去するのに使用します。

提供されたリストから、除去する ARP エントリー番号を選択します。

構文:

remove *arp-entry-number*

RIF-Timer (トークンリング・フォーラム準拠 LEC の場合のみ)

RIF-Timer コマンドは、RIF 内の情報が更新される前に維持されている最大時間数を設定するのに使用します。範囲は 0 ～ 4096 です。デフォルト値は 120 秒です。

構文:

rif-timer *value*

例:

```
rif-timer 100
```

Source-routing (トークンリング・フォーラム準拠 LEC の場合のみ)

source-routing コマンドは、エンド・ステーションのソース・ルーティングを使用可能または使用不可にするのに使用します。ソース・ルーティングというのは、エンド・ステーションがソース・ルーティング・ブリッジを経由するのに使用するソース・ルートを決めるプロセスです。ソース・ルーティングにより、IP、IPX、および AppleTalk フェーズ 2 プロトコルは、ソース・ルート・ブリッジの反対側のノードに到達することが可能になります。

ソース・ルーティングが使用可能でも使用不可でも、装置のこの機能は変更されません。デフォルトの設定値は「使用可能」です。

一部のステーションは、ソース・ルーティング RIF をもつフレームを正常に受信できません。これは特に NetWare ドライバーに共通に見られる特徴です。この状態のときは、ソース・ルーティングを使用不可にすれば、これらのステーションと通信できるようになります。

ソース・ルーティングを使用可能にするのは、IP、IPX、および AppleTalk フェーズ 2 パケットを通過させたいソース・ルーティング・ブリッジがこのリング上に存在する場合だけに限るべきです。また、LLC テスト応答メッセージを戻すようにしたい場合は、ソース・ルーティングを使用可能にする必要があります。

構文:

source-routing enable

disable

例:

```
source-routing disable
```

IP-Encapsulation (イーサネット ATM フォーラム準拠 LEC の場合のみ)

IP-encapsulation コマンドは、イーサネット (イーサネット・タイプ X'0800') または IEEE 802.3 (SNAP を備えたイーサネット 802.3) を選択するのに使用します。タイプ **E** (イーサネット) または **I** (EEE-803.3) のいずれかを指定します。

構文:

IP-encapsulation Ethernet

IEEE-802.3

List

list コマンドは、LE クライアントの構成をリストするのに使用します。

構文:

list

QoS

qos-configuration コマンドは、LEC QoS Config> プロンプトを表示させて、そこから、885ページの『LE クライアント QoS 構成コマンド』 で説明しているように、サービス品質 (QoS) を構成するのに使用します。

構文:

qos-configuration

Set

set コマンドは、LE クライアントのパラメーターを設定するのに使用します。

構文:

set
- arp-aging-time
- arp-cache-size
- arp-queue-depth
- arp-response-time
- auto-config
- best-effort-peakrate
- bus-connect-retries
- conn-completion-time
- control-timeout
- elan-name
- esi-address
- flush-timeout
- forward-delay
- forward-disconnect-timeout
- frame-size
- initial-control-timeout
- lecs-atm-address
- les-atm-address

mac-address

multicast-send-avg

multicast-send-peak

multicast-send-type

multiplier-control-timeout

path-switch-delay

reconfig-delay-min

reconfig-delay-max

retry-count

selector

trace

unknown-count

unknown-time

vcc-timeout

arp-aging-time

ARP エージング・タイムを設定します。これは、その関係の検証がない場合に、 LEC が LE_ARP キャッシュに項目を維持する最大時間です。エージング・タイムを大きくすると、セッションの設定時間が速くなりますが、メモリーの使用量が増え、ネットワーク構成の変更への対応が遅くなる可能性があります。

有効値:

10 ～ 300 秒の範囲の整数

デフォルト値:

300

例:

```
LEC Config> set arp-aging-time 200
```

arp-cache-size

ARP キャッシュ内のエントリー数を設定します。 ARP キャッシュのサイズは、同時伝送できるデータ・ダイレクト VCC の数を制限します。 ARP キャッシュを大きくすると、メモリーの所要量が増えますが、クライアントはより多くの着信先と同時に通話できるようになります。

有効値:

10 ～ 65535 の範囲の整数

デフォルト値:

5000

例:

```
LEC Config> set arp-cache-size 10
```

arp-queue-depth

ARP キャッシュ・エントリー当たりの待ち行列化フレームの最大数を設定し

ます。 LEC は、データ・パスを、マルチキャスト・センド VCC からデータ・ダイレクト VCC に切り替えるときに、フレームを待ち行列に入れます。待ち行列が満ぱいのときは、転送するために LEC に渡されたフレームは廃棄されます。待ち行列を大きくすると、メモリーの所要量は増えますが、データ・パスを切り替えるときに廃棄されるフレームの数が減ります。

有効値:

0 ～ 10 の範囲の整数

デフォルト値:

5

例:

```
LEC Config> set arp-queue-depth 10
```

arp-response-time

予期される ARP 応答時間を設定します。この値は、未応答 LE ARP 要求を再試行する頻度を制御します。値を大きくすると、LE ARP の数が少なくなり、その結果、トラフィックが減って、データ・ダイレクト VCC が確立される前の時間が長くなる可能性があります。

有効値:

1 ～ 30 秒の範囲の整数

デフォルト値:

1 秒

例:

```
LEC Config> set arp-response-time 20
```

auto-config

この LEC が LECS auto-config モードを使用するかどうかを指定します。YES または NO を指定します。LEC は LECS に連絡して、その LES のアドレスおよびその他の種々の構成パラメーターを入手することができます。

有効値:

YES のときは、LES の ATM アドレスを構成する必要はありません。

NO のときは、316 で説明しているように、**set les-atm-address** コマンドを使用して、LES の ATM アドレスを構成する必要 があります。

デフォルト値:

NO

例:

```
LEC Config> set auto-config yes
```

best-effort-peakrate

ベストエフォート・ピーク速度を設定します。ベストエフォート・マルチキャスト・センド接続を確立するときに使用されます。

最大ピーク速度は、ATM 装置の最大データ速度によって決まります。

以下のように、1 から最大ピーク速度 (定義は最大データ速度) までの範囲内の整数 (Kbps) を指定します。

- ATM 最大データ速度が 25 Mbps の場合、最大ピーク速度は 25,000 Kbps
- ATM 最大データ速度が 155 Mbps の場合、最大ピーク速度は 155,000 Kbps

有効値:

1 ～ 装置の最大データ速度の範囲の整数

デフォルト値:

155000

例:

```
LEC Config> set best-effort-peakrate 24000
```

bus-connect-retries

このパラメーターは、LEC が初期状態に戻る前に、BUS への再接続を試みる最大試行回数を設定します。

有効値:

0 ～ 2

デフォルト値:

1

connection-completion-time

接続完了時間を設定します。これは、発呼側からのデータまたは READY_IND メッセージが予期される時間間隔です。

クライアントへのデータ・ダイレクト VCC が確立されると、LEC は、この時間枠内にデータまたは READY_IND メッセージを受信することを予期します。 LEC は、データまたは READY_IND を受信するまでは、確立されたデータ・ダイレクト VCC を介してフレームを送信しません。このパラメーターは、LEC が READY QUERY (READY_IND を受信するホップ数) を出す前に経過する時間を制御します。値を小さくすると、応答時間が速くなりますが、不要な伝送も増えます。

有効値:

1 ～ 10 秒の範囲の整数

デフォルト値:

4

例:

```
LEC Config> set connection-completion-time 5
```

control-timeout

このパラメーターは、要求の最大累算制御タイムアウトを設定します。

現行タイムアウト値は、***initial-control-timeout*** の値に初期設定されます。要求に対するレスポンスを現行タイムアウト値以内に受け取らなかった場合、現行タイムアウト値に ***multiplier-control-timeout*** の値が乗算され、その後で再度その要求が出されます。現行タイムアウト値が満了するたびに、このプロセスが繰り返され、現行タイムアウト値が ***control-timeout*** の値を超えるまで続けられます。

有効値:

10 ～ 300 秒の範囲の整数

デフォルト値:

30

例:

```
LEC Config> set control-timeout 100
```

elan-name

LEC が加入を望む ELAN の名前を指定します。これは、構成要求で LECS に送信される (LEC が自動構成される場合)、または加入要求で LES に送信される ELAN ネームです。 LECS または LES は、レスポンスで異なる ELAN ネームを戻すことがあります。

有効値:

0 ～ 32 バイトの長さの文字列

デフォルト値:

Blank

注: ブランク名 (長さが 0 のストリング) は有効です。

例:

```
LEC Config> set elan-name FUZZY
```

esi-address

LEC の ATM アドレスの ESI 部分を設定します。

LEC の ATM アドレスの ESI 部分 (オクテット 13 ～ 19) を指定します。 LEC の ESI とセレクターの組み合わせは、装置上のすべての LAN エミュレーション・コンポーネント間で固有であることが必要です。

有効値:

任意の 12 の 16 進数字

デフォルト値:

Burned-in ESI

例:

```
set esi
Select ESI
   (1) Use burned in ESI
   (2) 11.22.33.44.55.66

Enter selection [1]?
```

flush-timeout

フラッシュ・タイムアウトを設定します。 LE_FLUSH_REQUEST の送信後、回復処置を取る前に LE_FLUSH_RESPONSE の受信を待つ制限時間です。回復時に、待ち行列化されていたフレームは廃棄され、新たなフラッシュ要求が送信されます。

データ・パスを、マルチキャスト・センドからデータ・ダイレクトに切り替えるときに、クライアントはマルチキャスト・センド VCC を介してフラッシュ要求を送信します。フラッシュ応答を受信するまで、またはパス・スイッチ遅延が満了するまで、フレームは宛先用の待ち行列に入れられます。

有効値:

1 ～ 4 秒の範囲の整数

デフォルト値:

4

例:

```
LEC Config> set flush-timeout 3
```

forward-delay

転送遅延を設定します。 LE ARP キャッシュ内のエントリーは、定期的に再検証する必要があります。転送遅延時間は、ネットワーク・トポロジーの変更時に、リモート・エントリーがキャッシュ内にとどまっていられる最大時間です。エージング・タイムを長くすると、古い (無効な) エントリーが増えますが、再検証のための通信量は減ります。

有効値:

4 ～ 30 秒の範囲の整数

デフォルト値:

15

例:

```
LEC Config> set forward-delay 10
```

forward-disconnect-timeout

このパラメーターは、LEC が BUS からの最後のマルチキャスト・フォワード VCC を失った後、初期状態に戻る前に待つ時間を設定します。この遅延により、BUS は初期状態に戻る前にクライアントへの再接続を試みることが可能になります。

有効値:

10 ～ 300 秒

デフォルト値:

60

frame-size

フレーム・サイズを設定します。

frame-size に指定される値は、 292ページで説明されているように、ATM INTERFACE> **set max-frame** コマンドを使用して ATM max-frame に対して指定される値以下であることが必要です。

有効値:

1516

4544

9234

18190

デフォルト値:

ELAN タイプがトークンリングの場合、デフォルト値は 4544 です。
ELAN タイプがイーサネットの場合、デフォルト値は 1516 です。

例:

```
LEC Config> set frame-size 4544
```

initial-control-timeout

このパラメーターは、314ページで説明されている制御タイムアウト・アルゴリズムで使用される初期制御タイムアウトの値を設定します。

有効値:

1 ～ 10

デフォルト値:

5

例:

```
LEC Config> set initial-control-timeout 10
```

lecs-atm-address

LECS の ATM アドレスを指定します。

自動構成に設定されている場合、クライアントは LECS への接続を試みます。ある LECS に接続できない場合には、別の LECS ATM アドレスを試行することができます。 LECS ATM アドレスを試行する順序は、次のとおりです。

1. この構成された LECS アドレス
2. ILMI を通して入手した任意の LECS アドレス
3. ATM フォーラムによって定義された事前割り当て LECS アドレス

デフォルト値は、提供されていません。

注: このコマンドは、1 行のコマンド行に入力しなければなりません。本書では、スペースの関係で 2 行に示してあります。

例:

```
LEC Config> set lecs-atm-address
39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.01
```

les-atm-address

LES ATM アドレスを設定します。 313ページの **set auto-config** コマンドの項に説明されている lecs-auto-config の設定値に応じて、このコマンドは任意選択または必須になります。

- auto-config が YES のときは、les-atm-address は構成できません。
- auto-config が NO のときは、les-atm-address は必須です。

LES の ATM アドレスを指定します。デフォルト値は、提供されていません。

注: このコマンドは、1 行のコマンド行に入力しなければなりません。本書では、スペースの関係で 2 行に示してあります。

例:

```
LEC Config> set les-atm-address
     39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
```

mac-address

この LE クライアントの MAC アドレスを設定します。クライアントが ATM インターフェースの出荷時設定 MAC アドレスを使用すると指定しても、あ

るいは別の MAC アドレスを指定しても構いません 。 2 つのクライアントがブリッジされている場合は、それぞれ異なる MAC アドレスを使用することが必要です。

この MAC アドレスは、クライアントが ELAN に加入するときに LES に登録されます。

有効値:

任意の有効な MAC アドレス

デフォルト値:

なし

例:

```
LEC Config> set mac-address
  Use adapter address for MAC? [No]
  MAC address []: 10.00.5a.00.00.01
```

multicast-send-avg

マルチキャスト・センド VCC の平均速度 (Kbps) を設定します。 VCC 上の帯域幅を BUS に予約するために LEC によって使用されます。これは、予約帯域幅マルチキャスト・センド VCC を設定するときに使用され、順方向と逆方向の持続セル速度を指定します。

このパラメーターは、multicast-send-type が予約帯域幅である場合にのみ適用されます。 multicast-send-avg と multicast-send-peak が等しいときには、固定ビット速度 (CBR) マルチキャスト・センドがシグナルされます。そうでない場合は、可変ビット速度 (VBR) マルチキャスト・センドがシグナルされます。 Multicast-send-avg は multicast-send peak 以下でなければなりません。

予約帯域幅マルチキャスト・センド VCC は、輻輳 (ふくそう) したネットワークではデータ転送速度が速くなる可能性がありますが、帯域幅を予約しておきながら、それを使用しないことは、ネットワーク・リソースの浪費になります。

multicast-send-type が予約されている場合は、multicast-send-avg および multicast-send-peak を指定する必要があります。

例:

```
LEC Config> set multicast-send-avg 4000
```

multicast-send-peak

マルチキャスト・センド・ピーク速度 (Kbps) を設定します。 VCC 上の帯域幅を BUS に予約するために LEC によって使用されます。これは、予約帯域幅マルチキャスト・センド VCC を設定するときに使用され、順方向と逆方向のピーク・セル速度を指定します。

このパラメーターは、multicast-send-type が予約帯域幅である場合にのみ適用されます。 multicast-send-avg と multicast-send-peak が等しいときには、固定ビット速度 (CBR) マルチキャスト・センドがシグナルされます。そうでない場合は、可変ビット速度 (VBR) マルチキャスト・センドがシグナルされます。 Multicast-send-avg は multicast-send peak 以下でなければなりません。

予約帯域幅マルチキャスト・センド VCC は、輻輳 (ふくそう) したネットワークではデータ転送速度が速くなる可能性がありますが、帯域幅を予約しておきながら、それを使用しないことは、ネットワーク・リソースの浪費になります。

multicast-send-type が予約されている場合は、multicast-send-avg および multicast-send-peak を指定する必要があります。

例:

```
LEC Config> set multicast-send-peak 155
```

multicast-send-type

マルチキャスト・センド・タイプを設定します。マルチキャスト・センド VCC を確立するときに LEC が使用する方式を指定します。

multicast-send-avg と multicast-send-peak が等しいときには、固定ビット速度 (CBR) マルチキャスト・センドがシグナルされます。そうでない場合は、可変ビット速度 (VBR) マルチキャスト・センドがシグナルされます。Multicast-send-avg は、少なくとも multicast-send peak に等しくなければなりません。

予約帯域幅マルチキャスト・センド VCC は、輻輳 (ふくそう) したネットワークではデータ転送速度が速くなる可能性がありますが、帯域幅を予約しておきながら、それを使用しないことは、ネットワーク・リソースの浪費になります。

multicast-send-type が予約されている場合は、multicast-send-no および multicast-send-peak を指定する必要があります。

有効値:

ベストエフォートまたは予約 (Reserved)

デフォルト値:

ベストエフォート

例:

```
LEC Config> set multicast-send-type best-effort
```

multiplier-control-timeout

このパラメーターは、314ページで説明されている制御タイムアウト・アルゴリズムで使用される制御タイムアウト乗数値を設定します。

有効値:

2 ～ 5

デフォルト値:

2

例:

```
LEC Config> set multiplier-control-timeout 5
```

path-switch-delay

パス・スイッチ遅延を設定します。

LEC は、データ・ダイレクト VCC の使用を開始する前に、BUS を通して着側に送信されたすべてのフレームが着信先に到達したことを確認する必要があります。この確認は、フラッシュ・プロトコルを使用して行うか、あるい

は BUS に最後のパケットを送信した後で path-switch-delay 秒数だけ待つことによって行います。値を小さくすると性能が改善しますが、非常に輻輳したネットワーク上では、順序誤り (out-of-order) パケットが発生する可能性があります。

有効値:

1 ～ 8 秒の範囲の整数

デフォルト値:

6

例:

```
LEC Config> set path-switch-delay 5
```

reconfig-delay-min

このパラメーターは、LEC が初期状態に戻るときの最小遅延時間を設定します。この値は ≤ ***reconfig-delay-max*** でなければなりません。

有効値:

1 ～ ***reconfig-delay-max*** の値

デフォルト値:

1

例:

```
LEC Config> set reconfig-delay-min  5
```

reconfig-delay-max

このパラメーターは、LEC が初期状態に戻るときの最大遅延時間を設定します。この値は ≥ ***reconfig-delay-min*** でなければなりません。

有効値:

1 ～ 10

デフォルト値:

5

例:

```
LEC Config> set reconfig-delay-max 9
```

retry-count

再試行カウントを設定します。これは、LEC が特定のフレームの LAN 着信先に対して LE_ARP_REQUEST を再試行する回数です。指定された回数の後も ARP レスポンスを受信しなかった場合、そのエントリーは LE ARP キャッシュから除去されます。

有効値:

0 ～ 2 の範囲の整数

デフォルト値:

1

例:

```
LEC Config> set retry-count 2
```

selector

クライアントの ATM アドレスのセレクター部分を指定します。 ESI とセレ

クターの組み合わせは、装置上のすべての LANE コンポーネント間で固有であることが必要です。デフォルトでは、構成された ESI に対して固有のセレクターが選択されます。

有効値:

同じ ESI を使用する別の LANE コンポーネントによって使用されていない、16 進数の任意のオクテット

例:

```
LEC Config> set selector 01
```

trace LEC のトレースを使用可能にします。パケット・トレースを実行するには、3 つのステップが必要です。

1. パケット・トレース・システムを使用可能にする (ELS 下で)
2. LEC サブシステム上のトレースを使用可能にする (ELS 下で)
3. 必要な LEC 上のパケット・トレースを使用可能にする (このコマンドを使用して)

有効値:

使用可能または使用不可

デフォルト値:

使用不可

例:

```
Token Ring LEC config>set trace
Trace packets on the LEC? [No]?yes
```

unknown-count

不明フレーム・カウントを設定します。これは、unknown-time パラメーターで指定された時間内に BUS に送信できる、特定のユニキャスト MAC アドレスまたはルート記述子のフレームの最大数です。値を大きくすると、廃棄されるフレーム数は減りますが、BUS の負荷が増えます。

有効値:

1 ～ 255 の範囲の整数

デフォルト値:

10

unknown-time

不明フレーム時間を設定します。これは、特定のユニキャスト MAC アドレスまたはルート記述子のフレームの最大数 (unknown-count パラメーターで示された) を BUS に送信できる時間間隔です。値を大きくすると、廃棄されるフレーム数が増えますが、BUS の負荷は減ります。

有効値:

1 ～ 60 秒の範囲の整数

デフォルト値:

1

例:

```
LEC Config> set unknown-time 5
```

vcc-timeout

VCC タイムアウトを設定します。この期間トラフィックの送信がなかった場合、データ・ダイレクト VCC を解放する必要があります。

有効値: 0 ～ 31536000 秒 (1 年)

デフォルト値: 1200

注: このパラメーターに意味があるのは、SVC 接続の場合だけです。

例:

```
LEC Config> set vcc-timeout 1000
```

LEC 監視環境へのアクセス

LEC 監視コマンドにアクセスするには、以下の手順を使用します。このプロセスによって、LEC 監視 プロセスにアクセスすることができます。

1. OPCON プロンプトで **talk 5** と入力する。(このコマンドの詳細については、29ページの『第3章 OPCON プロセスおよびコマンド』 を参照してください。) たとえば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、GWCON プロンプト (+) がコンソールに表示されます。最初に構成に入ったときにプロンプトが表示されない場合は **Return** をもう一度押してください。

2. + プロンプトで **network ?** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示し、監視したい LEC の *interface number* を入力する。たとえば、次のように入力します。

   ```
   + network ?

   1  : ATM Ethernet LAN Emulation: ETH
   2  : IP Protocol Network
   3  : Bridge Application
   5  : CHARM ATM Adapter
   Network number [0]? 1
   LEC+
   ```

   LEC 監視プロンプト (LEC+) が表示されます。

   監視したい LEC のインターフェース番号が分かっている場合は、 **network** コマンドに続けて、その LEC のインターフェース番号 を入力します。

   ```
   + network 1
   LEC+
   ```

LEC 監視コマンド

この節では、LEC 監視コマンドの要約を示し、個々のコマンドについて説明します。 LEC 監視コマンドには LEC+ プロンプトからアクセスできます。 表44 は、コマンドを示しています。

表 44. LE 構成監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	以下のものをリストします。 • LEC アドレス解決テーブル (ARP) • LEC 構成 • データ直送 VCC 情報 • LEC 統計 • VCC テーブル
MIB	以下を含む LEC MIB オブジェクトを表示します。 • LEC MIB 構成テーブル • LEC MAC ARP テーブル • LEC ルート記述子テーブル • LEC MIB サーバー VCC テーブル • LEC MIB 統計テーブル • LEC MIB 状態テーブル
QoS	LEC x QoS+ プロンプトを表示するので、 894ページの『サービス品質監視コマンド』 で説明しているように、そこからサービス品質 (QoS) を監視することができます。
Trace	パケット・トレースをオンまたはオフに設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、LEC アドレス解決テーブル (ART)、LEC 構成、データ・ダイレクト VCC 情報、または LEC 統計をリストするのに使用します。

構文:

list arp-table
configuration
data-direct-vccs
statistics
vcc-table

arp LEC アドレス解決テーブル (ARP キャッシュ内のエントリー) をリストします。

例:

```
LEC+ list arp

         LEC Address Resolution (LE ARP Cache) Table

  Max Table Size          = 10
  Free Table Entries      = 10
  Current Mac Entries     = 0
  Current RD Entries      = 0
  Arp Aging Time          = 300
  Verify Sweep Interval   = 60

                                Xmit  BUS   Arp
                          Conn  Queue Frame Retry Aging
 MAC Address     Remote Handle Depth Count Count Timer  Destination ATM Ad
                                                                    dress
 ------------------------------------------------------------------------
 40.00.00.00.00.09 False 652   0     0     0     60     39.99.99.99.99.99.
                               99.00.00.99.99.30.02.40.00.00.00.00.09.81
```

注: スイープ間隔は常に ARP エージング・タイマー値の 1/5 です。

Max Table Size
利用可能なエントリーの合計数

Free Table Entries
空きエントリーの数

Current MAC Entries

Current RD Entries
ルート記述子 ATM エントリー

ARP Aging Time
エントリーをエージングにより除去するまでの時間

Verify Sweep Interval

MAC Address

Remote

Connection Handle

Queue Depth

Xmit Frame Count

BUS Retry Count

ARP Aging Timer

Destination ATM Address

configuration
LEC 構成がリストされます。

イーサネットの場合:

例:

```
IBM LEC+ list config
                ATM IBM LEC Configuration
   Physical ATM interface number             = 0
   LEC interface number             = 7
   Primary ATM address
          ESI address               = Use burned in addr
          Selector byte             = 0x3
   Emulated LAN type                = Ethernet IBM
   Maximum frame size               = 1523
   LE Client MAC address            = Use burned in addr
   LE Server ATM address            = 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
   Forward Peak Rate                = 25000
   Backward Peak Rate               = 25000
    MAC cache size                   = 32
   MAC cache aging period           = 60
   Route Descriptor cache size      = 32
   Route Descriptor aging period    = 60
   LES Registration interval        = 60
   LES Registration retry count     = 3
   LES keep alive count             = 10
   Packet trace                     = No
   IP Encapsulation                 = ETHER
```

トークンリングの場合:

例:

```
IBM LEC+list config

                     ATM IBM LEC Configuration
   Physical ATM interface number             = 0
   LEC interface number             = 10
   Primary ATM address
          ESI address               = Use burned in addr
          Selector byte             = 0x6
   Emulated LAN type                = Token Ring IBM
   Maximum frame size               = 4551
   LE Client MAC address            = Use burned in addr
   LE Server ATM address            = 39.84.07.00.00.00.00.00.00.00.00.00.00.01.10.00.5A.DD.DA.02
   Forward Peak Rate                = 25000
   Backward Peak Rate               = 25000
    MAC cache size                   = 32
   MAC cache aging period           = 60
   Route Descriptor cache size      = 32
   Route Descriptor aging period    = 60
   LES Registration interval        = 60
   LES Registration retry count     = 3
   LES keep alive count             = 10
   Packet trace                     = No
   RIF Aging Timer                  = 120
   Source Routing                   = Enabled
```

例:

```
LEC+ list config

   Physical ATM interface number = 0
   LEC interface number          = 9
   LEC ATM address               = 39.99.99.99.99.99.99.00.00.99.99.31.01.09.FC.DD.D0.32.70.0A
   LEC MAC address               = 40.00.82.10.17.09
   lecConfigMode                 = Manual
   lecConfigLanType              = 802.5 - Token Ring
   lecConfigMaxDataFrameSize     = 4544
   lecConfigLanName              =
   lecConfigLesAtmAddress        = 39.99.99.99.99.99.99.00.00.99.99.31.01.40.00.82.10.17.00.09
   lecControlTimeout             = 30
   lecMaxUnknownFrameCount       = 10
   lecMaxUnknownFrameTime        = 1
   lecVccTimeoutPeriod           = 1200
   lecMaxRetryCount              = 1
   lecAgingTime                  = 300
   lecForwardDelayTime           = 15
   lecExpectedArpResponseTime    = 1
   lecFlushTimeout               = 4
   lecPathSwitchingDelay         = 6
   lecLocalSegmentId             = 0x0
   lecMulticastSendType          = 1
   lecMulticastSendAvgRate       = 365566
   lecMulticastSendPeakRate      = 365566
   lecConnectionCompleteTimer    = 4
   lecInitialControlTimeout      = 5
   lecControlTimeoutMultiplier   = 2
   V2 Capable                    = TRUE
```

```
   lecForwardDisconnectTimeout   = 60
   lecMinReconfigDelay           = 1
   lecMaxReconfigDelay           = 5
   lecMaxBusConnectRetries       = 0
   lecElanId                     = 0
   ExplorerExclude               = TRUE
   LE ARP queue depth            = 5
   LE ARP cache size             = 5000
   Forward peakrate              = 365566
   Backward peakrate             = 365566
   Packet trace                  = Off
   RIF aging timer               = 120
   Source Routing                = enabled
```

上記の例に示されているパラメーターの定義は、311ページの『Set』 を参照してください。

data LEC データ・ダイレクト VCC 情報をリストします。

例:

```
LEC+ list data

          LEC Data Direct VCC Table

   Max Table Size     = 1019    Max no of SVC connections
   Current Size       = 0       Currently used
   Inactivity Timeout = 1200    No Data Xfer Timeout before connection is
                                closed (seconds)
   Sweep Interval     = 60
      Conn              Inactive  User
      Handle  VPI  VCI   Timer    Count  Destination ATM Address
    ---------------------------------------------------------------------------

       652     0  7241    300       1    39.99.99.99.99.99.99.00.00.99.99.30.02.
                                          40.00.00.00.00.09.81


    ---------------------------------------------------------------------------
```

statistics

LEC 統計をリストします。

例:

```
LEC+ list stat

          LEC Statistics

   In Octets.high     = 0       No of Bytes received
   In Octets.low      = 346
   In Discards        = 2       Packets discarded
   In Errors          = 0       Rx.Errors
   In Unknown Protos  = 0       Unknown protocols received
   Out Octets.high    = 0       No of Bytes xmitted.
   Out Octets.low     = 0
   Out Discards       = 0
   Out Errors         = 0       Tx.Errors
   In Frames          = 0
   Out Frames         = 0
   In Bytes           = 0
   Out Bytes          = 0
```

VCC table

VCC テーブルをリストします。

例:

```
LEC+ list vcc
```

MIB

mib コマンドは、MIB オブジェクトを表示するのに使用します。

注: この情報の中には、**list** コマンドを使用して、別のフォーマットで表示できるものもあります。

構文:

mib config-table
mac-arp-table
rd-arp-table
server-vcc-table
statistics-table
status-table

config LEC MIB 構成テーブルを表示します。

例:

```
LEC+ mib config

 lecConfigTable:
 lecConfigMode                  = Manual
 lecConfigLanType               = 802.3 - Ethernet
 lecConfigMaxDataFrameSize      = 1516
 lecConfigLanName               =
 lecConfigLesAtmAddress         = 39.84.0F.00.00.00.00.00.11.23.24.24.24.24.55.66.77.88.99.00
 lecControlTimeout              = 120
 lecMaxUnknownFrameCount        = 1
 lecMaxUnknownFrameTime         = 0
 lecVccTimeoutPeriod            = 1200
 lecMaxRetryCount               = 1
 lecAgingTime                   = 300
 lecForwardDelayTime            = 15
 lecExpectedArpResponseTime     = 1
 lecFlushTimeout                = 4
 lecPathSwitchingDelay          = 6
 lecLocalSegmentId              = 0
 lecMulticastSendType           = 1
 lecMulticastSendAvgRate        = 25000000
 lecMulticastSendPeakRate       = 25000000


 lecConnectionCompleteTimer     = 4
```

lecConfigMode
LEC config モード: AUTO または MANUAL。 AUTO の場合、LEC は LECS を使用して LES ATM アドレスを入手します。

lecConfigLanType
LAN タイプ。イーサネットまたはトークンリングのいずれかです。

lecConfigMaxDataFrameSize
最大フレーム・サイズ

lecConfigLanName
ELAN ネーム

lecConfigLesAtmAddress
LE サーバー ATM アドレス

lecControlTimeout
要求/応答制御フレームのタイムアウト

lecMaxUnknownFrameCount
不明フレームの最大数

lecMaxUnknownFrameTime
この期間に、LEC は特定のユニキャスト LAN 着信先あての最大数の

MaxUnknownFrameCount フレームを BUS に送信し、さらにアドレス解決プロトコルを開始して、その LAN 着信先を変換する必要もあります。

lecVccTimeoutPeriod
SVC データ直送 VCC の非活動タイムアウト

lecMaxRetryCount
LE ARP 再試行カウント

lecAgingTime
ARP テーブル内の未検証エントリーの存続期間

lecForwardDelayTime

lecExpectedArpResponseTime
ARP 要求/応答サイクル・タイム

lecFlushTimeout
LE フラッシュ要求/フラッシュ応答タイムアウト期間

lecPathSwitchingDelay

lecLocalSegmentId
エミュレートされた LAN のセグメント ID。 802.5 クライアントの場合のみ

lecMulticastSendType
LEC がマルチキャスト・センド VCC で使用するシグナル・パラメーター

lecMulticastSendAvgRate
LEC がマルチキャスト・センド VCC で使用するシグナル・パラメーター

lecMulticastSendPeakRate
LEC がマルチキャスト・センド VCC で使用するシグナル・パラメーター

lecConnectionCompleteTimer

mac LEC MAC ARP テーブルを表示します。

rd LEC ルート記述子テーブルを表示します。

server LEC MIB サーバー VCC テーブルを表示します。

例:

```
LEC+ mib server

lecServerVccTable:
   lecConfigDirectInterface      = 0
   lecConfigDirectVpi            = 0
   lecConfigDirectVci            = 0
   lecControlDirectInterface     = 1
   lecControlDirectVpi           = 0
   lecControlDirectVci           = 38
   lecControlDistributeInterface = 1
   lecControlDistributeVpi       = 0
   lecControlDistributeVci       = 37
   lecMulticastSendInterface     = 1
   lecMulticastSendVpi           = 0
```

```
   lecMulticastSendVci           = 34
   lecMulticastForwardInterface  = 1
   lecMulticastForwardVpi        = 0
   lecMulticastForwardVci        = 33
```

lecConfigDirectInterface
コンフィグレーション・ダイレクト VCC に対応するインターフェース

lecConfigDirectVpi
上記の VCC (存在する場合) を識別する VPI

lecConfigDirectVci
上記の VCC (存在する場合) を識別する VCI

lecControlDirectInterface
コントロール・ダイレクト VCC に対応するインターフェース

lecControlDirectVpi
上記の VCC (存在する場合) を識別する VPI

lecControlDirectVci
上記の VCC (存在する場合) を識別する VCI

lecControlDistributeInterface
コントロール・ディストリビュート VCC に対応するインターフェース

lecControlDistributeVpi
上記の VCC (存在する場合) を識別する VPI

lecControlDistributeVci
上記の VCC (存在する場合) を識別する VCI

lecMulticastSendInterface
マルチキャスト・センド VCC に対応するインターフェース

lecMulticastSendVpi
上記の VCC (存在する場合) を識別する VPI

lecMulticastSendVci
上記の VCC (存在する場合) を識別する VCI

lecMulticastForwardInterface
マルチキャスト・フォワード VCC に対応するインターフェース

lecMulticastForwardVpi
上記の VCC (存在する場合) を識別する VPI

lecMulticastForwardVci
上記の VCC (存在する場合) を識別する VCI

statistics
LEC MIB 統計テーブルを表示します。

例:

```
LEC+ mib statistics

lecStatisticsTable:
   lecArpRequestsOut             = 1
   lecArpRequestsIn              = 0
   lecArpRepliesOut              = 0
```

```
   lecArpRepliesIn              = 1
   lecControlFramesOut          = 2
   lecControlFramesIn           = 2
   lecSvcFailures               = 1
```

lecArpRequestsOut
この LEC によって送信された LE ARP 要求の数

lecArpRequestsIn
この LEC によって受信された LE ARP 要求の数

lecArpRepliesOut
この LEC によって送信された LE ARP 応答の数

lecArpRepliesIn
この LEC によって受信された LE ARP 応答の数

lecControlFramesOut
この LEC によって送信された制御パケットの数

lecControlFramesIn
この LEC によって受信された制御パケットの数

lecSvcFailures
以下の合計数

- このクライアントがオープンを試行したが失敗した発信 LAN エミュレーション SVC の数
- このクライアントが確立を試行したが失敗した着信 LAN エミュレーション SVC の数
- このクライアントがプロトコルまたはセキュリティーを理由に拒否した着信 LAN エミュレーション SVC の数

status MIB 状態をリストします。

例:

```
LEC+ mib status

lecStatusTable:
   lecPrimaryAtmAddress          = 39.84.0F.00.00.00
   Client ATM address=           = 00.00.00.00.00.01.10.00.5A.00.DE.AD.03
   lecId                         = 1                  Assigned by LES
   lecInterfaceState             = Operational        State of the LEC
   lecLastFailureRespCode        = None               Error code from last
                                                      failed Config/Join resp.
   lecLastFailureState           = Initial State      State of LEC when
                                                      updating above field.
   lecProtocol                   = 1                  Protocol specified by
                                                      LEC in Join requests.
   LecVersion                    = 1                  LEC Protocol Version
                                                      of above
   lecTopologyChange             = False
   lecConfigServerAtmAddress     = 00.00.00.00.00.00.

   lecConfigSource               = Did not use LECS
   lecActualLanType              = 802.3 - Ethernet   Frame format currently
                                                      used by LEC
   lecActualMaxDataFrameSize     = 1516
   lecActualLanName              = ETH                Name of emulated LAN
                                                      that LEC joined.
   lecActualLesAtmAddress        = 39.84.0F.00.00.00.

   lecProxyClient                = False              Is LES acting like a
                                                      proxy ?
```

QoS Information

qos-information コマンドは、LEC x QoS+ プロンプトを表示するので、894ページの『サービス品質監視コマンド』 で説明しているように、そこからサービス品質を監視することができます。

構文:

qos-information

第26章 シリアル・ライン・インターフェースの構成

この章では、シリアル・インターフェースのインターフェース構成プロセスについて説明し、以下の節が含まれています。

- 『インターフェース構成プロセスへのアクセス』
- 334ページの『ネットワーク・インターフェースおよび GWCON インターフェース・コマンド』

重要: シリアル・インターフェース上のフレーム・リレー、PPP、X.25、V.25bis、SDLC リレー、および SDLC プロトコルを構成する場合は、本章のコマンドを使用した上で、特定プロトコルについて説明している章のコマンドを参照してください。

プロトコルのリストおよびこれらのプロトコルをサポートするインターフェースの一覧表は、20ページの『ネットワーク・インターフェースの構成』 を参照してください。

インターフェース構成プロセスへのアクセス

シリアル・インターフェースのインターフェース構成プロセスにアクセスするには、最初に `Config>` プロンプトにアクセスし、コマンド **set data-link** を出します。次に、`Config>` プロンプトで、インターフェースのタイプと番号を入力して、そのインターフェースの構成環境にアクセスします。

たとえば、X.25 のシリアル・インターフェースを構成する場合は、次のようなコマンドを出して、`X.25 config>` 環境にアクセスする必要があります。

```
Config> set data-link X25 2
Config>network 2
```

`X.25 config>` 環境から、シリアル・インターフェース上の X.25 の構成を完了させることができます。 335ページの『第27章 X.25 ネットワーク・インターフェースの使用』 を参照してください。

シリアル・インターフェースの構成が完了したら、OPCON プロンプト(*) の後に **restart** コマンドを入力し、新規構成を使用可能にするかどうかを尋ねるプロンプトに対して **yes** と応答します。

クロックおよびケーブルのタイプ

この節は、FR、PPP、X.25、SDLC リレー、および SDLC のシリアル・ポートの使用に適用されます。

モデムまたは CSU/DSU がシリアル・ポートに接続されている場合、ルーターはそのラインのクロックに関しては DTE の役割を果たすので、DTE ケーブル・タイプおよび外部クロックを構成します。

モデム、CSU/DSU、またはモデム・エリミネーターを使用せずに 2 つのルーターを直接接続したい場合は、一方のルーターが、そのラインのクロックに関して DCE の

シリアル・ライン・インターフェースの構成

役割を果たします。 DCE として働くルーターに直接接続ケーブルを接続し、そのシリアル・インターフェースに対して以下のパラメーターを構成します。

1. DCE ケーブル・タイプ
2. 内部クロック
3. クロック/ライン速度

他方のルーターは、クロックに関して DTE の役割を果たすので、モデムまたは CSU/DSU に接続されている場合と同様に構成することが必要です。

注: DTE ケーブルの構成は、DCE ケーブルの場合とは異なり、WAN ネット・ハンドラーが同位装置上で使用されるか否かに影響を与えません。たとえば、たとえフレーム・リレー・インターフェースが DCE ケーブルを使用するように構成されていても、ルーターは常にフレーム・リレー DTE 装置として働き、FR UNI インターフェースを使用します。

ネットワーク・インターフェースおよび GWCON インターフェース・コマンド

シリアル・ライン・インターフェースには、監視のための独自のコンソール・プロセスはありませんが、GWCON 環境から **interface** コマンドを使用すれば、ルーターはすべての導入済みネットワーク・インターフェースの完全な統計を表示することができます。 **interface** コマンドと統計の表示について詳しくは、第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド を参照してください。

第27章 X.25 ネットワーク・インターフェースの使用

X.25 ネットワーク・インターフェースは、ルーターを X.25 バーチャル・サーキット・スイッチド・ネットワークに接続します。 X.25 ネットワーク・インターフェースのソフトウェアとハードウェアにより、ルーターは公衆 X.25 ネットワークを介して通信することができます。 X.25 ネットワーク・インターフェースは、X.25 インターフェースの CCITT 1980、CCITT 1984、CCITT 1988、および ISO 8208 1990 仕様に準拠しており、多重化チャネルおよび広域ネットワークを経由する高信頼性エンド・エンド間データ転送を提供します。

本章には、以下の節が含まれています。

- 『基本構成手順』
- 338ページの『ISDN BRI D チャネル (X.31) を介した X.25 サポート』
- 338ページの『ヌル・カプセル化』
- 340ページの『閉域ユーザー・グループの概要』

TCP/IP を介して X.25 トラフィックを伝送するための X.25 トランスポート・プロトコル (XTP) の構成については、 381ページの『第29章 XTP の使用』を参照してください。

X.31 通信については、635ページの『X.31 サポート』を参照してください。

基本構成手順

この節では、X.25 インターフェースを立ち上げて実行するのに必要な最小構成ステップについて概説します。 X.25 パラメーターは、ルーター上のインターフェースが接続する X.25 ネットワークと一致していなければなりません。詳細については、本章で説明する構成コマンドを参照してください。

注: 構成変更を有効にするためには、ルーターをリスタートする必要があります。

1. OPCON プロンプト (*) で **talk 6** と入力する。

   `Config>` プロンプトが表示されます。
2. **list devices** を入力して、インターフェースのリストを表示すると、そこから選択することができます。以下のステップでは、該当するインターフェース番号を使用してください。
3. **set data-link x25** と入力する。

   `Interface Number [0]?` プロンプトが表示されます。
4. 該当するインターフェース番号を入力する。
5. `Config>` プロンプトで **net** `#` と入力して、ネットワークに接続する。

   `X.25 Config[#]>` プロンプトが表示されます。
6. このプロンプトで、**set address** *x.25-node-address* と入力する。

   X.25 アドレスは、呼設定時に使用される固有の X.121 アドレスです。 DDN 網の場合は、**add htf-addr** および **set htf-addr** コマンドを使用して、このインターフェースに対応するプロトコル・アドレスを DDN アドレス変換に必要な

X.121 アドレス・フォーマットに変換します。ネットワーク・アドレスを設定しないと、X.25 インターフェースを接続ネットワークに結合することができません。

7. **set equipment-type** と入力し、フレームおよびパケット・レベルが DCE または DTE のいずれで動作するのかを指定する。このコマンドのデフォルト値は DTE です。
8. **set svc** と入力して、使用する SVC 数の最低値と最高値を定義する。デフォルトは 1 SVC です。
9. **add protocol** *protocol_name* と入力して、X.25 インターフェースを介して実行されるプロトコルを追加する。ウィンドウ・サイズ、デフォルト・パケット・サイズ、最大パケット・サイズ、回線アイドル・タイム、および最大 VC 数を尋ねるプロンプトが出ます。

   注: ルーター上のすべてのX.25 ネットワークに対して 1 回だけプロトコルを追加すれば済みます。
10. **add address** *protocol_name* と入力して、このインターフェースを介して到達可能な各プロトコルの着信先アドレスのアドレス変換を追加する。
11. **exit** と入力して、`Config>` プロンプトに戻る。
12. **Ctrl-P** を押して、OPCON プロンプト (*) に戻る。
13. **restart** と入力し、プロンプトに対して **yes** と応答する。

ナショナル・パーソナリティーの設定

各公衆データ通信網 (GTE の Telenet や DDN の Defense Data Network など) は、それぞれ独自の標準構成を持っています。*ナショナル・パーソナリティー* という用語は、公衆データ通信網の特性を定義するのに使用される変数グループを指定します。ナショナル・パーソナリティー内の構成情報は、リンクを介して転送されるパケットの制御情報をルーターに提供します。ナショナル・パーソナリティー・オプションは、各公衆データ通信網の 27 のデフォルト・パラメーターを定義します。

X.25 ナショナル・パーソナリティーの構成値を表示するには、X.25 構成 **list detailed** コマンドを実行します。ルーターに接続されている各公衆データ通信網を構成するには、X.25 構成 **national-personality set** コマンドを実行します。

ナショナル・パーソナリティーは、網構成の汎用テンプレートです。必要な場合は、各フレームおよびパケット・レイヤー・パラメーターを個別に構成することができます。

X.25 のデフォルト値について

下表は、X.25 *set*、 *national set*、 および *national enable* コマンドの各種パラメーターのデフォルト値をリストしています。

表 45. Set コマンド

パラメーター	デフォルト値
address ...	なし
cable	なし

表 45. Set コマンド (続き)

パラメーター	デフォルト値
calls-out ...	4
clocking ...	外部
default-window-size ...	2
encoding	NRZ
equipment-type ...	DTE
htf addr ...	なし
inter-frame-delay ...	0
mtu	1500
national-personality ...	GTE Telenet
pvc ...	低=0 高=0
speed	9600
svc	低 着信=0、高 着信=0 低 両方向=1、高 両方向=64 低 発信=0、高 発信=0
throughput-class ...	着信=発信=2400
vc-idle ...	30

表 46. National Enable パラメーター

パラメーター	DDN デフォルト値	GTE デフォルト値
accept-reverse-charges	off	on
bi-cug	off	off
bi-cug-with-outgoing-access	off	off
cug	off	off
cug-deletion	off	off
cug-insertion	off	off
cug-with-incoming-access	off	off
cug-with-outgoing-access	off	off
cug-zero-override	off	off
flow-control-negotiation	on	on
frame-ext-seq-mode	off	off
packet-ext-seq-mode	off	off
request-reverse-charges	off	on
suppress-calling-addresses	off	off
throughput-class-negotiation	on	on
truncate-called-addresses	off	off

表 47. National Set パラメーター

パラメーター	DDN デフォルト値	GTE デフォルト値
call-req	20 デカ秒	20 デカ秒
clear-req ...	再試行=1 18 デカ秒	再試行=1 18 デカ秒

表 47. National Set パラメーター (続き)

パラメーター	DDN デフォルト値	GTE デフォルト値
disconnect-procedure ...	受動	受動
dp-timer	500 ミリ秒	500 ミリ秒
frame-window-size	7	7
n2-timeouts	20	20
packet-size ...	128、最大=256	128、最大=256
reset ...	再試行=1 18 デカ秒	再試行=1 18 デカ秒
restart ...	再試行=1 18 デカ秒	再試行=1 18 デカ秒
min-recall	10 秒	10 秒
min-connect	90 秒	90 秒
collision-timer	10 秒	10 秒
standard-version	1984	1984
t1-timer	4 秒	4 秒
t2-timer	0	0
truncate-called-addr-size	2	2

ISDN BRI D チャネル (X.31) を介した X.25 サポート

X.25 は ISDN BRI D チャネル (X.31) を介しても同じプロトコル・サポートを提供しますが、以下のような制約があります。

- パケット・サイズは 256 バイトを超えることはできません。
- フレーム拡張シーケンス・モードが使用可能でなければなりません。
- X.31 は DTE として構成されていなければなりません。

詳細については、635ページの『X.31 サポート』を参照してください。

ヌル・カプセル化

ヌル・カプセル化は、ユーザーが 1 つの X.25 回線上で複数のネットワーク・レイヤー・プロトコルを多重化することを可能にします。この機能は、過度のバーチャル・サーキットが使用されるのを回避するために使用することができます。

制限

ヌル・カプセル化は、QLLC に対してはサポートされません。この機能は SVC (スイッチド・バーチャル・サーキット) に対してサポートされています。

構成変更

カプセル化オプションの NULL が、以下の T6 コマンドに追加されました。

X25 config の下: add address IP (enc type = NULL と入力)

X25 config の下: add address IPX (enc type = NULL と入力)

X25 config の下: add address DNA (enc type = NULL と入力)

X25 config の下: add address VINES (enc type = NULL と入力)

X25 config の下: list addr は、priority 1 type が NULL の場合、active enc type = NULL を表示します。

T5 コマンド:

X25 config の下: List SVCS に enc type = NULL が含まれるようになります。

ヌル・カプセル化および閉域ユーザー・グループ (CUG) の構成

ヌル・カプセル化を使用しているときには、1 つのバーチャル・サーキットを介して複数のプロトコルを実行できるので、そのサーキット上の各プロトコルに定義された CUG は同一でなければなりません。ユーザーは、以下の方法を使用して、複数のプロトコルに対して同一の宛先を構成することを強くお勧めします。

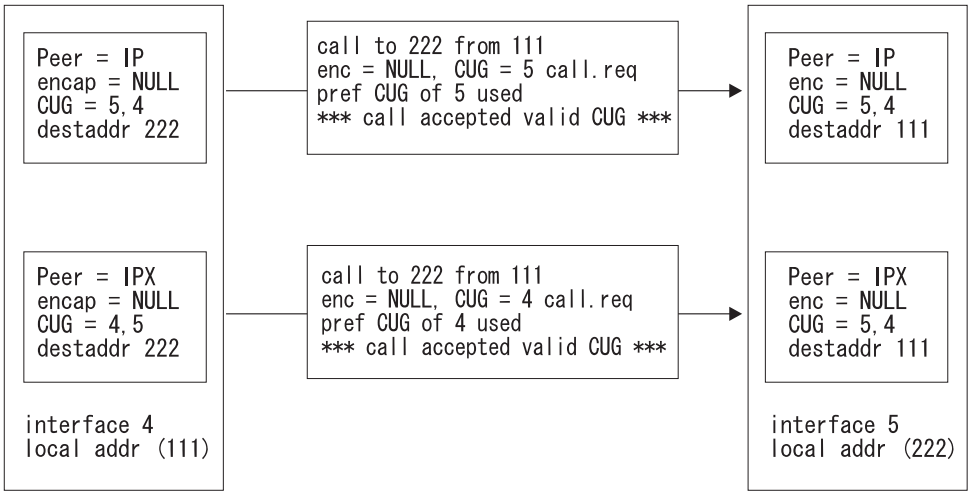
add address を使用して CUG を構成する。定義された CUG は、同じアドレスに定義された各プロトコルで同一でなければなりません。

CUG が add protocol レベルで定義されている場合は、CUG はすべての同位で同一でなければなりません (この方法は、より限定的です)。

インターフェース・レベルで CUG を構成する。これにより、すべての同位が同じ CUG 値を持つことが保証されます (この方法が最も限定的です)。

着呼 CUG 定義がその回線を共用するすべてのプロトコルに有効である限り、上述のどの方法を使用しても構いません。「有効」とは、CUG が特定のアドレスに定義されているか、もしくはデフォルトでプロトコルまたはインターフェースの回線定義が使用されるようになっていることを意味しています。

例 1: 両方の同位に有効な着信閉域
ユーザー・グループ (CUG)



例 2: 両方の同位に有効ではない着信閉域
ユーザー・グループ (CUG)

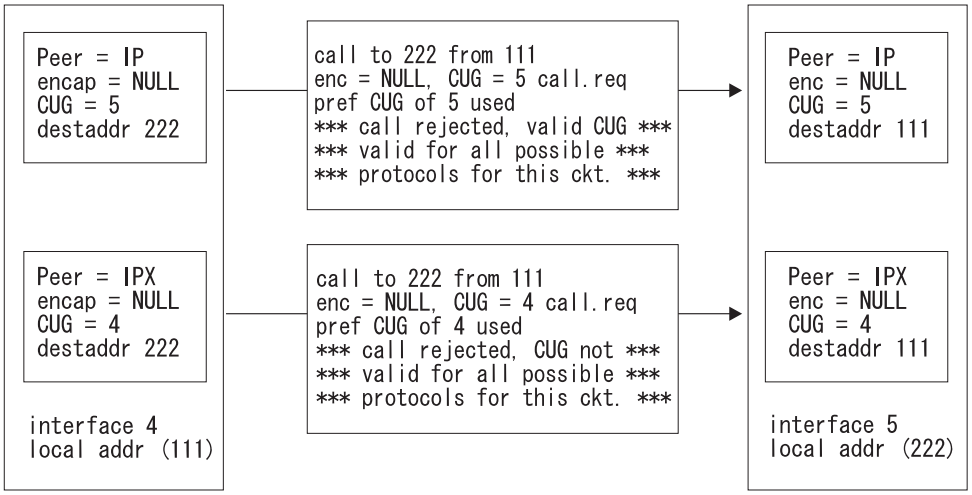


図 18. 閉域ユーザー・グループのヌル・カプセル化

閉域ユーザー・グループの概要

閉域ユーザー・グループ (CUG) とは、他の特定の DTE と接続を確立することが許可されている X.25 DTE のグループをいいます。 CUG 番号はネットワーク提供者によって定義され、ユーザーはネットワーク提供者が割り当てた CUG しか使用することができません。ユーザーは、アドレス特定 CUG、プロトコル特定 CUG、またはインターフェース特定 CUG を構成することができます。ある DTE に対してこの 3 つのタイプの CUG メンバーのすべてが構成されている場合、閉域ユーザー・グループ・ファシリティーは、別の DTE に接続するときの発呼要求で、アドレス特定の宛先 CUG を使用します。ある DTE に対してプロトコル特定およびインターフェース特定 CUG のみが構成されている場合、閉域ユーザー・グループ・ファシリティーは、別の DTE に接続するときの発呼要求で、プロトコル特定 CUG を使用します。

1 つの DTE が複数の CUG に属することも可能です。ユーザーは、その DTE の優先 CUG を指定する必要があります。ルーターは他の DTE に発呼するときに、優先 CUG を使用します。 1 つの DTE は、合計 5 つを超える優先または通常の閉域ユーザー・グループを持つことはできません。

相互形閉域ユーザー・グループ

相互形閉域ユーザー・グループ (BCUG) とは、2 つだけの DTE で構成される閉域ユーザー・グループです。 BCUG 内の DTE は、BCUG のメンバー、およびどの CUG または BCUG にも属さない任意の DTE に発呼することができます。 1 つの DTE は、合計 5 つを超える優先または通常の相互形 CUG を持つことはできません。

DTE が BCUG を使用して回線を確立する方法は、DTE が CUG を使用して回線を確立する方法 (342ページの表48を参照) と同じですが、インターフェース、プロトコル、またはアドレスに対して BCUG と CUG の両方が定義されている場合には、BCUG を使用して回線が確立されます。

拡張閉域ユーザー・グループのタイプ

閉域ユーザー・グループに対する以下の拡張がサポートされています。

出アクセスをもつ CUG
: DTE は 1 つまたは複数の CUG に属することができます。 DTE は、CUG のメンバー、および入アクセスをもつ他の CUG に属する任意の DTE に発呼することができます。

入アクセスをもつ CUG
: DTE は 1 つまたは複数の CUG に属することができます。 DTE は、どの CUG にも属さない DTE、または出アクセスをもつ他の CUG に属する DTE からの呼を受信することができます。

出アクセスをもつ BCUG
: DTE は 1 つまたは複数の BCUG に属することができます。 DTE は、BCUG のメンバー、およびどの BCUG にも属さない任意の DTE に発呼することができます。

装置上に閉域ユーザー・グループをもつ X.25 回線の確立

閉域ユーザー・グループ・ファシリティーが使用可能の場合、 DTE は発呼要求を受け取ると、その発呼要求の中の CUG を使用して、DTE からの呼を受諾するか、リジェクトするかを判別します。発呼要求の中の CUG が、インターフェース、プロトコル、または起呼 DTE に対応する宛先に構成されている CUG に一致しない場合、要求はリジェクトされます。 342ページの表48 は、インターフェース、プロトコル、およびアドレス CUG メンバーが異なっており、入アクセスが使用可能でない場合に、CUG に基づいて X.25 回線を確立する方法を要約しています。

表 48. 閉域ユーザー・グループの着信 X.25 回線の確立

着呼要求の内容	受信 DTE CUG 定義							
	インターフェース CUG のみ	プロトコル CUG のみ	アドレス特定 CUG	インターフェースおよびプロトコル CUG	インターフェースおよびアドレス CUG	プロトコルおよびアドレス CUG	すべての CUG	CUG なし
CUG なし	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	受諾
インターフェース CUG	受諾	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト	リジェクト
プロトコル CUG	リジェクト	受諾	リジェクト	受諾	リジェクト	リジェクト	リジェクト	リジェクト
アドレス特定 CUG	リジェクト	リジェクト	受諾	リジェクト	受諾	受諾	受諾	リジェクト

インターフェース上の発呼の場合、CUG または BCUG ファシリティーが使用可能のときには、着信先に構成された優先 CUG (もしあれば) が、各発呼要求に入れられます。アドレス特定 CUG が構成されていない場合、使用される CUG はプロトコルに定義された CUG になり、プロトコル特定 CUG が構成されていない場合は、使用される CUG はインターフェースに定義された CUG になります。 CUG メンバーが構成されていない場合には、CUG ファシリティーは発呼要求に組み込まれません。

CUG 0 の閉域ユーザー・グループ処理のオーバーライド

発呼要求の中に 0 の CUG が入っている着呼は妥当性検査をしないように DTE を構成することができます。この機能により、入アクセスが使用可能でなくても、特定の呼を完了させることが可能になります。 **national enable cug 0 override** コマンドを使用すると、CUG 番号が 0 のときには CUG ファシリティーを無視することを装置に強制できます。その発呼要求は、構成された CUG 番号との比較は行われません。

X.25 閉域ユーザー・グループの構成

X.25 インターフェース上で閉域ユーザー・グループを使用するには、次のようにします。

1. ネットワーク提供者から CUG 番号を入手する。これらの番号は、X.25 を構成するときに必要になります。
2. **national enable cug** コマンドと関連のコマンドを使用して、閉域ユーザー・グループ・ファシリティーを使用可能にする。
3. **national enable bi-cug** コマンドと関連のコマンドを使用して、相互形閉域接続ユーザー・グループを使用可能にする (必要な場合)。
4. DTE に対して該当の CUG 番号を構成する。必要に応じて、優先 CUG、CUG、優先相互形 CUG、および相互形 CUG を指定する。これは **add address** コマンドを使用して行います。
5. プロトコルに対して該当する CUG および相互形 CUG を構成する (必要な場合)。これは **add protocol** コマンドを使用して行います。

注: アドレス特定 CUG でオーバーライドしない限り、このプロトコルの X.25 インターフェースを介して確立されるすべての X.25 回線を、この固有 CUG または BCUG に属する DTE のみに限定したい場合は、これらの CUG のみを構成することが必要です。

6. インターフェースに対して該当する CUG および相互形 CUG を構成する (必要な場合)。これは **add cug** コマンドを使用して行います。

   注: アドレス特定またはプロトコル特定 CUG でオーバーライドしない限り、X.25 インターフェースを介して確立されるすべての X.25 回線を、この固有 CUG または BCUG に属する DTE のみに限定したい場合には、これらの CUG のみを構成することが必要です。

第28章 X.25 ネットワーク・インターフェースの構成および監視

この章では X.25 構成および動作コマンドについて説明し、以下の節が含まれています。

X.25 構成コマンド

この節では、すべての X.25 構成コマンドの要約を示し、個々のコマンドについて説明します。

X.25 構成コマンドでは、X.25 パケットを転送するルーター・インターフェースのネットワーク・パラメーターを指定することができます。構成コマンドで指定した情報は、ルーターをリスタートすると有効になります。

X.25 構成コマンドは `X.25 config>` プロンプトで入力します。 表49 は、コマンドをリストしています。

表 49. X.25 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Set	ローカルおよび DDN X.25 ノード・アドレス、パケット・レベルのウィンドウ・サイズを設定し、ナショナル・パーソナリティーの識別、MTU、および呼の最大数を識別します。 PVC および SVC チャネル範囲、交換回線が切断される前にアイドル状態でいられる秒数を定義し、1 つのルーターが DCE として動作する必要があるかどうか (X.25 ネットワークが介在せずに 2 つのルーターが直接接続されている場合) あるいは X.25 ネットワークに接続されている DTE で一般的な方式で動作するかを指定します。また、速度、符号化、クロック、スループット・クラス、およびケーブル・タイプも設定します。
Enable/Disable	着呼禁止機能、発呼禁止機能、動的 DDN アドレス変換、および lower-dtr 機能を使用可能/使用不可にします。
National Enable or National Disable	ナショナル・パーソナリティー構成で定義されたパラメーターを使用可能/使用不可にします。
National Set	ナショナル・パーソナリティー構成で定義されたパラメーターを設定します。
National Restore	ナショナル・パーソナリティー構成をそのデフォルト値に復元します。
Add/Change/Delete	アドレス変換、プロトコル・カプセル化、または PVC 定義を追加/変更/削除します。

表 49. X.25 構成コマンドの要約 (続き)

コマンド	機能
List	定義済みのアドレス変換、ナショナル・パーソナリティー・パラメーター、プロトコル・カプセル化、または PVC 定義をリストします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Set

set コマンドは、ローカル X.25 ノード・アドレス、呼の最大数、フレームおよびパケット・レベルのウィンドウ・サイズ、 PVC および SVC チャネル数の最低値と最高値、交換回線のアイドル・タイムを構成するのに使用します。

構文:

set
- address . . .
- cable
- calls-out . . .
- clocking . . .
- default-window-size . . .
- encoding
- equipment-type . . .
- htf addr . . .
- inter-frame-delay . . .
- mtu
- national-personality . . .
- pvc . . .
- speed . . .
- svc
- throughput-class . . .
- vc-idle . . .

address *x.25-node-addr*

ローカル X.25 インターフェース・アドレス (*x.25-node-addr*) を設定します。ローカル X.25 アドレスを削除する場合は、ローカル X.25 ノード・アドレスを 0 に (00 ではなく) 設定します。

例: `set address 8982800`

cable *type*

ケーブル・タイプを次のように設定します。

- RS-232 DTE
- RS-232 DCE
- V35 DTE

- V35 DCE
- V36 DTE
- X21 DTE
- X21 DCE

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときに使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときに使用します。

calls-out *value*
ローカルで開始し、同時にアクティブにできる SVC の最大数を設定します。

有効値: 1 ～ 239

デフォルト値: 4

clocking *external* **or** *internal*
モデムまたは DSU に接続する場合は、クロックを外部として構成します。別の DTE 装置に直接接続する場合は、DCE ケーブルを使用し、クロックを内部として設定し、回線速度を構成します。

外部

default-window-size *value*
発呼要求パケット内にウィンドウ・サイズ・ファシリティーが存在しない場合、ルーターによって割り当てられるパケット・レベルのウィンドウ・サイズを設定します。範囲は、ナショナル・パーソナリティーのパケット・モジュラス (PACKET-EXT-SEQ-MODE) によって決まります。

デフォルト値: 2

例: `set default-window-size 3`

encoding *NRZ* **OR** *NRZI*
インターフェースの HDLC 伝送符号化規則を設定します。符号化規則は、NRZ (非ゼロ復帰記録) または NRZI (非ゼロ復帰反転) に設定できます。NRZ は、広く一般的に使用されている符号化規則であり、一方の NRZI は一部の IBM 構成で使用されます。

デフォルト値: NRZ

equipment-type *DCE* **または** *DTE*
フレームおよびパケット・レベルが DCE として動作するのか、DTE として動作するのかを指定します。このコマンドは、使用しているケーブル・タイプには無関係です。

デフォルト: DTE (X.31 の場合は DTE が必須)

htf addr *x.25-node-addr*
DDN が使用されている場合、ローカル DTE アドレスを設定します。これは、CCITT が使用されているときにローカル DTE アドレスを設定するのに使用される **set address** コマンドとは反対に、IP アドレスを X.121 アドレスに変換します。

inter-frame-delay *value*
このパラメーターは、送信フレーム間の最小遅延を定義します。このパラメ

ーターを設定しておくと、1 つのフラグによって区切られた連続フレームを矛盾なく処理できない可能性のある（T1 タイムアウトのような誤りを受け取ります）旧式装置に、直接インターフェースする場合に役立ちます。

IBM 2210 では、フレームの間に 0 〜 15 個の余分なフラグを挿入する必要があります。

デフォルト値: 0

mtu *value*

最大送信単位 (MTU) をバイト数で設定します。これは、パッケージに入れてシリアル・ライン経由で転送するために X.25 インターフェースに送達される最大メッセージ・サイズです。範囲は 576 〜 16384 です。

デフォルト値: 1500

X.25 インターフェースを介してデータを転送するときにパケット再組み立てタイムアウトが発生する場合、エンドポイントに達するまでのすべての LAN またはシリアル・インターフェースの最小パケット・サイズを調べて、より適切な X.25 MTU を計算する必要があります。 X.25 は実際より小さいパケット・サイズを使用する傾向があるので、この計算では、実際の X.25 パケット・サイズを直接考慮しないでください。 X.25 は通常、最大 7 つのパケットを一度に送信して、確認応答を待ちます。

たとえば、以下のものが含まれているネットワーク・トポロジーを考えてみてください。

- パケット・サイズが 4000 のトークンリング LAN
- パケット・サイズが 128、ウィンドウ・サイズが 7、およびビット・レートが 9600 bps の X.25 シリアル・ライン
- パケット・サイズが 1500 のイーサネット LAN

この場合は、おそらく X.25 MTU を 1500 に設定する必要があります。これは、約 12 のパケットが X.25 インターフェースを介して送信されることを意味しています (MTU / X.25 パケット・サイズ = 送信される X.25 パケット数)。

MTU が 4096 のときは、X.25 インターフェースを介して 32 のパケットを送信する必要があります (4000 / 128 = 31.25)。この場合、X.25 モデムの速度が 9600 bps のときは、おそらくパケット再組み立てタイムアウトが発生することが予想されます。 X.25 モデムの速度を 56 Kbps であれ、この問題を解決できるものと思われます。

注:

1. MTU パラメーターは、装置のメモリー所要量とメモリー使用率に大きな影響を与えます。メモリーが 8M より小さい装置では、8192 以下の MTU 値を使用してください。
2. 装置の稼働中に使用可能なメモリーの量によって、SVC を確立し、しかも最適な性能に維持できる数が制限されます。推奨される SVC の最大数については、WWW 上の製品のホーム・ページを参照してください。

national-personality *GTE-Telenet* **または** *DDN*

GTE-Telenet または DDN ナショナル・パーソナリティーの 28 のデフォルト・パラメーターを設定します。

デフォルト値: GTE-Telenet

pvc low/high *value*

パーマネント・バーチャル・サーキットの最低と最高のチャネル番号を定義します。ゼロは、PVC がないことを示します。デフォルトでは「PVC なし」になります。

pvc low

0

pvc high

0

範囲は 1 ～ 4095 です。これらの値は、指定の VC 範囲の限界値を設定します。最大 400 の PVC があります。

例: `set pvc low 40`

注: 値は、SVC 用に設定した値とオーバーラップしてはなりません。

speed *speed-setting*

内部クロックの場合、このコマンドは送信および受信クロック回線の速度を指定します。

有効値: 2400 ～ 2048000 bps

外部刻時の場合は、このコマンドがハードウェアに影響することはありませんが、IPX などのような一部のプロトコルが、ルーティング・コスト・パラメーターを判別する場合に使用する速度が、このコマンドで設定されます。そのような場合には、実際の回線速度に一致するように速度を設定してください。速度が構成されない場合、プロトコルは、ルーティング・コスト・パラメーターを計算する際に 1000 000 bps の速度を想定します。外部刻時の場合、構成できる最大回線速度は 6 312 000 bps です。

デフォルト値: 9600

注: X.25 ソフトウェアがサポートされるのは、速度が 256 000 bps 以下の場合だけです。

svc low/high *inbound* **または** *two-way* **または** *outbound value*

スイッチド・バーチャル・サーキットの最低および最高チャネル番号を定義します。 low=high=0 のときは、このカテゴリーの VC は定義されていません。

例: `set SVC low-two-way 1`

Inbound

着信 SVC に割り当てられる論理チャネル番号の範囲を指定します。デフォルトでは、着信専用の SVC はないことになります。

有効値: 0 ～ 4095

デフォルト値: 0

Two-way

両方向 SVC に割り当てられる論理チャネル番号の範囲を指定します。デフォルトでは、64 の両方向 SVC があります。

有効値: 0 ～ 4095

デフォルト値:

svc low
1

svc high
64

Outbound
発信 SVC に割り当てられる論理チャネル番号の範囲を指定します。デフォルトでは、発信専用の SVC はないことになります。

有効値: 0 〜 4095

デフォルト値: 0

注: 各範囲の値は、他の SVC 範囲とも、PVC 範囲ともオーバーラップしてはなりません。 表50 は、可能な VC 構成を示しています。

表 50. VC 定義の例

	低	高
PVC	1	40
着信	0	0
両方向	41	59
発信	60	500

throughput-class inbound *または* **outbound** *bit-rate*
スループットのネゴシエーションが使用可能の場合、発呼要求をするときに要求されるスループット・クラスを定義します。

デフォルト値: 2400 bps

着呼要求の処理時には、この設定値は無視されます。

vc-idle *value*
ルーターによって切断される前に、交換回線がアイドル状態になれる秒数を定義します。ゼロは、ルーターがアイドル回線を切断しないことを示します。

有効値: 1 〜 255

デフォルト値: 30 秒

Enable

enable コマンドは、DDN アドレス変換、インターフェース・リセット、または着呼禁止、発呼禁止、および lower-dtr 機能を使用可能にするのに使用します。

構文:

enable ddn--address-translations

注: ddn-address-translations は、使用可能にすることができなくなりました。この機能は、選択されたナショナル・パーソナリティーが DDN の場合

は、デフォルトで使用可能になり、その他の場合は、デフォルトで使用不可になります。

incoming-calls-barred

lower-dtr

outgoing-calls-barred

incoming-calls-barred
ルーターは着呼を受け入れないことを指定します。このパラメーターのデフォルト設定値は、使用不可またはオフ で、これは着呼を受け入れます。

lower-dtr
このパラメーターは、使用不可にされている専用シリアル・ライン・インターフェースにおけるデータ端末レディー (DTR) 信号の処理方法を決めます。このパラメーターが ″使用不可″ (デフォルト値) に設定されている場合、インターフェースが使用不可のときは、DTR 信号は上がります。

lower-dtr が ″使用可能″ に設定されている場合、インターフェースが使用不可のときは、DTR は下がります。この動作が適している状況は、インターフェースが WAN 再ルートの代替リンクとして構成されており、インターフェースが、DTR 信号の状態に基づいてダイヤル接続を維持するダイヤルアウト・モデムに接続されているような場合です。

lower-dtr が使用可能で、インターフェースが使用不可のとき、DTR 信号は下がり、モデムはダイヤル接続をダウンに保持します。インターフェースが使用可能になると (WAN 再ルートのバックアップ・シナリオにより)、DTR は上がり、モデムは保管しているバックアップ・サイトへの番号をダイヤルします。 1 次インターフェースが復元すると、代替インターフェースは使用不可にされ、DTR は下がって、モデムはダイヤル接続を切断します。

以下のケーブル・タイプがサポートされます。

RS-232

V.35

V.36

デフォルト設定値は使用不可です。

outgoing-calls-barred
ルーターは発呼を許可しないことを指定します。このパラメーターのデフォルト設定値は、使用不可またはオフ で、これは発呼を許可します。

Disable

disable コマンドは、DDN アドレス変換、ネットワーク認証の一部としてのインターフェース・リセット、あるいは着呼禁止または発呼禁止機能を使用不可にするのに使用します。

注: DDN をナショナル・パーソナリティーとして設定した場合、DDN アドレス変換が自動的に使用可能になり、このパラメーターは無効になります。

構文:

disable ddn-address-translations

注: ddn-address-translations は、使用不可にすることができなくなりました。この機能は、選択されたナショナル・パーソナリティーが DDN の場合は、デフォルトで使用可能になり、その他の場合は、デフォルトで使用不可になります。

incoming-calls-barred

lower-dtr

outgoing-calls-barred

National Enable

national enable コマンドは、ナショナル・パーソナリティー構成で定義された機能を使用可能にするのに使用します。

構文:

national enable

accept-reverse-charges

bi-cug

bi-cug-outgoing-access

cug

cug-deletion

cug-incoming-access

cug-insertion

cug-outgoing-access

cug-zero-override

flow-control-negotiation

frame-ext-seq-mode (required for X.31)

packet-ext-seq-mode

request-reverse-charges

suppress-calling-addresses

throughput-class-negotiation

truncate-called-addresses

accept-reverse-charges

呼設定時の着信課金を受け入れます。このオプションは、DDN では利用不能です。

DDN デフォルト値

off

GTE デフォルト値

on

bi-cug この装置上の相互形閉域接続ユーザー・グループ・ファシリティーを使用可能にします。デフォルトでは、このファシリティーは使用不可です。

注: このパラメーターが使用可能でない場合は、相互形 CUG を追加することはできません。

bi-cug-outgoing-access
この装置上の出アクセスをもつ相互形 CUG を使用可能にします。デフォルトでは、このファシリティーは使用不可です。

cug この装置上の閉域接続ユーザー・グループ・ファシリティーを使用可能にします。デフォルトでは、このファシリティーは使用不可です。

注: このパラメーターが使用可能でない場合は、CUG を追加することはできません。

cug-deletion
X.25 を介して転送する前に、XTP から受信した発呼パケットから CUG ファシリティーを除去します。デフォルトでは、この機能は使用不可です。

cug-incoming-access
この装置上の入アクセスをもつ CUG を使用可能にします。デフォルトでは、このファシリティーは使用不可です。

cug-insertion
IP を介して要求を転送する前に、X.25 インターフェースから XTP が受信した発呼要求に、該当する (アドレス特定、プロトコル特定、またはインターフェース特定) 優先 CUG 番号を挿入します。発呼パケット内にすでに CUG ファシリティーが存在する場合は、それを置き換えません。デフォルトでは、この機能は使用不可です。

cug-outgoing-access
この装置上の出アクセスをもつ CUG を使用可能にします。デフォルトでは、このファシリティーは使用不可です。

cug-zero-override
閉域ユーザー・グループ・ファシリティーに対して、CUG 番号 0 をもつ発呼要求パケット内の CUG ファシリティーを無視させます。デフォルトでは、この機能は使用不可です。

flow-control-negotiation
SVC の呼設定時にパケットおよびウィンドウ・サイズのネゴシエーションを使用可能にします。

DDN デフォルト値
on

GTE デフォルト値
on

frame-ext-seq-mode
フレーム・レイヤーのシーケンス番号をモジュロ 128 (つまり、0 ～ 127) に設定します。

DDN デフォルト値
off (X.31 の場合は on が必須)

GTE デフォルト値
off

packet-ext-seq-mode
パケット・レイヤーが拡張シーケンス番号 (0 〜 127) を使用できるようにします。

DDN デフォルト値
off

GTE デフォルト値
off

request-reverse-charges
すべての発呼に対して着信課金を要求します。

DDN デフォルト値
off

GTE デフォルト値
on

suppress-calling-address
発呼パケット内の発信元アドレスを抑制します。

DDN デフォルト値
off

GTE デフォルト値
off

throughput-class-negotiation
スループット・クラスの登録を使用可能にします。

DDN デフォルト値
off

GTE デフォルト値
on

truncate-called-addresses
DTE への呼の転送時の被呼 DTE アドレスの切り捨てを使用可能にします。このオプションは XTP 回線にのみ適用されます。

DDN デフォルト値
off

GTE デフォルト値
off

National Disable

national disable コマンドは、ナショナル・パーソナリティー構成で定義された機能を使用不可にするのに使用します。

構文:

national disable accept-reverse-charges
bi-cug
bi-cug-outgoing-access

cug

cug-deletion

cug-incoming-access

cug-insertion

cug-outgoing-access

cug-zero-override

flow-control-negotiation

frame-ext-seq-mode

packet-ext-seq-mode

request-reverse-charges

suppress-calling-addresses

throughput-class-negotiation

truncate-called-addresses

National Set

national set コマンドは、ナショナル・パーソナリティー構成のデフォルト値の 1 つまたはすべてを設定するのに使用します。

構文:

national set

call-req

clear-req . . .

disconnect-procedure . . .

dp-timer

frame-window-size

n2-timeouts

packet-size . . .

reset . . .

restart . . .

min-recall

min-connect

collision-timer

standard-version

t1-timer

t2-timer

truncate-called-addr-size

call-req

発呼要求をあきらめて切断する前に許される 10 秒間隔の回数を指定します。ゼロは、無期限に待つことを示します。 list コマンドの出力では、これは t21 タイマーとして表示されます。

DDN デフォルト値
20 デカ秒

GTE デフォルト値
20 デカ秒

clear-req *retries* **または** *timer*

復旧要求の再送の回数を指定します。

Retries

アクションを取る前に許される復旧要求の伝送の回数。 list コマンドの出力では、これは r23 再試行カウントとして表示されます。

DDN デフォルト値
再試行=1

GTE デフォルト値
再試行=1

Timer 復旧要求パケットを再送する前に待つ 10 秒間隔の回数。タイマー値のゼロは、無期限に待つことを示します。 list コマンドの出力では、これは t23 タイマーとして表示されます。

DDN デフォルト値
18 デカ秒

GTE デフォルト値
18 デカ秒

disconnect-procedure *passive* **または** *active*

切断時に使用する切断手順のタイプを指定します。

DDN デフォルト値
passive

GTE デフォルト値
passive

Passive

切断時に DISC フレームを使用しないことを指定します。

Active 切断時に DISC フレームを使用することを指定します。

dp-timer

フレーム・レベルが切断状態のままでいるミリ秒数を指定します。ゼロは、即時に切断フェーズからリンク設定状態に移行することを示します。

DDN デフォルト値
500 ミリ秒

GTE デフォルト値
500 ミリ秒

frame-window-size
確認の前にアウトスタンディング状態に置くことができるフレーム数を指定します。

DDN デフォルト値
7

GTE デフォルト値
7

n2-timeouts
インターフェースがリサイクルされる前に再送タイマー (T1) を満了させることができる回数を指定します。

DDN デフォルト値
20

GTE デフォルト値
20

packet-size *default* **または** *maximum* **または** *window*
パケットのサイズを指定します。

default
パケットのデータ部分のバイト数。可能なオプションは、128、256、512、1024、2048、および 4096 です。この値は、パケット・サイズのネゴシエーションが行われない場合に使用されます。*Default* は *maximum* より大きい値であってはなりません。

DDN デフォルト値
128

GTE デフォルト値
128

maximum
パケットのデータ部分の最大バイト数。可能なオプションは、128、256、512、1024、2048、および 4096 です。

DDN デフォルト値
256

GTE デフォルト値
256

window
確認応答が必要になる前に許されるアウトスタンディング I フレームの数。範囲は、ナショナル・パーソナリティーのパケット・モジュラスによって決まります。

関連の構成パラメーターは、次のとおりです。

- Protocol max default window
- Set default window size

reset *retries* **または** *timer*
リセット要求の再送回数を指定します。

例: `national set reset retries 2`

retries

呼が切断される前に許されるリセット要求の伝送回数。範囲は 0 ～ 255 です。 list コマンドの出力では、これは r22 再試行カウントとして表示されます。

DDN デフォルト値
1

GTE デフォルト値
1

timer リセット要求パケットを再送する前に待つ 10 秒間隔の回数。範囲は 0 ～ 255 です。タイマー値のゼロは、無期限に待つことを示します。 list コマンドの出力では、これは t22 タイマーとして表示されます。

DDN デフォルト値
18 デカ秒

GTE デフォルト値
18 デカ秒

restart *retries* **または** *timer*
リスタート要求の伝送回数を指定します。

retries

インターフェースがリサイクルされる前に許されるリスタート要求の伝送回数。範囲は 0 ～ 255 です。 list コマンドの出力では、これは r20 再試行カウントとして表示されます。

DDN デフォルト値
1

GTE デフォルト値
1

timer リスタート要求パケットを再送する前に待つ 10 秒間隔の回数。範囲は 0 ～ 255 です。タイマー値のゼロは、無期限に待つことを示します。 list コマンドの出力では、これは t20 タイマーとして表示されます。

DDN デフォルト値
18 デカ秒

GTE デフォルト値
18 デカ秒

min-recall

SVC をオープンするために呼を再初期化する前に待つ最小秒数を指定します。範囲は 0 ～ 255 秒です。

DDN デフォルト値
10 秒

GTE デフォルト値
10 秒

min-connect

すべての誤り状態を禁止するコネクションが確立された後、SVC が確立状態に保たれる最小時間を秒数で指定します。範囲は 0 〜 255 秒です。

DDN デフォルト値

90 秒

GTE デフォルト値

90 秒

collision-timer

元の試行結果が呼衝突であった場合、SVC をオープンするために呼を再初期化する前に使用する時間遅延を秒数で指定します。範囲は 0 〜 255 秒です。

DDN デフォルト値

10 秒

GTE デフォルト値

10 秒

standard-version

オプションは、none、v1980、v1984、および v1988 です。

DDN デフォルト値

1984

GTE デフォルト値

1984

t1-timer

フレーム再送時間を秒数で指定します。範囲は 1 〜 255 です。

DDN デフォルト値

4 秒

GTE デフォルト値

4 秒

t2-timer

I フレームを確認応答する前の遅延時間を秒数で指定します。これは最適化パラメーターです。タイマーを 0 に設定すると、これは使用不可になります。範囲は 0 〜 255 です。

DDN デフォルト値

0

GTE デフォルト値

0

truncate-called-addr-size

被呼アドレスの末端から切り捨てられる文字数を指定します。このオプションは XTP 回線にのみ関係します。範囲は 0 〜 10 です。

DDN デフォルト値

2

GTE デフォルト値

2

National Restore

national restore コマンドは、**national set**、**national enable**、または **national disable** コマンドを使用してナショナル・パーソナリティー構成で設定したデフォルト値の 1 つまたはすべてを復元するのに使用します。

構文:

national restore

- all
- accept-reverse-charges
- bi-cug
- bi-cug-outgoing-access
- call-req
- clear-req . . .
- cug
- cug-deletion
- cug-incoming-access
- cug-insertion
- cug-outgoing-access
- cug-zero-override
- disconnect-procedure . . .
- dp-timer
- flow-control-negotiation
- frame-ext-seq-mode
- frame-window-size
- min-collission-timer
- min-connect-timer
- min-recall-timer
- network-type . . .
- n2-timeouts
- packet-size . . .
- packet-ext-seq-mode
- request-reverse-charges
- reset . . .
- restart . . .
- standard-version
- suppress-calling-addresses
- throughput-class-negotiation

t1-timer

t2-timer

truncate-called-addresses

truncate-called-addr-size

Add

add コマンドは、X.121 アドレス、DDN X.25 アドレス、プロトコル構成、または PVC 定義を追加するのに使用します。

構文:

add address

bi-cugs

cugs

htf-address

protocol

pvc

address

ルーターの構成でサポートされているプロトコルの X.121 アドレス変換を追加します。表示されるプロンプトは、追加するプロトコル・アドレスによって異なります。 (以下の例を参照してください。) 入力するプロトコル・アドレスおよび X.121 アドレスは、そのプロトコルと、ルーター X.25 インターフェースに接続するリモート DTE の X.121 DTE アドレスを表します。プロトコルが APPN または DLSw でない限り、プロトコル・アドレスと X.121 アドレスのマッピングは固有でなければなりません。プロトコル・アドレスは、複数の X.121 アドレスにマップすることはできません。また、特定の X.121 アドレスを複数のプロトコル・アドレスにマップすることもできません。ローカル X.25 アドレスを設定するのには **set address** コマンドを使用します。 ローカル X.25 アドレスを設定した後は、ダイヤルアウト用の X.25 リモート・アドレスおよびオプションの呼 ID 用の着信リモート・アドレスを使用できるようになります。リモート被呼アドレスのみを入力した場合、このアドレスが、発呼と着呼の検証に使用されます。

例: add address

IP の例:

```
Protocol [IP]?  IP
IP Address [0.0.0.0]? 128.185.1.2
Enc Priority 1 []? CC
Enc Priority 2 []? SNAP
Enc Priority 3 []? Null
X.25 Address []? 1234590
Remote address []?
Pref CUG  []? 11
CUG (2)  []? 12
CUG (3)  []? 13
CUG (4)  []? 14
CUG (5)  []? 15
Pref BI-CUG  []? 21
BI-CUG (2)  []? 22
BI-CUG (3)  []?
```

IPX の例:

```
Protocol [IP]? IPX
CUD Field Usage (Standard or Proprietary)
IPX Host Number (in hex) []?
Enc Priority 1 []? SNAP
Enc Priority 2 []?Null
X.25 Address []?
Pref CUG [] ?
Pref Bi-CUG[]? 1
BI-CUG (2)[]? 3
BI-CUG (3)[]
```

Protocol
追加するアドレス・マッピングのプロトコル・タイプを指定します。有効値は、APPN、DECnet、DLSw、IP、IPX、および VINES です。デフォルト値は IP です。

Enc Priority
CUD に書き込まれるカプセル化タイプ (RFC 1356 で定義) を決めます。 IP の場合、有効な選択は CC、SNAP または Null です。 IPX の場合、有効な選択は SNAP または Null です。呼の最初の試行では Enc Priority 1 が使用されます。これが失敗した場合は、次に Priority 2 が使用されるといった具合になります。

IP Address
着信先の IP アドレスを指定します。

CUD Field Usage
このフィールドは、IPX から X.25 へのアドレス・マッピング専用です。これは、IPX の発呼要求パケットを受信したときの起呼ユーザー・データ (CUD) フィールドの記入方法を決めます。 CUD フィールドは Standard または Proprietary のいずれかです。 Standard (標準) は、その使用法が RFC 1356 で使用されているプロトコル多重化であることを示します。 Proprietary (専有) は、2210 またはこれと整合性のあるルーターのみが使用できる専有の CUD フィールドであることを示します。デフォルト値は Standard です。

IPX Host Number
着信先の IPX ホスト番号を指定します。

X.25 Address
ルーター X.25 インターフェースに接続するリモート DTE の X.121 DTE アドレスを指定します。最大アドレス長は 15 桁です。

pref cug
この DTE の優先閉域ユーザー・グループ番号を指定します。 DTE は発呼でこの CUG を使用します。

有効値: 0 ～ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティーを使用可能にした場合は、この値を求めるプロンプトが出ます。

CUG この DTE の閉域ユーザー・グループ番号を指定します。優先 CUG を含めて、最大 5 つの CUG を定義することができます。

有効値: 0 〜 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティーを使用可能にした場合は、この値を求めるプロンプトが出ます。

pref bi-cug
この DTE の優先相互形閉域ユーザー・グループ番号を指定します。DTE は発呼でこの CUG を使用します。

有効値: 0 〜 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、相互形閉域ユーザー・グループ・ファシリティーを使用可能になかった場合は、この値を求めるプロンプトは出ません。

bi-cug この DTE の相互形閉域ユーザー・グループ番号を指定します。最大 5 つの CUG を定義することができます。

有効値: 0 〜 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、相互形閉域ユーザー・グループ・ファシリティーを使用可能になかった場合は、この値を求めるプロンプトは出ません。

cugs この X.25 インターフェースの閉域ユーザー・グループ番号を指定します。

有効値: 0 〜 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティーを使用可能にした場合は、この値を求めるプロンプトが出ます。

例:

```
add cugs
Pref CUG  []? 23
CUG (2)  []? 24
CUG (3)  []? 25
CUG (4)  []? 26
CUG (5)  []? 27
```

pref cug
この DTE の優先閉域ユーザー・グループ番号を指定します。この DTE は発呼でこの CUG を使用します。

有効値: 0 〜 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティーを使用可能にした場合は、この値を求めるプロンプトが出ます。

cug この DTE の閉域ユーザー・グループ番号を指定します。最大 5 つの CUG を定義することができます。

有効値: 0 ～ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティーを使用可能にした場合は、この値を求めるプロンプトが出ます。

bi-cugs

この DTE の閉域ユーザー・グループ番号を指定します。

有効値: 0 ～ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、閉域ユーザー・グループ・ファシリティーを使用可能にした場合は、この値を求めるプロンプトが出ます。

例:

```
add bi-cugs
Pref BI-CUG  []? 23
BI-CUG (2)  []? 24
BI-CUG (3)  []? 25
BI-CUG (4)  []? 26
BI-CUG (5)  []? 27
```

pref bi-cug

この DTE の優先閉域ユーザー・グループ番号を指定します。この DTE は発呼でこの BI-CUG を使用します。

有効値: 0 ～ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、相互形閉域ユーザー・グループ・ファシリティーを使用可能になかった場合は、この値を求めるプロンプトは出ません。

bi-cug この DTE の閉域ユーザー・グループ番号を指定します。最大 5 つの CUG を定義することができます。

有効値: 0 ～ 9999

デフォルト値: なし

注: **national enable** コマンドを使用して、相互形閉域ユーザー・グループ・ファシリティーを使用可能になかった場合は、この値を求めるプロンプトは出ません。

htf-address

Defense Data Network (DDN) の X.25 アドレス変換を追加します。

例:

```
add htf-address
Protocol [IP]
Convert HTF address
```

Protocol

X.25 インターフェースを介して実行するプロトコルを指定します。DDN は IP のみをサポートします。

Convert HTF address

プロトコル・アドレスをホスト・テーブル・フォーマット (HTF) 形式の着信先 X.121 アドレスに変換します。 Enable/Disable コマンドの ddn-address-translations の項も参照してください。

protocol

プロトコル・カプセル化を使用可能にし、関連のパラメーターを定義します。

例:

```
add protocol
Protocol [IP]?
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
Circuit Idle Time [30]?
Max VCs [4]?
Pref CUG  []? 1
CUG (2)  []? 2
CUG (3)  []? 3
CUG (4)  []? 4
CUG (5)  []? 5
Pref BI-CUG  ]? 11
BI-CUG (2)  []? 12
BI-CUG (3)  []? 13
BI-CUG (4)  []? 14
BI-CUG (5)  []? 15
```

QLLC の例:

```
X.25 Config> add prot
Protocol [IP]? dls
Idle timer [30]?
QLLC response timer (in decaseconds) [2]?
QLLC response count [3]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI  (2) SEC  (3) (PEER) [3]?
Max Packet Size [128]?
Packet window size [7]?
Max Message Size [1500]?
Call User Data (in hex, 0 for null) []?
Pref CUG  []? 20
CUG (2)  []? 21
CUG (3)  []?
Pref BI-CUG  []?
```

Protocol

カプセル化パラメーターを追加したいプロトコル (APPN、XTP、IP、DECnet、IPX、DLSw、または Banyan VINES) を指定します。デフォルト値は IP です。

Window Size

パケットの確認が必要になる前にアウトスタンディング状態に置け

るパケット数を表す、最大交渉可能パケット・ウィンドウ・サイズを指定します。デフォルト値は 2 です。ウィンドウ・サイズは被呼側 DTE によって最低 1 まで交渉できます。

関連の構成パラメーターは、次のとおりです。

- Set Default Window

Default Packet Size

SVC のデフォルトの要求パケット・サイズを指定します。この値は、最低交渉可能パケット・サイズとして使われ、**national set packet-size** コマンドで指定された最大パケット・サイズ以下でなければなりません。最小 *default packet size* は 4096 バイトです。このパラメーターのデフォルト値は 128 バイトです。

関連の構成パラメーターは、次のとおりです。

- National Set Packet Size Default
- National Set Packet Size Maximum

Maximum Packet Size

SVC の最大交渉可能パケット・サイズを指定します。この値は、**national set packet-size** コマンドで指定された最大パケット・サイズ以下でなければなりません。このパラメーターのデフォルト値は 256 バイトです。このパラメーターに構成できる最大値は 4096 バイトです。この値は、この X.25 インターフェースの最大フレーム・サイズを計算するのに使用されます。

関連の構成パラメーターは、次のとおりです。

- National Set Packet Size Default
- National Set Packet Size Maximum

Circuit Idle Time

ルーターによって切断される前に、SVC がアイドル状態でいられる秒数を指定します。範囲は 0 ～ 65365 です。デフォルト値は 30 秒です。 0 (ゼロ) は、その回線はルーターによって切断されることがないことを示します。

Maximum VCs

あるプロトコルの同じ DTE アドレスに対してオープンできる回線の最大数を指定します。このパラメーターの使用法については、 RFC 1356 を参照してください。有効範囲は 1 ～ 10 です。デフォルト値は 4 です。

pref CUG, CUG, pref bi-cug, bi-cug

add address コマンドを参照してください。

以下は、QLLC 固有のパラメーターです。

QLLC response timer

再送する前に Q レスポンス・パケットを待つ秒数

QLLC response count

QLLC を再送するする最大回数。この再試行回数が尽きると、回線がルーターによって切断またはリセットされる可能性があることを高位レイヤーに通知します。

Accept Reverse Charges
このプロトコルを使用して、このナショナル・パーソナリティー・パラメーターの設定値を指定変更することができます。これは、ナショナル・パーソナリティー・パラメーターには影響を与えません。

Request Reverse Charges
このプロトコルを使用して、このナショナル・パーソナリティー・パラメーターの設定値を指定変更することができます。これは、そのナショナル・パーソナリティー・パラメーターには影響を与えません。

Station Type
このプロトコルのデフォルトのステーション・タイプを指定します。

Pri 1 次ステーション

Sec 2 次ステーション

Peer 同位ステーション

Max message size
このプロトコルの最大メッセージ・サイズ。インターフェースの最大 MTU サイズ以下の値を指定します。

Call User Data
このプロトコルの発呼パケットで使用されるデフォルトの CUD フィールドを指定します。 1 ～ 16 文字を指定します。文字を指定しない場合は、デフォルトの 0xC3 が使用されます。

pvc PVC、ウィンドウ・サイズ、およびパケット・サイズの定義を追加します。

例: add pvc

IP の例:

```
Protocol [IP]?  IP
Packet Channel [1]?
Destination X.25 Address []?
Window Size [2]?
Packet Size [128]?
```

Protocol
カプセル化を変更したいプロトコル (APPN、XTP、DECnet、Banyan Vines、DLSw、IP、または IPX) を指定します。デフォルト値は IP です。

Packet Channel
PVC の回線番号を指定します。

Destination X.25 Address
PVC の着信先の X.25 アドレスを指定します。

Remote Address
受信した呼の発呼側 ID のリモート・アドレスを指定します。

Window Size
パケットの確認が必要になる前にアウトスタンディング状態に置けるパケット数を指定します。デフォルト値は 2 です。

関連の構成パラメーターは、次のとおりです。

- Set Default Window

Packet Size

PVC の最大交渉可能パケット・サイズを指定します。この値は、**national set packet-size** コマンドで指定された最大パケット・サイズ以下でなければなりません。このパラメーターのデフォルト値は 128 バイトです。このパラメーターに構成できる最大値は 4096 バイトです。 X.31 の最大値は 256 バイトです。この値は、この X.25 インターフェースの最大フレーム・サイズを計算するのに使用されます。

関連の構成パラメーターは、次のとおりです。

- Nat Set Packet Size Default
- Nat Set Packet Size Maximum

Change

change コマンドは、X.121 アドレス、DDN X.25 アドレス、プロトコル構成、または PVC 定義を変更するのに使用します。

注: X.121 アドレスに関連付けられている IP アドレスを変更する場合は、アドレス相関が入っているレコードを削除した後で、アドレス・マッピングを再定義する必要があります。

構文:

change address
htf-address
protocol
pvc

address

X.121 アドレス変換を変更します。表示されるプロンプトは、変更するプロトコル・アドレスによって異なります。

例: change address

IP の例:

```
Protocol [IP]  IP
IP Address [0.0.0.0]?
Enc Priority []?
X.25 Address [00000124040000]?
```

IPX の例

```
Protocol [IP]  IPX
CUD Field Usage (Standard or Proprietary) [Standard]?
IPX Host number (in hex) []?
Enc Priority []?
X.25 Address [00000124040000]?
```

htf address

Defense Data Network (DDN) X.25 アドレス変換を変更します。

例:

```
change htf-address
Protocol [IP]
Change HTF address [0.0.0.0]?
New HTF address [10.4.0.124]?
```

protocol

プロトコル構成定義を変更します。

例:

```
change protocol
Protocol [IP]
Window Size [2]
Default Packet Size [128]
Maximum Packet Size [256]
Circuit Idle Time [30]
Maximum VCs [6]
```

QLLC の例:

```
X.25 Config>
change prot
Protocol [IP]? dls
Idle Timer [30]?
QLLC response timer (in decaseconds) [15]?
QLLC response count [255]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI (2) SEC (3) PEER [3]?
Max Packet Size [256]?
Packet Window size [7]?
Max message size [2048]?
Call User Data (in HEX, 0 for Null) []? C3010000525450
```

pvc PVC、ウィンドウ・サイズ、およびパケット・サイズの定義を変更します。

注: プロトコル、パケット・チャネル、または着信先 X.25 アドレスを変更する場合は、その定義が入っているレコードをいったん削除した後、変更されたパラメーターを使用して再び追加する必要があります。

例:

```
change pvc
Protocol [IP]?  IP
Packet Channel [1]?
Destination X.25 Address []?
Window Size [2]?
Packet Size [128]?
```

Delete

delete コマンドは、X.121 アドレス、プロトコル構成定義、または PVC 定義を削除するのに使用します。

構文:

delete address
bi-cugs
cugs
protocol . . .
pvc

address

X.121 アドレス変換を削除します。

例: delete address

IP の例:

```
Protocol [IP]?
IP Address [0.0.0.0]?
```

IPX の例

```
Protocol [IP]? IPX
IPX Host Number (in hex) [2]?
```

bi-cugs

このインターフェースによって使用される相互形閉域接続ユーザー・グループ番号を削除します。

有効値:

Y 現行の CUG を削除します。

N 現行の CUG を削除しません。

ALL 残りの CUG をすべて削除します。

Q 残りの CUG の削除を中止します。

例:

```
delete bi-cugs
Delete Pref BI-CUG [Y]?
Delete BI-CUG (2) [Y]? N
Delete BI-CUG (3) [Y]? q
```

cugs このインターフェースによって使用される閉域接続ユーザー・グループ番号を削除します。このコマンドの機能は **delete bi-cug** コマンドに似ています。

例:

```
del cug

Delete Pref CUG [Y]?
Delete CUG (2) [Y]?
Delete CUG (3) [Y]? q
```

protocol *prot-type*

プロトコル・カプセル化構成定義を削除します。 *Prot-type* は、ルーターの構成に現在定義されているプロトコル・カプセル化の名前または番号です。

pvc PVC 定義を削除します。

例:

```
delete pvc
Protocol [IP]?
Destination X.25 Address []?
```

List

list コマンドは、指定されたパラメーターの現行構成を表示するのに使用します。

構文:

list address / all / cugs

detailed

protocols

pvc

summary

address

すべての X.121 アドレス変換をリストします。

例:

```
list address
IF#      Prot #     Active Enc     Protocol ->    X.25 address
1         0(IP)        CC          10.1.2.3 ->    1238765742
1         7(IPX)       SNAP        10       ->    12389
              CUGS: 11 12 13 14 15         BI-CUGS: 21 22
```

all すべての X.25 アドレス、ナショナル・パーソナリティー・パラメーター、すべての定義済みプロトコルとそれらの値、およびすべての定義済み PVC をリストします。

例:

```
 list all

X.25 Configuration Summary

Node Address:       313131
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:           64000        Clocking:  Internal
MTU:              2048        Cable:     V.35 DCE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC              low: 1    high: 1
Inbound          low: 0    high: 0
Two-Way          low: 2    high: 64
Outbound         low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400

X.25 National Personality Configuration

Request Reverse Charges:  on  Accept Reverse Charges:     on
Frame Extended seq mode:  off Packet Extended seq mode:   off
Incoming Calls Barred:    off Outgoing Calls Barred:      off
Throughput Negotiation:   on  Flow Control Negotiation:   on
Suppress Calling Addresses: off  DDN Address Translation:  off
Truncate Called Addresses:  off
Number of digits to truncate called addresses to:  2
CUG Support: off                BI-CUG Support: off
CUG Outgoing Access: off        CUG Incoming Access : off
BI-CUG Outgoing Access: off     CUG 0 Override: off
CUG Isertion: off               CUG deletion: off
Call Request Timer:     20 decaseconds
Clear Request Timer:    18 decaseconds (1 retries)
Reset Request Timer:    18 decaseconds (1 retries)
Restart Request Timer:  18 decaseconds (1 retries)
Min Recall Timer        10 seconds
Min Connect Timer       90 seconds
Collision Timer          5 seconds
T1 Timer:  4.00 seconds     N2 timeouts: 20
T2 Timer:  2.00 seconds     DP Timer:    500 milliseconds
Standard Version:     1984      Network Type: CCITT
Disconnect Procedure: passive
Window Size     Frame:   7      Packet:  2
Packet Size     Default: 128    Maximum: 256

X.25 protocol configuration

No protocols defined
```

```
X.25 PVC configuration

No PVCs defined

X.25 address translation configuration
No address translations defined
```

cugs この装置内の各 X.25 インターフェースの CUG および BI-CUG 番号をリストします。

例:

```
li cugs
CUGS: 23 24 25 26 27
```

detailed

national set コマンドで変更したすべてのデフォルト・パラメーターの値をリストします。画面表示の説明は、本章の後方で説明する **national set** コマンドの項に示してあります。

例:

```
list detail

X.25 National Personality Configuration

Follow CCITT: on    OSI 1984:     on        OSI 1988: off
Request Reverse Charges:  off   Accept Reverse Charges:     off
Frame Extended seq mode:  off   Packet Extended seq mode:   off
Incoming Calls Barred:    off   Outgoing Calls Barred:      off
Throughput Negotiation:   on    Flow Control Negotiation:   off
Suppress Calling Addresses: off DDN Address Translation:    off
Truncate Called Addresses:  off
Number of digits to truncate called address to:  2
CUG Support: off                BI-CUG Support: off
CUG Outgoing Access: off        CUG Incoming Access : off
BI-CUG Outgoing Access: off     CUG 0 Override: off
CUG Isertion: off               CUG deletion: off
T21 (Call Request Timer):     20 decaseconds
T23 (Clear Request Timer):    18 decaseconds (1 retries)
T22 (Reset Request Timer):    18 decaseconds (1 retries)
T20 (Restart Request Timer):  18 decaseconds (1 retries)
Min Recall Timer:       10 seconds
Min Connect Timer:      90 seconds
Collision Timer:        8 seconds
T1 Timer:  4.00 seconds     N2 timeouts: 20
T2 Timer:  0.00 seconds     DP Timer:    500 milliseconds
Standard Version:     1984      Network Type: CCITT
Disconnect Procedure: active
Window Size     Frame:   7      Packet:  2
Packet Size     Default: 256    Maximum: 256
```

protocols

すべての定義済みプロトコル構成をリストします。パラメーターの説明は、361ページの『Add』 を参照してください。

例:

```
list protocols

X.25 protocol configuration

Protocol       Window         Packet-Size        Idle    Max
 Number         Size          Default Maximum    Time    VCs

 0(IP)           2              128   256         30      4
             CUGS: 11 12 13 14 15         BI-CUGS: 21 22
QLLC Protocols

Protocol     Packet        Idle    Response    Reverse Charges   Max       Station
 Number    Window MaxSize  Time   Timer Count  Accept Request   Message     Type

26(DLSW)     7      256     30     15    255      N      N        2048       PEER
          CUD : [C3 01 00 00 52 54 50 ]
          CUGS: 11 12 13 14 15      BI-CUGS: 21 22
```

pvc すべての定義済み PVC をリストします。

例:

```
list pvc

X.25 PVC configuration

Prtcl    X.25 Address    Active Enc    Window    Pkt_len   Pkt_chan
0          8383838383        CC           4       1024       3
```

summary

set および **enable** コマンドで設定されたすべての値をリストします。これらの値は X.25 構成を変更します。

例:

```
list summary

X.25 Configuration Summary

Node Address:       313131
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:           64000        Clocking:  Internal
MTU:              2048        Cable:     V.35 DCE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC              low: 1    high: 1
Inbound          low: 0    high: 0
Two-Way          low: 2    high: 64
Outbound         low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400
```

インターフェース監視プロセスへのアクセス

X.25 ネットワーク・インターフェースに関連する情報を監視するには、以下の手順を使用して、インターフェース監視プロセスにアクセスします。

1. OPCON プロンプトで **talk 5** と入力する。たとえば、次のように入力します。

   ```
   *talk 5
   +
   ```

   GWCON プロンプト (+) がコンソールに表示されます。最初に GWCON に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

   ```
   + configuration
   ```

   (**configuration** コマンドの出力例については、137ページの『Configuration』を参照してください。)

3. **network** コマンドと X.25 インターフェース番号を入力する。

   ```
   + network 2
   X.25>
   ```

   X.25 監視プロンプトが、コンソールに表示されます。次に、X.25 監視コマンドを入力すると、X.25 インターフェースに関する情報を表示することができます。

X.25 監視コマンド

この節では、X.25 監視コマンドの要約を示し、個々のコマンドについて説明します。X.25 監視コマンドを使用して、X.25 パケットを転送するインターフェースおよびネットワークのパラメーターと統計を表示することができます。監視コマンドは、物理レベル、フレーム・レベル、およびパケット・レベルの構成値を表示します。この 3 つのプロトコル・レベルのすべての値を同時に表示するオプションもあります。

X.25 監視コマンドは X.25> プロンプトで入力します。 表51 は、コマンドを示しています。

表 51. X.25 監視コマンドの要約

監視コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	個々の PVC または SVC 統計および一般情報をリストします。
Parameters	X.25 構成の任意のレベルの現行パラメーターを表示します。
Statistics	X.25 構成の任意のレベルの現行統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、現在アクティブの PVC および SVC を表示するのに使用します。

構文:

list pvcs

svcs

pvc 構成されたパーマネント・バーチャル・サーキットを表示します。

svc アクティブのスイッチド・バーチャル・サーキットを表示します。

例:

```
list svc

LCN/  Destination  Originate Transmits  Protocol    Totals
State      Address     Call   Queued  Encapsulated Xmts Rcvs Resets

13 D   898280077113   YES     0          IP      8943  261    1
20 D   898280077114    NO     0          IP       943   43    0
42 P   898280077116   YES     6          IP         0    0    0
23 C   898280077117   YES     0          IP      3054  110    0


D  - Data Transfer      P  - Call Progressing
C  - Call Clearing
```

Parameters

parameters コマンドは、X.25 構成の任意のレベルの現行パラメーターを表示するのに使用します。

構文:

parameters all

frame

packet

physical

all パケット、フレーム、および物理レベルのパラメーターを表示します。

frame フレーム・レベルのパラメーターを表示します。

例:

```
parameters frame
Frame Layer Parameters:
Maximum Frame Size  = 262 Maximum Window Size  =     7
Protocol Enabled    = YES Equipment Type       =   DTE
T1 Retransmit Timer =   4 T2 Acknowledge Timer =     2
N2 Retry Counter    =  20 Disconnect Procedure =   PASSIVE
Disconnect Timer    = 500 Network Type         =   GTE
Protocol Options: Inhibit Idle RRs No   MOD 128 NO   Enable SARM  NO
```

packet

パケット・レベルのパラメーターを表示します。

例:

```
parameters packet
Packet Layer Parameters:
Default Packet Size = 128  Maximum Packet Size =   256
Log 2 Packet size   =   2  Acknowledge Delay  =     0
Layer Enabled       = YES Default Window Size =     2
Lowest SVC          =   1  Highest SVC        =    64
Lowest PVC          =   0  Highest PVC        =     0
T20 (Restart)       = 18  R20 (Retry)         =     1
T21 (Call)         =     20
T22 (Reset)         = 18  R22 (Retry)         =     1
T23 (Clear)         = 18  R23 (Retry)         =     1
Network Type        = GTE  Equipment Type     =   DTE
Recall Timer        = 10 seconds
Min Connect         = 90 seconds
Collision           = 5 seconds
```

physical

物理レベルのパラメーターを表示します。

例:

```
parameters physical
Physical Layer Parameters:
Interface Type        =    V.35

Maximum Frame Size    =    264   InterFrame Delay    =         2
Configured Speed      =      0   Clocking            =  External
Encoding              =    NRZ
Protocol Enabled      =    Yes
```

Statistics

statistics コマンドは、X.25 構成の任意のレベルの現行統計を表示するのに使用します。

構文:

statistics

all

frame

packet

physical

all パケット、フレーム、および物理レベルの統計を表示します。

frame フレーム・レベルの統計を表示します。

例:

```
statistics frame
Frame Layer Counters:      Received             Transmitted
Information Frames              0                       0
RR Command                      0                       0
RR Response                     0                       0
RNR Command                     0                       0
RNR Response                    0                       0
REJ Command                     0                       0
REJ Response                    0                       0
SABM                            0                      71
SABME                           0                       0
UA                              0                       0
DISC                            0                       0
DM                              0                       0
FRMR                            0                       0
Total Bytes                     0                       0
T1 Timeouts   0   T2 Timeouts         0   N2 Timeouts   1
Bad Address   0   Unsolicited F-Bit   0   Invalid Ctl   0
 Frame Layer Miscellaneous:
Queued Output Frames = 0 Protocol Layer State = Link Setup
Send Sequence N(S)   = 0 Receive Sequence N(R)= 0
```

packet

パケット・レベルの統計を表示します。

例:

```
statistics packet
Packet Counters:           Received             Transmitted
Call Request                    0                       0
Call Accepted                   0                       0
Clear Request                   0                       0
Clear Confirm                   0                       0
Interrupt Request               0                       0
Interrupt Confirm               0                       0
RR Packet                       0                       0
RNR Packet                      0                       0
REJ Packet                      0                       0

Reset Request                   0                       0
Reset Confirm                   0                       0
Restart Request                 0                       0
Restart Confirm                 0                       0
Diagnostic                      0                       0
Data Packet                     0                       0
Data Bytes                      0                       0
Buffers Queued                  0                       0
Invalid Packets Received =      0
Switched Circuits Opened =      0
```

physical

物理レベルの統計を表示します。

例:

```
statistics physical
X.25 Physical Layer Counters:
  Rx Bytes                       0   Tx Bytes                    0

  Adapter cable:          V.35 DTE

  V.24 circuit: 105 106 107 108 109 125 141
   Nicknames:    RTS CTS DSR DTR DCD RI  LL
   PUB 41450:    CA  CB  CC  CD  CF
   State:        ON  ON  ON  ON  ON  OFF OFF

  Line speed:             unknown
  Last port reset:        12 minutes, 21 seconds ago

 Input frame errors:
  CRC error                   0   alignment (byte length)         0
  missed frame                0   too long (>     0 bytes)        0
  aborted frame               0   DMA/FIFO overrun                0
  L & F bits not set          0
 Output frame counters:
  DMA/FIFO underrun errors       0   Output aborts sent           0
```

X.25 ネットワーク・インターフェースおよび GWCON インターフェース・コマンド

X.25 インターフェースには独自の監視用コンソール・プロセスがありますが、GWCON 環境から **interface** コマンドを使用すれば、ルーターも導入済みネットワーク・インターフェースの統計を表示します。 (**interface** コマンドについて詳しくは、第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド を参照してください。)

X.25 インターフェースに関して表示される統計

GWCON 環境から X.25 インターフェースに対して **interface** コマンドを入力すると、以下の統計が表示されます。

```
+interface
2
 Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
 2  2   X25/0        81640   5C          0          0            0

   X.25 MAC/data-link on SCC Serial Line interface
 Interface State:  DCD  CTS   Packet Layer   Frame Layer
                   OFF  OFF       DOWN          DOWN

   Packet Counters:           Received             Transmitted
    Data Packet                     0                       0
    Data Bytes                      0                       0
    Buffers Queued              0                       0
    Invalid Packets Received =      0
    Switched Circuits Opened =      0

    Frame Layer Counters:      Received             Transmitted
    Information Frames              0                       0

   X.25 Physical Layer Counters:
     Rx Bytes                       0   Tx Bytes              0

     Adapter cable:         Generic DTE  RISC Microcode Revision:       2

      V.24 circuit: 105 106 107 108 109 125 141
      Nicknames:    RTS CTS DSR DTR DCD RI  LL
      PUB 41450:    CA  CB  CC  CD  CF
      State:        ON  OFF OFF ON  OFF OFF OFF

     Line speed:              unknown
     Last port reset:         23 minutes, 48 seconds ago

     Input frame errors:
    CRC error                    0   alignment (byte length)         0
    missed frame                 0   too long (>     0 bytes)        0
    aborted frame                0   DMA/FIFO overrun                0
    L & F bits not set           0
   Output frame counters:    DMA/FIFO underrun errors      0   Output aborts sent     0

   Interface buffer pool: Total = 30, Free = 30
```

下のリストは、インターフェース統計を説明しています。

Nt グローバル・インターフェース番号

Nt ' 将来のダイヤル回線使用に予約

Interface
インターフェース名と番号 (同一タイプのインターフェース内の)

CSR COMM および状況レジスター・アドレス

Vec 割り込みベクトル

Self-Test Passed
成功した自己テストの回数

Self-Test Failed
失敗した自己テストの回数

Maintenance Failed
保守障害の数

Interface state
入力モデム制御信号、パケット・レイヤー (X.25 レイヤー 3)、およびフレーム・リレー (X.25 レイヤー 2) の現在の状態を表示します。

Packet Counters
送受信パケットに関する統計を表示します。

Data Packets
インターフェースがネットワーク上で送受信したデータ・パケット数を表示します。

Data Bytes
インターフェースがネットワーク上で送受信したデータ・バイト数を表示します。

Buffers Queued
ネットワーク上に転送するため現在待ち行列化されているバッファーの数を表示します。これらは、フレームまたはパケット・レイヤーの監視メッセージや転送パケットである場合もあります。

Invalid Packets Received
ネットワークから受信した無効な X.25 パケットの数を表示します。

Switched Circuits Open
現在オープンしている交換回線の数を表示します。

Frame Layer Counters
フレーム・レイヤー・カウンターから生成された統計を提供します。

Information Frames
インターフェースが送受信した X.25 情報フレームの数を表示します。

X.25 Physical Layer Counters
物理レイヤー・カウンターから生成された統計を提供します。

RX Bytes
物理レイヤーによって受信されたバイト数を表示します。

TX Bytes
物理レイヤーによって送信されたバイト数を表示します。

V.24 circuit Nicknames State
回線、制御信号、ピン割り当てとそれらの状態 (ON または OFF)。

注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

Line speed
送信クロック・レート

Last port reset
前回のポート・リセット以降の時間の長さ

Input frame errors:

CRC error
チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment
長さが 8 ビットの偶数倍でなかったために廃棄された受信パケットの数

Too short
長さが 2 バイト未満であったために廃棄された受信パケットの数

Too long
構成されたサイズより大きかったために廃棄されたパケットの数

Aborted frame
送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーにデータを送信する速度が遅かったために、データをネットワークから受信できなかった回数。

Missed frame
フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

L & F bits not set
シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、`L & F bits not set` カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: `L & F bits not set` カウンターはトラフィックによる影響は受けません。

Output frame counters:

DMA/FIFO underrun errors
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーからデータを取り出す速度が遅かったために、データをネットワーク上に送信できなかった回数。

Output aborts sent
高位レベルのソフトウェアの要求によって打ち切られた伝送の数

X.25 ネットワーク・インターフェースの構成

第29章 XTP の使用

この章では、TCP/IP を介して X.25 トラフィックを伝送するための X.25 トランスポート・プロトコル (XTP) について説明します。本章には、以下の節が含まれています。

- 『X.25 トランスポート・プロトコル』
- 386ページの『XTP の構成』
- 386ページの『構成手順』

X.25 トランスポート・プロトコル

X.25 トランスポート・プロトコル (XTP) は、『プロトコル転送機能』 のサービスを提供します。プロトコル転送機能は、着信および発信プロトコル・パケット処理の中心拠点です。転送機能は、あるネットワーク・インターフェース上でパケットを受信し、それを別のインターフェースに送信します。

XTP は 複数のリモート・サイトに設置された X.25 装置に対応できるように設計されています。このような環境で、XTP は X.25 パケット交換網を使用せずに、1 つまたは複数の中央サーバーと通信できるようにします。

これを使用可能にするには、サーバー位置とリモート位置のルーターを使用してデータをカプセル化し、TCP/IP を介してクライアントとサーバー間で X.25 パケットを送達します。

382ページの図19 は、XTP の使用前と使用後のネットワーク構成を示しています。

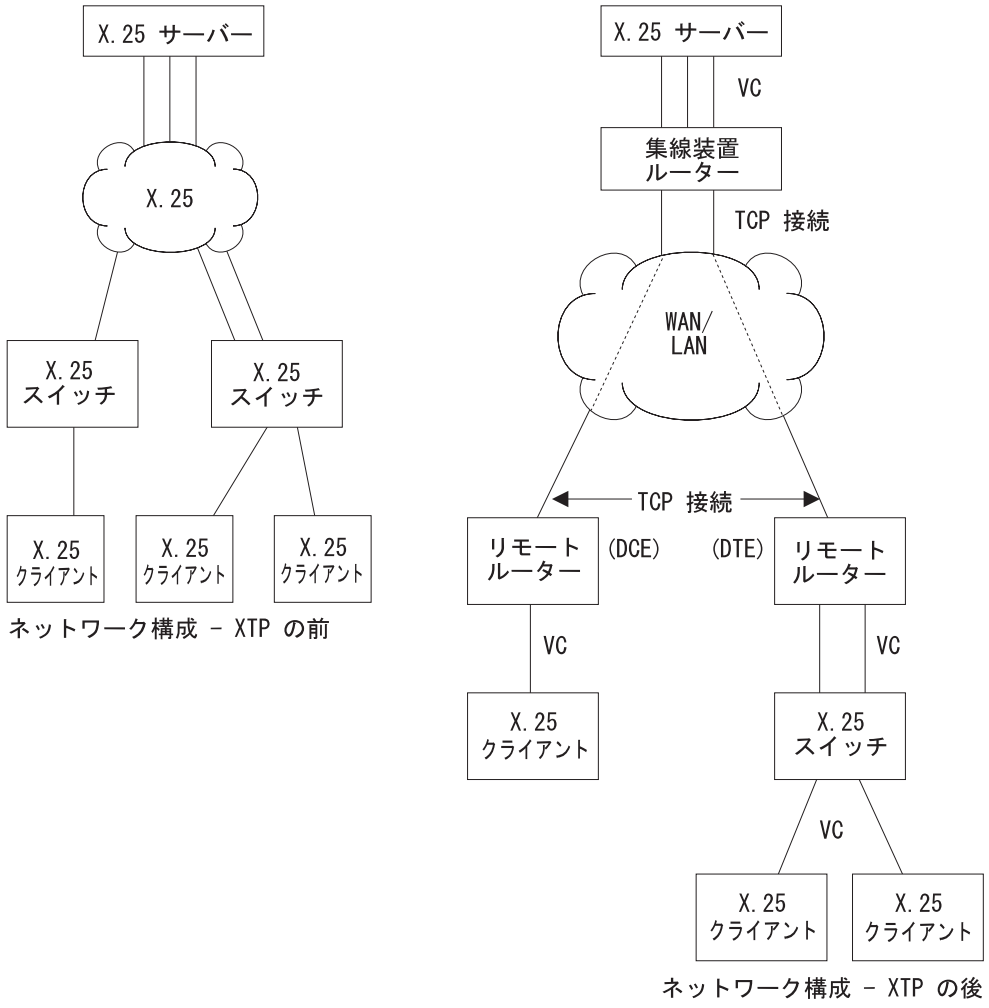


図 19. XTP の使用前と使用後の構成

構成情報

X.25 は、XTP 用に構成されたノード・アドレスに基づいて、XTP の着呼を認知します。したがって、X.25 ノード間で X.25 トラフィックを伝達するためには、データ端末装置 (DTE) アドレスおよびノードが接続されているルーターの IP アドレスにマップするように X.25 を構成する必要があります。

たとえば、図19 では、リモート・ルーターと集線装置ルーター上に X.25 クライアントを構成しています。この例では、*リモート・ルーター* は、X.25 サーバーにアクセスするための TCP/IP ネットワークに X.25 クライアントを接続します。*集線装置ルーター* は、リモート・ルーターにアクセスするための TCP/IP ネットワークに X.25 サーバーを接続します。

注: XTP を構成する場合、ルーターは、X.25 スイッチに接続されている場合は DTE と見なされます。スイッチに接続されていない場合は DCE (データ回線終端装置) と見なされます。

ルーターを XTP 用に構成するには、`XTP config>` プロンプトから以下の情報を定義した後で、ルーターをリスタートします。

- ローカル DTE
- 同位ルーター
- リモート DTE
- PVC
- CUG

ローカル DTE
ルーターの X.25 インターフェースに接続されている X.25 ノード。

ローカル DTE を構成するには、ローカル DTE に割り当てられている X.121 アドレスを使用します。 1 つのインターフェースに複数のローカル DTE を構成することもできます。

同位ルーター
TCP/IP を介して通信する相手のルーター

同位ルーターは 『観点』 によって異なります。たとえば、382ページの図19では、集線装置側から見ると、*2 つのリモート・ルーター* が同位ルーターになります。 2 つのリモート・ルーター側から見ると、*集線装置ルーター* が同位ルーターになります。

同位ルーターは、内部 IP アドレスによって指定します。

リモート DTE
ローカル X.25 ノードがコネクションをオープンし、データを交換するリモート X.25 ノード。リモート DTE に割り当てられている X.121 アドレスを使用します。

それぞれの同位ルーターに*固有* の IP アドレスを構成します。たとえば、382ページの図19 では、集線装置ルーターは各リモート・ルーターの固有の IP アドレスを知っている必要があり、各リモート・ルーターは集線装置ルーターの固有の IP アドレスを知っていることが必要です。

PVC X.25 のリスタート後も接続されたままになるパーマネント・チャネル。

PVC は固定されたチャネルなので、専用電話回線に似ています。 PVC は、XTP のコンテキストでは、ローカル X.25 DTE ノードからリモート X.25 DTE への PVC です。

ルーターを PVC 用に構成する場合は、同位ルーターの IP アドレスと、リモートおよびローカル DTE の PVC 番号をマップします。 PVC は、次の 4 つの情報によって識別されます。

- ローカル PVC の論理チャネル番号
- ローカル DTE の X.121 アドレス
- リモート (同位）ルーター上の PVC の論理チャネル番号
- リモート DTE の X.121 アドレス

CUGS XTP プロトコルの閉域ユーザー・グループ。 340ページの『閉域ユーザー・グループの概要』を参照してください。

追加の構成情報は、386ページの『XTP の構成』、および 395ページの『XTP 構成コマンド』 に記載されています。

DTE アドレス・ワイルドカード

DTE アドレス構成には、『*』 ワイルドカードを使用することができます。この他に『?』 文字も使用できます。これを DTE アドレスの中で指定すると、アドレスのその位置は任意の 1 桁の数字であることを表します。たとえば、『1?2?3』 という指定は、アドレス 18243 (2 番目、3 番目、および 5 番目の数字がそれぞれ 1、2、および 3）に一致します。

『*』 ワイルドカード文字は、ゼロ桁またはそれ以上の桁数の任意の文字列を表すことができます。これを使用できる位置は、DTE アドレスの指定の末尾だけに限定されます。たとえば、『123*』、『5555*』、『9*』、または 『*』 というように使用します。 DTE アドレスの特殊な例である 『*』 は、任意の DTE アドレス (ヌル・アドレスも含む）を表します。ヌル・アドレスは、X.25 発呼要求パケットに発信元アドレスが入っていない着呼を処理するのに便利です。

『*』 ワイルドカードを使用すると、既存のアドレスと競合するローカルまたはリモート DTE アドレスが加わる確率が高くなります。 **add local-dte** および **add remote-dte** コマンドは、ユーザーが既存のアドレスと競合する DTE アドレスを追加しようとすると、競合アドレスを表示するように機能強化されています。

例:
```
xtp config> add local-dte

            Interface number [0]? 1
            DTE address [ ] 123456
            DTE address [ ]?

            XTP config>add local-dte
            Interface number [0]?1
            DTE address [ ]?1*
            DTE address conflicts with existing DTE address 123456
```

XTP バックアップ同位機能

バックアップ同位機能は、複数の同位ルーターとリモート DTE とのアソシエーションを可能にします。ユーザーは、リモート DTE に対応する同位ルーターのリストを指定します。

例:
```
              XTP config>add rem
              DTE address [ ]?123456
              Peer router's internal IP Address [0.0.0.0]?10.0.0.2
              Peer router's internal IP Address [0.0.0.0]?10.0.0.4
              Peer router's internal IP Address [0.0.0.0]?11.0.0.1
              Peer router's internal IP Address [0.0.0.0]?
```

リモート DTE への着呼を受信すると、リスト内の各ルーターを経由するリモート DTE への接続が、リストに表示されている順序で試行されます。

リモート DTE の検索

DTE がリモート DTE への呼を開始すると、両方の DTE アドレスを検査して、X.25 トランスポートのために受け入れ可能かどうかを調べます。受け入れ可能の場合、X.25 トランスポート・プロトコル転送機能は、どの同位ルーターを介して呼を接続するかを決めます。リモート DTE の同位ルーター・リストの最初のルーターから検索

を開始します。満たしている必要がある第 1 条件は、同位ルーターへのアクティブの TCP 接続が存在することです。同位ルーターへのアクティブ TCP 接続がない場合は、リストの中の次のルーターを検査します。アクティブの TCP 接続が見つかると、発呼されます。接続プロセスの時間を計るために、接続要求タイマーがスタートします。

リモート DTE の検索は、次のイベントの 1 つによって終了します。

- 呼が同位ルーターを介して正常に接続された。

  この場合は、呼設定処理は完了し、リモート DTE の検索は終了します。
- 呼が同位ルーターによってリジェクトされた。

  この場合は、リモート DTE の検索が同位ルーター・リスト内の次のルーターに進みます。
- 接続要求タイマーが満了した。

  この場合は、リモート DTE の検索が同位ルーター・リスト内の次のルーターに進みます。

どの同位ルーターを介した接続も成功しないうちに同位ルーター・リストの終わりに達してしまった場合、ローカル DTE への呼は解除されます。

接続要求タイマー

接続要求タイマーは、呼設定手順が不特定時間ハングしていることがないようにするために使用されます。各同位ルーターごとにタイマーを構成します。

例:

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?10.0.0.2
Connection setup timeout [230]?60
```

接続要求タイマーは 10 ～ 480 秒に構成できます。デフォルト値は 230 秒です。このデフォルト値は、X.25 発呼要求タイマーのデフォルト設定値が 200 秒であることに基づいています。

タイマーは、同位ルーターを介して発呼した時点でスタートします。発呼が同位ルーターによって受け入れられるか、リジェクトされた時点でストップします。

ローカル XTP

ローカル XTP は、着信 X.25 トラフィックを現行ルーター上の同一の、または異なるインターフェースに転送することができます。ローカル XTP を構成するには、**add peer** コマンドで、ルーターの内部 IP アドレスを同位アドレスとして指定します。

XTP と閉域ユーザー・グループ

XTPは、**add local** または **add cug** コマンドによって定義されたローカル DTE アドレスを使用する閉域ユーザー・グループをサポートします。 XTP が閉域ユーザー・グループを使用できるようにするには、以下のことが必要です。

- 該当する X.25 インターフェース上の CUG または BI-CUG を使用可能にする。

XTP の使用

- **add cug** および **add bi-cug** コマンドを使用して、XTP プロトコル特定 CUG を提供する (必要な場合)。
- **add local** コマンドで、該当する閉域ユーザー・グループ番号を提供する。これには、以下のものが含まれます。
  - 閉域ユーザー・グループ番号
  - 優先閉域ユーザー・グループ番号
  - 相互形閉域接続ユーザー・グループ番号
  - 優先相互形閉域接続ユーザー・グループ番号
- **national enable cug_insertion** または **national enable cug_deletion** コマンドで、インターフェースの CUG の挿入または削除を使用可能にする (必要な場合)。
- **national enable cug 0 override** コマンドで、CUG 0 オーバーライド・オプションを使用可能にする (必要な場合)。

XTP の構成

XTP は、TCP/IP を介して X.25 トラフィックをトランスポートするのに使用されるプロトコル転送機能です。 XTP を使用すると、既存の X.25 装置が TCP/IP バックボーンを介して通信し、X.25 ネットワークからユーザーが選択したネットワークに移行することが可能になります。

構成手順

この節では、387ページの図20 に表示されているネットワークを構成するための詳細を定義します。

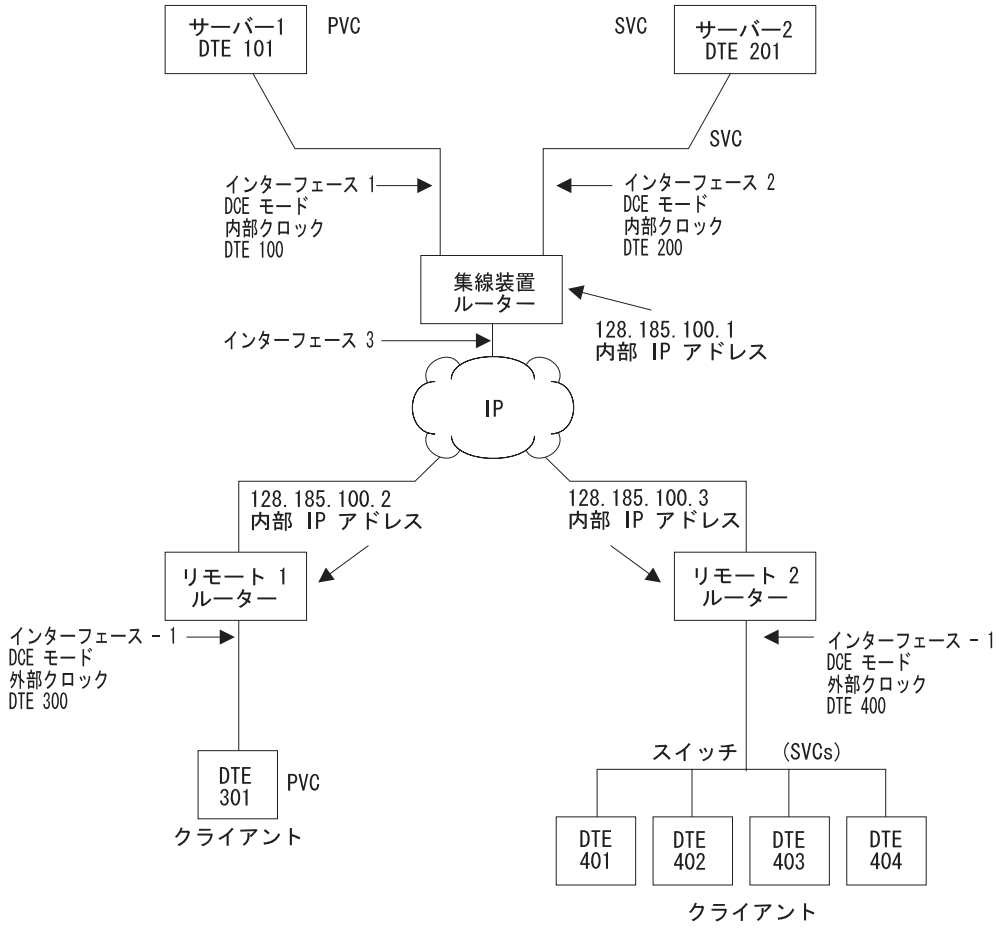


図 20. サンプル XTP 構成

この構成は、3 つのルーター (集線装置ルーター、リモート 1 ルーター、およびリモート 2 ルーター）を示しています。このネットワーク上で XTP を運用できるようにするためには、それぞれのルーターに対して以下のステップを実行します。

- データ・リンクを設定する
- IP インターフェースを構成する
- X.25 を構成する
- ナショナル・パーソナリティー値を設定する
- IP アドレスを定義する
- 内部 IP アドレスを設定する
- XTP を構成する

注: 新規の構成は、ルーターをリスタートするまでは有効になりません。

データ・リンクの設定

データ・リンクは、ネットワーク上でデータ・パケットを送信するのに使用するプロトコルを定義します。構成するルーターと各シリアル・インターフェースの間のデータ・リンクを定義します。 図20 の例は、3 つのシリアル・インターフェース (X.25 用に 2 つと、PPP 用に 1 つ）を持つ集線装置ルーターを構成します。

XTP の使用

シリアル・インターフェースのデータ・リンク・プロトコルを設定します。

```
Config>set data-link X25 1
Config>set data-link x25 2
Config>set data-link ppp 3
```

IP インターフェースの構成

387ページの図20 では、IP インターフェースは PPP です。この PPP インターフェースを構成するには Config> プロンプトで **network 3** と入力します。

```
Config>network 3
PPP interface configuration
```

注: この手順では PPP の構成については詳しく説明しません。詳細については、*Nways マルチプロトコル・ルーティング・サービス ソフトウェア使用者の手引きバージョン 3.1* を参照してください。

X.25 の構成

XTP を構成する前に、各インターフェースの X.25 パラメーターを構成します。次の例は、X.25 の基本パラメーターを構成しており、387ページの図20 のトポロジーに基づいています。

構成する必要があるパラメーターは、ネットワーク・トポロジーによって異なります。すべての X.25 パラメーターの詳細については、*Nways マルチプロトコル・ルーティング・サービス ソフトウェア使用者の手引きバージョン 3.1* を参照してください。

インターフェース 1

387ページの図20 に定義されている集線装置ルーター上の *インターフェース 1* は、以下の手順で構成します。

1. Config> プロンプトで **network** と入力し、続いて X.25 インターフェースの番号を入力する。この例では、インターフェース 1 になります。

   ```
   Config>network 1
   X.25 User Configuration
   X.25 Config>
   ```

2. XTP プロトコルを X.25 インターフェースに追加し、汎用のインターフェース値を定義する。 X.25 Config> プロンプトで **add protocol xtp** と入力します。このコマンドは *1 回だけ* 入力します。

   ```
   X.25 Config>add protocol xtp
   Window Size [2]?
   Default Packet Size [128]?
   Maximum Packet Size [256]?
   ```

3. **set address** X.25 node address と入力して、ネットワーク・アドレスを指定する。 387ページの図20 では、ノード・アドレス (DTE アドレス) は 100 です。

   ```
   X.25 Config>set address 100
   ```

4. **set clocking** と入力し、その後に、ルーター・タイプに応じて **internal** または **external** と入力する。

   ```
   X.25 Config>set clocking internal
   ```

5. **set speed** と入力し、続いてアクセス速度 (ライン速度) を入力する。

```
X.25 Config>set speed
Access rate in bps [9600]?19200
```

6. **set equipment-type** と入力し、フレームおよびパケット・レベルが DCE または DTE のいずれとして動作するのかを指定する。

```
X.25 Config>set equipment-type dce
```

7. **set pvc** と入力し、使用する最低および最高の PVC を定義する。

```
X.25 Config>set pvc low 1
X.25 Config>set pvc high 1
```

8. **add pvc** と入力し、個々の PVC を定義する。

```
X.25 Config>add pvc
Protocol [IP]?xtp
Packet Channel [1]?
Destination X.25 Address [ ]?101
Window Size [2]?
Packet Size [128]
```

9. (オプション) **national enable truncate-called-addresses** と入力する。被呼アドレス・サイズを切り捨てたい場合は、**national set truncate-called-addr-size** と入力し、続けて被呼 DTE アドレスの切り捨て後の桁数を入力します。
10. (オプション) 必要に応じて、CUG サポート、CUG 挿入、および CUG 削除を使用可能にする。

インターフェース 2

インターフェース 2 は、以下の手順で構成します。

1. Config> プロンプトで **network** と入力し、続いて X.25 インターフェースの番号を入力する。 387ページの図20 では、これは 2 になります。

```
Config>network 2
X.25 User Configuration
X.25 Config>
```

2. 388ページの『インターフェース 1』 で定義したのと同じ手順を使用して、インターフェース 2 に対して以下のパラメーターを設定する。
   - アドレス = 200
   - クロック = 内部
   - 速度 = 19200
   - 装置 = dce
3. **set svc** と入力し、使用する最低および最高の SVC を定義する。

   SVC には、両方向、着信、および発信の 3 つのタイプがあります。デフォルト値は 『svc low-two-way = 1』 および 『svc high-two-way = 64』 です。その他の SVC タイプはすべて、デフォルト値は 0 になります。 SVC および PVC についての詳細は、*Nways マルチプロトコル・ルーティング・サービス ソフトウェア使用者の手引きバージョン 3.1* を参照してください。

```
X.25 Config>set svc ?
X.25 Config>set svc low-inbound 0
X.25 Config>set svc high-inbound 0
X.25 Config>set svc low outbound 0
X.25 Config>set svc high outbound 0
X.25 Config>set svc low-two-way 2
X.25 Config>set svc high-two-way 2
```

4. X.25 Config> プロンプトを終了する。

```
X25 Config>exit
Config>
```

ナショナル・パーソナリティーの設定

各 X.25 公衆網には、それぞれ独自の標準構成があります。ナショナル・パーソナリティーというのは、公衆データ通信網の特性を定義する 28 の変数のグループです。これらの変数は、リンクを介して転送されるパケットの制御情報をルーターに提供し、XTP ルーターとそのローカル DTE 間で使用される X.25 ファシリティーに影響を及ぼします。

着呼要求に入っているファシリティーは、ローカル・ルーターがそのファシリティーをサポートするように構成されているかどうかに関係なく、すべて同位ルーターに渡されます。たとえば、パケット・サイズ・ネゴシエーションが着呼で要求されており、フロー制御ネゴシエーションがルーターに構成されていないといった場合です。

ルーターは、交渉されたパケット・サイズおよびウィンドウ・サイズが、必ず X.25 インターフェースの定義時に指定された範囲内になるようにします。たとえば、packet-ext-seq-mode が X.25 インターフェースに定義されていない場合、7 より大きいパケット・ウィンドウは、交渉によって 7 まで下げられます。

構成値を見たい場合は `X.25 Config>` プロンプトで **list detailed** と入力します。ナショナル・パーソナリティーのデフォルト値を設定するには、`X.25 Config>` プロンプトで **set national-personality** と入力します。詳細については、 *Nways マルチプロトコル・ルーティング・サービス ソフトウェア使用者の手引きバージョン 3.1* を参照してください。

IP アドレスの定義

集線装置ルーター (387ページの図20 に表示）を XTP 用に構成する前に、このルーターの IP アドレスを定義します。 `Config>` プロンプトで **protocol ip** と入力し、`IP config>` プロンプトで **add address** と入力します。

```
Config>protocol ip
IP config>add address
Which net is this address for [0]?3
New address [0.0.0.0]?128.185.100.7
Address mask [255.255.0.0]?255.255.255.0
```

内部 IP アドレスの設定

ルーターはその同位ルーターを、同位ルーターの内部 IP アドレスによって識別します。

同位ルーターの内部 IP アドレスを設定するには、`IP Config>` プロンプトで **set internal IP address** と入力します。

```
IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.1
```

XTP の構成

X.25 を構成し、IP アドレスを定義したら、ルーターの XTP を構成する準備が整ったことになります。

XTP を構成する際に、詳しい構成情報が必要になった場合は、395ページの『XTP 構成コマンド』を参照してください。

注: ユーザーのネットワークを XTP 用に構成する場合、同位ルーターは常にユーザーが TCP/IP を介して通信する相手のルーターであることを念頭においてください。すなわち、同位ルーターは観点によって異なります。 387ページの図20 でリモート 1 ルーターおよびリモート 2 ルーターとして定義されたルーターを構成する場合、これらにとっての同位ルーターは、集線装置ルーターになります。

ルーターの XTP を構成するには、以下のステップを実行します。

1. XTP config> プロンプトにアクセスするために、Config> で **protocol xtp** と入力する。
2. インターフェース 1 を XTP 構成に追加する。 XTP Config> プロンプトで **add local-dte** と入力します。

```
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?101
Pref CUG []? 18
CUG (2) []? 2
CUG (3) []?
Pref BI-CUG [0]?
DTE address [ ]?
```

   ヌル DTE アドレスを入力すると、コマンドの入力を終了します。

3. インターフェース 2 を XTP 構成に追加する。 XTP Config> プロンプトで **add local-dte** と入力します。

```
XTP config>add local-dte
Interface number [0]?2
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?201
DTE address [ ]?
```

   ヌル DTE アドレスを入力すると、コマンドの入力を終了します。

4. (オプション) XTP プロトコル特定 CUG を追加する。

```
add cug
        Pref CUG  []? 11
        CUG (2)  []? 12
        CUG (3)  []? 13
        CUG (4)  []? 14
        CUG (5)  []? 15
add bi-cug
        Pref BI-CUG  []? 21
        BI-CUG (2)  []? 22
        BI-CUG (3)  []?
```

5. リモート 1 ルーターを同位ルーターとして追加する。 **add peer-router** と入力し、このルーターの IP アドレスを入力します。

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?128.185.100.2
Connection setup timeout [230]?
```

6. リモート 1 ルーターのリモート DTE を入力する。 **add remote-dte** と入力し、この DTE の IP アドレスおよび DTE アドレスを入力します。

```
XTP config>add remote-dte
DTE address [ ]?301
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

   注: リモート DTE が*必須* なのは、以下のいずれかに該当する場合だけです。

- 集線装置ルーターが、そのローカル DTE からの着呼のために、リモート DTE への XTP 接続を開始する場合
- DTE が XTP PVC 定義に含まれている場合

7. リモート 2 ルーターを (同位ルーターとして) 追加する。 **add peer-router** と入力し、このルーターの IP アドレスを入力します。

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?128.185.100.3
Connection setup timeout [230]?
```

8. リモート 2 ルーターのリモート DTE を追加する。 add remote-dte と入力し、この DTE の IP アドレスと DTE アドレスを入力します。

```
XTP config>add remote-dte
DTE address [ ]?401
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?

XTP config>add remote-dte
DTE address [ ]?402
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?

XTP config>add remote-dte
DTE address [ ]?403
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?

XTP config>add remote-dte
DTE address [ ]?404
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

9. XTP PVC を追加して、サーバー 1 へのローカル PVC とリモート DTE 301 とを論理的に関連付ける。

```
XTP config>add pvc
Local PVC number [1]? 1
Local X.25 DTE address [ ]? 101
Remote PVC number [1]? 1
Remote X.25 DTE address [ ]?301
```

DTE アドレスを入力するときには、次のいずれかを指定できます。

'?' を任意の数字の代わりに指定します。 '?' は、この桁位置は任意の 1 つの数字であることを意味します。

'*' をアドレスの最後の桁として指定し、ゼロ桁またはそれ以上の桁数の任意の組み合わせを表します。

リモート・ルーターのサンプル構成

以下に示すのは、リモート 1 ルーターおよびリモート 2 ルーターのサンプル構成です (387ページの図20 を参照)。このプロセスは、386ページの『構成手順』の節で定義されているものと同じです。

リモート 1 ルーター

```
*talk 6

Config>set data-link x25 1
Config>set data-link ppp 2
Config>network 1

X.25 Config>set address 300
X.25 Config>set clocking internal
X.25 Config>set speed 19200
X.25 Config>set equipment-type dce
X.25 Config>set pvc low 1
```

```
X.25 Config>set pvc high 1
X.25 Config>add pvc
Protocol [IP]?xtp
Packet Channel [1]?1
Destination X.25 Address [ ]?301

Window Size [2]?
Packet Size [128]?
X.25 Config>exit
Config>

Config>protocol ip
IP config>add address
Which net is this address for [0]?2
New address [0.0.0.0]?128.185.100.8
Address mask [255.255.0.0]?255.255.255.0

IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.2
IP Config>exit
Config>

Config>protocol xtp
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?301
DTE address [ ]?

XTP config>add peer-router
Router's IP address?128.185.100.1

XTP config>add remote-dte
DTE address [ ]?101
Peer router's internal IP Address ]0.0.0.0]?128.185.100.1
Peer router's internal IP Address [0.0.0.0]?

XTP config>add pvc
Local PVC number [1]? 1
Local X.25 DTE address [ ]? 101
Remote PVC number [1]? 1
Remote X.25 DTE address [ ]?301
```

リモート 2 ルーター

```
*talk 6

Config>set data-link x25 1
Config>set data-link ppp 2
Config>network 1

X.25 Config>set address 400
X.25 Config>set clocking external
X.25 Config>set speed 19200
X.25 Config>set equipment-type dte
X.25 Config>set svc low-inbound 0
X.25 Config>set svc high-inbound 0
X.25 Config>set svc low-outbound 0
X.25 Config>set svc high-outbound 0
X.25 Config>set svc low-two-way 1
X.25 Config>set svc high-two-way 64
X.25 Config>add protocol
Protocol [IP]?xtp
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
X.25 Config>exit

Config>protocol ip
IP config>add address
Which net is this address for [0]?2
New address [0.0.0.0]?128.185.100.9
Address mask [255.255.0.0]?255.255.255.0

IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.3
IP Config>exit
Config>
```

```
Config>protocol xtp
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?401
Pref CUG  []? 23
CUG (2)  []? 24
CUG (3)  []? 25
CUG (4)  []? 26
CUG (5)  []? 27

DTE address [ ]?402
Pref CUG  []?
DTE address [ ]?403
Pref CUG  []?
DTE address [ ]?404
Pref CUG  []?
DTE address [ ]?


XTP Config>add peer-router
Router's IP address?128.185.100.1

XTP config>add remote-dte
DTE address [ ]?201
Peer router's internal IP Address [0.0.0.0]?128.185.100.1
Peer router's internal IP Address [0.0.0.0]?
XTP config>exit

Config>
```

第30章 XTP の構成および監視

この章では、XTP 構成コマンドおよび監視コマンドについて説明します。本章には、以下の節が含まれています。

- 『XTP 構成コマンド』
- 402ページの『XTP 監視コマンド』

XTP 構成コマンド

この節では、XTP 構成コマンドについて説明します。

XTP 構成環境にアクセスするには、`Config>` プロンプトで **protocol xtp** コマンドを入力します。

```
Config> p xtp
XTP config>
```

XTP 構成コマンドは `XTP config>` プロンプトで入力します。

表 52. XTP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Add	インターフェース、同位ルーター、閉域ユーザー・グループ、リモート DTE、または PVC 定義を追加します。
Change	同位ルーター、リモート DTE または PVC 定義を変更します。
Delete	ローカル DTE、同位ルーター、閉域ユーザー・グループ、リモート DTE、または PVC 定義を削除します。
Enable-XTP	XTP 転送機能を起動します。
Disable-XTP	XTP 転送機能を停止します。
Set	XTP キープアライブ・タイマーの値を設定します。
List	インターフェース、同位ルーター、リモート DTE および PVC 定義をリストします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

ローカル X.25 ノード、同位ルーター、リモート X.25 ノード (対応するルーターと共に)、またはローカル X.25 ノードからリモート X.25 ノードへの PVC を追加します。

XTP 転送機能には、ワイルドカード・アドレス指定が組み込まれています。ローカルまたはリモート DTE アドレスを入力するときには、ワイルドカード文字 (? または *) を含めることができます。ワイルドカードの使用についての詳細は、384ページの『DTE アドレス・ワイルドカード』を参照してください。

構文:

add bi-cug

cug

local-dte

peer-router

remote-dte

pvc

cug XTP プロトコルの閉域ユーザー・グループ番号を指定します。入力を求められる最初の CUG は、優先 cug です。

有効値: 0 to 9999

デフォルト値: None

例:

```
add cug
Pref CUG []? 114
CUG (2) []? 314
CUG (3) []? 478
CUG (4) []?
```

bi-cug XTP プロトコルの相互形閉域ユーザー・グループ番号を指定します。入力を求められる最初の bi-cug は、優先 bi-cug です。

有効値: 0 to 9999

デフォルト値: None

例:

```
add bi-cug
Pref BI-CUG []? 50
BI-CUG (2) []? 51
BI-CUG (3) []? 52
BI-CUG (4) []? 53
BI-CUG (5) []? 54
```

local-dte

指定されたインターフェース上のルーターと通信する X.25 DTE アドレス、または X.25 ノードを追加します。

複数のローカル・ノードを構成することも可能です。ただし、発呼 DTE アドレスを選択せずに着呼を認めるオプションを選択した場合は、ローカル・ノードは 1 つしか構成できません。

例:

```
add local-dte

Interface number [0]?4
Allow inbound calls without calling DTE address? (Y or N) [N]? y
DTE address [ ]?101
Pref CUG  []? 23
CUG (2)  []? 24
CUG (3)  []? 25
CUG (4)  []? 26
CUG (5)  []? 27
Pref BI-CUG []? 6
BI-CUG (2) []? 7
BI-CUG (3) []? 8
BI-CUG (4) []? 9
BI-CUG (5) []? 10
DTE address [ ]?
```

peer-router

同位ルーターを追加します。リモート X.25 ノードが接続するルーターの内部

IP アドレスを入力します。これらの IP アドレスを使用して TCP 接続をオープンし、接続要求と X.25 データが入っている X.25 パケットを伝達することができます。

同位ルーターに構成されている内部 IP アドレスが、このルーターの内部 IP アドレスである場合、ソフトウェアはローカル XTP 接続を確立します。

例:

```
add peer-router

Router's internal IP Address [0.0.0.0]?128.185.100.2
Connection setup timeout [230]?
```

remote-dte

リモート X.25 ノードと、対応するルーターを追加します。リモート・ノードとローカル X.25 ノードを接続し、データを交換できるようにします。構成する各リモート X.25 ノードごとに IP アドレスを構成する必要があります。このリモート・ノードに送信された要求またはデータは、すべてルーターに送られます。ルーターはそのローカル X.25 インターフェースの 1 つを使用して、データを X.25 ノードに転送します。

リモート DTE を定義するのは、このルーターがローカル DTE からの着呼のためにリモートへの XTP 接続を開始する必要がある場合、またはリモート DTE が XTP PVC 定義に含まれている場合です。

ローカル XTP を使用するためには、同位ルーター・アドレスがローカル・ルーターの内部アドレスであること、および DTE アドレスが以前に **add local** コマンドを使用して定義されていることが必要です。

例:

```
add remote-dte

DTE address [ ]?301
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

pvc ローカル X.25 ノードからリモート X.25 ノードへの PVC を追加します。

PVC 構成を起動するためには、次の 3 つが存在している必要があります。

- ルーターからローカル X.25 ノードへの X.25 PVC
- 同位ルーターからリモート X.25 ノードへの X.25 PVC
- リモート・ノードが常駐している同位ルーターへの TCP 接続

例:

```
add pvc

Local PVC Number [1]?1
Local X.25 DTE address [ ]?100
Remote PVC Number [1]?1
Remote X.25 DTE address [ ]?301
```

注:

1. ルーター構成に PVC を追加する場合は、X.25 にも PVC を構成する必要があります。 X.25 インターフェースの構成につての詳細は、*Nways マルチプロトコル・ルーティング・サービス ソフトウェア使用者の手引きバージョン 3.1* を参照してください。
2. ローカル XTP の場合、両方向に PVC を定義する必要があります。ルーターはローカル機能とリモート機能の両方を実行するので、この定義が

必要です。たとえば、ローカル XTP を使用している場合、ローカル PVC 8 とリモート PVC 10 を定義するには、次のように指定します。

```
add pvc

Local PVC Number [1]?8
Local X.25 DTE address [ ]?108
Remote PVC Number [1]?10
Remote X.25 DTE address [ ]?310
add pvc

Local PVC Number [1]?10
Local X.25 DTE address [ ]?310
Remote PVC Number [1]?8
Remote X.25 DTE address [ ]?108
```

注: ルーター構成に PVC を追加する場合は、X.25 にも PVC を構成する必要があります。 X.25 インターフェースの構成につての詳細は、*Nways マルチプロトコル・ルーティング・サービス ソフトウェア使用者の手引き バージョン 3.1* を参照してください。

Change

XTP 構成から同位ルーター、リモート DTE、または PVC を変更します。

構文:

change peer-router
remote-dte
pvc

peer-router

XTP 構成から特定の同位ルーターを変更します。

例:

```
change peer-router

Router IP Address [0.0.0.0]?128.185.100.2
```

remote-dte

XTP 構成から特定のリモート DTE を変更します。

例:

```
change remote-dte

DTE address [ ]?401
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

pvc XTP 構成から PVC 定義を変更します。

例:

```
change pvc

Local PVC number [1]?1
Local DTE address [ ]?301
```

Delete

XTP 構成からローカル DTE、同位ルーター、リモート DTE、または PVC を削除します。

構文:

delete bi-cug
cug
local-dte
peer-router
remote-dte
pvc

bi-cug このインターフェースによって使用される相互形閉域ユーザー・グループ番号を削除します。

有効値:

Y 現行の CUG を削除します。

N 現行の CUG を削除しません。

ALL 残りの CUG をすべて削除します。

Q 残りの CUG の削除を中止します。

例:

```
delete bi-cug
Delete Pref BI-CUG [Y]?
Delete BI-CUG (2) [Y]? N
Delete BI-CUG (3) [Y]? q
```

cug このインターフェースによって使用される閉域ユーザー・グループ番号を削除します。このコマンドの機能は **delete bi-cug** コマンドと同様です。

例:

```
del cug

Delete Pref CUG [Y]?
Delete CUG (2) [Y]?
Delete CUG (3) [Y]? q
```

local-dte

XTP 構成から特定の同位インターフェースを削除します。

例:

```
delete local-dte

Interface number [0]?1
DTE address [ ]?101
Record deleted
```

peer-router

XTP 構成から特定の同位ルーターを削除します。

例:

```
delete peer-router

Router IP Address [0.0.0.0]?128.185.100.2
Record deleted
```

remote-dte

XTP 構成から特定のリモート DTE を削除します。

例: delete remote-dte

DTE address [ ]?**401**

pvc XTP 構成から PVC 定義を削除します。

例:

```
delete pvc

Local PVC number [1]?1
Local DTE address [ ]?301
Record deleted
```

Enable

XTP 転送機能を起動します。

構文: enable-xtp

例: enable-xtp

Disable

XTP 転送機能を停止します。

構文: disable-xtp

例: disable-xtp

Set

XTP キープアライブ・タイマーを設定します。

構文: keep-alive-timer

例:

```
set keep-alive-timer

Keepalive timer in seconds [10]?60
```

List

インターフェース、同位ルーター、リモート DTE、または PVC をリストします。

構文:

list

all

cugs

keep-alive-timer

local-dtes

peer-routers

remote-dtes

pvcs

xtp-status

all XTP 用に構成されたすべてのインターフェース、同位ルーター、リモート DTE、および PVC を表示します。

例:

```
 list all

STATUS: XTP-DISABLED

Local DTEs:

Interface      DTE Address
    1          44444                    Calling DTE address is optional
             Pref CUG     : 7777  Others : 9999 0
             Pref BI-CUG  : 0     Others :

    4          33333                    Calling DTE address is optional
             Pref CUG     : 1     Others : 2 3 4 5
             Pref BI-CUG  : 6     Others : 7 8 9 10


   Peer Routers    Connection Timeout

Remote DTEs:
      DTE Address    Peer Router(s)

PVCs:
Local PVC         Local DTE      Remote PVC        Remote DTE
 Number             Address        Number            Address

Pref CUG     : 114   Others : 314 478
Pref BI-CUG  : 1     Others : 1 1 1 1111


KEEP-ALIVE-TIMER: 10 seconds
```

cugs XTP プロトコル用に定義された CUG および BI-CUG 番号をリストします。

keep-alive-timer

XTP 用に構成されたすべてのキープアライブ・タイムを表示します。

local-dtes

XTP 用に構成されたすべてのローカル DTE を表示します。

例:

```
list local-dtes

Local DTEs:
Interface        DTE Addr
   1             101 Calling DTE address is required
   2             201 Calling DTE address is required
```

peer-routers

XTP 用に構成されたすべての同位ルーターを表示します。

例:

```
list peer-routers

Peer Routers:
128.185.100.2
128.185.100.3
```

pvcs XTP 用に構成されたすべての PVC を表示します。

例

```
list pvcs

PVCs:

Local PVC      Local DTE      Remote PVC      Remote DTE
 Number          Address        Number          Address
  1                100              1              301
```

remote-dtes

XTP 用に構成されたすべてのリモート DTE を表示します。

例:

```
list remote-dtes

Remote DTEs:
DTE Address      Peer Router
    301         128.185.100.2
    401         128.185.100.3
    402         128.185.100.3
    403         128.185.100.3
    404         128.185.100.3
```

xtp-status

XTP の状態 (使用可能か使用不可か) を表示します。

例:

```
list xtp-status

STATUS:  XTP-ENABLED
```

XTP 監視コマンド

この節では、XTP 監視コマンドについて説明します。これらのコマンドでは、現在アクティブのインターフェース、同位ルーター、リモート DTE、PVC、および SVC を表示することができます。また、インターフェース、DTE、または同位ルーターを動的に追加または削除することもできます。

XTP> プロンプトを表示するには、監視 (+) プロンプトで **protocol xtp** と入力します。

```
+protocol xtp
X.25 Transport Console
XTP>
```

XTP 監視コマンドは、XTP> プロンプトで入力します。

表 53. XTP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	ローカル DTE、リモート DTE、または同位ルーターを動的に追加します。
Delete	ローカル DTE、リモート DTE、または同位ルーターの構成を動的に削除します。
List	個々の PVC または SVC の統計および一般情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Add

インターフェース、同位ルーター、またはリモート DTE を XTP 構成に追加します。

構文:

add local-dtes
peer-router
remote-dtes

local-dtes

ローカル・インターフェースを XTP 構成に追加します。

例:

```
add local-dtes

Interface number [0]?1
DTE address [ ]?101
```

peer-router

同位ルーターを XTP 構成に追加します。

例:

```
add peer-router

Router's IP Address [0.0.0.0]?128.185.100.2
```

remote-dtes

リモート DTE を XTP 構成に追加します。

例:

```
add remote-dtes

Peer router's IP Address [0.0.0.0]?128.185.100.2
DTE address [ ]?301
DTE address [ ]?
```

Delete

ローカル DTE、同位ルーター、またはリモート DTE をルーター構成から削除します。

構文:

delete local-dtes

peer-router

remote-dtes

local-dtes

ローカル・インターフェースを XTP 構成から削除します。

例:

```
delete local-dtes

Interface Number [0]?1
DTE address [ ]?101
DTE address [ ]?
```

peer-router

同位ルーターを XTP 構成から削除します。

例: delete peer-router

```
Router's IP Address [0.0.0.0]?123.185.100.2
```

remote-dtes

リモート DTE を XTP 構成から削除します。

例:

```
delete remote-dtes

DTE address [ ]?401
DTE address [ ]?
```

List

現在アクティブのインターフェース、同位ルーター、リモート DTE、PVC、および SVC を表示します。

構文:

list all

xtp-status

local-dtes

peer-routers

remote-dtes

pvcs

pvc-detailed

pvcs-all-detailed

svcs

svc-detailed

svc-all-detailed

all すべての list コマンド・オプションの出力を表示します。

例:

```
 list all


STATUS:  XTP-ENABLED
KEEP-ALIVE TIMER = 20 seconds


LIST OF LOCAL DTES
------------------
Interface     Local
  No           DTE
  1            101     Calling DTE address is required
  2            201     Calling DTE address is required


LIST OF PEER ROUTERS
--------------------
 Router             CNN      Number        Received           Sent
                   State    of  Ckts     Pkts    Bytes     Pkts    Bytes
128.185.100.3     Active      15          60      1533      12      142
128.185.100.2     Active      12          63      1620      10      130


LIST OF REMOTE DTES
-------------------
      Remote         Router
       DTE             IP
       404           128.185.100.3
       403           128.185.100.3
       402           128.185.100.3
       401           128.185.100.3
       301           128.185.100.2


LIST OF PVCS
------------
Index     Int    PVC    Local       Local   Remote      Remote
 No        No   State    LCN         DTE      LCN         DTE
  1         1   Active               100                 301


LIST OF SVCS   (list svcs)
------------
Index   Int   Logical    SVC        Local     Remote         Peer
  No     No   Channel   State       DTE         DTE        Router
```

```
  1       2       5      ACT     333333333333 4444444444444 3.3.3.3


SVC  1 IN DETAIL   (list svc-detailed)
----------------
Int    Log     SVC        Received            Sent             Dropped
 No    Chn    State      Pkts   Bytes      Pkts   Bytes      Pkts   Bytes

  2      5     ACT          2     116         2     106         0       0


LIST OF SVCS   (svcs-all-detailed)
------------
Int    Log     SVC        Received            Sent             Dropped
 No    Chn    State      Pkts   Bytes      Pkts   Bytes      Pkts   Bytes

  2      5     ACT          1       7         1       2         0       0
```

xtp-status

XTP が使用可能/使用不可のいずれか、およびキープアライブ・タイマーに指定された時間を表示します。

例:

```
list xtp-status

STATUS:  XTP-ENABLED
         KEEP-ALIVE-TIMER = 20 seconds
```

local-dtes

XTP 用に構成されたすべてのインターフェースを表示します。

例:

```
list local-dtes

LIST OF LOCAL DTES
------------------
Interface     Local
  No           DTE
  1            101     Calling DTE address is required
  2            201     Calling DTE address is required
```

peer-routers

XTP 用に構成されたすべての同位ルーターを表示します。

例:

```
list peer-routers

LIST OF PEER ROUTERS
--------------------
 Router             CNN      Number        Received            Sent
                   State    of  Ckts     Pkts    Bytes     Pkts    Bytes
128.185.100.3     Active      15          60      1533      12      142
128.185.100.2     Active      12          63      1620      10      130
```

remote-dtes

XTP 用に構成されたすべてのリモート・インターフェースを表示します。

例:

```
 list remote-dtes

LIST OF REMOTE DTES
-------------------
      Remote         Router
       DTE             IP
       404           128.185.100.3
       403           128.185.100.3
       402           128.185.100.3
       401           128.185.100.3
       301           128.185.100.2
```

pvcs

XTP 用に構成されたすべての PVC を表示します。

例:

```
list pvcs

LIST OF PVCS
------------
Index     Int    PVC   Local     Local    Remote      Remote
 No        No   State   LCN       DET      LCN         DTE
  1         1   Active            100                  301
```

pvc-detailed

特定の PVC 定義の詳細情報を表示します。インデックス番号をリストしたい場合は、xtp> プロンプトで **list all** と入力します。

例:

```
list pvc-detailed

PVC Index Number [1]?1

PVC  1 IN DETAIL
----------------
Int     PVC          Received            Sent             Dropped
 No    State      Pkts     Bytes    Pkts     Bytes    Pkts      Bytes
 1     ACTIVE      55       3220     35       2350     15        1870
```

pvcs-all-detailed

すべての PVC 定義の詳細情報を表示します。

例:

```
list pvcs-all-detailed

LIST OF PVCS
------------
INT Local     PVC          Received            Sent             Dropped
 No  LCN     State      Pkts     Bytes    Pkts     Bytes    Pkts     Bytes
 1           ACTIVE      55       3220     35       2350     15       1870
```

svcs

すべての SVC 定義を表示します。

例:

```
list svcs

LIST OF SVCS
------------
Index     Int LOG    SVC       Local      Remote  Peer
 No        No Chan  State       DTE         DTE   Router
  1         1       Active      200         401   3.3.3.3
  2         1       Active      200         402   3.3.3.3
  3         2       Active      200         403   3.3.3.3
  4         2       Active      200         404   3.3.3.3
```

svc-detailed

特定の SVC 定義の情報を表示します。

例:

```
list svc-detailed

SVC Index Number [1]?1
SVC  1 IN DETAIL
----------------
Int  LOG    SVC         Received            Sent             Dropped
 No  Chan  State      Pkts     Bytes    Pkts     Bytes    Pkts      Bytes
  1        ACTIVE      75       4220     55       3350     20        870
```

svcs-all-detailed

すべての SVC 定義の情報を表示します。

例:

```
list svcs-all-detailed

LIST OF SVCS
------------
Index     Int Log    SVC          Received           Sent            Dropped
No        No  Chn  State       Pkts    Bytes   Pkts     Bytes   Pkts    Bytes
1          1       ACTIVE     4220     55     550        20      870
```

```
2          1        ACTIVE     3220     40     2350        15      970
3          2        ACTIVE     4003     50     3892        20      870
4          2        ACTIVE     3967     58     4167        12      800
```

第31章 フレーム・リレー・インターフェースの使用

この章では、フレーム・リレー・インターフェースの使用法について説明します。本章には、以下の節が含まれています。

フレーム・リレーの概説

フレーム・リレー (FR) プロトコルとは、X.25 のパケット交換とポート共用を、高速で遅延の少ない時分割多重 (TDM) 回線交換と組み合わせて、相互接続パケットを転送するする方式です。 FR を使用すると、複数の LAN を、複数のポイント・ポイント・パーマネント・バーチャル・サーキット (PVC) をもつ単一の高速 (1.54 Mbps) WAN リンクに接続することができます。 FR は、以下の機能を提供します。

- *高いスループットと少ない遅延。* D チャネル (LAPD) データ・リンク・プロトコルであるリンク・アクセス・プロトコルの *中心機能* (誤り検出、アドレッシング、および同期) を利用することにより、FR ではすべてのネットワーク・レイヤー (レイヤー 3) の処理を不要にします。 FR は、中心機能のみを使用することにより、各フレームの処理の遅延を減らします。
- *輻輳 (ふくそう) 検出。* 逆方向明示的輻輳通知 (BECN) または順方向明示的輻輳通知 (FECN) を受信すると、ルーターは制御下でトラフィックを減速し、FR ネットワークが完全に遮断されるのを回避します。

  ルーターは、統合リンク・レイヤー・マネージメント (CLLM) 輻輳メッセージを受信した場合も、トークンリングの減速を開始することができます。 CLLM は、フレーム・リレー・ネットワークの動作に関する追加管理情報を、接続された DTE に提供する、フレーム・リレー標準のオプション部分です。
- *回線アクセスと制御。* ルーターは非構成回線 (オーファン回線) の利用可能性を動的に確認するので、これらの新規回線へのアクセスを制御することができます。
- *ネットワーク管理オプション。* ネットワークの要件に応じて、FR プロトコルは、ローカル・ネットワーク管理インターフェースを使用して動作することも、使用せずに動作することもできます。
- *多重化プロトコル。* 1 つの PVC を使用して複数のプロトコルを渡します。
- *データ圧縮。* FRF.9 標準をサポートします。詳細については、831ページの『第62章 データ圧縮サブシステムの使用』 を参照してください。

- *データ暗号化*。 専有の暗号化方式を使用します。詳細については、873ページの『第66章 暗号化の概説』 を参照してください。

FR は、誤り訂正または再送の機能は提供しません。 FR は、ホスト装置の機能に依存して、誤りのないエンド・エンド間のデータ転送を行います。

フレーム・リレー・ネットワーク

FR ネットワークは、FR サービスを提供する FR バックボーン (FR キャリアによって提供される FR スイッチから成る) から構成されます。ルーターは、FR 接続装置として機能します。ルーターは FR フレームをカプセル化し、それらをデータ・リンク接続識別子 (DLCI) に基づいてネットワーク上でルーティングします。 DLCI は、ルーターと FR 着側装置間の PVC を識別する媒体アクセス制御 (MAC) アドレスです。たとえば、図21 では、ルーター B からルーター D に送られるパケットは、ルーター D に到達するために DLCI は 19 になりますが、ルーター D からルーター B に送られるパケットの DLCI は 16 になります。

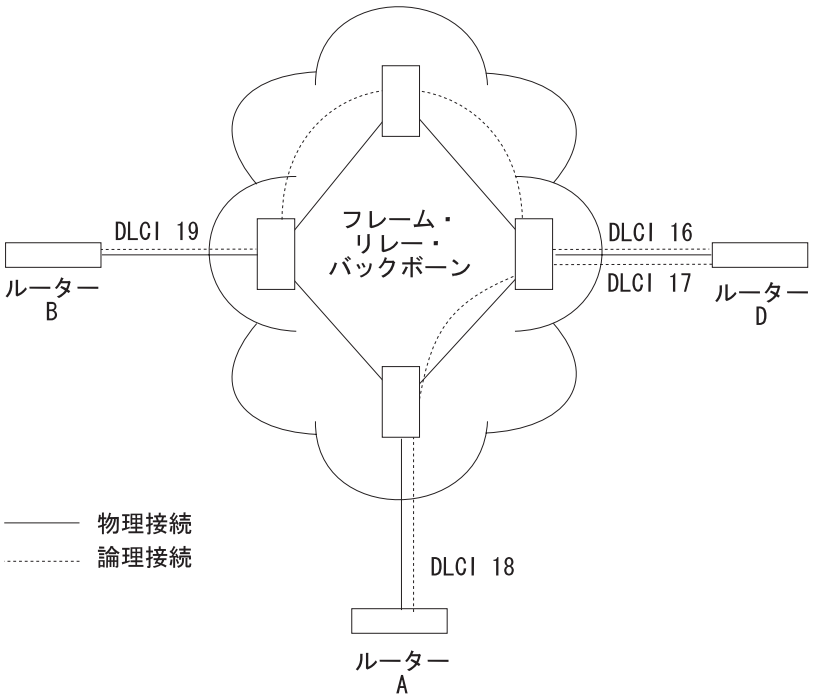


図 21. フレーム・リレー・ネットワーク内の DLCI

DLCI は、ローカルまたはグローバルの意味を持つことができます。ローカル DLCI は、ネットワークへの入り口点で有効であり、グローバル DLCI はネットワーク全体で有効です。ただし、ユーザーから見ると、ルーターがパケットをルーティングするのに使用する DLCI は、ユーザーがフレームのグローバルまたはローカル着信先に対応付ける DLCI ということになります。 DLCI は、FR 構成プロセスで構成するか、あるいは FR マネージメントを通して確認されます。

フレーム・リレー・ネットワークには、次のような特性があります。

- フレームを透過的に伝達します。ネットワークが変更できるのは、DLCI、輻輳ビット、およびフレーム・チェック・シーケンスだけです。ハイレベル・データ・リンク制御 (HDLC) フラグおよびゼロ・ビット挿入により、フレームの区切り、配列、および透過性を実現します。
- 伝送誤り、フォーマット誤り、および運用誤り (不明 DLCI を持つフレーム) を検出します。
- 個々の PVC 上のフレーム転送順序を保存します。
- フレームの確認または再送は行いません。

フレーム・リレー・インターフェースの初期化

ローカル管理インターフェース (LMI) が使用可能の場合、ルーターと FR スイッチ間の LMI フレームの交換が正常に行われると、FR インターフェースはアクティブになります。しかし、その DLCI の相手側ルーターへの PVC 状態がアクティブであることが LMI 状態メッセージで示されるまでは、別のルーターとの間でのデータの受信または送信を行うことはできません。 また、FR インターフェースの状態が PVC の状態と結合されているために、LMI 交換が正常に行われてもインターフェースが起動しないといった事態が生じることもあります (詳細については、413ページの『フレーム・リレー・インターフェースの状態に影響を与える PVC 状態の構成』 を参照してください)。

PVC 状態は、すべての PVC について、アクティブまたは非アクティブとして示されます。アクティブ PVC は、エンド・システムへの完全なコネクションが確立されています。非アクティブ PVC は、エンド・システムまたは FR スイッチのいずれかがオフラインであるために、エンド・システムへの完全なコネクションが確立されていません。

たとえば、412ページの図22 では、ルーター B はルーター D への PVC が構成されています。ルーター B は、FR スイッチ B を介して FR マネージメントと正常に相互動作しています。別の FR スイッチがダウンしているか、エンド・システムがダウンしているために、エンド・エンド PVC コネクションは確立されていません。ルーター B は、その PVC について非アクティブ状態を受け取ります。

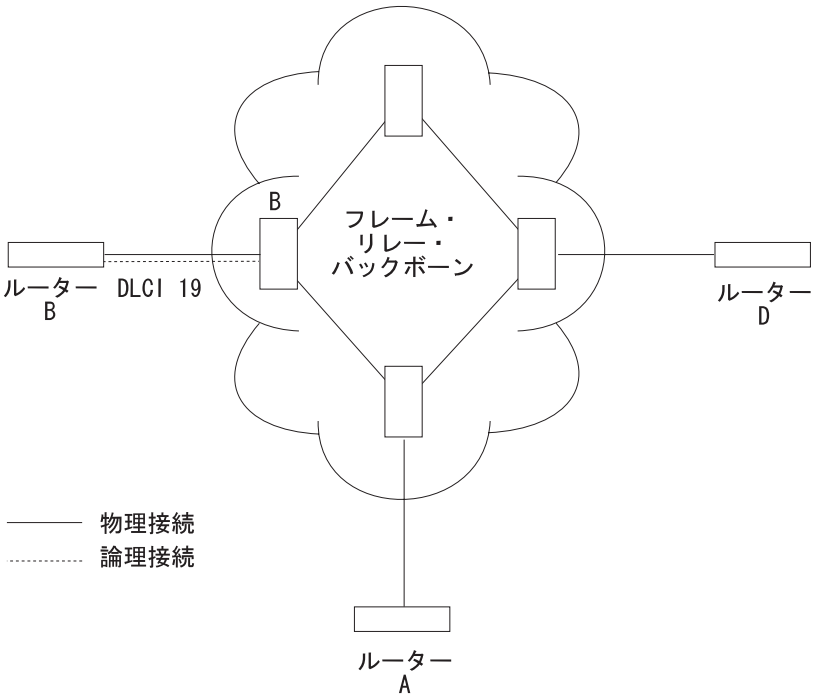


図 22. フレーム・リレー・ネットワーク内の DLCI

ローカル管理インターフェース (LMI) が使用不可にされ、FR インターフェースがシリアル・ライン上で稼働し、DTE ケーブルが使用されている場合、FR 制御機能が DTR および RTS モデム制御信号を代入します。 (X.21 の場合は、Control 信号が代入されます。) DSR、CTS、および DCD モデム制御信号がオンになると、FR インターフェースはアップになります。 (X.21 が使用されている場合、Indication モデム制御信号がオンになると、FR インターフェースはアップになります。) DSR、CTS、または DCD がオフであるか、あるいは X.21 が使用されている場合は、Indication 信号がオフのときは、FR インターフェースはダウンしているか、テスト状態にあります。したがって、FR スイッチまたは他の FR DTE (FR DTE と DTE の接続性のために構成されている場合) が失われた場合、使用されているモデム、モデム・エリミネーター、または DSU が、これらの信号の 1 つまたは複数を廃棄していないか確認する必要があります。

オーファン回線

オーファン回線 とは、ルーターには構成されていないが、ネットワーク管理エンティティーのアクションを通して間接的に確認された PVC のことです。たとえば、413ページの図23 では、ルーター B には、ルーター D への構成された PVC がありますが、ルーター A への構成された PVC はないものと想定しています。ルーター A がルーター B への PVC を構成すると、ルーター B は、LMI メッセージからルーター A への PVC を確認し、それをオーファンとして分類します。

オーファン回線は、**enable orphan-circuit** および **disable orphan-circuit** コマンドを使用してそれらを使用可能または使用不可にすることを除いて、構成された回線と同じに扱われます。

オーファン回線を使用不可にすると、構成されていない回線からネットワークに無許可で入るのを防止できるので、ネットワークのセキュリティー手段を追加できます。オーファン回線を使用可能にすると、ルーターは、構成されていなかった回線を介してパケットを転送することができます。通常ならば廃棄されていたパケットが転送できるようになります。

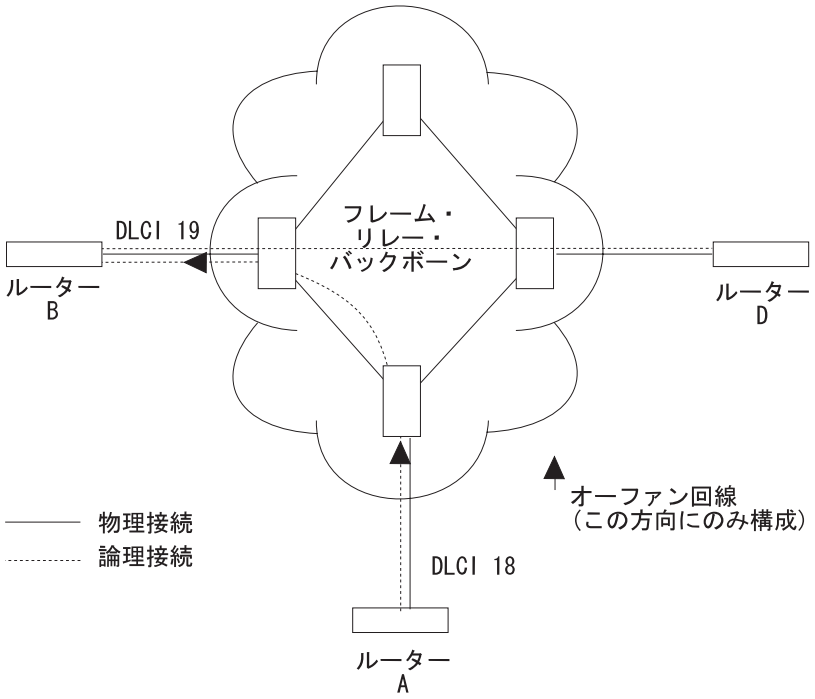


図 23. オーファン回線

フレーム・リレー・インターフェースの状態に影響を与える PVC 状態の構成

以下により、フレーム・リレー・インターフェースの動作を制御することができます。

1. 『No-PVC』 機能を使用可能にする
2. 『必須 PVC』 を構成する
3. 『必須 PVC グループ』 を構成する

フレーム・リレー 『No-PVC』 機能を使用可能にした場合、インターフェース上にアクティブの PVC が存在しないと、フレーム・リレー・インターフェースは非アクティブになります。少なくとも 1 つの PVC がアクティブの場合、ルーターと FR スイッチ間で LMI 交換が正常に行われると、フレーム・リレー・インターフェースはアクティブになります。

PVC を 『必須 PVC』 として構成することができます。ある PVC が必須であるが、グループに含まれていない場合、その PVC が非アクティブになると、フレーム・リレー・インターフェースは非アクティブになります。その PVC がアクティブになった場合、ルーターとフレーム・リレー・スイッチ間での LMI フレーム交換が正常に行われると、インターフェースはアクティブになります。

フレーム・リレーの使用

複数の PVC が必須であり、PVC グループに含まれていない場合、すべての必須 PVC がアクティブになるまで、インターフェースはアクティブになりません。

必須 PVC が PVC グループに属している場合、PVC グループ内のすべての PVC が非アクティブになると、フレーム・リレー・インターフェースは非アクティブになります。グループ内の少なくとも 1 つの PVC がアクティブになった場合、ルーターと FR スイッチ間での LMI フレーム交換が正常に行われると、インターフェースはアクティブになります。複数の PVC グループが存在する場合、各グループ内の 少なくとも 1 つの PVC がアクティブになるまでは、インターフェースはアクティブになりません。

『必須 PVC グループ』 は、名前によって対応付けられている回線の集りです。ここにおける 『名前』 は、必須 PVC グループの名前を指します。

これらの機能を WAN 再ルートで使用すると、1 次 FR リンク上のすべての PVC、必須 PVC、または PVC グループが非アクティブになった場合に、代替リンクを起動させることができます。

フレーム・リレーのフレーム

FR フレームは、固定サイズのアドレス・フィールドと可変サイズのカプセル化されたユーザー・データから構成されます。 図24 は、フレーム・リレーのフレーム・フォーマットを示しています。

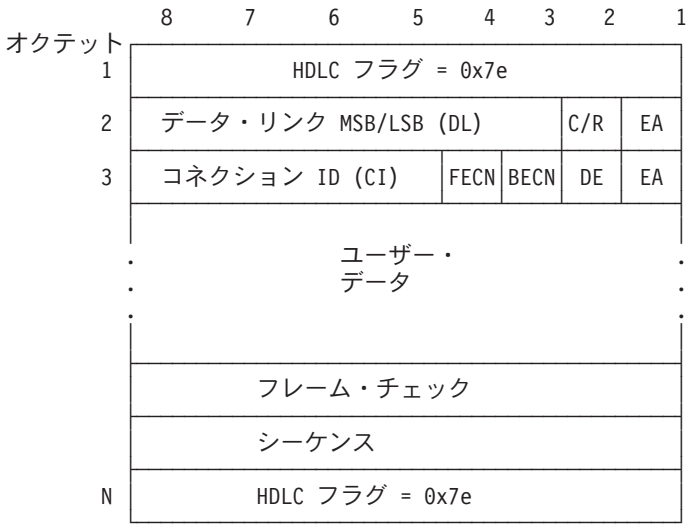


図 24. フレーム・リレーのフレーム・フォーマット

HDLC フラグ

これらのフラグは、最初と最後のオクテットにあり、フレームの開始と終了を示します。

データ・リンク接続識別子 (DLCI)

この 10 ビットのルーティング ID は、オクテット 2 のビット 3 ～ 8 およびオクテット 3 のビット 5 ～ 8 にあります。 DLCI は、回線の MAC アドレスです。DLCI により、ユーザーおよびネットワーク管理は、そのフレームが特定の PVC から来たことを識別することができます。また DLCI により、1 つの物理リンクを介する複数の PVC の多重化が可能になります。

コマンド/レスポンス (C/R)

このフィールドの使用は、フレーム・リレー標準には定義されていません。このフィールドはネットワークを経由して透過的に渡されます。

拡張アドレス

このバージョンの FR は、拡張アドレス方式をサポートしません。

順方向明示的輻輳通知 (FECN)

FR バックボーン・ネットワークはこのビットを 1 にセットすることにより、PVC 上のこのフレームが送信されている方向で輻輳 (ふくそう) が発生していることを、フレームを受信するユーザーに通知します。 **enable throttle-transmit-on-fecn** コマンドを使用すれば、FECN を受信した方向のデータ転送を減速するように装置を構成できます。また、**enable notify-fecn-source** コマンドを使用して、FECN の発信元に送信するデータ・フレームに BECN ビットをセットすることもできます。

APPN 高性能ルーティング (HPR) は、このビットがセットされているのを検出し、高速トランスポート・プロトコルの適応速度フロー/輻輳制御アルゴリズムにより、データ送信速度を調整できるようにします。このアルゴリズムは、トラフィックのバーストと輻輳を防止し、スループットを高レベルに維持します。

逆方向明示的輻輳通知 (BECN)

FR バックボーン・ネットワークはこのビットを 1 にセットすることにより、この PVC 上でこのルーターによって送信されたフレームが輻輳に遭遇したことをユーザーに通知します。次にルーターは、CIR または輻輳監視が使用可能にされている場合、ユーザー定義の CIR 以下の速度まで*減速* し始めます。 PVC の CIR は、FR サービス提供者によって提供され、**add permanent-virtual-circuit** コマンドを使用して構成されます。

廃棄可能性 (DE)

フレーム・リレー・ネットワークは、PVC 上の CIR を超過した転送データを廃棄することがあります。ルーターは、DE ビットをセットすることにより、一部のトラフィックを廃棄可能と見なすように指示することができます。該当する場合、フレーム・リレー・ネットワークは廃棄可能としてマーク付けされたフレームを廃棄します。これによって、廃棄可能のマークが付いていないフレームがネットワークを通過できるようになることがあります。廃棄可能なトラフィックを識別するには、次のようにします。

フレーム・リレーの使用

1. フレーム・リレー・インターフェースおよび廃棄可能にするトラフィックが通るすべての FR 回線上に BRS を構成する。
2. **assign** コマンドを使用して、BRS トラフィック・クラスにプロトコルまたはフィルターを割り当てる。このプロトコルまたはフィルター・トラフィックについて、DE ビットをオンにセットするかどうかを指定します。

ユーザー・データ

このフィールドには、転送されるプロトコル・パケットが入っています。このフィールドには最大 8188 オクテットを含めることが可能ですが、フレーム・チェック・シーケンス (FCS) が効率的に誤りを検出できるのは、最大 4096 オクテットまでのデータです。プロトコル・データの前に、RFC 1490 で定義されているフレーム・リレー・カプセル化ヘッダーが置かれています。

フレーム・チェック・シーケンス

このフィールドは、HDLC および LAPD フレームが使用する標準 16 ビット巡回冗長検査 (CRC) です。このフィールドは、フレームの開始フラグと FCS の間のビットに発生したビット誤りを検出します。

フレーム・リレー・ネットワークを介したフレーム転送

FR プロトコルは、カプセル化のためにパケットを受信すると、パケットのネットワーク・アドレスをアドレス解決プロトコル (ARP) キャッシュ内のエントリーと比較します。 ARP キャッシュにネットワーク・アドレスに一致する DLCI 番号が含まれている場合、FR プロトコルは、そのパケットをフレームにカプセル化し、指定されたローカル DLCI を介してフレームを転送します。 ARP キャッシュに一致するものが含まれていない場合、FR プロトコルは、インターフェース上のすべての構成済み PVC 上に ARP 要求を送信します。該当するエンドポイントが ARP レスポンスで応答した場合、FR プロトコルは、その ARP レスポンスを受信したローカル DLCI を ARP キャッシュに追加します。同じネットワーク・アドレスあての後続のデータ・パケットは、フレームにカプセル化され、そのローカル DLCI を介して転送されます。

プロトコル・アドレス

プロトコル・アドレスは、静的に FR ネットワーク PVC アドレスにマップすることも、逆 ARP または ARP を介して動的に見つけることもできます。 (ARP および逆 ARP についての詳細は、*プロトコルの構成と監視 解説書* を参照してください。) いずれの方法も、表54 に示すように、プロトコルに依存します。

注: 静的プロトコル・アドレスは、静的 ARP エントリーとも呼ばれます。静的 ARP エントリーは、**add protocol-address** コマンドを使用して構成に追加します。

表 54. プロトコル・アドレス・マッピング

プロトコル・タイプ	ARP および逆 ARP の使用	静的マッピング	プロトコル構成で構成された PVC
AP2	可	可	不可
IP	可	可	不可
IPX	可	可	不可
Banyan VINES	不可	不可	不可

表 54. プロトコル・アドレス・マッピング (続き)

プロトコル・タイプ	ARP および逆 ARP の使用	静的マッピング	プロトコル構成で構成された PVC
DNA IV	可	可	不可
OSI*	不可	不可	可

* プロトコル・アドレスを FR PVC にマップするためには、プロトコル・レベルで OSI を構成する必要があります。

マルチキャスト・エミュレーションとプロトコル・ブロードキャスト

マルチキャスト・エミュレーションは、ARP のようなマルチキャストを必要とするプロトコルが FR インターフェース上で正常に機能できるようにするオプション機能です。マルチキャスト・エミュレーションを使用すると、マルチキャスト・フレームが各アクティブ PVC 上に転送されます。 **enable** および **disable multicast** コマンドを使用して、この機能をオンまたはオフにすることができます。マルチキャストを使用するプロトコルは、AP2、ARP、Banyan VINES、DNA4、IP、および IPX です。

プロトコル・ブロードキャストは、FR インターフェース上で IP RIP プロトコルが正常に機能できるようにする、もう 1 つのオプション機能です。 **enable protocol-broadcast** および **disable protocol-broadcast** コマンドを使用して、この機能をオンまたはオフにすることができます。

フレーム・リレーを介する ARP/InARP をサポートするプロトコルの場合、プロトコル・アドレスが回線で確認されたか、回線に構成されている場合にのみ、フレーム・リレーはその回線を介してプロトコル・パケットをマルチキャストします。

フレーム・リレー・ネットワーク管理

FR ネットワークのバックボーンの提供者が FR ネットワーク管理機能を提供します。インターフェースで利用可能な PVC の状態情報および構成情報を FR エンド・ステーション (ルーター) に提供するのはネットワーク管理の責任です。

FR プロトコルは、ANSI T1.617 付録 D、ITU-T Q.933 付録 A (CCITT Q.933 付録 A とも呼ばれる)、および中間ローカル管理インターフェース (LMI) マネージメント・エンティティーをサポートします。 これらのエンティティーは、**enable** および **disable** LMI 構成コマンドを使用して、オンまたはオフにすることができます。特に、FR ネットワーク管理は以下の情報を提供します。

- 追加 PVC (オーファン) およびそれらがアクティブか非アクティブかの通知、または PVC の削除の通知
- 構成された PVC の利用可能性の通知。 PVC の利用可能性は、PVC エンドポイントがハートビート・ポーリング プロセスに正常に参加できるかどうかに間接的に関係します。これについては、 418ページの『リンク整合性検証報告書』 で詳しく説明します。
- キープアライブ シーケンス番号交換の使用による、エンド・ステーションとネットワーク間の物理リンクの整合性の検証

フレーム・リレーの使用

FR インターフェースはネットワーク管理をサポートしますが、インターフェースが FR バックボーンを介して動作するためには、マネージメントを FR バックボーン上で実行する必要はありません。たとえば、バックツーバック・テストのマネージメントを使用不可にすることができます。

管理状態報告書

要求に応じて、FR マネージメントは 2 種類の状態報告書、つまり、全状態報告書とリンク整合性検証報告書を提供します。全状態報告書は、インターフェースが知っているすべての PVC に関する情報を提供します。リンク整合性検証報告書は、特定のエンド・ステーションとネットワーク・スイッチの間のコネクションを検証します。すべての状態照会および応答は、ANSI T1.617 付録 D および ITU-T Q.933 付録 A の場合は DLCI 0 を介して、また中間 LMI マネージメントの場合は DLCI 1023 を介して送信されます。

全状態報告書

FR インターフェースが全状態報告書を必要とする場合、ルーターの FR プロトコルは、全状態報告書を要求する状態照会メッセージを FR ネットワーク・バックボーンに送信します。状態照会メッセージは、インターフェース上のすべての PVC の状態に対する要求です。この要求を受信すると、FR マネージメントは、リンク整合性検証要素と各 PVC の PVC 状態情報要素から成る全状態報告書で応答する必要があります。 (『リンク整合性検証報告書』 を参照してください。)

PVC 状態情報要素には、以下の情報が入っています。すなわち、特定 PVC のローカル DLCI 番号、PVC の状態 (アクティブまたは非アクティブ)、および PVC が新しいものか、あるいはマネージメントがすでに知っている既存の PVC であるかです。

注: FR インターフェースで提供される PVC の数は、ネットワークのフレーム・サイズ、および全状態報告書に入れることができる個々の PVC 情報要素の量によって制限されます。たとえば、フレーム・サイズが 1K のネットワークの PVC の最大数は 202 です。

リンク整合性検証報告書

リンク整合性検証報告書 (*ハートビート・ポーリング* とも呼ばれる) には、リンク整合性検証要素が入っています。この要素は、送信シーケンス番号と受信シーケンス番号の交換が行われる場所です。シーケンス番号を交換することによって、マネージメントとエンド・ステーションは、同期リンクの整合性を評価することができます。送信シーケンス番号は、メッセージ発信元の現在の送信シーケンス番号です。受信側はこの番号を見つけ、それを前回の送信シーケンス番号と比較して、この番号が正しく増分されているかどうかを検証します。受信シーケンス番号は、発信元がインターフェースを介して送信した前回の送信シーケンス番号です。送信シーケンス番号のコピーを受信シーケンス番号フィールドに入れるのは、受信側の責任です。この方法で、発信元は受信側がフレームの受信と解釈を正しく行ったことを確認できます。

あるエンド・ステーションがこのポーリング・プロセスに参加できなかった場合、マネージメントの全状態報告書機構を介して、論理接続された PVC をもつすべてのリモート・エンド・ステーションに、その PVC は非アクティブであることが通知されます。

統合リンク・レイヤー・マネージメント (CLLM)

CLLM は、業界で広くサポートされてはいませんが、一部のフレーム・リレー・スイッチの製造元で採用されているオプションの FR 管理機能です。 CLLM は、LMI によって提供されるのと同じ管理情報のいくつか(特に、故障通知) を提供します。CLLM の主な用途は、接続装置に非同期輻輳 (ふくそう) 通知を提供することです。1 つの CLLM メッセージで、複数の PVC の故障または輻輳を示すことができます。フレーム・リレー・プロトコルは、CLLM について以下の標準をサポートしています。すなわち、ANSI T1.618, ITU-T (CCITT) Q.922 付録 A および ITU-T (CCITT) X.36 付録 C です。

フレーム・リレー・データ速度

この節では、フレーム・リレーのパーマネント・バーチャル・サーキット (PVC) のデータ速度について説明します。

認定情報速度 (CIR)

CIR は、通常の輻輳のない条件下の PVC に対して、ネットワークがサポートすることを認定しているデータ速度です。構成または確認されたすべての PVC に対して、CIR が提供されます (FR サービス提供者によって)。 CIR は、PVC 用に予約されている総帯域幅の一部分で、0 または 300 bps 〜 2 Mbps です。 64 Kbps または単一 DS0 チャネルが、最も一般的です。

add permanent-virtual-circuit または **change permanent-virtual-circuit** 構成コマンドを使用して、CIR を定義することができます。 **set circuit** コンソール・コマンドを使用すれば、CIR を動的に変更できます。また、**set CIR-defaults** コマンドを使用して、このインターフェース上のすべてのフレーム・リレー回線のデフォルト CIR を設定することもできます。

一部のフレーム・リレー・スイッチでは、CIR を値 0 に構成することが可能です。CIR が 0 のときは、フレーム・リレー・ネットワーク・バックボーンには PVC 用に予約されている帯域幅はほとんど、あるいはまったくなく、PVC のトラフィックは予約されていない帯域幅を使用します。

オーファン回線の CIR

ルーターは、インターフェース・レベルで構成された CIR デフォルトに基づいて、オーファン回線に CIR を割り当てます。重要なデータのルーティングをオーファン回線に依存しており、CIR、Bc、および Be 値がインターフェース・レベルで構成された値と異なっている場合は、オーファン回線の代わりに PVC を定義することをお勧めします。これにより、ネットワークがサポートすることを認定している CIR を割り当てることができます。

認定バースト (Bc) サイズ

認定バースト (Bc) サイズ とは、*算定時間 (Tc) 間隔* に送達することをネットワークが認定しているデータの最大量 (ビット数) です。 Tc は、Bc を CIR で割った値に等しくなります (Tc = Bc / CIR)。 CIR を 0 に構成すると、フレーム・リレーは Tc に 1 秒の値を使用します。

たとえば、PVC の CIR を 9600 bps に設定し、認定バースト・サイズを 14 400 ビットに設定した場合、時間間隔は 1.5 秒になります。 (14 400 ビット/9600 bps = 1.5 sec)。これは、PVC は 1.5 秒間に最大 14 400 ビットを転送できることを意味しています。

認定バースト・サイズと最大フレーム・サイズの関係から、このパラメーターは重要です。 最大フレーム・サイズ (ビット数) が認定バースト・サイズより大きい場合、ネットワークはサイズが認定バースト・サイズを超過しているフレームを廃棄する可能性があります。したがって、認定バースト・サイズは最大フレーム・サイズ以上にすることが必要です。また、ネットワークの提供者と共に設定したバースト・サイズに等しくすることも必要です。

add permanent-virtual-circuit および **change permanent-virtual-circuit** 構成コマンドを使用して、認定バースト・サイズを設定します。 **set circuit** コンソール・コマンドを使用すると、認定バースト・サイズを動的に変更することができます。また、**set CIR-defaults** コマンドを使用して、このインターフェース上のすべてのフレーム・リレー回線のデフォルトの認定バースト・サイズを設定することもできます。

装置は、**set CIR-defaults** コマンドによって設定されたデフォルトに基づいて、オーファン回線に認定バースト・サイズを割り当てます。 CIR を 0 に構成すると、認定バースト (Bc) サイズも 0 になります。

超過バースト (Be) サイズ

超過バースト (Be) サイズ は、CIR および Bc が非ゼロの場合、Tc (Tc = Bc/CIR) 期間中にルーターが PVC 上で Bc を超過して転送できる非認定データの最大量です。 CIR = 0 のとき、フレーム・リレーは Tc に 1 秒の値を使用します。

ネットワーク上では、この超過データは、認定バースト・サイズよりも成功の確率が低い状態で送達されます。 Be をゼロより大きい値に設定するのは、データが廃棄されるリスクと高位レイヤーのプロトコルの性能に与える影響を容認できる場合に限ってください。 Be は、ネットワークの提供者と共に設定した値に等しくする必要があります。

フレーム・リレーの構成時に **add permanent-virtual-circuit** コマンドまたは **change permanent-virtual-circuit** コマンドを使用して、超過バースト・サイズを設定します。 **set circuit** コンソール・コマンドを使用すると、超過バースト・サイズを動的に変更することができます。オーファン回線は、**set CIR-defaults** コマンドで設定された値に等しい超過バースト・サイズを受け取ります。 CIR を 0 に構成する場合は、超過バースト (Be) サイズを非ゼロ値に構成する必要があります。また、**set CIR-defaults** コマンドを使用して、このインターフェース上のすべてのフレーム・リレー回線に対するデフォルト超過バースト・サイズを設定することもできます。

回線速度

回線速度 とは、インターフェースの回線速度のことです。

FR インターフェースの回線速度は、**set line-speed** 構成コマンドを使用して構成します。内部クロックを使用する場合は、回線速度の構成は必須です。ただし、外部クロックの場合も回線速度を構成することをお勧めします。輻輳 (ふくそう) 監視が使用可能になっている場合、ルーターは最大情報速度として回線速度を使用するからです。また、一部のプロトコルは、ルートのコストを計算するときに、インターフェースに構成されている回線速度を使用します。

フレーム・リレー・ダイヤル回線インターフェース上では、回線速度は構成不能です。ダイヤル回線が ISDN 基本インターフェースにマップされる場合は、64 Kbps が回線速度として使用されます。

チャネル化 T1/E1 を基本ネットとして使用するダイヤル回線の場合、回線速度は、割り当てられたタイム・スロット数に 64 Kbps を掛けた値、もしくは 56 Kbps (チャネル化回線の帯域幅を 56 Kbps に設定した場合) です。たとえば、チャネル化回線のタイム・スロットの数を 3 に設定した場合、回線速度は 192 Kbps (3 * 64 Kbps) になります。

ダイヤル回線が V.25bis 基本インターフェースにマップされる場合は、V.25bis インターフェースの回線速度が FR ダイヤル回線として使用されます。

最小情報速度

最小情報速度 (IR) は、輻輳が通知されたときにルーターがそこまで減速する PVC の最小データ速度です。 **set ir-adjustment** 構成コマンドを使用して、最小 IR を CIR の比率として設定します。 **set ir-adjustment** コンソール・コマンドを使用すれば、動的に変更することができます。 CIR を 0 に構成した場合、最小 IR は 1500 bps になります。

最大情報速度

maximum information rate は、ルーターが PVC 上で転送する最大データ速度です。CIR 監視機能が使用可能であり、CIR および Bc が非ゼロの場合、最大情報速度は、CIR、Bc、および Be を使用して、次のように計算します。

```
( Bc + Be )
```

CIR 監視機能が使用可能であり、CIR および Bc が 0 に構成されている場合、最大情報速度は超過バースト・サイズ (Be) に等しくなります。

CIR 監視機能が使用可能でない場合、最大情報速度は回線速度に等しくなります。

可変情報速度

CIR 監視または輻輳監視機能が使用可能である場合、*可変情報速度* (VIR) は、構成された最小 IR から計算された最大 IR までの範囲です。ルーターが回線の輻輳を通知されると、VIR は徐々に最小情報速度まで減速され、ルーターが輻輳通知を受信しなくなると、徐々に最大情報速度まで加速されます。 **set ir-adjustment** 構成コマンド

を使用して、ルーターが輻輳を通知されたときに VIR を減速する情報速度の比率を構成します。輻輳が終わったときに VIR を徐々に加速する情報速度の比率も、このコマンドを使用して構成します。

ネットワークのインパルス・ロードを避けるために、ルーターは PVC がアクティブになったときに、VIR を CIR に初期設定します。 CIR を 0 に構成した場合、VIR は超過バースト (Be) に MIR 調整比率を掛けた値に初期設定されます。たとえば、Be が 64 000 に設定され、MIR 調整比率が 25% に設定されている場合、初期 VIR は 16 000 bps になります。

場合によっては、VIR が実際上は最大値を超えても構わないことがあります。フレームの長さ (ビット数) が最大 IR より大きくても、フレーム・リレーはともかくフレームを転送します。

回線輻輳

回線の輻輳 (ふくそう) は、次の理由の 1 つによって発生します。

- 送信側が許容されるスループットより高速で転送している。
- 受信側のフレームの処理が遅過ぎる。
- 中間バックボーン・リンクが輻輳しており、結果的に、送信側が利用可能なスループット許容値より高速で転送することになる。

回線の輻輳が発生すると、ネットワークはパケットを廃棄するか、遮断する (もしくは、その両方を行う) ことが必要になります。

回線輻輳に応じて、ルーターは*減速* を実施します。これは、構成された最小 IR まで、パケット転送の速度を段階的に減らして行くこと言います。減速は、以下の条件を満たすときに行われます。

- 回線が輻輳している。
- ルーターがフレームの送信側である。
- CIR 監視または輻輳監視が使用可能になっている。

この節では、フレーム・リレーのデータ速度および回線輻輳の監視について説明します。

CIR の監視

CIR 監視は、ルーターが FR ネットワーク上に輻輳状態が生じるのを防止するために各インターフェースに設定することができる、オプションのフレーム・リレー機能です。 CIR 監視により、PVC の VIR を、構成された最小 IR と最大 IR の間の範囲に設定することができます。

CIR 監視は、**enable cir-monitor** 構成コマンドを使用して構成し、デフォルトでは使用不可になります。 CIR 監視が使用可能にされている場合、輻輳監視をオーバーライドします。また、**enable cir-monitor** および **disable cir-monitor** コンソール・コマンドを使用して、動的に CIR 監視を使用可能にしたり、使用不可にしたりすることもできます。

輻輳監視

輻輳監視は、インターフェースごとに設定されるオプション機能で、PVC の VIR をネットワークの輻輳に応じて変えることができます。 VIR は、回線速度の最小 IR と最大 IR の間の値を取ります。デフォルトでは、輻輳監視は使用可能になります。 使用不可にするときは **disable congestion-monitor** 構成コマンドを使用し、再び使用可能にするときは **enable congestion-monitor** コマンドを使用します。また、**enable congestion-monitor** および **disable congestion-monitor** コンソール・コマンドを使用して、動的に輻輳監視を使用可能および使用不可にすることもできます。

CIR 監視が使用可能の場合、輻輳監視をオーバーライドします。 CIR 監視と輻輳監視の両方とも使用不可にされている場合には、インターフェース上の各 PVC の VIR は回線速度に設定され、ネットワーク輻輳に応じて減速されません。

注: 圧縮が使用可能の場合であっても、装置は非圧縮サイズのフレームを使用して、VIR が超過しているかどうかを判別します。

輻輳通知と回避

輻輳が発生すると、FR バックボーン・ネットワークは、FECN または BECN 信号を送って、送信側と受信側に通知する責任があります。 FECN および BECN は、輻輳が発生していることを PVC の各端の DTE に通知するために、フレーム内に設定されるビットです。 FECN は、フレームを受信したのと同じ方向で輻輳が発生していることを示します。送信側が輻輳の原因になっています。 BECN は、この DTE によって送信されたフレームがネットワーク輻輳の原因になっていることを示します。

オプションで、ネットワークは CLLM メッセージを使用して、輻輳情報を伝えることができます。 CLLM メッセージは、輻輳の発生源にのみ送信され、DTE は BECN メッセージと同様に処理する必要があります。

424ページの図25 の例は、フレームがルーター X からルーター Y に送信される場合の、スイッチ B における輻輳状態を示しています。 FR バックボーン・ネットワークは、ルーター X に送信するフレームに BECN ビットをセットして、送信するフレームが輻輳に遭遇していることをルーター X に通知します。また、FR バックボーン・ネットワークはルーター Y に対しても、FECN ビットをセットして、それが受信するフレームが輻輳に遭遇していることを通知します。

ルーターが BECN の入っているフレームを受信した場合、CIR 監視または輻輳監視のいずれかが使用可能のときは、ルーターは PVC の VIR (可変情報速度) を減速する責任があります。ルーターは、最小 IR に達するか、BECN のないフレームが到着するまで、 BECN が入っている連続フレームを受信している間、徐々に減速します。FR スイッチは、輻輳限界値に達すると複数のフレームに BECN をセットすることがしばしばあります。ネットワークが複数のフレームに BECN をセットしている場合、FR がネットワーク輻輳に対して過剰に反応するのを回避するために、FR は PVC の VIR を多くても毎秒 1 回に減らします。これによって、VIR は徐々に減少します。BECN のない連続フレームを受信するようになったら、VIR を最大 IR まで徐々に加速します。

FR ネットワークの運用によっては、装置が FECN を受信した場合、装置は PVC の VIR を減速して、ネットワークに送られるトラフィックの全体量をできるだけ速やか

に最小化することが必要になる場合があります。ネットワーク上の全体的な負荷を削減すると、輻輳を緩和するためにすべての PVC で廃棄されるパケットの数を減らすことができます。 CIR または輻輳監視オプションと合わせて、***throttle-transmit-on-fecn*** パラメーターを使用可能にすると、装置は FECN をBECN と同様に扱うので、輻輳通知を受け取ったときに、全体的な FR ネットワーク輻輳を軽減することができます。 throttle-transmit-on-fecn パラメーターは、入力と出力の両方について、専用のバッファーを提供しない待ち行列化方式を採用している FR ネットワークでのみ使用してください。 ***throttle-transmit-on-fecn*** が使用可能の場合、FR は各 BECN または FECN を受信するたびに、PVC の VIR を多くても毎秒 1 回に減らします。

一部の FR ネットワーク・スイッチは、輻輳を通知するために FECN をセットしますが、BECN はセットしません。輻輳の発生元に輻輳通知を提供したい場合、***notify-fecn-source*** パラメーターを使用可能にすると、装置は FECN を受信した PVC を介して送信するフレームに BECN をセットします。このアクションは、ネットワーク輻輳の原因になっている装置に、その PVC の VIR を減速するように知らせる信号を提供します。

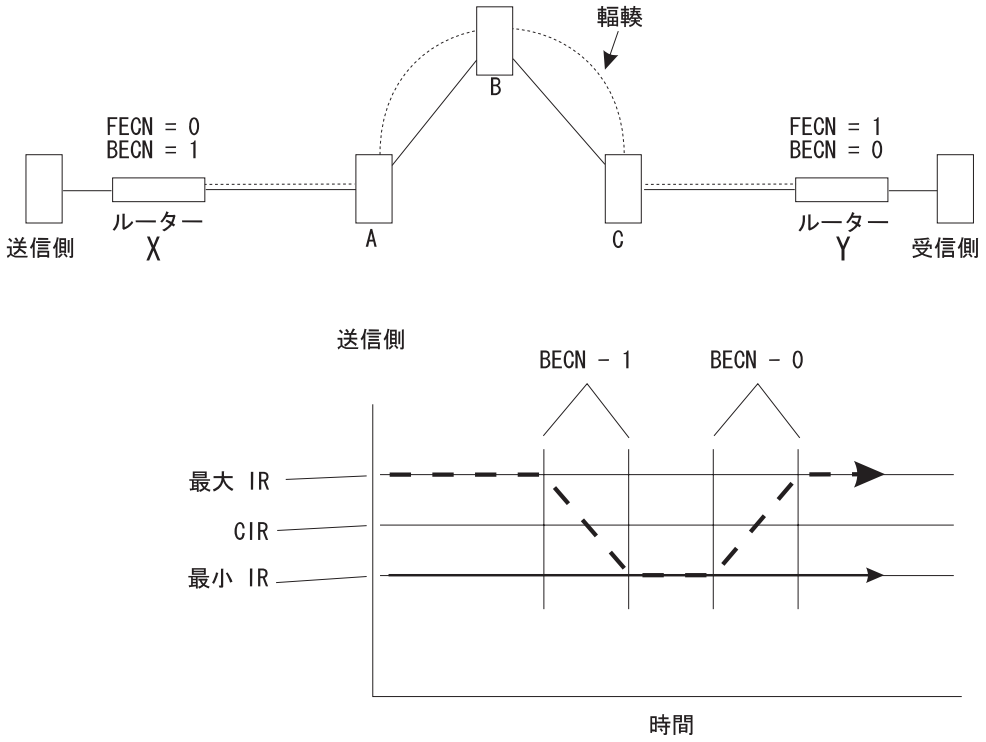


図 25. 輻輳通知と減速

注: 輻輳が発生したときに 2 つのエンド・ステーション間に複数の DLCI が構成されている場合、最初の DLCI 上の輻輳状態が解決されるまで、第 2 の DLCI を使用すれば、より高いスループットでデータを転送できる可能性があります。

同様に、ネットワークの提供者が CLLM をサポートしている場合、CLLM メッセージに入っている PVC の伝送速度を*減速* するようにフレーム・リレーを構成することができます。 CLLM メッセージには、報告されている問題のタイプと重大度を示す原因符号が入っています。装置の反応は、原因符号および CLLM メッセージ内の各

PVC に構成されている CIR によって異なります。装置が受け取る CLLM メッセージの内容とそれに対する反応は、次のとおりです。

- 短期的状態を受け取り、PVC に構成されている CIR が非ゼロの場合、フレーム・リレー・プロトコルは、該当する PVC の伝送速度を、構成された IR 減分率で減速します。
- 長期的状態を受け取った場合、フレーム・リレー・プロトコルは、該当する PVC の伝送速度を、計算された最小情報速度に設定します。
- ファシリティーまたは装置の障害あるいは保守作業を受信した場合、または CIR がゼロに構成されていた場合、FR プロトコルは、該当する PVC への待ち行列データの転送は続けますが、輻輳状態が解消されるまでは、高位レイヤー・プロトコルからの発信パケットは受け付けません。

ある PVC の CLLM メッセージを受信した後、装置が *Ty* タイマーの期間内に CLLM メッセージまたは BECN を受信しない場合、あるいは BECN を含まないフレームを受信した場合、装置は輻輳状態が解消されたものと見なし、徐々に PVC を構成された伝送速度に戻します。 輻輳制御のために CLLM を使用している場合は、他の用途のために DLCI 1007 を構成してはなりません。

フレーム・リレー上の帯域幅予約

フレーム・リレー上の帯域幅予約については、703ページの『第53章 帯域幅予約および優先待ち行列の使用』 から 721ページの『第54章 帯域幅予約の構成および監視』を参照してください。

フレーム・リレー構成プロンプトの表示

フレーム・リレー構成環境にアクセスするには、次のようにします。

1. OPCON プロンプト (*) で **talk 6** と入力する。
2. 構成プロンプト (Config>) で **list devices** コマンドを入力して、ルーターに構成されているインターフェースのリストを表示する。
3. **network** コマンドを入力して、フレーム・リレー構成プロンプトを表示する。ネットワーク番号は、フレーム・リレー・インターフェースの番号です。

```
Config>network
What is the network number [0] 2
Frame Relay user configuration
FR 2 Config >
```

4. フレーム・リレー・インターフェース構成プロンプト (FR Config>) で、本章で説明するコマンドを使用して、フレーム・リレー・パラメーターを構成する。

フレーム・リレー基本構成手順

この節では、フレーム・リレー・プロトコルを立ち上げて実行するのに必要な最小構成ステップについて概説します。詳しい構成情報および説明が必要な場合は、本章の構成コマンドの説明個所を参照してください。

注: 新しい構成変更を有効にするためには、ルーターをリスタートする必要があります。

- **FR マネージメントを選択する。** FR ローカル管理インターフェース (LMI) プロトコルは、デフォルトでは ANSI になります。中間 LMI (REV1)、ANSI T1.617 付録 D マネージメント、または ITU-T/CCITT Q.933 付録 A マネージメントを使用するネットワークに接続するオプションが提供されています。 **enable** および **set** コマンドを使用して、必要なマネージメントを使用可能にしたり、設定したりしてください。
- **PVC を追加する。** FR マネージメントが使用不可のとき、またはオーファン回線が使用不可のときに必要な必須 PVC を追加します。 FR PVC を介してブリッジしたい場合、または FR PVC を介して APPN を実行したい場合には、その PVC も構成する必要があります。 **add permanent-virtual-circuit** コマンドを使用してください。
- **FR 着信先アドレスを構成する。** FR インターフェースを介して IP または IPX のようなプロトコルを実行しており、FR 上のアドレス解決プロトコル (ARP) または逆 ARP をサポートしない装置と接続している場合、**add protocol-address** コマンドを使用して、静的プロトコルとアドレス・マッピングを追加します。
- **フレーム・リレー上の帯域幅予約を構成する。** 必須の基本フレーム・リレー構成に加えて、フレーム・リレー上の帯域幅予約 (オプション機能) も構成することができます。帯域幅予約の構成については、703ページの『第53章 帯域幅予約および優先待ち行列の使用』 を参照してください。
- **廃棄可能性を構成する。** 帯域幅予約を使用しての廃棄可能性 (DE) 輻輳制御を構成することができます。廃棄可能性の構成については、703ページの『第53章 帯域幅予約および優先待ち行列の使用』 を参照してください。
- **データ圧縮を構成する。** フレーム・リレーに対するデータ圧縮を構成することができます。データ圧縮の構成については、831ページの『第62章 データ圧縮サブシステムの使用』 を参照してください。

フレーム・リレー・マネージメントの使用可能化

フレーム・リレーのもとには 3 つのマネージメント・オプションがあります。

- 中間ローカル管理インターフェース 改訂 1
- ANSI T1.617 付録 D マネージメント
- ITU-T/CCITT Q.933 付録 A マネージメント

フレーム・リレーのデフォルトでは、ANSI が使用可能になります。マネージメント・タイプを変更したい場合、あるいは ANSI マネージメントを再び使用可能にしたい場合は、以下の手順で行います。フレーム・リレー上のマネージメントを使用可能にするには、2 つのステップで行います。

1. `FR Config>` プロンプトで **enable lmi** コマンドを入力して、マネージメント・アクティビティーを使用可能にする。
2. **set lmi-type** コマンドを入力して、そのインターフェースのマネージメントのタイプを選択する。

   set コマンドで利用可能なマネージメント・タイプについての詳細は、427ページの表55 を参照してください。

これらのマネージメント・タイプの設定方法の例を、表の後に示してあります。詳細については、この章の **enable** および **set** コマンドの節も参照してください。

表 55. フレーム・リレー・マネージメント・オプション

コマンド	オプション	説明
set	lmi-type rev1	LMI 改訂 1 (Stratacom のフレーム・リレー・インターフェース仕様) に準拠します。
set	lmi-type ansi	ANSI T1.617 ISDN-DSS1-Signalling Specification for Frame Relay Bearer Service (付録 D と呼ばれます) に準拠します。
set	lmi-type ccitt	ITU-T/CCITT 勧告 Q.933 の付録 A - DSS1 Signalling Specification for Frame Mode Basic Call Control に準拠します。

例:

```
enable lmi

set lmi-type ansi
```

第32章 フレーム・リレー・インターフェースの構成および監視

この章では、フレーム・リレーの構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

- 453ページの『フレーム・リレー監視プロンプトへのアクセス』
- 453ページの『フレーム・リレー監視コマンド』
- 464ページの『フレーム・リレー・インターフェースおよび GWCON インターフェース・コマンド』

注: フレーム・リレー上の帯域幅予約の監視については、721ページの『第54章 帯域幅予約の構成および監視』 を参照してください。

フレーム・リレー構成コマンド

この節では、フレーム・リレー構成コマンドについて説明します。コマンドはすべて `Frame Relay>` プロンプトで入力します。

新しい構成変更を有効にするためには、ルーターをリスタートする必要があります。

表 56. フレーム・リレー構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Add	PVC、必須 PVC グループ、および着信先プロトコル・アドレスを、フレーム・リレー・インターフェースに追加します。
Change	以前に **add** コマンドによって定義された PVC または必須 PVC グループを変更します。
Disable	使用可能にされたフレーム・リレー機能を使用不可にします。
Enable	回線監視、マネージメント・オプション、マルチキャスト、プロトコル・ブロードキャスト、およびオーファンなどのフレーム・リレー機能を使用可能にします。
List	LMI、PVC、必須 PVC グループ、HDLC 情報、およびプロトコル・アドレスの現行構成を表示します。
LLC	フレーム・リレー・インターフェース上の LLC パラメーターを構成します。 これらの LLC パラメーターは、フレーム・リレーを介して APPN を実行するときに必要です。
Remove	以前に追加された PVC、必須 PVC グループ (空のとき)、またはプロトコル・アドレスを削除します。
Set	フレーム・リレー・マネージメント・オプションおよびパラメーター (N1-parameter、N2-parameter、N3-parameter、P1 parameter、および T1-parameter) を構成します。 FR シリアル・インターフェースの物理レイヤー・パラメーターを構成します。最大フレーム・サイズを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

注: この節では、*回線番号* および *PVC* という用語は、DLCI (データ・リンク回線識別子) という用語と同義です。

Add

add コマンドは、フレーム・リレー・インターフェースによってサポートされる PVC、必須 PVC グループ、または着信先プロトコル・アドレスを追加するのに使用します。

構文:

add permanent-virtual-circuit . . .
protocol-address . . .
pvc-group . . .

permanent-virtual-circuit

フレーム・リレー・インターフェースの予約された範囲 0 〜 15 を超えて PVC を追加します。追加が可能な PVC の最大数は約 992 ですが、インターフェースが実際にサポートできる PVC の数は、各 PVC に必要なスループット、回線速度、インターフェース上で実行されているプロトコルのタイプ、および最大フレーム・サイズに収めることができるローカル管理インターフェース PVC 情報要素の数によって決まります。

例:

```
add permanent-virtual-circuit
Circuit Number [16]?
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign Circuit name []?
Is circuit required for interface operation [N]?
Does the circuit belong to a required PVC group [N]?
What is the group name []?
Do you want to have data compression performed [Y]?
Do you want to have data encryption performed [N]? y

Data encryption requires a key that is 16 hexadecimal characters long
You will be asked to enter the key twice for security reasons

Please enter the key for the first time now

A valid encryption key has been entered

Please confirm the key by entering it again

The encryption keys match - the key has been accepted
```

Circuit Number

この PVC の回線番号を示します。

有効値: 16 〜 1007

注: 輻輳の制御のために CLLM を構成している場合は、1007 を PVC として構成することはできません。

Committed Information Rate

認定情報速度 (CIR) を示します。 CIR は、0 または 300 bps 〜 2 048 000 bps の範囲の値です。詳しくは、419ページの『認定情報速度 (CIR)』 を参照してください。最大値は、インターフェースに構成されているデフォルト CIR の値です。

Committed Burst Size

ネットワークで合意されている、認定バースト (Bc) サイズ/CIR 秒数に相当する測定期間に送達できる最大データ量 (ビット)。範囲は 300 ～ 2048000 ビットです。最大値は、インターフェースに構成されているデフォルトの認定バースト値です。

注:

1. CIR が 0 として構成されている場合、認定バースト・サイズも 0 に設定され、値の入力を求めるプロンプトは出ません。詳しくは、420ページの『認定バースト (Bc) サイズ』 を参照してください。

Excess Burst Size

(認定バースト・サイズ/CIR) 秒数に相当する測定期間にネットワークが送達を試みることができる、認定バースト・サイズを超過する未認定データの最大量 (ビット数)。範囲は 0 ～ 2 048 000 ビットです。最大値は、インターフェースに構成されている超過バースト・サイズの値です。詳しくは、420ページの『超過バースト (Be) サイズ』を参照してください。

Assign Circuit Name

回線を記述するために割り当てられる ASCII ストリングを示します。デフォルト値は unassigned (未割り当て) です。

Is the circuit required for operation

その回線がインターフェースの運用に必要であるかどうかを示すために、Y または N を指定します。

Does the circuit belong to a required PVC group

このプロンプトは、必須の回線に対してのみ表示されます。その回線が必須 PVC グループに属するかどうかを示すために、Y または N を指定します。

What is the group name

PVC を必須グループに所属するとして定義した場合、必須 PVC グループの名前を指定することができます。疑問符 (?) を入力すると、現在定義されているグループのリストが表示されます。

Do you want to have compression performed

回線がデータ・パケットを圧縮するかどうかを指定することができます。この質問は、インターフェースで圧縮が使用可能にされている場合にのみ出されます。

注: PVC 上の圧縮を使用可能にし、インターフェースの圧縮 PVC 限界を超過した場合、メッセージが出ます。回線上の圧縮は、可能な場合 (つまり、回線がアクティブになったときにアクティブ圧縮限界を超えていなかった場合) に実行されます。

Do you want to have data encryption performed

回線がデータ・パケットを暗号化するかどうかを指定することができます。この質問は、インターフェースで暗号化が使用可能にされ

ている場合にのみ出されます。この質問に対して 『yes』 (または 『y』) と応答した場合にのみ、暗号化キーの入力を求めるプロンプトが出ます。

Specifying the Encryption Key: 暗号化キーは 16 字の長さの 16 進文字です。暗号化キーは X'0000000000000000' ～ X'FFFFFFFFFFFFFFFF' の間の値を指定しなければなりません。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

protocol-address

このコマンドは、静的に構成された着信先プロトコル (プロトコル名) アドレスを、フレーム・リレー・インターフェースに追加します。静的に構成された着信先プロトコル・アドレスは、逆 ARP も ARP も選択できない場合やセキュリティーの上で役立ちます。プロトコル名とアドレス・マッピング (静的 ARP) を追加するのは、逆 ARP または ARP より非効率的です。

- 逆 ARP は、ブロードキャストせずに動的にアドレス・マッピングを行うので、推奨される効率的な方法です。
- ARP は、逆 ARP を選択できない場合に使用することをお勧めします。これは、アドレスをブロードキャストし、一定の間隔でマッピングを再確認するので、逆 ARP より非効率的です。

このパラメーターでは、追加するプロトコルのタイプによって、異なる情報を求めるプロンプトが出ます。

例:

```
add protocol-address
Protocol name or number [0]?
```

IP プロトコル:

```
IP Address [0.0.0.0]?
Circuit Number [16]?
```

IPX プロトコル:

```
Host Number (in hex)[]?
Circuit Number [16]?
```

AppleTalk フェーズ 2 プロトコル:

```
Network Number (1-65279) []?
Node Number (1-253) []?
Circuit Number [16]?
```

DN プロトコル:

```
Node address [0.0]?
Circuit Number [16]?
```

Protocol name or number

追加するプロトコルの名前または番号を定義します。サポートされないプロトコルを指定すると、システムはエラー・メッセージを出して知らせます。

```
Unknown protocol name, try again
```

たとえば、次のいずれかを誤って指定している可能性があります。

```
Prot#  Name
0      IP
4      DN
7      IPX
22     AP2
```

サポートされるプロトコル・タイプのリストを見たい場合は、`Protocol name or number [IP]?` プロンプトで `?` を入力します。

IP Address
リモート IP ホストの 32 ビット・インターネット・アドレスを小数点表記法で定義します。

Host Number
リモート IPX ホストの 48 ビット IPX ノード・アドレスを定義します。

Network Number
リモート AppleTalk ホストの AppleTalk フェーズ 2 ネットワーク番号を定義します。

Node Number
リモート AppleTalk ホストに接続されているインターフェースのノード番号を定義します。

Node address
リモート DECnet ホストの DECnet ノード・アドレスを定義します。ノード・アドレスは *x.y* フォーマットで構成します。ただし、*x* は 6 ビットのエリア・アドレスで、*y* は 10 ビットのノード番号です。

Circuit Number
このプロトコルを実行する PVC を 16 ～ 1007 の範囲で定義します。

pvc-group *groupname*

必須 PVC グループ名を追加します。

Change

change permanent-virtual-circuit コマンドは、以前に **add permanent-virtual-circuit** コマンドを使用して追加された PVC を変更するのに使用します。

構文:

change permanent-virtual-circuit . . .

例:

```
change permanent-virtual-circuit
Circuit Number [16]?
Committed Information Rate in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign Circuit Name: []?
Is the circuit required for interface operation [N]?
Does the circuit belong to a required group [N]?
What is the group name []?
Do you want to have data compression performed []?
Do you want to have data encryption performed []?
```

Circuit Number
この PVC の回線番号を示します。

有効値: 16 ～ 1007

注: 輻輳の制御のために CLLM を構成している場合は、1007 を PVC として構成することはできません。

Committed Information Rate
認定情報速度 (CIR) を示します。 CIR は、0 または 300 bps ～ 2048000 bps の範囲の値です。インターフェースのデフォルト値は 64000 bps ですが、個々の回線のデフォルト値は、**set cir-defaults** コマンドで構成された値になります。

Committed Burst Size
ネットワークで合意されている、(認定バースト・サイズ/CIR) 秒数に等しい測定期間中に送達できる最大データ量 (ビット数)。 CIR が 0 として構成されている場合、認定バースト・サイズも 0 に設定されます。そうでない場合、有効な範囲は 300 ～ 2 048 000 ビットです。インターフェースのデフォルト値は 64000 ビットですが、個々の回線のデフォルト値は、**set cir-defaults** コマンドで構成された値になります。

Excess Burst Size
(認定バースト・サイズ/CIR) 秒数に等しい測定期間中にネットワークが送達を試みることができる、認定バースト・サイズを超過した未認定データの最大量 (ビット数)。範囲は 0 ～ 2 048 000 ビットです。インターフェースのデフォルト値は 64000 bps ですが、個々の回線のデフォルト値は、**set cir-defaults** コマンドで構成された値になります。

Assign circuit Name
変更したい回線の ASCII ストリングの名前を示します。

Is the circuit required for operation
その回線がインターフェースの運用に必要であるかどうかを示すために、Y または N を指定します。

Does the circuit belong to a required PVC group
このプロンプトは、必須の回線に対してのみ表示されます。その回線が必須 PVC グループに属するかどうかを示すために、Y または N を指定します。

What is the group name
PVC を必須グループに所属するとして定義した場合、必須 PVC グループの名前を指定することができます。疑問符 (?) を入力すると、現在定義されているグループのリストが表示されます。

Do you want to have data compression performed
回線がデータ・パケットを圧縮するかどうかを指定することができます。この質問は、インターフェースで圧縮が使用可能にされている場合にのみ出されます。

注: PVC 上の圧縮を使用可能にし、インターフェースの圧縮 PVC 限界を超過した場合、メッセージが出ます。回線上の圧縮は、可能な場合 (つまり、回線がアクティブになったときにアクティブ圧縮限界を超えていなかった場合) に実行されます。

Do you want to have data encryption performed

回線がデータ・パケットを暗号化するかどうかを指定することができます。この質問は、インターフェースで暗号化が使用可能にされている場合にのみ出されます。

この質問のデフォルト値は、PVC 上の現在の暗号化の状態によって異なります。 PVC が現在データを暗号化していないときに、ユーザーがその状態を変更して、データを暗号化するようにした場合、ソフトウェアは **add permanent-virtual-circuit** コマンドの項で説明したように、暗号化キーの入力を求めるプロンプトを出します。暗号化キーの入力についての詳細は、 431 を参照してください。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Disable

disable コマンドは、以前に **enable** コマンドを使用して使用可能にした機能を使用不可にするのに使用します。

構文:

disable

- cir-monitor
- cllm
- compression
- congestion-monitor
- dn-length-field
- encryption
- lmi
- lower-dtr
- multicast-emulation
- no-pvc
- notify-fecn-source
- orphan-circuits
- protocol-broadcast
- throttle-transmit-on-fecn

cir-monitor

この機能を使用不可にすると、回線の情報速度は **add permanent-virtual-circuit** コマンドで構成したパラメーターを用いて計算された最大情報速度を超えることが許されます。この機能のデフォルト設定は、使用不可です。詳細については、422ページの『回線輻輳』 を参照してください。

cllm 装置が CLLM メッセージに応答して*減速* するのを使用不可にします。デフォルトは使用不可です。 422ページの『回線輻輳』 を参照してください。

compression
インターフェース上の圧縮を使用不可にします。どの PVC でも圧縮は行われなくなります。

congestion-monitor
輻輳監視機能を使用不可にします。この機能を使用不可にすると、回線の情報速度が、輻輳に応じて最小情報速度から回線速度までの間で変えられなくなります。詳細については、422ページの『回線輻輳』 を参照してください。この機能のデフォルト設定は、使用可能です。

dn-length-field
フレーム・リレーのフレーム内の DECnet パケットの前に長さフィールドを必要とする DECnet フェーズ IV の実現を、フレーム・リレーを介して相互運用できなくしますが、DECnet パケットの前に長さフィールドを使用しない DECnet フェーズ IV フレーム・リレー・ソフトウェアとの相互運用は許されます。 dn-length-field を使用不可にすると、フレーム・リレーは DECnet パケットが入っている転送フレームに長さフィールドを挿入せず、また DECnet パケットが入っている受信フレームからの長さフレームの除去も試みません。

注: このオプションは、構成オプションとしてのみ提供されています。

encryption
インターフェース上の暗号化を使用不可にします。このインターフェース上の PVC が暗号化が可能であっても、暗号化は行われません。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

lmi

注: このパラメーターを使用不可にすると、実際のネットワークまたは管理インターフェースを使用せずに、通常の運用またはエンド・エンド間のフレーム・リレー・テストを行うことができます。エンド・エンド間のフレーム・リレー・テストの場合は、リンクの両端に同様の PVC (同じ PVC 番号、たとえば、16 と 16 のように) を追加することが必要です。

lower-dtr
このパラメーターは、ルーター上の専用シリアル・ライン・インターフェースのデータ端末レディー (DTR) 信号の扱い方を決めます。フレーム・リレー・ダイヤル回線インターフェースではサポートされません。 lower-dtr パラメーターについての詳しい説明は、**enable lower-dtr** コマンドの項を参照してください。

以下のケーブル・タイプがサポートされます。

EIA 232 (RS-232)

V.35

V.36

デフォルト設定値は **disable lower-dtr** です。

multicast-emulation
各アクティブ PVC 上のマルチキャスト・エミュレーションを使用不可にしま

す。この機能のデフォルト設定は、使用可能です。この機能を使用不可にする場合は、プロトコル静的アドレス・マップを追加する必要があります。

マルチキャスト・エミュレーションが使用不可にされている場合、一部のプロトコル (IPX RIP など) はフレーム・リレー・インターフェース上で機能しません。また、プロトコル・ブロードキャスト (protocol-broadcast) 機能も、正しく機能するためにはマルチキャスト・エミュレーションを必要とします。詳細については、417ページの『マルチキャスト・エミュレーションとプロトコル・ブロードキャスト』 を参照してください。

no-pvc

インターフェースをアクティブと見なすか、非アクティブと見なすかを制御します。 no-pvc が使用不可にされている場合、インターフェース上のアクティブ PVC の存在は、フレーム・リレー・インターフェースをアクティブまたは非アクティブのいずれに見なすかには影響を与えません。

notify-fecn-source

ルーターが、FECN ビットがセットされた受信パケットの発信元の装置に最初に送るパケットに BECN ビットをセットするのを使用不可にします。詳細については、422ページの『回線輻輳』 を参照してください。

orphan-circuits

インターフェースでのすべての未構成オーファン回線の使用を禁止します。オーファン回線のデフォルト設定は、使用可能です。オーファン回線を使用不可にすると、未構成回線からの不許可侵入が防止されるので、ネットワークのセキュリティー手段が追加されます。ただし、オーファン回線を使用不可にする場合は、インターフェースで使用する PVC を追加することが必要になります。

protocol-broadcast

IP RIP のようなプロトコルがフレーム・リレー・インターフェースを介して機能するのを禁止します。詳細については、417ページの『マルチキャスト・エミュレーションとプロトコル・ブロードキャスト』 を参照してください。この機能のデフォルト設定は、使用可能です。

throttle-transmit-on-fecn

FECN ビットがオンにセットされているパケットに応答して、装置がパケットの転送を*減速* するのを禁止します。デフォルトは使用不可です。詳細については、422ページの『回線輻輳』 を参照してください。

Enable

enable コマンドは、フレーム・リレー機能を使用可能にするのに使用します。

構文:

enable

cir-monitor

cllm

compression

congestion-monitor

dn-length-field

encryption

lmi

lower-dtr

multicast-emulation

notify-fecn-source

no-pvc

orphan-circuits

protocol-broadcast

throttle-transmit-on-fecn

cir-monitor

回線監視機能を使用可能にします。回線監視機能は、**add permanent-virtual-circuit** コマンドまたは **change permanent-virtual-circuit** コマンドで構成されたパラメーターを用いて計算された最小情報速度と最大情報速度の間で、回線の情報速度を変化させます。

注: 輻輳が存在するときは、回線監視機能は輻輳監視機能をオーバーライドします (両方の機能が使用可能にされている場合)。 この機能のデフォルト設定は、使用不可です。

CIR 監視について詳しくは、422ページの『CIR の監視』 を参照してください。

注: データ圧縮を実行している回線のスループットを最大化するために、圧縮を使用可能にしたのと同じインターフェースでは、CIR 監視を使用可能にすべきでありません。装置は PVC の VIR を超過しているかどうかを調べる際には未圧縮サイズのフレームを使用しますが、圧縮されたフレームはそれより少ない帯域幅しか必要としないので、装置が監視を厳重に実施して構成済み CIR を超過しないようにすると、PVC の CIR が十分に活用されないことになります。 代わりに、輻輳監視を使用して、装置が FR ネットワークから送られた輻輳表示に反応できるようにすれば、フレームの損失を回避できます。

cllm 装置が CLLM メッセージに応答して*減速* するのを使用可能にします。このサポートが利用可能かどうかについては、FR ネットワークの提供者に尋ねてください。詳細については、422ページの『回線輻輳』 を参照してください。

compression

インターフェース上の圧縮を使用可能にします。コンテキストが利用可能であり、アクティブ圧縮 PVC 限界を超えていない場合、インターフェース上のすべての圧縮可能 PVC がデータ・パケットを圧縮できます。 (詳細については、831ページの『第62章 データ圧縮サブシステムの使用』 を参照してください。)

注: データ圧縮を実行している回線のスループットを最大化するために、圧縮を使用可能にしたのと同じインターフェースでは、CIR 監視を使用可能にすべきでありません。 装置は PVC の VIR を超過しているかどうかを調べる際には未圧縮サイズのフレームを使用しますが、圧縮されたフ

レームはそれより少ない帯域幅しか必要としないので、装置が監視を厳重に実施して構成済み CIR を超過しないようにすると、PVC の CIR が十分に活用されないことになります。 代わりに、輻輳監視を使用して、装置が FR ネットワークから送られた輻輳表示に反応できるようにすれば、フレームの損失を回避できます。

congestion-monitor

輻輳監視機能を使用可能にします。この機能は、回線の情報速度を輻輳に応じて最小情報速度から回線速度までの間で変化させることができます。

注: 輻輳が存在するときは、回線監視機能は輻輳監視機能をオーバーライドします (両方の機能が使用可能にされている場合)。この機能のデフォルト設定は、使用可能です。

輻輳監視についての詳細は、423ページの『輻輳監視』 を参照してください。

dn-length-field

フレーム・リレーのフレーム内の DECnet パケットの前に長さフィールドを必要とする DECnet フェーズ IV の実現を、フレーム・リレーを介して相互運用することをサポートします。 dn-length-field を使用可能にすると、フレーム・リレーは DECnet パケットが入っている転送フレームに長さフィールドを挿入し、また DECnet パケットが入っている受信フレームからの長さフレームを除去します。このオプションは、デフォルトでは使用不可になります。デフォルトでは、フレーム・リレーは長さフィールドの挿入も除去も行いません。

注: このオプションは、ルーター・ソフトウェアに DECnet フェーズ IV プロトコルが含まれている場合に、構成オプションとしてのみ提示されます。

encryption

インターフェース上の暗号化を使用可能にします。暗号化が使用可能として構成されているすべての PVC が、すべての転送データを暗号化します。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

lmi マネージメント・アクティビティーを使用可能にします。

enable lmi コマンドを出した後、**set lmi-type** コマンドを使用して、フレーム・リレー・インターフェースの管理モードを選択します。 426ページの『フレーム・リレー・マネージメントの使用可能化』 を参照してください。システムのデフォルトでは ANSI T1.617 付録 D マネージメントになります。

以前にフレーム・リレー・マネージメントを使用不可にした場合は、**enable lmi** コマンドを使用して、LMI マネージメントを再開してください。

lower-dtr

このパラメーターは、使用不可にされている専用シリアル・ライン・インターフェースのデータ端末レディー (DTR) 信号の扱い方を決めます。フレーム・リレー・ダイヤル回線インターフェースではサポートされません。このパラメーターが 『使用不可』 (デフォルト値) に設定されている場合、インターフェースが使用不可のときは DTR 信号は上がったままになります。

lower-dtr が使用可能の場合は、インターフェースが使用不可にされると、DTR は下がります。この動作が適している状況は、インターフェースが WAN 再ルートの代替リンクとして構成されており、インターフェースが、DTR 信号の状態に基づいてダイヤル接続を維持するダイヤルアウト・モデムに接続されているような場合です。

この機能が使用可能で、インターフェースが使用不可のとき、DTR 信号は下がり、モデムはダイヤル接続をダウンに維持します。インターフェースが使用可能になると (WAN 再ルートのバックアップ・シナリオにより)、DTR は上がり、モデムは保管しているバックアップ・サイトへの番号をダイヤルします。 1 次インターフェースが復元すると、代替インターフェースは使用不可にされ、DTR は下がって、モデムはダイヤル接続を切断します。

以下のケーブル・タイプがサポートされます。

EIA 232 (RS-232)

V.35

V.36

デフォルト設定値は **disable lower-dtr** です。

multicast-emulation

マルチキャスト・エミュレーションを使用可能にします。これにより、各アクティブ PVC 上でマルチキャスト/ブロードキャスト・フレームを転送できるようになります。 ARP、IPX RIP、および IP RIP などのプロトコルは、フレーム・リレー・インターフェースを介して正しく機能するためには、マルチキャスト・エミュレーションを使用可能にしておく必要があります。詳細については、417ページの『マルチキャスト・エミュレーションとプロトコル・ブロードキャスト』 を参照してください。このパラメーターのデフォルト値は、使用可能です。

no-pvc

インターフェースをアクティブと見なすか、非アクティブと見なすかを制御します。この機能が使用可能のとき、インターフェース上にアクティブの PVC が存在しないと、フレーム・リレー・インターフェースは非アクティブになります。少なくとも 1 つの PVC がアクティブの場合、ルーターと FR スイッチ間で LMI 交換が正常に行われると、フレーム・リレー・インターフェースはアクティブになります。

notify-fecn-source

ルーターが、FECN ビットがセットされた受信パケットの発信元の装置に最初に送るパケットに BECN ビットをセットするのを使用可能にします。このパラメーターは、FR スイッチ自体は BECN をセットしないが、FECN はセットするネットワークで、装置の輻輳制御機構を拡張するのに使用します。詳細については、422ページの『回線輻輳』 を参照してください。

orphan-circuits

すべての未構成オーファン回線の使用を使用可能にします。この機能のデフォルトは、使用可能です。デフォルト CIR 値についての詳細は、419ページの『オーファン回線の CIR』 を参照してください。

protocol-broadcast

IP RIP のようなプロトコルがフレーム・リレー・インターフェースを介して正しく機能するようにします。プロトコル・ブロードキャスト機能が正しく

機能するには、マルチキャスト・エミュレーション機能を使用可能にする必要があります。この機能のデフォルト設定は、使用可能です。

throttle-transmit-on-fecn

FECN ビットがオンにセットされているパケットに応答して、装置がパケットの転送を*減速* するのを使用可能にします。このパラメーターは、輻輳表示を受信したときに FR ネットワーク全体の輻輳を最小化するのに使用します。これにより、装置は BECN に反応するのと同様の方法で FECN に反応します。

List

list コマンドは、現在構成されている管理情報および PVC 情報を表示するのに使用します。

構文:

list all
hdlc
lmi
permanent-virtual-circuits
protocol-address
pvc-groups

all フレーム・リレー構成を表示します。この表示は、**list hdlc**、**list lmi**、および **list permanent virtual circuits** コマンドの組み合わせです。

パラメーターの説明は、**list hdlc** および **list lmi** の項を参照してください。

hdlc フレーム・リレー・ハイレベル・データ・リンク制御 (HDLC) 構成を表示します。

例:

```
list hdlc
                        Frame Relay HDLC Configuration


 Maximum frame size     = 2048
 Encoding               = NRZ
 Idle state             = Flag
 Clocking               = External
 Cable type             = V.35 DTE
 Line speed (bps)       = 64000
 Transmit delay         = 0
 Lower DTR              = Enabled
```

Encoding

シリアル・インターフェースの伝送符号化法。符号化法は NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) です。

Idle データ・リンク・アイドル状態: フラグまたはマーク

Clocking

クロックのタイプ: 内部または外部

Cable type

シリアル・アダプター・ケーブル・タイプ: RS-232、V.35、V.36、または X.21

Line Speed (bps)
フレーム・リレー・インターフェースの物理データ速度を示します。

Maximum frame size
任意の時間にネットワークを介して送信または受信できる最大フレーム・サイズを示します。

Transmit delay
フレーム間に送信されるフラグ・バイト数を示します。

Lower DTR
WAN 再ルート代替リンクが不要になったときに、ルーターが DTR 信号を下げるかどうかを示します。 DTR 信号が降下すると、モデムは代替リンクの専用回線接続を終了します。ケーブル・タイプが X.21 のときは、Lower DTR は表示されません。

注:

1. FR ダイヤル回線インターフェースの場合は、最大フレーム・サイズのみが表示されます。

lmi フレーム・リレー・インターフェースの論理マネージメントおよび関連構成情報を表示します。

例:

```
list lmi
                        Frame Relay Configuration


  LMI enabled            =  Yes   LMI DLCI                      =    0
  LMI type               =  ANSI  LMI Orphans OK                =  Yes
  CLLM enabled           =   Yes  Timer Ty seconds    = 10

  Protocol broadcast     =   Yes  Congestion monitoring         =  Yes
 Emulate multicast       =   Yes  CIR monitoring                =   No
  Notify FECN Source     =   Yes  Throttle Transmit on FECN     =  Yes

  Data compression       =  Yes   Orphan compression           =   No
  Compression PVC limit  =   10   Number of compression PVCs    =    5 1
  Data encryption        =  Yes  Number of encryption circuits  =    1 2

  PVCs P1 allowed        =    64  Interface down in no PVCs     =   No
  Timer T1 seconds       =    10  Counter N1 increments         =    6
  LMI N2 error threshold =     3  LMI N3 error threshold window =    4
  MIR % of CIR           =    25  IR % Increment                =   25
  IR % Decrement         =    25  DECnet length field          =   No
  Default CIR            = 64000  Default Burst Size            = 64000
  Default Excess Burst   =     0
```

注:

1. この行は、データ圧縮がオン (yes) のときにのみ表示されます。
2. この行は、データ暗号化がオン (yes) のときにのみ表示されます。

LMI enabled
フレーム・リレー・インターフェース上でマネージメント機能が使用可能になっているかどうか (yes または no) を示します。

LMI DLCI
マネージメント回線番号を示します。この番号は LMI タイプを反映します。ANSI および ITU-T/CCITT の場合は 0 で、REV1 の場合は 1023 です。

LMI Type
LMI タイプ (REV1、ANSI、または CCITT) を示します。

LMI Orphans OK
未構成回線を使用できるかどうか (yes または no) を示します。

CLLM Enabled
フレーム・リレー・インターフェース上で CLLM が使用可能かどうかを示します。

Timer Ty seconds
装置が輻輳状態は解消されたものと見なして徐々に PVC を構成された伝送速度に戻す前に、装置が CLLM メッセージまたは BECN を受信せずに経過する必要がある時間の長さを指定します。

Protocol Broadcast
IP RIP のようなプロトコルがフレーム・リレー・インターフェースを介して機能できるかどうか (yes または no) を示します。

Emulate multicast
各アクティブ PVC 上のマルチキャスト・エミュレーション機能が使用可能かどうか (yes または no) を示します。

Congestion Monitoring
ネットワーク輻輳に対応する輻輳監視機能が使用可能かどうか (yes または no) を示します。

CIR monitoring
伝送速度を強制する回線監視機能が使用可能かどうか (yes または no) を示します。

Notify FECN Source
この装置が、FECN ビットがセットされた受信パケットの発信元の装置に最初に送るパケットに BECN ビットをセットするかどうかを示します。

Throttle Transmit on FECN
この装置が、FECN ビットがオンにセットされているパケットに応答して、パケットの転送を*減速* するかどうかを示します。

Data compression
このインターフェースではデータ圧縮が使用可能にされているかどうかを示します。

Data encryption
このインターフェースではデータ暗号化が使用可能にされているかどうかを示します。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Orphan compression
このインターフェース上のオーファン回線で、データ圧縮が使用可能かどうかを示します。

注: オーファン回線上の圧縮を使用可能にすると、装置上のネイティブ PVC が利用可能な圧縮コンテキストの数が減ります。

Compression PVC limit
データ圧縮に参加できる PVC の最大数を示します。

Number of compression PVCs
データ圧縮を行っている現行の PVC 数を示します。

PVCs P1 allowed
このインターフェースで使用できる PVC の数を示します。

Timer T1 seconds
フレーム・リレー・インターフェースがフレーム・リレー・スイッチ LMI エンティティーとシーケンス番号交換を行う頻度を示します。

Counter N1 increments
完全な LMI 状態照会を実行する前に満了する必要がある T1 タイマー間隔の回数を示します。

LMI N2 error threshold
N3 ウィンドウ内で発生した、フレーム・リレー・インターフェースのリセットの原因になる管理イベント誤りの数を示します。

LMI N3 error threshold window
N2 誤り限界値を測定するのに使用される、監視された管理イベントの数を示します。

MIR % of CIR
CIR の比率として表される最小 IR

IR % Increment
最大 IR に達するまで、ルーターが BECN のないフレームを受信するたびに IR を増分する比率

IR % Decrement
最小 IR に達するまで、ルーターが BECN を含むフレームを受信するたびに IR を減分する比率

Default CIR
このインターフェース上の PVC のデフォルト値として使用される認定情報速度 (ビット/秒)

Default Burst Size
このインターフェース上の PVC のデフォルト値として使用される認定バースト・サイズ (ビット数)

Default Excess Burst Size
このインターフェース上の PVC のデフォルト値として使用される超過バースト・サイズ (ビット数)

permanent-virtual-circuits
フレーム・リレー・インターフェース上のすべての構成済み PVC を表示します。

例:

```
FR Config>li perm

  Maximum PVCs allowable =      64
  Total PVCs configured  =       7
```

```
            Circuit              Circuit   Circuit   CIR     Burst  Excess
             Name                Number     Type    in bps   Size   Burst
 -------------------------------- ------- ---------- ------- ------- -------
 cir16                              16 $@#Permanent   64000   64000       0
 cir244                            244   #Permanent   64000   64000       0
 cir33                              33    #Permanent   64000   64000       0
 cir1005                           1005  #Permanent   64000   64000       0
 cir55                              55    #Permanent   64000   64000       0
 cir22                              22   @Permanent   64000   64000       0
 cir66                              66  @*Permanent   64000   64000       0

* = circuit is required
# = circuit is required and belongs to a Required PVC group
@ = circuit is data compression capable
$ = circuit is data encryption capable
```

Maximum PVCs allowable
このインターフェースに存在できる PVC の数を示します。この数には、**add permanent-virtual-circuit** コマンドを使用して追加された PVC、および管理インターフェースを通して動的に確認された PVC も含まれます。

Total PVCs configured
このインターフェースに現在構成されている PVC の合計数を示します。

Circuit Name
構成された PVC の ASCII 名を示します。

Circuit Number
現在構成されている PVC の番号を示します。

Circuit Type
現在構成されているバーチャル・サーキットのタイプを示します。フレーム・リレーのこのリリースでは、パーマネント・バーチャル・サーキットのみがサポートされます。

Committed Information Rate
ネットワークで合意されている、通常の条件下でのデータ転送の情報速度を示します。

Committed Burst Size
ネットワークで合意されている、(認定バースト・サイズ/CIR) 秒数に等しい測定期間中に送達できる最大データ量 (ビット数)。

Excess Burst Size
(認定バースト・サイズ/CIR) 秒数に等しい測定期間中にネットワークが送達を試みることができる、認定バースト・サイズを超過した未認定データの最大量 (ビット数)。

pvc-groups
フレーム・リレー・インターフェース上のすべての必須 PVC グループを表示します。

例:

```
list pvc-groups
    Required PVC group = group1

          Circuit # 16
```

protocol-addresses
フレーム・リレー・インターフェースのすべての静的に構成された回線マッピングのプロトコル・アドレスを表示します。

例:

```
list protocol-addresses
                Frame Relay Protocol Address Translations

  Protocol Type              Protocol Address      Circuit Number
  -------------              ----------------      --------------
       IP                     125.2.29.4                21
       IPX                    000000004503
16
```

Protocol Type
インターフェースを介して実行されているプロトコルの名前を表示します。

Protocol Address
回線の相手側の装置のプロトコル・アドレスを表示します。

Circuit Number
プロトコルを扱っている PVC を表示します。

LLC

LLC コマンドは、LLC 構成環境にアクセスするのに使用します。これらの各コマンドの説明は、241ページの『LLC 構成コマンド』 を参照してください。

注: LLC コマンドは、ソフトウェア・ロードに APPN が含まれている場合にのみサポートされます。

構文:

llc

Remove

remove コマンドは、PVC、必須 PVC グループ、または以前に **add** コマンドを使用して追加されたプロトコル・アドレスを削除するのに使用します。

構文:

remove permanent-virtual-circuit . . .
protocol-address
pvc-group

permanent-virtual-circuit *pvc#*

16 ～ 1007 の範囲の構成された PVC を削除します。

注:

1. 圧縮を実行している PVC を削除すると、インターフェースはアクティブ圧縮 PVC のカウントを減らします。このアクションによって圧縮 PVC のカウントが限界以下になる場合、それを知らせるメッセージを受け取ります。
2. 暗号化を実行している PVC を削除すると、インターフェースはアクティブの暗号化 PVC のカウントを減らします。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

protocol-address

構成されたプロトコル・アドレス (静的 ARP エントリー) を削除します。このパラメーターでは、追加するプロトコルのタイプによって、異なる情報を求めるプロンプトが出ます。

例:

```
remove protocol-address
Protocol name or number [IP]?
```

IP プロトコル:

```
IP Address [0.0.0.0]?
Circuit Number [16]?
```

IPX プロトコル:

```
Host Number (in hex)[]?
Circuit Number [16]?
```

AppleTalk フェーズ 2 プロトコル:

```
Network Number (1-65279) []?
Node Number (1-253) []?
Circuit Number [16]?
```

DN プロトコル:

```
Node address [0.0]?
Circuit Number [16]?
```

Protocol name or number

削除するプロトコルの名前または番号を定義します。サポートされないプロトコルを削除しようとすると、システムは誤りメッセージを出します。

```
Unknown protocol name, try again
```

サポートされるプロトコルのリストを見たい場合は、 `Protocol name or number [IP]?` プロンプトで `?` を入力します。

IP Address

リモート IP ホストの 32 ビット・インターネット・アドレスを小数点表記法で定義します。

Host Number

リモート IPX ホストの 48 ビット・ノード・アドレスを定義します。

Network Number

AppleTalk フェーズ 2 ネットワーク番号を定義します。

Node Number

リモート AppleTalk ホストに接続されているインターフェースのノード番号を定義します。

Node address

リモート DECnet ホストの DECnet ノード・アドレスを定義します。ノード・アドレスは *x,y* フォーマットで構成します。ただし、*x* は 6 ビットのエリア・アドレスで、*y* は 10 ビットのノード番号です。

Circuit Number
プロトコルを実行する PVC を 16 ～ 1007 の範囲で定義します。

pvc-group *groupname*

構成された PVC グループを名前によって削除します。グループは、メンバー回線をもっていない場合にのみ削除されます。

例:remove pvc-group PVC group name [IP]?

Set

set コマンドは、フレーム・リレー・プロトコルを実行するインターフェースを構成するのに使用します。

Set コマンドの考慮事項

構成を始める前に、2 つのパラメーター (n2-parameter と n3-parameter) について説明しておきます。 n2-parameter は、管理イベントの誤り限界値を設定し、n3-parameter は、イベント・ウィンドウで監視されるイベントの数を設定します。イベント・ウィンドウ内の管理誤りの数が n2 に等しくなると、フレーム・リレー・インターフェースはリセットされます。たとえば、次のように入力します。

set n3-parameter 4
set n2-parameter 3

ここでは、ウィンドウ・サイズは 4 (n3 = 4)、誤り限界値は 3 (n2 = 3) に設定されました。これは、システムは 4 つの管理イベントを監視して、いずれかに誤りがないかチェックします。誤りのあるイベントの数が 3 (n2 parameter) に等しくなると、フレーム・リレー・インターフェースはリセットされ、ネットワークの状態はネットワークがダウン と見なされます。

ネットワークの状態がネットワークがアップ と見なされるためには、状態が変更される前の、ウィンドウ内の誤りのあるイベント数が n2 より少なくなければなりません。

構文:

set
- cable*
- cir-defaults
- clocking*
- encoding*
- frame-size
- idle . . .*
- ir-adjustment . . .
- line-speed*
- lmi-type n1-parameter
- n2-parameter
- n3-parameter

p1-parameter

t1-parameter

transmit-delay . . .*

ty-parameter

*** Note:** 後ろに * が付いているコマンドは、FR ダイヤル回線インターフェースでは利用不能です。

cable *physical-interface-link-type data-connection-type*
ネットワークの物理リンクのケーブル・タイプを設定します。

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときに使用します。 DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときに使用します。

利用可能なオプションを以下に示します。

物理インターフェース・リンク・タイプ	データ接続タイプ
EIA 232 (RS-232)	DTE, DCE
V35	DTE, DCE
V36	DTE
X21	DTE, DCE

cir-defaults
回線輻輳パラメーターのデフォルト値を設定します。パラメーターを以下に示します。

cir *cir* のデフォルト値を、フレーム・リレー・ネットワークの提供者によって提供された値に設定します。

有効値: 0 または 300 ～ 204 800 bps

デフォルト値: 64 000

bc *bc* のデフォルト値を、フレーム・リレー・ネットワークの提供者によって提供された値に設定します。

有効値: 420ページの『認定バースト (Bc) サイズ』 を参照してください。

デフォルト値: 64 000

be *be* のデフォルト値を、フレーム・リレー・ネットワークの提供者によって提供された値に設定します。

有効値: 420ページの『超過バースト (Be) サイズ』 を参照してください。

デフォルト値: 0

例:

```
FR 6 config>
set cir-default
Default Committed Information Rate (CIR) in bps [64000]? 48000
Default Committed Burst Size (Bc) in bits [64000]? 40000
Default Excess Burst Size (Be) in bits [0]? 52000
```

clocking [external or internal]
モデムまたは DSU に接続する場合は、クロックを外部として構成します。別の DTE 装置に直接接続する場合は、DCE ケーブルを使用し、クロックを内

部として設定します。内部クロックの場合は、 **set line-speed**コマンドを入力して、クロック速度を 2400 ～ 2048000 bps の間に構成する必要があります。

外部クロックの場合、最大回線速度は 6 312 000 bps です。

encoding [NRZ or NRZI]

HDLC 符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) に設定します。ほとんどの構成では NRZ が使用され、これがデフォルト値です。

frame-size *#*

インターフェース上で送受信されるフレームのネットワーク・レイヤー部分の最大サイズを設定します。この最大サイズには、図 39-4 に示されている 2 バイトの DLCI アドレスとユーザー・データが含まれています。構成するサイズは、フレーム・リレー・スイッチおよびフレーム・リレー・ネットワークの他の FR DTE によってサポートされる最大フレーム・サイズに矛盾しない値でなければなりません。値は 262 ～ 8190 です。デフォルト値は 2048 です。構成されたフレーム・サイズには、DLCI アドレスと FR RFC 1490 マルチプロトコル・カプセル化ヘッダーが含まれているので、転送できる最大プロトコル・パケット・サイズは、構成されたフレーム・サイズより小さくなり、その大きさはプロトコルによって異なります。下の表は、インターフェース上で送受信できる最大プロトコル・パケット・サイズを算定するために、構成されたフレーム・サイズから差し引く必要があるバイト数を示しています。

IP	4 バイト
IPX	10 バイト
Appletalk フェーズ 2	10 バイト
DECnet フェーズ IV (DNA IV)	12 バイト
Banyan Vines	10 バイト
OSI	10 バイト
ブリッジング	10 バイト
APPN	58 バイト (注を参照)

注: FR ヘッダーのバイト数の他に T/R MAC アドレス・ヘッダーと LLC ヘッダーも追加された、APPN BAN の最悪のケースを想定しています。

FR データ暗号化が使用可能の場合には、さらに最大 12 バイトを差し引く必要があります。

idle [flag or mark]

HDLC フレームの伝送アイドル状態を設定します。デフォルト値は **flag** で、これはフレーム間に連続フラグ (7E 16 進数) を提供します。マーク・オプションは、フレーム間の伝送路をマーキング状態 (OFF, 1) にします。マーク・アイドルでは、フレーム間で送信 LED が暗転します。フラグ・アイドルは、フレーム間で送信 LED を部分的にオンにします。

ir-adjustment *increment-% decrement-% minimum-IR*

最小情報速度 (IR) と、ネットワークの輻輳に応じて IR を増分および減分する比率を設定します。

最小 IR (CIR の比率で表す) は、情報速度の下限です。最小比率は 1 で、最大比率は 100 です。 デフォルト値は 25 です。

ネットワークの輻輳が解消されると、情報速度は、最大情報速度に達するまで、IR 調整増分比率ずつ徐々に増分されます。最小比率は 1 で、最大比率は 100 です。デフォルト値は 12 です。

ネットワークの輻輳が発生すると、情報速度は、最小情報速度に達するまで、BECN が入ったフレームを受信するたびに IR 調整減分比率ずつ減分されます。最小比率は 1 で、最大比率は 100 です。デフォルト値は 25 です。

例:

```
set ir-adjustment
    IR adjustment % increment [12]?
    IR adjustment % decrement [25]?
    Minimum IR as % of CIR [25]?
```

line-speed *rate*

内部クロックの場合、このコマンドは送信および受信クロック回線の速度を指定します。範囲は 2400 ～ 2 048 000 bps です。

外部クロックの場合、このコマンドはハードウェア (つまり、回線の実際の速度) には影響を与えませんが、一部のプロトコル (IPX など) がルーティング・コスト・パラメーターを決めるのに使用する速度を設定します。輻輳監視も、構成された回線速度を使用して、最大情報速度を決めます。そのため、この速度は実際の回線速度に一致するように設定することをお勧めします。速度が構成されていない場合、プロトコルおよび輻輳監視は 1 000 000 bps の速度を想定します。

注:

1. 外部クロックを使用している場合、最大回線速度は 6 312 000 です。
2. 内部クロックを使用している場合、最大回線速度は 2 048 000 です。

lmi-type [rev1 or ansi or ccitt]

インターフェースのマネージメント・タイプを設定します。フレーム・リレー・マネージメントの設定についての詳細は、426ページの『フレーム・リレー・マネージメントの使用可能化』 を参照してください。デフォルトでは、タイプ **ansi** が使用可能になります。

表 57. フレーム・リレー・マネージメント・オプション

コマンド	マネージメント・タイプ	説明
set	lmi-type rev1	LMI 改訂 1 (Stratacom のフレーム・リレー・インターフェース仕様) に準拠します。
set	lmi-type ansi	ANSI T1.617 ISDN-DSS1-Signalling Specification for Frame Relay Bearer Service (付録 D とも呼ばれます) に準拠します。
set	lmi-type ccitt	ITU-T/CCITT 勧告 Q.933 の付録 A - DSS1 Signalling Specification for Frame Mode Basic Call Control に準拠します。

n1-parameter *count*

完全な PVC 状態照会を実行する前に満了する必要がある T1 タイマー間隔の回数を構成します。 *Count* は、1 ～ 255 の範囲の間隔です。デフォルト値は 6 です。

n2-parameter *max#*

フレーム・リレー・インターフェースがリセットされる前に、n3-parameter によって監視される管理イベント・ウィンドウで発生しても構わない誤りの数を構成します。 Max# は、1 〜 10 の範囲の数です。デフォルト値は 3 です。このパラメーターは、n3-parameter の値以下でなければなりません。そうでない場合は、誤りメッセージを受け取ります。

n3-parameter *max#*

n2-parameter を測定するのに使用される、監視された管理イベントの数を構成します。 Max# は、1 〜 10 の範囲の数です。デフォルト値は 4 です。

p1-parameter *max#*

フレーム・リレー・インターフェースによってサポートされる PVC の最大数を構成します。これには、アクティブ、非アクティブ、除去済み、および構成済み PVC が含まれます。 Max# は、0 〜 992 の範囲の数です。デフォルト値は 64 です。 0 (ゼロ) は、インターフェースが PVC をサポートしないことを意味します。

t1-parameter *time*

フレーム・リレー・マネージメントとのシーケンス番号交換の間の間隔 (秒数) を構成します。マネージメントの T2 タイマーは、エンド・ステーションがマネージャーとのシーケンス番号交換を要求するのに許される間隔です。 T1 間隔は、ネットワークの T2 間隔より小さくなければなりません。 *Time* は、5 〜 30 の範囲の値です。デフォルト値は 10 です。

transmit-delay *#*

転送されるパケット間に遅延を挿入することができます。このコマンドの目的は、シリアル・ラインを減速して、相手側の旧型で低速のシリアル装置に整合させることです。伝送路間でシリアル・ライン・ハロー・パケットが失われるのも防止できます。 # は、 0 〜 15 個の余剰フラグです。デフォルト値はゼロ (0) です。このパラメーターを設定すると、送信フレーム相互間に 0 〜 15 個の余剰フラグが挿入されます。 表58 は、シリアル・インターフェースの単位と範囲を示しています。

表 58. 2210 シリアル・インターフェースの転送遅延の単位と範囲

単位	最小	最大
余剰フラグ	0	15

ty-parameter *time*

装置が CLLM メッセージの受信によって示された既存の輻輳状態が解消されたと見なす前に経過する必要があるインターバルを構成します。このタイマーが満了する前に、装置が CLLM メッセージを受信した場合、装置はこのタイマーをリセットします。

有効値: 5 〜 30 秒

デフォルト値: 11 秒

フレーム・リレー監視プロンプトへのアクセス

フレーム・リレー動作コマンドにアクセスし、ルーター上でフレーム・リレーを監視するには、次のステップを実行します。

1. OPCON プロンプト (*) で **talk 5** と入力する。
2. GWCON プロンプト (+) で、**interface** コマンドを入力して、ルーター上に構成されているインターフェースのリストを表示する。
3. **network** コマンドに続けて、フレーム・リレー・インターフェースのネットワーク番号を入力する。たとえば、次のように入力します。

```
+ net 2
Frame Relay Monitoring
FR 2 >
```

フレーム・リレー監視コマンド

この節では、フレーム・リレー監視コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドは、データベースから情報を収集するのに使用します。 表59 は、コマンドを示しています。

表 59. フレーム・リレー監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Clear	フレーム・リレー・インターフェースに関する統計情報を消去します。
Disable	フレーム・リレー・インターフェース上の CIR 監視および輻輳監視を使用不可にします。
Enable	フレーム・リレー・インターフェース上の CIR 監視および輻輳監視を使用可能にします。
List	データ・リンク・レイヤーおよびフレーム・リレー・マネージメントに特有の統計を表示します。
LLC	LLC 監視プロンプトを表示します。
Set	フレーム・リレー PVC の CIR、認定バースト・サイズ、および超過バースト・サイズを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

注: この節における *回線番号* および *PVC* という用語は、*データ・リンク回線識別子 (DLCI)* という用語と同等です。

Clear

clear コマンドは、フレーム・リレー・インターフェースに関するすべての統計を除去するのに使用します。

注: 統計は、OPCON **clear** コマンドを使用して除去することもできます。

構文:

clear

Disable

disable コマンドは、フレーム・リレー CIR 監視機能および輻輳監視機能を使用不可にするのに使用します。

disable コマンドは、ルーター構成を動的に変更します。これらの変更は、ルーターをリスタートすると失われます。

構文:

disable

- cir-monitor
- cllm
- congestion-monitor
- notify-fecn-source
- throttle-transmit-on-fecn

Enable

enable コマンドは、フレーム・リレー CIR 監視機能および輻輳監視機能を使用可能にするのに使用します。

enable コマンドは、ルーター構成を動的に変更します。これらの変更は、ルーターをリスタートすると失われます。

構文:

enable

- cir-monitor
- cllm
- congestion-monitor
- notify-fecn-source
- throttle-transmit-on-fecn

List

list コマンドは、データ・リンク・レイヤーおよびフレーム・リレー・インターフェースに特有の統計を表示するのに使用します。

構文:

list

- all
- circuit . . .
- lmi
- permanent-virtual-circuits
- pvc-groups

all フレーム・リレー・インターフェースの回線、マネージメント、および PVC 統計を表示します。このコマンドで表示される出力は、**list lmi** コマンドと **list permanent-virtual-circuit** コマンドの組み合わせです。

circuit *pvc#*

指定された PVC (pvc#) の詳細 PVC 構成および統計情報を表示します。

例:

```
list circuit 347

 Circuit name = Valencia

 Circuit state        =    Active  Circuit is orphan   =     No
 Frames transmitted   =         0  Bytes transmitted   =      0
 Frames received      =         0  Bytes received      =      0
 Total FECNs          =         0  Total BECNs         =      0
 Times congested      =         0  Times Inactive      =      0
 CIR in bits/second   =     64000  Potential Info Rate =  56000
 Committed Burst (BC) =      1200  Excess Burst (Be)   =  54800
 Minimum Info Rate    =     16000  Maximum Info Rate   =  64000
 Required             =       Yes  PVC group name      = group1

 Compression capable  =       Yes  Operational         =    Yes
 R-Rs received        =         0  R-Rs transmitted    =      0
 R-As received        =         0  R-As transmitted    =      0
 R-R mode discards    =         0  Enlarged frames     =      0
 Decompress discards  =         0  Compression errors  =      0
 Compression ratio    = 1.72 to 1  Decompression ratio = 1.10 to 1

 Encryption capable   =        Yes  Operational         =          Yes
 Encryption errors    =          0  Decryption errors   =            0
 Rcv error discards   =          0

 Current number of xmit frames queued                  =      0
 Xmit frames dropped due to queue overflow             =      0
```

Circuit state

回線の状態 (非アクティブ、アクティブ、または輻輳) を示します。非アクティブ (Inactive) は、フレーム・リレー・インターフェースがダウンしているか、もしくはフレーム・リレー・マネージメント・エンティティーが回線がアクティブであることをフレーム・リレー・プロトコルに通知しなかったために、トラフィックのために回線を利用できないことを示しています。アクティブ (Active) は、データを転送中であることを示しています。輻輳 (Congested) は、データ・フローが制御されていることを示しています。

Circuit is orphan

その回線が LMI マネージメントを通して確認された未構成の回線であるかどうかを示します。

Frames/Bytes transmitted

この PVC が送信したフレーム数およびバイト数を示します。

Frames/Bytes received

この PVC が受信したフレーム数およびバイト数を示します。

Total FECNS

この PVC がインバウンドまたはダウンストリームの輻輳を通知された回数を示します。

Total BECNS

この PVC がアウトバウンドまたはアップストリームの輻輳を通知された回数を示します。

Times congested

この PVC が輻輳状態になった回数を示します。

Times inactive

この PVC が運用不可になった回数を示します。

CIR in bits/sec
300 bps ～ 2048000 bps の間の PVC の情報速度を示します。値 0 もサポートされます。

Potential Info Rate
回線上のデータ転送の現行の最大速度 (ビット/秒) を示します。実際のデータ速度は、待ち行列の長さおよび回線に対応付けられている優先順位によって決まります。

このフィールドの値が 『Line Speed』 の場合は、このインターフェースに対して回線速度が構成されていなかったり、間違って構成されていても、最大データ速度は実際の回線速度になります。

Committed Burst (BC)
算定された*時間間隔* (Tc) の間に送達することをネットワークが認定しているデータの最大量 (ビット数)。 (Tc=Bc/CIR。)

Excess Burst (Be)
この時間間隔 (Tc) の間に、ルーターが PVC 上で Bc を超過して転送できる未認定データの最大量

Minimum Info Rate
最小情報速度。輻輳を通知されたときにルーターがそこまで減速する PVC の最小データ速度

Maximum Info Rate
最大情報速度。ルーターが PVC 上で転送する最大データ速度

Required
Yes または No。yes の場合、PVC は必須 PVC です。

PVC group name
PVC が必須 PVC グループのメンバーの場合、その名前がここに表示されます。そうでない場合は 『Unassigned』 が表示されます。

Compression capable
回線がデータ・パケットを圧縮できるかどうかを示します。

Operational
回線上で圧縮がアクティブかどうかを示します。これが yes の場合、このリンク上でデータが圧縮中です。

R-Rs received
同位解凍機能によって送信されたリセット要求パケットの数を示します。同位解凍機能は、同位圧縮機能との同期が外れたことを検出するたびに、リセット要求を送信します。この数が急激に増える場合は、この回線上のパケットは失われているか、破壊されています。

R-Rs transmitted
回線上で圧縮が開始された以降に送信されたリセット要求パケットの数を示します。この数が急激に増える場合は、この回線上のパケットは失われているか、破壊されています。

R-As received
リセット要求への応答として受信されたリセット確認の数を示しま

す。圧縮機能は、圧縮ヒストリーをリセットしたことを知らせるときも、このパケットを送信します。

R-As transmitted
これは、同位に送信されたリセット確認の数です。

R-R mode discards
R-R を送信した後 R-A を待っている間に廃棄された圧縮データ・フレームの数を示します。

Enlarged frames
これは圧縮できなかったフレームの数です。通常は、圧縮不能なフレームは、圧縮しない形で特殊な圧縮フレーム・タイプに入れて送信され、圧縮機能と解凍機能の同期が保たれます。

Decompress discards
解凍誤りのために廃棄された圧縮フレームの数を示します。

Compression errors
圧縮されない形で転送された圧縮誤りのあるフレームの数を示します。

Compression ratio
圧縮機能の概略の効率を示します。

Decompression ratio
解凍機能の概略の効率を示します。

Encryption capable
この回線で暗号化が使用可能かどうかを示します。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Operational
回線上で暗号化がアクティブかどうかを示します。これが yes の場合、このリンク上でデータが暗号化中です。

Encryption errors
暗号化誤りが生じたフレームの数を示します。

Decryption errors
復号誤りが生じたフレームの数を示します。

Rcv error discards
受信に問題があったために廃棄された圧縮フレームの数を示します。

Current number of xmit frames queued
FR によってこの回線のために現在待ち行列化されているフレームの数を示します。これらのフレームは、このインターフェースのシリアル装置ハンドラー送信待ち行列上のスペースが利用可能になるのを待っています。

Xmit frames dropped due to queue overflow
出力待ち行列オーバーフローのためにこの PVC に送信できなかったフレームの数を示します。

lmi フレーム・リレー・インターフェース上の論理マネージメントに関する統計を表示します。

例:

```
list lmi

  Management Status:
  ------------------
    LMI enabled   =   Yes  LMI DLCI         = 1023
    LMI type      =  REV1  LMI Orphans OK   =  Yes
    CLLM enabled  =   Yes  Timer Ty seconds =   11
    Last CLLM cause code = Network congestion - short term (0x02)
    Protocol broadcast   =     Yes  Congestion monitoring     =   Yes
    Emulate multicast    =     Yes  CIR monitoring            =    No
    Notify FECN source   =      No  Throttle transmit on FECN  =   No
    PVCs P1 allowed      =      64  Interface down if no PVCs =    No
    Line speed (bps)     =   64000  Maximum Frame size        =  2048
    Timer T1 seconds     =      10  Counter N1 increments     =     6
    LMI N2 threshold     =       3  LMI N3 threshold window   =     4
    MIR % of CIr         =      25  IR % Increment            =    12
    IR % Decrement       =      25  DECnet length field       =    No
    Default CIR          =   65636  Default burst size        = 64000
    Default Excess Burst =       0

    Current receive sequence  =  0
    Current transmit sequence =  0
    Total status enquires     =  0    Total status responses    =    0
    Total sequence requests   =  0    Total responses           =    0

    Data compression enabled  =  Yes  Orphan compression              =   No
    Compression PVC limit     = None  Active compression PVCs   =    1

    Data encryption enabled   =  Yes  Active encryption circuits =    1

  PVC Status:
  -----------
    Total allowed  =      64  Total configured  =       3
    Total active   =       0  Total congested   =       0
    Total left net =       0  Total join net    =       0
```

Management Status:

LMI enabled
フレーム・リレー・マネージメントがアクティブかどうか (yes または no) を示します。

LMI DLCI
マネージメント回線番号を示します。この番号は 0 (ANSI デフォルトまたは ITU-T/CCITT) または 1023 (中間 LMI REV1) です。

LMI type
使用されているフレーム・リレー・マネージメントのタイプ (ANSI、ITU-T/CCITT、または LMI 改訂 1) を示します。

LMI orphans OK
フレーム・リレー・マネージメントから確認されたすべての未構成回線を使用できるかどうか (yes または no) を示します。

CLLM enabled
CLLM フレームを受信したときに、この回線が減速するかどうかを指定します。

Timer Ty seconds
CLLM Ty タイマーの値を示します。このフィールドは、CLLM が使用可能のときにのみ表示されます。

Last CLLM cause code
受信した最後の CLLM メッセージに示されていた輻輳の原因符号を示すか、あるいは CLLM メッセージを受信しなかった場合は ***None*** が示されます。このフィールドは、CLLM が使用可能のときにのみ表示されます。

Protocol broadcast
IP RIP のようなプロトコルがフレーム・リレー・インターフェースを介して動作できるかどうかを示します。

Congestion monitoring
ネットワーク輻輳に対応する輻輳監視機能が使用可能かどうか (yes または no) を示します。

Emulate multicast
各アクティブ PVC 上のマルチキャスト・エミュレーション機能が使用可能かどうか (yes または no) を示します。

CIR monitoring
伝送速度を強制する回線監視機能が使用可能かどうか (yes または no) を示します。

PVCs P1 allowed
このインターフェースで使用できる PVC の数を示します。この数は、インターフェース上でサポートできるアクティブ、輻輳、非アクティブ、および除去された PVC の最大数です。

Interface down if no PVCs
アクティブ PVC が存在しないときに、ルーターがインターフェースを利用不能と見なすかどうかを示します。

Line speed (bps)
フレーム・リレー・インターフェースの構成されたデータ速度を示します。

Timer T1 seconds
フレーム・リレー・インターフェースがフレーム・リレー・スイッチ LMI エンティティーとシーケンス番号交換を行う頻度を示します。

Counter N1 increments
完全な LMI 状態照会を実行する前に満了する必要がある T1 タイマー間隔の回数を示します。

LMI N2 error threshold
N3 ウィンドウ内で発生した、フレーム・リレー・インターフェースのリセットの原因になる管理イベント誤りの数を示します。

LMI N3 error threshold window
N2 誤り限界値を測定するのに使用される、監視された管理イベントの数を示します。

MIR % of CIR
CIR の比率として表される最小 IR。

IR % Increment
最大 IR に達するまで、ルーターが BECN のないフレームを受信するたびに IR を増分する比率

IR % Decrement
最小 IR に達するまで、ルーターが BECN を含むフレームを受信するたびに IR を減分する比率。

DECnet length field
DECnet 長さフィールド機能が使用可能かどうかを示します。一部のフレーム・リレー DECnet フェーズ IV 実現では、フレーム・リレー・マルチプロトコル・カプセル化ヘッダーと DECnet パケットの間に長さフィールドが必要です。 DECnet 長さフィールド機能が使用可能の場合は、長さフィールドが挿入されます。

Default CIR
このインターフェースのデフォルト CIR を指定します。

Default Burst Size
このインターフェースのデフォルト・バースト・サイズを指定します。

Default Excess CIR
このインターフェースのデフォルト超過バースト・サイズを指定します。

Current receive sequence
フレーム・リレー・インターフェースがフレーム・リレー管理エンティティーから受信した現行の受信シーケンス番号を示します。

Current transmit sequence
フレーム・リレー・インターフェースがフレーム・リレー管理エンティティーに送信した現行の送信シーケンス番号を示します。

Total status enquiries
フレーム・リレー・インターフェースがフレーム・リレー管理エンティティーに行った状態照会の合計数を示します。

Total status responses
フレーム・リレー・インターフェースが、状態照会への応答としてフレーム・リレー管理エンティティーから受け取ったレスポンスの合計数を示します。

Total sequence requests
フレーム・リレー・インターフェースがフレーム・リレー管理エンティティーに送信したシーケンス番号要求の合計数を示します。

Total responses
フレーム・リレー・インターフェースがフレーム・リレー管理エンティティーから受信したシーケンス番号レスポンスの合計数を示します。

Data compression enabled
このインターフェース上でデータ圧縮が使用可能かどうかを示します。

Orphan compression
このインターフェース上のオーファン回線で、データ圧縮が使用可能かどうかを示します。

注: オーファン回線上の圧縮を使用可能にすると、装置上のネイティブ PVC が利用可能な圧縮コンテキストの数が減ります。

Compression PVC limit
このインターフェース上でデータを圧縮できる PVC の最大数を指定します。

Active compression PVCs
このインターフェース上で現在データを圧縮中の PVC 数を指定します。

Data encryption enabled
このインターフェース上のデータ暗号化が使用可能かどうかを示します。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Active encryption circuits
現在データを暗号化している PVC の数を示します。

PVC Status:

Total allowed
このインターフェースでの使用状態がアクティブ、輻輳、除去、または非アクティブであることが許容される PVC の数 (オーファンを含む) を示します。

Total configured
このインターフェースに現在構成されている PVC の合計数を示します。

Total active
このインターフェース上のアクティブ PVC の数を示します。

Total congested
ネットワーク内の輻輳のために減速されている PVC の数を示します。

Total left net
ネットワークから除去された PVC の数を示します。

Total join net
ネットワークに追加された PVC の合計数を示します。

permanent-virtual-circuit
フレーム・リレー・インターフェース上に構成されているすべての PVC の一般リンク・レイヤー統計および構成情報を表示します。

例:

```
list permanent-virtual-circuit
                              Orphan   Type/    Frames       Frames
 Circuit#     Circuit Name    Circuit  State  Transmitted   Received
 --------  ----------------   -------  -----  -----------   ---------
     16    Valencia              No   %@*P/A            2          1
     17    Raleigh               No    @#P/A           15         14
     18    Boston                No    &#P/A            0          0
     19    Orlando               No     *P/A            0          0
     20    Port Royal            No     $P/A            0          0
     21    New York              No     @P/A            2          0

    A - Active     I - Inactive   R - Removed   P - Permanent  C - Congested
    * - Required                  # - Required and belongs to a PVC group
    @ - Data compression capable but not operational
    & - Data compression capable and operational
    $ - Data encryption capable but not operational
    % - Data encryption capable and operational
```

Circuit#

PVC の番号を示します。

Circuit Name

回線の名前の ASCII ストリングです。

Orphan Circuit

PVC が未構成回線かどうか (yes または no) を示します。

Type/State

回線の状態、A (アクティブ)、I (非アクティブ)、 P (固定)、C (輻輳)、または R (除去) を示します。

Frames Transmitted

この PVC が送信したフレームの数を示します。

Frames Received

この PVC が受信したフレームの数を示します。

pvc-groups

すべての必須 PVC グループの必須 PVC グループ情報を表示します。各グループは、グループ名、グループ内の回線、および各回線の状態 (アクティブ、非アクティブ、または除去) からなっています。

例:

```
list pvc-groups
Group name               Circuits in group    Circuit status
----------               -----------------    --------------

group1                             16             active
                                   44             inactive
                                  240             removed
```

LLC

LLC コマンドは、LLC 監視プロンプトにアクセスするのに使用します。 LLC コマンドは、この新たに表示されたプロンプトで入力します。これらの各コマンドの説明は、245ページの『LLC 監視コマンド』 を参照してください。

構文:

llc

注: LLC コマンドは、ソフトウェア・ロードに APPN が含まれている場合にのみサポートされます。

Set

set コマンドは、指定された PVC の認定情報速度 (CIR)、認定バースト速度、および超過バースト速度の値を設定するのに使用します。 IR 調整比率の値も設定できます。

このコマンドで行った変更は、構成データには影響を与えず、ルーターがリスタートされるまでしか有効でありません。

構文:

set circuit . . .

ir-adjustment . . .

circuit *circuit# cirvol bcval beval*

指定された PVC の認定情報速度 (CIR)、認定バースト速度、および超過バースト速度の値を設定します。

例:

```
set circuit
Circuit number [16]?
Committed Information Rate (CIR) in bps [1200]?
Committed Burst Size (Bc) in bits [1200]?
Excess Burst Size (Be) in bits [56000]?
```

Circuit Number

16 ～ 1007 の範囲で回線番号を示します。

Committed Information Rate

認定情報速度 (CIR) を示します。 CIR は、0 または 300 bps ～ 2048000 bps の範囲の値です。デフォルトは 64000 bps です。詳しくは、419ページの『認定情報速度 (CIR)』 を参照してください。

Committed Burst Size

ネットワークで合意されている、認定バースト (Bc) サイズ/CIR 秒数に相当する測定期間に送達できる最大データ量 (ビット)。範囲は 300 ～ 2048000 ビットです。デフォルト値は 64000 ビットです。

注: CIR が 0 として構成されている場合、認定バースト・サイズも 0 に設定され、値の入力を求めるプロンプトは出ません。詳しくは、420ページの『認定バースト (Bc) サイズ』 を参照してください。

Excess Burst Size

(認定バースト・サイズ/CIR) 秒数に相当する測定期間にネットワークが送達を試みることができる、認定バースト・サイズを超過する未認定データの最大量 (ビット数)。範囲は 0 ～ 2048000 ビットです。デフォルト値は 0 です。詳しくは、420ページの『超過バースト (Be) サイズ』 を参照してください。

ir-adjustment *increment-% decrement-% minimum-IR*

最小情報速度 (IR) と、ネットワーク輻輳に応じて IR を増分および減分する比率を設定します。

最小 IR (CIR の比率で表す) は、情報速度の下限です。最小比率は 1 で、最大比率は 100 です。 デフォルト値は 25 です。

ネットワークの輻輳が解消されると、情報速度は、最大情報速度に達するまで、IR 調整増分比率ずつ徐々に増分されます。最小比率は 1 で、最大比率は 100 です。デフォルト値は 12 です。

ネットワークの輻輳が発生すると、情報速度は、最小情報速度に達するまで、BECN が入ったフレームを受信するたびに IR 調整減分比率ずつ減分されます。最小比率は 1 で、最大比率は 100 です。デフォルト値は 25 です。

例:

```
set ir-adjustment
    IR adjustment % increment [12]?
    IR adjustment % decrement [25]?
    Minimum IR as % of CIR [25]?
```

フレーム・リレー・インターフェースおよび GWCON インターフェース・コマンド

フレーム・リレー・インターフェースには監視用の監視プロセスがありますが、GWCON 環境から **interface** コマンドを使用すれば、ルーターも導入済みインターフェースの完全な統計を表示します。 (**interface** コマンドについての詳細は、133ページの『第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』 を参照してください。)

フレーム・リレー・インターフェースについて表示される統計

フレーム・リレー・インターフェースに対して GWCON 環境から **interface** コマンドを実行すると、次のような統計が表示されます。

```
+interface 1
                                Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
1  1   FR/0         81620   5D          1          0            0

  Frame Relay MAC/data-link on SCC Serial Line interface

  Adapter cable:               V.35 DTE  RISC Microcode Revision:
    1

   V.24 circuit: 105 106 107 108 109 125 141
   Nicknames:    RTS CTS DSR DTR DCD RI  LL
   PUB 41450:    CA  CB  CC  CD  CF  CE
   State:        ON  ON  ON  ON  ON  OFF OFF

  Line speed:              unknown
  Last port reset:         5 hours, 8 minutes, 11 seconds ago

 Input frame errors:
   CRC error                          0   alignment (byte length)
   missed frame                       0   too long (>  2062 bytes) 0
   aborted frame                      0   DMA/FIFO overrun         0
   L & F bits not set                 0
  Output frame counters:
   DMA/FIFO underrun errors           0   Output aborts sent
0
```

Nt 初期構成時にソフトウェアによって割り当てられたインターフェース番号を示します。

Nt' 初期構成時にソフトウェアによって割り当てられたインターフェース番号を示します。

注: FR ダイヤル回線インターフェースの場合、Nt' は Nt と異なります。 Nt' は、ダイヤル回線が実行されている基本インターフェース (ISDN) を示します。

Interface
インターフェースのタイプとそのインスタンス番号を示します。フレーム・リレーは FR 名を持っています。

CSR フレーム・リレー・インターフェースの制御状況レジスターのメモリー・ロケーションを示します。

Vec フレーム・リレー・インターフェースのベクトル番号を示します。

Self-test Passed
フレーム・リレー・インターフェースが自己テストに合格した回数を示します。

Self-test Failed
フレーム・リレー・インターフェースが自己テストに失敗した回数を示します。

Maintenance Failed
インターフェースがフレーム・リレー・マネージメントと通信できなかった合計回数を示します。

V.24 circuit, Nicknames, and State
回線、制御信号、ピン割り当てとそれらの状態 (ON または OFF)。注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

Line speed
送信クロック・レート

Last port reset
前回のポート・リセット以降の時間の長さ

Input frame errors:

CRC error
チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment
長さが 8 の偶数倍でないために廃棄された受信パケットの数

Too short
長さが 2 バイト未満であったために廃棄された受信パケットの数

Too long
構成されたサイズより大きかったために廃棄されたパケットの数

Aborted frame
送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun
シリアル・インターフェースがシステム・パケット・バッファー・メモリーにデータを送信する速度が遅かったために、データをネットワークから受信できなかった回数。

Missed frame
フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

L & F bits not set
シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

Output frame counters:

DMA/FIFO underrun errors
シリアル・インターフェースがシステム・パケット・バッファー・メモリーからデータを取り出す速度が遅かったために、データをネットワーク上に送信できなかった回数。

Output aborts sent
高位レベルのソフトウェアの要求によって打ち切られた伝送の数

GWCON 環境から interface コマンドを実行すると、フレーム・リレー・ダイヤル回線について次のような統計が表示されます。

```
+interface
4

                                              Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec    Passed      Failed       Failed
4  3    FR/0          81640   5C             0            4              0

  Frame Relay MAC/data-link on ISDN Basic Rate interface
```

第33章 ポイント・ポイント・プロトコル・インターフェースの使用

この章では、装置上のインターフェースのポイント・ポイント・プロトコルの使用法について説明します。本章には、以下の節が含まれています。

- 『PPP の概説』
- 470ページの『PPP リンク制御プロトコル (LCP)』
- 479ページの『PPP ネットワーク制御プロトコル』
- 474ページの『PPP 認証プロトコル』

マルチリンク PPP プロトコルの使用については、527ページの『第35章 マルチリンク PPP プロトコルの使用』 および 531ページの『第36章 マルチプロトコル PPP プロトコル (MP) の構成および監視』 を参照してください。

PPP の概説

PPP は、シリアル・ポイント・ポイント・リンクを介して、データ・リンク・レイヤーでプロトコル・データグラムを転送する方法を提供します。 PPP は、以下のサービスを提供します。

- リンク接続を確立、構成、およびテストするためのリンク制御プロトコル (LCP)
- シリアル・ポイント・ポイント・リンク上でプロトコル・データグラムをカプセル化するためのカプセル化プロトコル
- 同位 (リモート) 装置の識別子の妥当性を検査し、またユーザー自身の識別子を同位に転送して妥当性検査を依頼するための認証プロトコル (AP)
- 各種のネットワーク・レイヤー・プロトコルの設定および構成を行うためのネットワーク制御プロトコル (NCP)。 PPP では、複数のネットワーク・レイヤー・プロトコルを使用できます。

468ページの図26 は、ポイント・ポイント・シリアル・リンクの例を示しています。

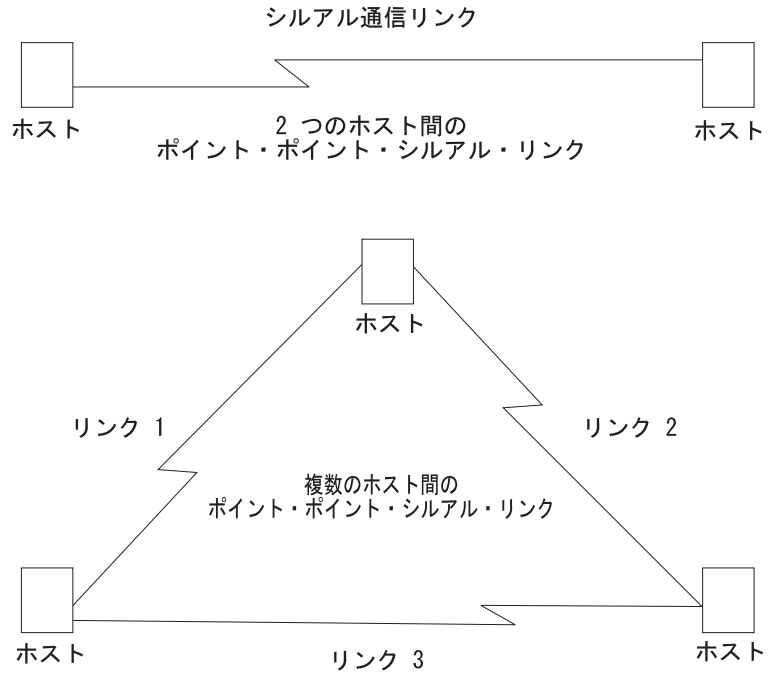


図 26. ポイント・ポイント・リンクの例

PPP は現在、AppleTalk 制御プロトコル (ATCP)、DECnet プロトコル制御プロトコル、(DNCP)、Banyan VINES 制御プロトコル (BVCP)、 ブリッジング・プロトコル (BCP、NBCP、および NBFCP)、インターネット・プロトコル制御プロトコル (IPCP)、IPX 制御プロトコル (IPXCP)、APPN HPR 制御プロトコル (APPN HPRCP)、APPN ISR 制御プロトコル (APPN ISRCP)、および OSI 制御プロトコル (OSICP) をサポートしています。

各端は、始めに LCP パケットを送信して、データ・リンクを構成し、テストします。リンクが確立された後、PPP は NCP パケットを送信して、1 つまたは複数のネットワーク・レイヤー・プロトコルを選択し、構成します。ネットワーク・レイヤー・プロトコルを構成すると、各ネットワーク・レイヤーからのデータグラムをリンクを介して送信できるようになります。以下の節では、これらの概念についてさらに詳しく説明します。

PPP データ・リンク・レイヤー・フレーム構造

PPP は、ハイレベル・データ・リンク制御 (HDLC) フレームと同じ構造のデータ・フレームを転送します。 PPP は、単一のフレーム・フォーマットを用いてすべてのデータ交換および制御交換を行うバイト指向の伝送方式を使用します。 図27 は PPP フレーム構造を示しており、その後に各フィールドの詳しい説明があります。

フラグ	アドレス	制御	プロトコル	情報	FCS	フラグ
8ビット	8ビット	8ビット	16ビット	可変	16ビット	8ビット

図 27. PPP フレーム構造

フラグ・フィールド

フラグ・フィールドは、各フレームを開始および終了し、固有のパターン 01111110 をもっています。通常は、1 つのフラグが、あるフレームを終了し、次のフレームを開始します。リンクに接続されている受信側は、このフラグ・シーケンスを継続的に探索して、次のフレームの開始と同期します。

アドレス・フィールド

アドレス・フィールドは 1 オクテット (8 ビット) で、2 進シーケンス 11111111 (16 進 0xff) が入っています。これは、全ステーション・アドレスと呼ばれます。 PPP は個別ステーション・アドレスは割り当てません。

制御フィールド

制御フィールドは 1 オクテットで、2 進シーケンス 00000011 (16 進 0x03) が入っています。このシーケンスは、P/F ビットがゼロにセットされた非番号制情報 (UI) コマンドを識別します。

プロトコル・フィールド

プロトコル・フィールドは PPP によって定義されます。このフィールドは 2 オクテット (16 ビット) で、その値はフレームの情報フィールドにカプセル化されたプロトコル・データグラムを識別します。

'0xC000' 〜 '0xFFFF' の範囲のプロトコル・フィールドは、LCP、PAP、CHAP、SPAP、および CCP のようなレイヤー 3 データ (プロトコル・データグラム) を示します。 '8000' 〜 'BFFF' の範囲の値は、データグラムがネットワーク制御プロトコル (NCP) に属することを示します。 '0' 〜 '3FFF' の範囲の値は、特定のデータグラムのネットワーク・プロトコルを識別します。

情報フィールド

情報フィールドには、プロトコル・フィールドに指定されているプロトコルのデータグラムが入っています。これは、ゼロまたはそれ以上のオクテットです。

プロトコル・タイプが LCP の場合、PPP データ・リンク・レイヤー・フレームの情報フィールドには、正確に 1 つの LCP パケットがカプセル化されています。

フレーム・チェック・シーケンス (FCS) フィールド

フレーム・チェック・シーケンス・フィールドは、16 ビット巡回冗長検査 (CRC) です。

PPP リンクは、各種のオプションの使用をネゴシエート (交渉) することにより、基本フレーム・フォーマットを変更することができます。以下の説明は、このような変更を行う前のフレーム・フォーマットに適用されます。 PPP LCP パケットは、交渉で決められたオプションに関係なく、常にこのフォーマットでも送信され、伝送路上の同期が失われた場合でも、LCP パケットを認識できるようにされています。

ルーターは、このようなオプションのうちの 2 つをサポートしています。すなわち、アドレスおよび制御フィールド圧縮 (ACFC) とプロトコル・フィールド圧縮 (PFC) です。これらについては、後で詳しく説明します。

PPP リンク制御プロトコル (LCP)

PPP のリンク制御プロトコル (LCP) は、ポイント・ポイント・リンクを確立、構成、保守、および終了します。このプロセスは 4 つのフェーズで行われます。

1. PPP は、ネットワーク・レイヤー・データグラムを交換する前に、最初に LCP 構成パケットを交換して、コネクションをオープンします。このネゴシエーション・プロセスの一部として、PPP は、転送できる最大パケット・サイズや、リンクの各端がネットワーク・トラフィックを伝送する前に認証機構を使用してそれぞれの同位に自分自身を識別する必要があるかどうかなど、さまざまな基本的リンク・レベル・パラメーターついて、リンクの各端で合意が得られるように処理します。

   このネゴシエーションが不成功の場合、リンクは 『ダウン』 と見なされ、ネットワーク・トラフィックを伝送することはできません。ネゴシエーションに成功した場合、LCP が 『オープン』 状態になり、PPP は次のフェーズに進みます。

2. LCP が正常にオープン状態になったら、リンク確立の次のステップは、認証を実行することです。つまり、リンクの各端は、LCP ネゴシエーションで相手側が指定した 『認証プロトコル』 を使用して、相手側に自分自身を識別します。

   認証が不成功の場合、リンクは 『ダウン』 としてマークされ、ネットワーク・トラフィックを伝送することはできません。認証に成功した場合、または認証が不要の場合、PPP リンクは次のフェーズに移ります。

3. 認証を交渉した後で、同位間でリンクの暗号化を交渉します。認証フェーズが完了した後、ルーターは暗号化制御プロトコル (ECP) パケットを使用して、暗号化の使用を交渉します。つまり、リンクの各端は、この PPP リンク上のデータを暗号化するのに使用する暗号化アルゴリズムを交渉します。 ECP が 『オープン』 状態に達することができなかった場合、リンクは 『ダウン』 としてマークされ、ネットワーク・トラフィックを伝送することはできません。 ECP が正常に 『オープン』 状態に達した場合、または暗号化は不要の場合、PPP リンクは次のフェーズである NCP ネゴシエーション (ECP を除く、これも技術的には NCP です) に移ります。リンクは 『オープン』 またはこの場合は 『アップ』 (ただし、まだレイヤー 3 プロトコル・データグラムは転送できません) と見なされます。

4. リンクがオープンしたら、ルーターはネットワーク制御プロトコル (NCP) パケットを使用して、各種のレイヤー 3 プロトコル (たとえば、IP、IPX、DECnet、Banyan Vines) の使用を交渉します。各レイヤー 3 プロトコルには、それぞれ独自の関連ネットワーク制御プロトコルがあります。たとえば、IP には IPCP があり、IPX には IPXCP があります。これらの NCP パケットの基本フォーマットとメカニズムは、すべてのプロトコルで同一であり、基本的には、この節で後述する LCP 機構のスーパーセットです。

   各レイヤー 3 プロトコルは、それぞれ個別に交渉されます。特定の NCP の交渉に成功した場合、リンクはそのプロトコルのトラフィックに対して 『アップ』 になります。 LCP の場合と同様に、この交渉の中で構成情報を交換することができます。たとえば IPCP は、IP アドレスを交換したり、″Van Jacobson IP ヘッダー圧縮″ の使用を交渉したりすることができます。

   LCP と同様に、NCP もその同位との交渉が不成功に終わる可能性があります。同位が特定のプロトコルをサポートしなかったり、一部の構成オプションが受け入れられなかった場合にそうなります。 NCP が 『オープン』 状態に達しなかった

場合、他のレイヤー 3 プロトコルが PPP リンクを介して正常にトラフィックの受け渡しを行っていても、そのプロトコルのレイヤー 3 プロトコル・パケットは交換することができません。

5. 最後に、LCP はいつでもリンクを終了させることができます。通常はユーザーからの要求によって終了しますが、他の理由で終了することもあります。たとえば、管理上の理由でのリンクのクローズ、アイドル・タイマーの満了、あるいは CHAP 再チャレンジ時に再認証に失敗した場合などです。

PPP LCP、認証、および汎用 NCP 交渉機構の詳細については、RFC 1331、1334、1570、および 1661 を参照してください。

LCP パケット

LCP パケットは、PPP リンクを確立し、管理するのに使用され、おおまかに 3 つのカテゴリーに分けることができます。

- *リンク確立パケット* は、構成情報を交換し、リンクを確立します。
- *リンク終了パケット* は、リンクを切断するか、あるいは特定の時点にリンクが接続を受け入れていないことを知らせます。また、特定のプロトコルが認知されない (たとえば、NCP ネゴシエーション時に) ことを知らせるのにも使用できます。
- *リンク保守パケット* は、リンクを監視し、デバッグします。

PPP データ・リンク・レイヤー・フレームの情報フィールドには、正確に 1 つの LCP パケットがカプセル化されます。 LCP パケットの場合、プロトコル・フィールドには “リンク制御プロトコル” (16 進 C021) が入ります。 図28 は LCP パケットの構造を示しており、その後に各フィールドの詳しい説明があります。

符号	識別子	長さ	データ (オプション)

図 28. LCP フレーム構造 (PPP 情報フィールド内の)

符号 符号フィールドは 1 オクテットの長さで、LCP パケットのタイプを識別します。 表60 の符号は、パケット・タイプの区別を示します。これらについては、後で詳しく説明します。

表 60. LCP パケット符号

符号	パケット・タイプ
1	Configure-Request (リンク確立)
2	Configure-Ack (リンク確立)
3	Configure-Nak (リンク確立)
4	Configure-Reject (リンク確立)
5	Terminate-Request (リンク終了)
6	Terminate-Ack (リンク終了)
7	Code-Reject (リンク確立)
8	Protocol-Reject (リンク確立)
9	Echo-Request (リンク保守)
10	Echo-Reply (リンク保守)
11	Discard-Request (リンク保守)

識別子 識別子フィールドは 1 オクテットの長さで、パケット要求と応答を一致させるのに使用されます。

長さ 長さフィールドは 2 オクテットの長さで、LCP パケットの全長 (すなわち、すべてのフィールドを含めた) を示します。

データ (オプション)
データ・フィールドは、長さフィールドに示されているゼロまたはそれ以上のオクテット数です。このフィールドのフォーマットは、符号によって決まります。

NCP パケットは、構造は LCP パケットと同一ですが、異なる PPP 『プロトコル』 値を持っているので識別できます。各 LCP パケット・タイプ (符号フィールドによって識別) は、各 NCP に対しても同じ意味を持ちます。ただし、個々の NCP にすべての可能な LCP パケット・タイプが実現されているわけではありません。 NCP は通常、LCP で定義されているリンク確立タイプ・パケットはすべて実現されています。また、いくつかの追加 LCP パケット・タイプが実現されている場合もあり、LCP で使用されている以外の追加パケット・タイプを定義することもできます。 LCP パケットの場合とは異なり、リンク確立フェーズで LCP によって交渉されたオプションに従って NCP フレームの構造を変更することが可能です。

リンク確立パケット

リンク確立パケットは、ポイント・ポイント・リンクを確立し、構成するもので、以下のパケット・タイプが含まれます。

Configure-Request
LCP パケット符号フィールドは 1 にセットされます。LCP はポイント・ポイント・リンクをオープンしたいときに、このパケット・タイプを送信します。 Configure-Request を受信すると、同位ステーションの LCP エンティティーは、パケットを処理する準備ができているかどうかに応じて、該当する応答を送信します。

Configure-Ack
LCP パケット符号フィールドは 2 にセットされます。Configure-Request パケット内の各構成オプションが受け入れ可能な場合、相手側はこのパケット・タイプを送信します。 Configure-Ack (ack = 確認) を受信すると、発信元ステーションは識別子フィールドを検査します。このフィールドは、最後に送信された Configure-Request からの値に一致していなければなりません。そうでない場合、そのパケットは無効です。

両側が Configure-Request を送信し、両側が Configure-Ack を受信しなければ、リンクはオープンしません。ある方向について交渉されたオプションが、他の方向について交渉されたオプションと異なっていても構いません。『マスター・スレーブ』 の関係はなく、それぞれの端が対称的に動作します。

Configure-Nak
LCP パケット符号フィールドは 3 にセットされます。Configure-Request パケット内の構成オプションのある部分が受け入れ不能である場合、同位はこのパケット・タイプを送信します。識別子フィールドは受信した Configure-Request からコピーされ、データ (オプション) フィールドには、受信した受け入れ不能の構成オプションが記入されます。識別子フィールドは

最後に送信された Configure-Request からの値に一致していなければなりません。そうでない場合、そのパケットは無効であり、廃棄されます。

発信元は、Configure-Nak パケットを受信すると、修正された、受け入れ可能な構成オプションを入れた新たな Configure-Request パケットを送信します。

Configure-Reject

LCP パケット符号フィールドは 4 にセットされます。Configure-Request パケット内の構成オプションのある部分が受け入れられない場合、同位はこのパケット・タイプを送信します。識別子フィールドは受信した Configure-Request からコピーされ、データ (オプション) フィールドには、受信した受け入れ不能の構成オプションが記入されます。識別子フィールドは最後に送信された Configure-Request からの値に一致していなければなりません。そうでない場合、そのパケットは無効であり、廃棄されます。

発信元は、Configure-Reject パケットを受信すると、Configure-Reject パケットで受信した構成オプションのいずれも含んでいない新たな Configure-Request パケットを送信します。

Code-Reject

LCP パケット符号フィールドは 7 にセットされます。このパケット・タイプの送信は、受信したパケットの LCP 『符号』 フィールドが有効な値と見なされないことを示します。これは誤りを示している可能性がありますが、ユーザーが使おうとしている機能が同位で実現されていないことを示している場合もあります。

Protocol-Reject

LCP パケット符号フィールドは 8 にセットされます。このパケット・タイプの送信は、サポートされない、または不明のプロトコルが含まれている PPP フレームが受信された (パケットの PPP 『プロトコル』 フィールドが認知されなかった) ことを示しています。これは通常、相手側がサポートしないプロトコルの NCP を交渉しようとした場合に起こります。たとえば、DECnet CP (DNCP) が Config-Request を送信し、相手側が DECnet について知らない場合、相手側は DNCP に対して LCP Protocol-Reject で応答します。Protocol-Reject パケットを受信すると、リンクは不正なプロトコルの送信を停止します。

注: NCP パケット・タイプと構造は LCP と同じですが、一部の NCP に関連したいくつかの追加 『符号』 フィールドがあります。

リンク終了パケット

リンク終了パケットはリンクを終了させるもので、以下のパケット・タイプが含まれます。

Terminate-Request

LCP パケット符号フィールドは 5 にセットされます。ポイント・ポイント・リンクをクローズする必要があるときに、LCP はこのパケット・タイプを送信します。これらのパケットは、Terminate-Ack パケットが返送されるまで、または Ack を待っている間に再試行カウンターが超過するまで送信されます。

Terminate-Ack

LCP パケット符号フィールドは 6 にセットされます。Terminate-Request パケットを受信した場合、符号フィールドを 6 にセットして、このパケット・タイプを送信しなければなりません。予期していなかった Terminate-Ack パケットの受信は、リンクがクローズされたことを示します。

リンク保守パケット

リンク保守パケットは、リンクを管理し、デバッグするもので、以下のパケット・タイプが含まれます。

Echo-Request および Echo-Reply

LCP パケット符号フィールドは、それぞれ 9 および 10 にセットされます。LCP は、リンクの両方向のデータ・リンク・レイヤー・ループバック機構を提供するために、これらのパケット・タイプを送信します。これらの機能は、たとえば、障害のあるリンクをデバッグした後でリンクの品質を調べる場合などに便利です。これらのパケットは、リンクがオープン状態にあるときにのみ送信されます。

Discard-Request

LCP パケット符号フィールドは 11 にセットされます。 LCP は、データ・リンク・レイヤーのテストのために、このパケット・タイプをデータ受信側に提供します。 Discard-Request を受け取った同位は、そのパケットを廃棄する***必要があります***。これは、リンクをデバッグする場合に便利です。これらのパケットは、リンクがオープン状態にあるときにのみ送信されます。

PPP 認証プロトコル

PPP 認証プロトコルは、PPP リンクを介して接続されている 2 つのノード間に一種のセキュリティーを提供します。あるボックスで認証が必要な場合、2 つのボックスは LCP レイヤーのリンクの使用に関するネゴシエーションに成功した直後に (LCP が『オープン』 状態になるまで LCP パケットが交換されます) 『認証』 フェーズに入り、認証パケットを交換します。認証のネゴシエーションが正常に完了するまでは、ボックスはネットワーク・データ・パケットを伝送することも、ネットワーク・プロトコル (NCP トラフィック) の使用を交渉することもできません。

異なるタイプの認証プロトコルを使用できます。つまり、PAP (パスワード認証プロトコル) と CHAP (チャレンジ/ハンドシェーク認証プロトコル) です。これらについては RFC 1334 に詳細に記述されていますが、この節の後方でも簡単に説明しておきます。リモート・ダイヤルイン・アクセス・ポートでは、第 3 の認証プロトコルが使用可能です。これは、Shiva が所有権をもつプロトコルである SPAP (Shiva Password Authentication Protocol) です。詳細については、475ページの『Shiva パスワード認証プロトコル (SPAP)』を参照してください。

あるボックスが相手側に対してそれ自身の認証を要求しているかどうか (要求している場合は、どのプロトコルを使用するか) については、LCP ネゴシエーション・フェーズで判別されます。一方の側が相手側に必要な認証プロトコルの使用法を知らなかったり、その使用を拒否する場合、リンク確立フェーズ (LCP ネゴシエーション) の段階でも、認証は 『不成功』 と見なすことができます。

リンクの各端は、相手側が自身を認証する方法について、独自の要件を設定します。たとえば、2 つのルーター 『A』 と 『B』 が PPP リンクを介して接続されている場合、A 側は B が PAP を使用して自身を A に認証することを要求し、同様に B 側は A が CHAP を使用して自身を識別することを要求するといったことが可能です。また、一方の側が認証を必要とし、他方の側は認証を必要としないというのも有効です。

リンク確立時の初期認証に加えて、一部のプロトコルの認証機能は、同位が定期的に再証明することを要求することもできます。たとえば、CHAP では、認証機能はいつでも再チャレンジを出すことができ、同位は正常に応答できなければなりません。そうでないと、リンクは失われます。

リンク上に複数の認証プロトコルが使用可能にされている場合、初期時にルーターは、ユーザーが指定した優先順位で使用を試みます。

1. CHAP
2. PAP
3. SPAP

注: SPAP は、ダイヤルイン回線が構成された IBM DIAL を備えたインターフェース上でのみ利用可能です。

リモート側が認証要求に対して NAK で応答し、代替を提案した場合、ルーターは、その代替がリンク上で使用可能になっていれば代替を使用します。リモート側がルーターの提案に対して NAK で応答し続け、ルーターで使用可能にされている代替を提案しない場合、リンクは終了されます。

パスワード認証プロトコル (PAP)

パスワード認証プロトコル (PAP) は、同位が両方向ハンドシェークを使用して自身のアイデンティティーを設定する簡単な方法を提供します。これは初期リンク確立時にのみ行われます。リンク確立の後、認証が確認されるかコネクションが終了されるまで、同位は認証機能に ID/パスワードの組みを送信します。パスワードは 『解放された』 回線を介して送信され、再生や反復的試行および誤ったアタックに対する保護はありません。同位が試行の頻度とタイミングを制御します。

チャレンジ/ハンドシェーク認証プロトコル (CHAP)

チャレンジ/ハンドシェーク認証プロトコル (CHAP) は、両方向ハンドシェークを使用して、同位のアイデンティティーを定期的に確認するのに使用します。これは初期リンク確立時に行われ、リンク確立後の任意の時点で反復しても構いません 。初期リンク確立後に、認証機能は同位に 『チャレンジ』 メッセージを送ります。同位は、『単方向ハッシュ』 機能を使用して計算された値で応答します。認証機能は、その応答を、自身が計算した予想ハッシュ値と突き合わせて検査します。値が一致している場合、認証は確認されます。そうでない場合、コネクションは終了します。

Shiva パスワード認証プロトコル (SPAP)

注: SPAP は、ダイヤルイン回線が構成された IBM DIAL を備えたインターフェース上でのみ利用可能です。

Shiva パスワード認証プロトコル (SPAP) は、PAP と同様に、同位が両方向ハンドシェークを使用して自身のアイデンティティーを設定する簡単な方法を提供します。リンク確立フェーズが完了した後、認証が確認されるか、接続が終了するか、あるいは再試行カウンターが満了するまで、同位は認証機能に ID/パスワードを繰り返し送信します。

SPAP は、専有のパスワード暗号化アルゴリズムを使用する、中程度の強さの認証プロトコルです。このプロトコルは、認証と合わせて、いくつかの機能を提供します。

- パスワードを変更することができる。

  注: SPAP のパスワード変更サポートは、認証のためにローカル PPP ユーザー・リストを使用する場合にのみ使用可能です。
- パスワード認証の後、ルーターは、クライアントからの確認応答を要求する構成可能なバナーを送信することができる。
- 追加のセキュリティー機能としてコールバックを使用することができる。

PPP 認証の構成

以下では、2 つの状況での PPP 認証の構成について説明します。

- リモート装置を認証する 2210 を構成する。
- リモート装置によって認証される 2210 を構成する。

この 2 つの状況は、それぞれ独立しています。一方または他方を構成することができます。

リモート装置を認証する PPP インターフェースの構成

リモート装置またはダイヤルイン・クライアントを認証するには、次のようにします。

1. PPP インターフェース上の認証を使用可能にする。
   - `Config>` プロンプトで **network** コマンドを入力して、構成する PPP インターフェースを選択する。
   - `PPP Config>` プロンプトで、使用する認証プロトコルを使用可能にする。

     次のプロトコルを使用できます。
     - PAP
     - CHAP
     - SPAP

       注: SPAP は、ダイヤルイン回線が構成された IBM DIAL を備えたインターフェース上でのみ利用可能です。
2. 認証をローカルで行うか、認証サーバーを通して行うかを決める。
   - ローカルで認証する場合は、名前とパスワードを PPP ユーザー・データベースに入力します。

     `Config>` プロンプトで **add ppp_user** コマンドを使用します。詳細については、56ページの『Add』 を参照してください。

2210 は単一の PPP ユーザー・データベースを維持しています。認証フェーズで、リモート・ルーターまたは装置がその名前とパスワードを装置に送ると、装置はその名前とパスワードが PPP ユーザー・データベース内に存在するかどうか検査します。

- TACACS、TACACS+、または RADIUS を使用して、認証サーバーを通して認証する場合は、認証サーバーに到達するように装置を構成する必要があり、その名前とパスワードがサーバーのデータベースに存在していなければなりません。 847ページの『第64章 ローカルまたはリモート認証の使用』 を参照してください。

リモート装置によって認証される PPP インターフェースの構成

リモート装置またはダイヤルイン・クライアントによって認証されるように装置を構成するには、装置の名前とパスワードを構成します。

1. Config> プロンプトで **network** コマンドを使用して、構成するインターフェースを選択する。
2. PPP Config> プロンプトで **set name** コマンドを使用して、認証フェーズで装置が自身をリモート・ルーターまたは装置に識別する名前とパスワードを提供する。

重要: 装置が847ページの『第64章 ローカルまたはリモート認証の使用』 に説明されている認証を行うのでない限り、次のコマンドは使用しないでください。

- **enable pap**
- **enable chap**
- **enable spap**

  注: SPAP は、ダイヤルイン回線が構成された IBM DIAL を備えたインターフェース上でのみ利用可能です。

PPP コールバックの構成

コールバックは、シングル・ユーザー・ダイヤルイン・ソリューションに関連した PPP 機能です。これは 2 つの目標の達成を試みます。目標は、次のとおりです。

- コールバックは、セキュリティーの 1 種として使用することができます。この方法で使用されるコールバックは通常、必須コールバックと呼ばれます。必須コールバックがネゴシエーションされる場合、ユーザーの事前設定された番号にダイヤルしてコールバックされます。その場合にのみ、PPP リンクはアップになることが許可されます。
- コールバックは、通話料節約機能として実現することもできます。この方法で使用されるコールバックは通常、ローミング・コールバックと呼ばれます。必須コールバックとは異なり、ローミング・コールバックはクライアントによって要求されます。ローミング・コールバックの主な機能は、通話料金をユーザーではなく、DIAL サーバー を維持している会社に請求することです。

コールバックは、V.34 または ISDN ネットワークを介したダイヤルイン・ダイヤル回線上でのみサポートされます。

例 1: 必須コールバックが使用可能

```
Config>add PPP
Enter user name: []? sallydoe
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user sallydoe [0.0.0.0]?
Enter HostName: []?
Give 'sallydoe' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'sallydoe' ? (Yes, No): [No] yes
Type of Callback (Roaming Callback, Required Callback): [Roaming Callback] Requ
Dialback number for this user []? 555-1234
Will 'sallydoe' be able to dial-out ? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:

PPP User Name: sallydoe
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Alotted: Box Default
Call-Back Type: Required Callback
Phone Number: 543-3186
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes
```

例 2: コールバックが使用不可

```
Config>add PPP
Enter user name: []? sallydoe
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user sallydoe [0.0.0.0]?
Enter HostName: []?
Give 'no callback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'no callback' ? (Yes, No): [No]
Will 'no callback' be able to dial-out ? (Yes, No): [No]
Enable encryption for this user/port (y/n) [No]:


PPP User Name: no callback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Alotted: Box Default
Call-Back Type: Not Enabled
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes
```

例 3: ローミング・コールバックが使用可能

```
Config>add PPP roaming_callback
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user roaming_callback [0.0.0.0]?
Enter HostName: []?
Give 'roaming_callback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'roaming_callback' ? (Yes, No): [No] yes
Type of Callback (Roaming Callback, Required Callback): [Roaming Callback]

Will 'roaming_callback' be able to dial-out ? (Yes, No): [No]n
Enable encryption for this user/port (y/n) [No]:


PPP User Name: roaming_callback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Alotted: Box Default
Call-Back Type: Roaming Callback
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes
```

PPP を用いた AAA の使用

この情報については、847ページの『第64章 ローカルまたはリモート認証の使用』、および 853ページの『第65章 認証の構成』を参照してください。

PPP ネットワーク制御プロトコル

PPP には、各種のネットワーク・レイヤー・プロトコルを設定および構成するためのネットワーク制御プロトコル (NCP) ファミリーがあります。 NCP は、ポイント・ポイント・リンクの両端で、ネットワーク・レイヤー・プロトコルの構成、使用可能化、および使用不可化を行います。 LCP がコネクションをオープンし、リンクがオープン状態に達するまでは、NCP パケットを交換することはできません。

PPP は、以下のネットワーク制御プロトコルをサポートします。

- AppleTalk 制御プロトコル (ATCP)
- Banyan VINES 制御プロトコル (BVCP)
- ブリッジング・プロトコル (BCP、NBCP、および NBFCP)
- DECnet 制御プロトコル (DNCP)
- IP 制御プロトコル (IPCP)
- IPX 制御プロトコル (IPXCP)
- OSI 制御プロトコル (OSICP)
- APPN 高性能ルーティング制御プロトコル (APPN HPRCP)
- APPN 中間セッション・ルーティング制御プロトコル (APPN ISRCP)

AppleTalk 制御プロトコル

ATCP は Request for Comments (RFC) 1378 に指定されています。 IBM の ATCP の実現は AppleTalk アドレス・オプションをサポートします。この実現は、全ルーター・モードおよび半ルーター・モードをサポートします。詳細については、*Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 2 巻 バージョン 3.1* の『PPP を介する AppleTalk』の項を参照してください。

Banyan VINES 制御プロトコル

RFC 1763 に BVCP の記述があります。 IBM の BVCP の実現は、どのオプションもサポートしません。

ブリッジング・プロトコル

ブリッジング制御プロトコル (BCP) は RFC 1220 に指定されています。 IBM の BCP の実現は、IEEE 802.5 回線識別オプションおよび Tinygram 圧縮オプションをサポートします。

NetBIOS 制御プロトコル (NBCP) は、Shiva Corporation によって開発された専有の NCP で、IBM Dial In Access to LAN Client for OS/2、DOS、および Windows for single-user dial-in によって使用されます。 NBCP は、2210 DIAL サーバー にダイ

ヤルされた、これらのクライアントからの NetBIOS および LLC/802.2 ブリッジ・トラフィックを、接続された LAN にトランスポートします。 IBM で実現された NBCP は、MAC-Address および NetBIOS Name Projection オプションをサポートします。

NetBIOS Frame Control Protocol (NBFCP) の仕様は、RFC 2097 に規定されています。 NBFCP は、Microsoft Windows 95 および Windows NT Dial-Up Networking clients for single-user dial-in によって使用されます。 NBFCP は、2210 DIAL サーバーにダイヤルインされた、これらのクライアントからの NetBIOS ブリッジ・トラフィックを、接続された LAN にトランスポートします。 IBM で実現された NBFCP は、Name-Projection、Peer-Information、および IEEE-MAC-Address-Required オプションをサポートします。

DECnet 制御プロトコル

DNCP は RFC 1376 に指定されています。 IBM の実現は、どの DNCP オプションもサポートしません。

IP 制御プロトコル

IPCP は RFC 1332 に指定されています。 IBM の実現は、次のオプションをサポートします。

- RFC 1144 に記述されている Van Jacobsen IP ヘッダー圧縮
- IP アドレス

  ルーターは、その IP アドレスを送信したり、同位からの IP アドレスを受け入れたり、あるいは要求された場合は、同位に IP アドレスを提供したりすることができます。特定のインターフェース上のルーターが 『Send Our Address』 用に構成されており、そのインターフェースに有効な番号制 IP アドレスがある場合、IPCP は初期 Configure-Request でオプション 3 (IP アドレス) としてそのアドレスを送信します。また、その PPP インターフェースに有効な番号制アドレスが構成されている場合、同位がオプション 3 (IP アドレス) を 0.0.0.0 にセットした Configure NAK を送信した場合にも、IPCP はそのアドレスを送信します。 IPCP は、非番号制アドレスは同位に送信しません。

  同位はこのアドレスを指定することも (『クライアント指定』 と呼ばれます)、初期構成要求のオプション 3 で 0.0.0.0 を送信してルーターからアドレスを要求することもできます。ルーターはこのアドレスを、認証されたユーザー・プロファイル (『User ID』 と呼ばれる)、インターフェース自体 (『Interface』 と呼ばれる)、または動的ホスト構成プロトコル (『Proxy DHCP』 と呼ばれる) から入手することができます。同位の IP アドレスを指定するためのこの 4 つの方法はいずれも、2210 レベルで使用不可または使用可能にすることができます。これらの項目を使用可能および使用不可にする方法についての詳細は、663ページの『第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用』を参照してください。

  ルーターは、ネゴシエーションに成功したアドレスの PPP インターフェースへの静的ルートを自動的に追加して、データがそのダイヤルイン・クライアントに正しく送達されるようにします。 IPCP コネクションが何らかの理由で終了した場合、この静的ルートは除去されます。デフォルトでは、このルートのネットマスクは 255.255.255.255 (ホスト・ルート) になりますが、認証されたユーザーのプロファイルにネットマスクを指定すれば (476ページの『PPP 認証の構成』を参照)、

これ以外のネットマスクを使用して、PPP リンクを介して複数のホストにルーティングすることも可能です (必要な場合は、ルートを発見するために RIP またはその他のルーティング・プロトコルも使用できます)。

IPX 制御プロトコル

IPXCP は RFC 1552 に指定されています。 IBM の実現は、どの IPXCP オプションもサポートしません。

OSI 制御プロトコル

OSICP は RFC 1377 に指定されています。 IBM の OSICP の実現は、どのオプションもサポートしません。

APPN HPR 制御プロトコル

拡張対等通信ネットワーキング機能 (APPN) 高性能ルーティング (HPR) 制御プロトコルは、RFC 2043 に指定されています。この制御プロトコルでは、どのオプションも交渉されません。

APPN ISR 制御プロトコル

拡張対等通信ネットワーキング機能 (APPN) 中間セッション・ルーティング (ISR) 制御プロトコルは、RFC 2043 に指定されています。この制御プロトコルでは、どのオプションも交渉されません。

PPP インターフェースの暗号化の構成については、873ページの『第66章 暗号化の概説』を参照してください。

第34章 ポイント・ポイント・プロトコル・インターフェースの構成および監視

この章では、装置内のポイント・ポイント・プロトコル・インターフェースの構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

インターフェース構成プロセスへのアクセス

ルーターの構成プロセスにアクセスするには、以下の手順を使用します。このプロセスにより、特定のインターフェースの *構成* プロセスにアクセスすることができます。

1. OPCON プロンプト (*) で **status** コマンドを入力して、CONFIG の PID を見つける。 (**status** コマンドの出力例については、11ページを参照してください。)
2. OPCON プロンプトで、OPCON **talk** コマンドと CONFIG の PID を入力する。 (このコマンドの詳細については、29ページの『第3章 OPCON プロセスおよびコマンド』 を参照してください。) たとえば、次のように入力します。

   ```
   *talk 6
   ```

   talk 6 コマンドを入力すると、CONFIG プロンプト (Config>) がコンソールに表示されます。最初に **CONFIG** に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。
3. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。 たとえば、次のように入力します。

   ```
   Config>
   list devices

   Ifc 0 Ethernet                      CSR  81600, CSR2  80C00, vector 94
   Ifc 1 WAN X.25                      CSR  81620, CSR2  80D00, vector 93
   Ifc 2 WAN X.25                      CSR  81640, CSR2  80E00, vector 92
   Ifc 3 WAN PPP                       CSR 381620, CSR2 380D00, vector 125
   Ifc 4 WAN Frame Relay               CSR 381640, CSR2 380E00, vector 124
   Ifc 5 Token Ring                    CSR 600000, vector 95
   ```
4. インターフェース番号を記録する。
5. CONFIG **network** コマンドと、構成するインターフェースの番号を入力する。 たとえば、次のように入力します。

   ```
   Config> network 1
   ```

   これで、該当する構成プロンプト (たとえば、トークンリングの場合は TKR Config>) がコンソールに表示されます。

PPP インターフェースの構成

注: ネットワーク・インターフェースは、すべてがユーザーによる構成が可能とは限りません。構成できないインターフェースの場合は、次のようなメッセージが出ます。

```
That network is not configurable
```

PPP インターフェース構成プロンプトへのアクセス

PPP config> プロンプトを表示するには、次のようにします。

1. Config> プロンプトで **list devices** コマンドを入力して、インターフェースのリストを表示する。
2. まだ行っていない場合は、Config> プロンプトで **set data-link ppp** と入力して、シリアル・インターフェースの 1 つのデータ・リンク・プロトコルを PPP に設定する。たとえば、次のように入力します。

```
Config> set data-link ppp
Interface Number [0]? 2
```

3. **network** と入力し、続けて PPP インターフェースの番号を入力する。たとえば、次のように入力します。

```
Config> network 2
PPP config>
```

ポイント・ポイント構成コマンド

表61 は、PPP 構成コマンドの要約を示しており、本節の残りの部分で、これらのコマンドについて説明します。コマンドは PPP config> プロンプトで入力します。

表 61. ポイント・ポイント構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Disable	データ圧縮 (CCP)、DTR 回線処理、CHAP、PAP、ECP を使用不可にします。リモート LAN アクセス機能イメージの SPAP 認証も使用不可にします。
Enable	データ圧縮 (CCP)、DTR 回線処理、CHAP、PAP、ECP を使用可能にします。リモート LAN アクセス機能イメージの SPAP 認証も使用可能にします。
List	ポイント・ポイント・インターフェース・プロトコル、パラメーター、およびオプションに関連するすべての情報をリストします。
Set	物理回線 (HDLC) パラメーター、LCP パラメーター、一般 NCP パラメーター、および各種の NCP 特有のオプションを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Disable

データ圧縮、認証プロトコル、マルチリンク PPP、Lower DTR 機能、DIAL 機能、および SPAP 認証 (SPAP 認証は DIAL サーバー・イメージにのみ サポートされます) を使用不可にします。

構文:

disable ccp
chap
dials
ecp
lower-dtr
mp
pap
spap

ccp インターフェース上のデータ圧縮の使用を使用不可にします。詳細については、831ページの『第62章 データ圧縮サブシステムの使用』 を参照してください。

chap チャレンジ/ハンドシェーク認証プロトコルの使用を使用不可にします。詳細については、475ページの『チャレンジ/ハンドシェーク認証プロトコル (CHAP)』 を参照してください。

dials このインターフェース上の DIAL 機能を使用不可にします。詳細については、663ページの『第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用』を参照してください。

ecp これは、ルーターがこのインターフェースでの暗号化の使用を強制しないようにすることができます。同位が ECP を使用している場合には、インターフェースは暗号化制御プロトコル (ECP) を受け入れ、これを実行します。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

lower-dtr
使用不可にされている専用シリアル・ライン・インターフェースのデータ端末レディー (DTR) 信号の扱い方を決めます。このパラメーターが 『使用不可』 (デフォルト) に設定され、インターフェースが使用不可の場合、DTR 信号は降下しません。

mp このインターフェース上のマルチリンク・プロトコル (MP) を使用不可にします。詳細については、527ページの『第35章 マルチリンク PPP プロトコルの使用』 を参照してください。

例:

```
disable mp
Disabled as a MP link
```

pap パスワード認証プロトコルの使用を使用不可にします。詳細については、475ページの『パスワード認証プロトコル (PAP)』 を参照してください。

spap Shiva パスワード認証プロトコル (SPAP) の使用を使用不可にします。

注: SPAP は、ダイヤルイン回線が構成された IBM DIAL を備えたインターフェース上でのみ利用可能です。

Enable

この PPP インターフェース上のデータ圧縮、暗号化、認証プロトコル、Lower-DTR、マルチリンク PPP プロトコル、および DIAL 機能を使用可能にします。複数の認証プロトコルが使用可能にされている場合、装置は次の優先順位でそれらの使用を試みます。

1. SPAP
2. CHAP
3. PAP

構文:

enable ccp
chap
dials
ecp
lower-dtr
mp
pap
spap

ccp インターフェース上のデータ圧縮の使用を使用可能にします。詳細については、831ページの『第62章 データ圧縮サブシステムの使用』 を参照してください。

chap チャレンジ/ハンドシェーク認証プロトコルの使用を使用可能にします。再チャレンジ間隔を指定するように求めるプロンプトがでます。初期認証フェーズが完了した後に定期的に再チャレンジしない場合は、0 を指定します。詳細については、475ページの『チャレンジ/ハンドシェーク認証プロトコル (CHAP)』 を参照してください。

例:

```
enable chap
Rechallenge Interval in seconds (0=NONE)  [0] 10
CHAP enabled
```

dials このインターフェース上の DIAL 機能を使用可能にします。詳細については、663ページの『第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用』を参照してください。

ecp 暗号化制御プロトコル (ECP) と交渉して、このインターフェース上でデータ暗号化を使用することを使用可能にします。これが行われると、暗号化が使用可能にされ、有効な暗号化キーを持っているすべての PPP ユーザーは、このポートに接続するために ECP を使用しなければなりません。暗号化が使用可能にされていない PPP ユーザーはまだこのインターフェースに接続することができます。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

lower-dtr

使用不可にされている専用シリアル・ライン・インターフェースのデータ端末レディー (DTR) 信号の扱い方を決めます。このパラメーターが 『使用不可』 (デフォルト) に設定され、インターフェースが使用不可の場合、DTR 信号は降下しません。

Lower DTR が 『使用可能』 に設定されている場合は、インターフェースが使用不可のときには、DTR 信号は降下します。この動作が適している状況は、インターフェースが WAN 再ルートの代替リンクとして構成されており、インターフェースが、DTR 信号の状態に基づいてダイヤル接続を維持するダイヤルアウト・モデムに接続されているような場合です。

インターフェースが使用不可のときは、DTR 信号は下がり、モデムは接続をダウンに保ちます。インターフェースが使用可能になると (WAN 再ルートのバックアップ・シナリオにより)、DTR は上がり、モデムは保管しているバックアップ・サイトへの番号をダイヤルします。 1 次インターフェースが復元すると、代替インターフェースは使用不可にされ、DTR は下がって、モデムはダイヤル接続を切断します。

以下のケーブル・タイプがサポートされます。

RS-232

V.35

V.36

注: enable lower-dtr コマンドは、PPP ダイヤル回線インターフェースではサポートされません。

mp このインターフェース上のマルチリンク・プロトコル (MP) を使用可能にします。詳細については、527ページの『第35章 マルチリンク PPP プロトコルの使用』 を参照してください。

例:

```
enable mp
Enabled as a MP link
Is this link a dedicated MP link? [no] yes
MP interface for this MP link? [0] 3
```

pap パスワード認証プロトコルの使用を使用可能にします。詳細については、475ページの『パスワード認証プロトコル (PAP)』 を参照してください。

spap Shiva パスワード認証プロトコル (SPAP) の使用を使用可能にします。詳細については、475ページの『Shiva パスワード認証プロトコル (SPAP)』を参照してください。 **enable spap** コマンドは、DIAL 機能をもつソフトウェア・ロードでのみ利用可能です。

List

list コマンドは、PPP インターフェースとそのプロトコル・パラメーターおよびオプションに関連する情報を表示するのに使用します。

構文:

list all

bcp

ccp

ecp

hdlc

ipcp

lcp

ncp

all PPP インターフェースに関連するすべてのオプションおよびパラメーターをリストします。

list all コマンドは、以下で説明する個々の **list...** パラメーターのすべて の出力を表示します。

bcp ブリッジング・ネットワーク制御プロトコル・オプションをリストします。

例:

```
list bcp
BCP Options
------------
Tinygram Compression:DISABLED
```

Tinygram Compression:
Tinygram 圧縮の使用可能/使用不可を表示します。

ccp 現在選択されているデータ圧縮オプションを表示します。詳細については、831ページの『第62章 データ圧縮サブシステムの使用』を参照してください。

ecp 暗号化制御プロトコルの現在の状態を表示します。

例:

```
list ecp
 ECP Options
 -----------
 Data Encryption enabled
 Algorithm list: DESE-CBC
 DESE (Data Encryption Standard Encryption Protocol)
```

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Data Encryption Enabled/Disabled
インターフェース上のデータ暗号化が使用可能か使用不可かを示します。

Algorithm List
サポートされる暗号化アルゴリズムを表示します。 DES (RFC 1969 に記述) が、現在サポートされている唯一の暗号化アルゴリズムです。

hdlc ハイレベル・データ・リンク制御 (HDLC) プロトコルに関連するパラメーターを表示します。 PPP ダイヤル回線インターフェースでは、『list hdlc』 オプションは利用不能です。ダイヤル回線の場合、ハードウェア・データ・リンク・パラメーターは、PPP ダイヤル回線ではなく、基本ネットの機能です。詳細については、653ページの『第47章 ダイヤル回線の使用』を参照してください。

例:

```
list hdlc
Encoding:  NRZ
Idle State:  Flag
Clocking:  Internal
Cable type:  V.35 DCE
Speed (bps): 6400

Transmit Delay Counter:  0
Lower DTR:   Disabled
```

Encoding:
HDLC 伝送符号化法、NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転)。

Idle State:
インターフェースがデータを転送していないときにポイント・ポイント・リンク上で転送されるビット・パターン、フラグまたはマーク

Clocking:
インターフェースのクロック、外部または内部

Cable type:
使用するケーブルのタイプ (RS-232、V.35、または V.36) を指定します。

Speed (bps):
インターフェースの物理データ速度。クロックが内部の場合、これは内部クロックによって生成されるデータ速度です。

Transmit Delay Counter:
フレーム相互間に送信されるフラグの数。

Lower DTR:
使用可能または使用不可。 Lower DTR が使用可能のとき、WAN 再ルートの代替リンクが不要になると、ルーターは DTR 信号を下げます。 DTR 信号が降下すると、モデムは代替リンクの専用回線接続を終了します。

注:

1. **list hdlc** コマンドは、PPP ダイヤル回線インターフェースではサポートされません。
2. このコマンドは、構成されたケーブル・タイプの Lower DTR がサポートされている場合にのみ、Lower DTR 状態を表示します。
3. HSSI アダプター上の PPP インターフェースに対するこのコマンドは、上記の HDLC パラメーター・リストのサブセットを表示します。

ipcp インターネット・プロトコル制御プロトコル・オプションをリストします。

例:

```
list ipcp
IPCP Options
------------
IPCP Compression:                None
Send Our IP Address:              Yes
Remote IP Address to Offer if Requested: 10.0.0.3
```

IPCP compression
PPP ハンドラーが圧縮された IP ヘッダーを受け入れるかどうかを示します。 PPP は Van Jacobson TCP/IP ヘッダー圧縮 (RFC 1144) を

サポートします。ポイント・ポイント・リンクが低いボー・レートで動作しているときは、このオプションを使用可能にしてください。

値 『Van Jacobson』 は、ヘッダー圧縮がサポートされることを示します。値 『NONE』 は、ヘッダー圧縮が受け入れられていないことを示します。

Send Our IP Address
IPCP が初期 『構成要求』 でこの PPP インターフェースのローカル IP アドレスをリンクのリモート側に送信するように構成されているかどうかを示します。一部の PPP 実現では、この情報を必要とします。

lcp リンク制御プロトコルのパラメーターおよびオプションをリストします。

例:

```
list lcp
LCP Parameters
--------------
Config Request Tries:          20   Config Nak Tries:             10
Terminate Tries:               10   Retry Timer:                3000

LCP Options
-----------
Max Receive Unit:            2048   Magic Number:                Yes
Peer to Local (Rx) ACCM:    A0000
Protocol Field Comp (PFC)      No   Addr/Cntl Field Comp(ACFC)   Yes

Authentication Options
--------------- -------
Authenticate remote using:  none
Identify Self As              ibm
```

Config Request Tries:
PPP リンクのオープンを試みているときに、LCP が同位ステーションに configure-request パケットを送信した回数

Config Nak Tries:
PPP リンクのオープンを試みているときに、LCP が同位ステーションに configure-nak (『not acknowledged』) パケットを送信した回数

Terminate Tries:
PPP リンクをクローズするときに、LCP が同位ステーションに terminate-request パケットを送信した回数

Retry Timer:
『Config tries』 パラメーターによって設定された回数に従ってパケット転送を続行する前に経過するミリ秒数

Max Receive Unit:
リンクによって処理される最大情報フィールド (パケット) サイズを表示します。

Peer to Local (Rx) ACCM
非同期伝送路上のルーターにパケットを転送するときに、同位が 『エスケープ』 する必要がある文字を表示します。

Magic Number:
マジック番号ループバック検出オプションが使用可能かどうかを示します。

Protocol Field Comp (PFC):
PFC オプションが使用可能かどかを示します。

Addr/Cntl Field Comp(ACFC):
ACFC が使用可能かどうかを示します。

Authenticate remote using:
使用可能にされている認証プロトコルのリスト。

Identify Self As:
set name コマンドで設定された名前。

ncp すべてのネットワーク制御プロトコルのパラメーターをリストします。

例:

```
list ncp
NCP Parameters
---------------
Config Request Tries:        20   Config Nak Tries:         10
Terminate Tries:             10   Retry Timer:              3000
```

Config Request Tries:
PPP リンクのオープンを試みているときに、NCP が同位ステーションに configure-request パケットを送信した回数

Terminate Tries:
Terminate-Ack を待っている間に、NCP が PPP リンクをクローズする前に Terminate-Request を送信した回数

Config Nak Tries:
PPP リンクのオープンを試みているときに、NCP が同位ステーションに configure-nak (not acknowledged) パケットを送信した回数

Retry Timer:
NCP の configure-request パケット (リンクをオープンするため) および terminate-request パケット (リンクをクローズするため) の転送がタイムアウトになる前に経過するミリ秒数

LLC

LLC コマンドは、LLC 構成環境にアクセスするのに使用します (ソフトウェア・ロードに APPN が含まれている場合にのみ利用可能です)。各コマンドについての説明は、241ページの『LLC 構成コマンド』 を参照してください。

構文:

llc

Set

set コマンドは、HDLC パラメーター、LCP オプションとパラメーター、IPCP オプション、BCP オプション、および NCP パラメーターを設定するのに使用します。『パラメーター』 は、再試行カウントのように内部動作に関連するものです。『オプション』 は、相手側と交渉されるものです。

注:

1. コマンド・オプション・プロンプトの直後の値は、そのオプションの現行設定値です。それらは必ずしも、この章に示されているデフォルト値とは限りません。
2. **set hdlc** コマンドは、PPP ダイヤル回線インターフェースではサポートされません。

構文:

set

bcp

ccp options

ccp algorithms

hdlc...

ipcp

lcp...

name

ncp...

bcp ブリッジング制御プロトコル (BCP) パラメーターを設定します。

例:

```
set bcp
TINYGRAM COMPRESSION  [no]:
```

Tinygram Compression

Tinygram 圧縮が使用されるかどうかを示します。このオプションは、低速 (64 Kbps 以下) 伝送路を介してブリッジするときに問題が起こりやすいプロトコルには便利です。これらのプロトコルは、データとフレーム・チェックサムの間にゼロを追加して、プロトコル・データ単位 (PDU) を最小サイズまで埋め込みます。 Tinygram 圧縮は、ゼロを除去し、フレーム・チェックサムを送信側で保存します。受信側でパケットを最小長さに復元します。

ccp options

圧縮アルゴリズムの構成可能オプションに関するプロンプトを出します。一部のオプションは、WAN リンク上の同位ルーターとの PPP ネゴシエーションによって、後で変更することができます。詳細については、831ページの『第62章 データ圧縮サブシステムの使用』を参照してください。

例:

```
set ccp options
STAC: # histories [1]?
STAC: check mode (0=none, 1-LCB, 2=CRC, 3=Seq) [3]?
```

STAC: # histories

これは、STAC 圧縮エンジンによって使用される圧縮 『コンテキスト』または 『ヒストリー』 の数を設定します。

非ゼロ値は、圧縮エンジンが指定された数のヒストリーを維持し、そこに以前にパケットで送信されたデータに関する情報を保持することを意味します。このヒストリー・データは、圧縮の効率を改善するのに使用されます。

受信側も同様のヒストリーを維持しており、送信側と受信側のヒストリーの同期が保たれている限り、受信側は受信したパケットを正しく解凍することができます。ヒストリーの同期が外れると、パケットは使用不能データとして廃棄されます。リンクの品質が非常に悪くない限り、通常はヒストリーの数は 1 に設定します。

ゼロの値は、送信される各パケットは、過去に送信されたパケットに関係なく圧縮されることを意味しており、常に受信側によって高信頼性で解凍される可能性があります。しかし、圧縮機能は残っている過去のパケットから何も情報を取り出せないので、圧縮の効率はあまりよくないのが一般的です。

一部の実現は、複数のヒストリーをサポートし、データ・ストリームを別々のストリームに分けて、独立して圧縮します。ルーターは、PPP リンクでの複数のヒストリーの使用をサポートしません。

STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq)
STAC 圧縮データグラムには通常、リンクの両端が圧縮パケットの紛失または破壊を認知するのに使用する検査値が含まれており、送信側と受信側のヒストリーを再同期するための何らかのアクションが必要です。

注: 不良パケットを検出できないと、後続のすべてのデータが正しく圧縮されない可能性があります。

このオプションは、使用する正確な形の検査値を設定します。以下の 1 つを選択してください。

0 None: 検査値は使用されません。検査値がないと、パケットの紛失、シーケンス誤り、または破壊を調べる方法がありません。基礎のデータ・リンクが高信頼性の順序保存パケット送達を行わない限り、このモードは使用しないでください。

1 LCB: 『縦方向制御バイト』 が使用されます。これは単純な 8 ビット排他 OR チェックサムです。受信側はパケットの紛失またはシーケンス誤りを検出できず、PPP フレーム・チェックサムの方が高い信頼性でパケットの整合性をテストできるので、*これを使用することは、まったくお勧めできません。*

2 CRC: 16 ビットの巡回冗長検査文字が使用されます。これは、パケットの整合性のテストとして LCB よりは良いと言えますが、受信側はやはりパケットの紛失やシーケンス誤りを検出できず、またフレーム・チェックサムと大きく重複することになるので、この使用もあまりお勧めできません。

3 SEQ: 8 ビットのシーケンス番号が使用されます (デフォルト)。これは運用上すぐれた方式です。ヒストリーの数が 0 でない場合は、これ以外のモードを使用しないように強くお勧めします。ただし、ある種の RFC 非準拠のルーターとの相互運用性のために別のモードを使用するとことが必要になる場合あります。

4 EXT: シーケンス番号モードに似ている拡張モード。各パケッ

トにシーケンス番号が組み込まれますが、圧縮されたフレーム・フォーマットが、より大きく変更されます。拡張モードは、同位との再同期の方法が、他のモードとは異なっています。つまり、2 つのノード間のシグナルは、別個の CCP 制御パケットではなく、圧縮されたデータグラムのヘッダーで渡されるフラグに基づいて行われます。

拡張モードは、ある種の非 RFC 準拠の実現との整合性のために提供されています。モード 3 をサポートしないクライアントの場合にのみ使用してください。

ccp algorithms ***list-of-algorithms***

使用する圧縮プロトコルの正確なリストを指定します。優先順位は、リスト内のエントリーの順序によって決まります。

リンクは、別のノードと圧縮を交渉するときに、プロトコルの全リストを優先順に同位ノードに提供します。同位ノードは、優先順位リストから使用できる最初のプロトコルを選択する必要があります。複数のプロトコルを使用可能にすると、同位はリンク上で使用する圧縮アルゴリズムを指示できるようになります。あるアルゴリズムを避けたい場合は、そのアルゴリズムをリストに指定しないようにします。

none を指定すると、圧縮を使用不可にするのに有効なプロトコルが使用できなくなります。有効な圧縮アルゴリズムは、次のとおりです。

STAC-LZS
RFC 1974 に記述されている STAC-LZS

MPPC RFC 2118 に記述されている Microsoft ポイント・ポイント圧縮アルゴリズム

例:

```
set ccp protocols
Enter a prioritized list of enabled compressors
(first is preferred), all on one single line.
Choices (can be abbreviated) are:
Stac-LZS, MPPC
Compressor list [Stac-LZS:]?
```

hdlc cable *cable type*

HDLC ケーブル・タイプ (インターフェースに接続されている) を、以下のタイプの 1 つに設定します。

RS-232 DTE

RS-232 DCE

V35 DCE

V35 DTE

V36 DTE

X21 DCE

X21 DTE

例: set hdlc cable rs-232 dce

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときに使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときに使用します。

hdlc clocking *external* **または** *internal*

モデムまたは DSU に接続する場合は、クロックを外部として構成します。別の DTE 装置に直接接続する場合は、DCE ケーブルを使用し、一方の側ではクロックを 『内部』 に設定し、他方は 『外部』 に設定します。

内部クロックの場合、まだ回線速度を設定していない場合は、2400 ～ 2048000 の範囲の回線速度を入力するようにプロンプトで指示されます。

例: `set hdlc clocking internal`

hdlc encoding *NRZ* **または** *NRZI*

インターフェースの HDLC 伝送符号化法を設定します。符号化法は、NRZ (非ゼロ復帰記録) または NRZI (非ゼロ復帰反転) に設定できます。 NRZ は、広く一般的に使用されている符号化規則であり、一方の NRZI は一部の IBM 構成で使用されます。デフォルト値は NRZ です。

例: `set hdlc encoding nrz`

hdlc idle *flag* **or** *mark*

データ・リンク・アイドル状態をフラグまたはマークに設定します。

フラグ・オプションは、フレーム間に連続フラグ (7E 16 進数) を提供します。

マーク・オプションは、フレーム間の伝送路をマーキング状態 (OFF, 1) にします。

例: `set hdlc idle flag`

hdlc speed *value*

内部クロックの場合、このコマンドは送信および受信クロック回線の速度を指定します。範囲は 2400 ～ 2 048 000 bps です。

外部クロックの場合、このコマンドはハードウェアには影響を与えませんが、一部のプロトコル (IPX など) がルーティング・パラメーターを決めるのに使用する速度を設定します。そのような場合には、実際の回線速度に一致するように速度を設定してください。速度が構成されていないか、0 に設定されている場合、ソフトウェアは速度を 1 000 000 bps と想定します。外部クロックが使用されている場合、構成できる最大速度は 6 312 000 bps です。

例: `set hdlc speed 56000`

hdlc transmit-delay *value*

フレーム相互間に送信されるフラグの数を設定します。このコマンドの目的は、シリアル・ラインを減速して、相手側の旧型で低速のシリアル装置に整合させることです。

範囲は 0 ～ 15 です。デフォルトは 0 です。

例: `set hdlc transmit-delay 15`

ipcp そのリンクのインターネット・プロトコル制御プロトコル・オプションを設定します。

例:

```
set ipcp
IP COMPRESSION [yes]:
Number of Slots:   [16]?
Send our IP address [yes]:
Note: unnumbered interface addresses will not be sent.
Interface remote IP address to offer if requested (0 for none) [0.0.0.0]?
10.0.0.3
```

IPCP compression

PPP ハンドラーが圧縮 IP データを受け入れるかどうかを選択します。 PPP は、RFC 1144 に記述されている Van Jacobson (VJ) TCP/IP ヘッダー圧縮をサポートします。ポイント・ポイント・リンクが低いボー・レートで動作しているときは、このオプションを使用可能にする必要があります。

この値を yes に設定すると、圧縮オプションが使用可能になります。この値を no に設定すると、オプションは使用不可になります。デフォルト設定値は no です。

Slots 使用可能にされている圧縮のタイプを調べるときに参照するために保存される IP ヘッダーの数を設定します。範囲は 1 〜 16 です。デフォルト値は 16 です。

Send our IP address

ローカル IP アドレスをリンクのリモート側に送信するかどうかを指定します。リンクの相手側が IP アドレスを必要とする場合は、このオプションを 『yes』 に設定する必要があります。

『yes』 に設定すると、インターフェースに番号制 IP アドレスが構成されている場合 (つまり、アドレスが 0 で始まっていない場合)、IPCP は PPP インターフェースの IP アドレスを送信します。このオプションが 『no』 に設定され、同位が IP アドレス・オプションを 0.0.0.0 にセットした Configure NAK を送信した場合、2210 は、番号制アドレスが構成されている場合には、PPP インターフェースのアドレスで応答します。

lcp *options* **or** *parameters*

PPP リンクのリンク制御プロトコル・オプションおよびパラメーターを設定します。

例:

```
set lcp options
Maximum Receive Unit (bytes) [2048]?
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) [A0000] ?
Protocol Field Compression (PFC) [no]?
Addr/Cntl Field Compression (ACFC) [no]?
```

Maximum receive unit

1 つのデータグラムで転送される情報フィールドの最大サイズを設定します。範囲は 576 〜 4089 バイトです。デフォルト値は 2048 です。

Magic number

マジック番号オプションが使用可能かどうかを指定します。マジック番号は、シリアル・ライン構成内のループバック・リンクを検出する方法を提供します。このオプションが使用可能の場合、リンクはシステム・クロックを乱数発生ルーチンとして使用します。生成された乱数は、マジック番号と呼ばれます。

LCP は、マジック番号が存在する (つまり、マジック番号オプションが使用可能にされている) 構成要求を受信すると、受信したマジック番号を同位に送信した最後の構成要求内のマジック番号を比較します。 2 つのマジック番号が異なっている場合、リンクはループバックと見なされません。 2 つの番号が同一の場合、PPP ハンドラーはリンクをダウンにし、マジック番号を再交渉するために再度アップにすることを試みます。

この値を Yes に設定すると、マジック番号オプションが使用可能になります。この値を no に設定すると、オプションは使用不可になります。デフォルト設定値は Yes です。

Async Control Character Map

非同期伝送路上のルーターにパケットを転送するときに、同位が 『エスケープ』 する必要がある文字を示します。これにより、特定の重要な ASCII 制御文字 (XON や XOFF など) をリンク上で透過的に転送することができます。

32 ビットのビット・マスクを 16 進数で指定します。マスクの位置 'N' のビットがセットされている場合、対応する ASCII 文字 'N' をエスケープする必要があります (LSB はビット番号 0 で、ASCII NUL 文字に対応します)。

このオプションのデフォルト値は '0A0000' で、XON および XOFF (control-Q および control-S) をエスケープする必要があることを示します。これは、XON/XOFF を使用してソフトウェアのハンドシェークを行うモデムのために取られている処置です。これが問題でない場合には、ACCM をゼロ (どの文字もエスケープしない) に変更することをお勧めします。

LCP は常に ACCM の交渉を望み (同期伝送路でさえも)、PPP 監視プロセスの **list lcp** コマンドによって、交渉された値が表示されます。しかし、同期伝送路では 『エスケープ』 機構ではなく『ビット・スタッフィング』 機構が採用されているので、ACCM は同期伝送路上では意味をもたないのが通常です。ただし、ルーターが同期から非同期への変換を行うモデムに接続されている場合は、意味を持つことがあります。その場合、その値は非同期側に接続されているモデムの要件を反映させることが必要です。

Addr/Cntl Field Compression (ACFC)

同位がアドレスおよび制御フィールドの圧縮を採用できるかどうかを指定します。

ACFC オプションが LCP によって正常に交渉されている場合には、リンク上でやり取りされるデータグラムでは、各パケットを開始するアドレスおよび制御フィールド・バイトを省略しても構わないことを意味します。これらのバイトは常に 0xFF 03 で、実際の情報は提供しません。ACFC を使用可能にすることは、転送されるデータグラムが 2 バイト短くなることを意味します。

正確に言うと、ユーザーが ACFC を使用可能に設定することは、受信側の能力を示していることになります。 ACFC を使用可能にし、LCP がその交渉に成功した場合、相手側はローカル側に転送するパケ

ットに ACFC を採用できるようになります (ほとんどの PPP オプションはこのように動作します)。ローカル側は、相手側もそのようなパケットを処理する能力があることを示した場合にのみ、アドレスおよび制御フィールドを含まない パケットを転送します。

ACFC を使用可能にすることは、たとえ、相手側がそのオプションを受け入れたとしても、相手側にアドレスおよび制御フィールドなしでパケットを送信することを義務付けるものではありません。 ACFC を使用可能にすることは、オプションで ACFC を使用しても構わない こと、およびルーターはその着信パケットを処理できることを、同位に通知するに過ぎません。同位が ACFC を処理できることを示した場合、ACFC がローカルで使用可能にされているかどうかに関係なく、ルーターは常に転送するパケットで ACFC を実行します。

LCP パケットは、常にアドレスおよび制御フィールドを付けて送信されます。これにより、リンクの同期が失われても、LCP パケットが認知されることが保証されます。

Protocol Field Compression (PFC)

同位がプロトコル・フィールドの圧縮を採用するかどうかを指定します。

『yes』 を指定し、PFC オプションが LCP によって正常に交渉された場合、転送するパケットで 1 バイト節約するために、'0x0000'～'0x00FF' の範囲のこれらのプロトコル値の 『プロトコル』 フィールドから先行ゼロ・バイトを省略しても構いません。この範囲には、大多数のレイヤー 3 プロトコル・データグラムが含まれます。

PPP プロトコル値はすべて、プロトコルの上位バイトには偶数値、下位バイトには奇数値が割り当てられています (ISO 3309 アドレス・フィールドの拡張機構に記述されている汎用機構の使用の一部)。そのため、受信側はプロトコル値の先行バイトが省略されていることを容易に検出できるので (プロトコル・フィールドの最初のバイトは偶数ではなく奇数)、 PFC を使用してもフレームの解釈があいまいになることはありません。

PFC は、ACFC と同様に、受信側の能力であり、前述の ACFC の説明が PFC にも当てはまります。

例:

```
set lcp parameters
Config tries  [20]?
NAK tries  [10]?
Terminate tries  [10]?
Retry timer (mSec)  [3000]?
```

注: コマンド・オプション・プロンプトの直後の値は、そのオプションの現行設定値です。これは必ずしも、この章に示されているデフォルト値とは限りません。

Retry timer

LCP の configure-request パケット (リンクをオープンするため) および terminate-request パケット (リンクをクローズするため) の転送がタイムアウトになる前に経過する時間 (ミリ秒) を設定します。このタイマーが満了するとタイムアウトになり、configure-request および

terminate-request パケットの転送が停止します。範囲は 200 ～ 30000 ミリ秒です。 デフォルト設定値は 3000 ミリ秒です。

Config tries

PPP リンクをオープンするために LCP が configure-request パケットを同位ステーションに送信する回数を設定します。デフォルト値は 20 です。範囲は 1 ～ 100 です。

最初の configure-request パケットが送信された後、再試行タイマーがスタートします。これはパケット紛失を防止するために行われます。

NAK tries

PPP リンクのオープンを試みているときに、LCP が同位ステーションに configure-nak (nak = not acknowledged) パケットを送信する回数を設定します。デフォルト値は 10 です。 範囲は 1 ～ 100 です。

LCP は、受け入れ不能の構成オプションを含んでいる configure-request パケットを受信すると、configure-nak パケットを送信します。これらのパケットは、提供された構成オプションを拒否し、変更された受け入れ可能な値を提案するために送信されます。

Terminate tries

PPP リンクをクローズするために LCP が同位ステーションに terminate-request パケットを送信する回数を設定します。デフォルト値は 10 です。 範囲は 1 ～ 100 です。

最初の terminate-request パケットが送信された後、再試行タイマーがスタートします。これはパケット紛失を防止するために行われます。

name *routerid key*

ルーターが別のルーターからの認証要求に応答するときに使用する名前を設定します。また、装置の暗号化キーも設定します。

注:

1. この製品では、リンク上の同位に送信する名前およびパスワードに使用する 『大文字小文字』 はそのまま保たれますが、すべての名前およびパスワードを小文字 で入力した方が、他のベンダーの製品との相互運用が容易です。
2. 他の実現では、この製品でサポートされているのと同じ最大長の名前およびパスワードを扱えない場合があります。そのような場合、認証機能から無効な名前またはパスワードがあることを知らせるメッセージが出るだけです。このタイプのメッセージを受け取った場合は、ルーター ID およびキーを短くしてみてください。

暗号化キーを 16 進文字で入力するように求められます。

例:

```
set name routerid key
Config>
Config>net x
PPP x Config>
PPP x Config>set name
Enter Local Name:  []?newyork
Password:
Enter password again:
Enable encryption for this user/port (y/n) [No]:y
```

```
Encryption key should be 16 characters long.
Encryption Key (16 characters ) in Hex(0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex(0-9, a-f, A-F):
PPP Local Name = newyork
PPP x Config>
```

ncp parameters

ほとんどの NCP の基本動作パラメーターを設定します。

注: このコマンドには特定のインターフェースを通してアクセスしますが、このコマンドはすべての PPP インターフェースのパラメーターをリセットします。

例:

```
set ncp parameters
Config tries  [20]
NAK tries  [10]?
Terminate tries  [10]?
Retry timer (mSec)  [3000]?
```

Config tries

PPP リンクをオープンするために NCP が configure-request パケットを同位ステーションに送信する回数を設定します。範囲は 1 ～ 100 です。デフォルト値は 20 です。

このアクションは、指定された 1 組の構成オプションを使用して NCP コネクションをオープンしたいことを示します。
configure-request パケットが送信された後、再試行タイマーがスタートします。これはパケット紛失を防止するために行われます。

NAK tries

PPP リンクのオープンを試みているときに、NCP が同位ステーションに送信する configure-nak (nak = not acknowledged) パケットの数を設定します。範囲は 1 ～ 100 です。 デフォルト値は 10 です。

受け入れ不能の構成オプションを含んでいる configure-request パケットを受信すると、NCP は configure-nak パケットを送信します。これらのパケットは、提供された構成オプションを拒否し、変更された受け入れ可能な値を提案するために送信されます。

Terminate tries

PPP リンクをクローズするために NCP が同位ステーションに送信する terminate-request パケットの数を設定します。範囲は 1 ～ 100 です。デフォルト値は 10 です。

このアクションは、NCP コネクションをクローズいしたいことを示します。 terminate-request パケットが送信された後、再試行タイマーがスタートします。これはパケット紛失を防止するために行われます。

Retry timer

NCP の configure-request パケット (リンクをオープンするため) および terminate-request パケット (リンクをクローズするため) の転送がタイムアウトになる前に経過する時間 (ミリ秒) を設定します。このタイマーが満了するとタイムアウトになり、configure-request および terminate-request パケットの転送が停止します。範囲は 200 ～ 30000 ミリ秒です。デフォルト設定値は 3000 ミリ秒です。

インターフェース監視プロセスへのアクセス

PPP インターフェース監視プロセスにアクセスするには、次のようにします。

1. + プロンプトで **interface** と入力して、構成されたインターフェースのリストを表示する。
2. **network** と入力し、続けて PPP インターフェースの番号を入力する。

```
+ network 2
PPP>
```

ポイント・ポイント監視コマンド

この節では、ポイント・ポイント監視コマンドの要約を示し、個々のコマンドについて説明します。コマンドは PPP> プロンプトで入力します。 表62 は、コマンドを示しています。

注: このコマンドで利用可能なオプションは、ルーター・ソフトウェアで利用可能なプロトコルによって決まります。たとえば、ルーター・ソフトウェア (イメージ) に APPN サポートが含まれていない場合、**list isrcp**、**list isr**、 **list hprcp**、**list hpr**、および **llc** コマンドは利用不能です。

表 62. ポイント・ポイント監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Clear	ポイント・ポイント・インターフェースからすべての統計を消去します。
List	ポイント・ポイント・インターフェースと PPP パラメーターおよびオプションに関連した情報およびカウンターを表示します。
LLC	LLC 監視プロンプトを表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Clear

clear コマンドは、ポイント・ポイント・インターフェースからすべての統計を消去するのに使用します。

構文:

clear

List

list コマンドは、ポイント・ポイント・インターフェースと PPP パラメーターおよびオプションに関連した情報およびカウンターを表示するのに使用します。

構文:

list all

control

errors

interface

lcp - PPP link CP

pap - PAP Authentication CP

chap - CHAP Authentication CP

ecp - Encryption Control Protocol

edp- Encrypted packet statistics

spap - SPAP Authentication CP

ccp - PPP Compression CP

cdp - PPP compression

compression - PPP compression

bcp - Bridging (ASRT) CP

brg - Bridging (ASRT)

stp - Spanning Tree Protocol

nbcp - Netbios

nbfcp - Netbios Frame

ipcp - Internet Protocol CP

ip - Internet Protocol

ipxcp - Novell IPX CP

ipx - Novell IPX

atcp - AppleTalk (Phase 2) CP

ap2 - AppleTalk (Phase 2)

dncp - DECnet IV CP

dn - DECnet IV

osicp - ISO's OSI CP

osi - ISO's OSI

bvcp - Banyan VINES CP

vines - Banyan VINES

isrcp - APPN ISR CP

isr - APPN ISR

hprcp - APPN HPR CP

hpr - APPN HPR

all ポイント・ポイント・インターフェースと PPP パラメーターおよびオプショ

ンに関連したすべての情報およびカウンターをリストします。このコマンドで表示される出力は、すべての個別の **list** *item* コマンドからの表示の組み合わせです。

注: あるネットワーク制御プロトコルがインターフェース上で利用不能の場合、そのネットワーク制御プロトコルの list コマンドに対して、プロトコルまたは統計情報が得られないことを知らせるメッセージが表示されます。

control

制御プロトコルの交渉されたオプションまたはその他の状態情報をリストします。

ccp

ecp

lcp

bcp

nbcp

nbfcp

ipcp

ipxcp

atcp

dncp

osicp

bvcp

isrcp

hprcp

例:

```
list control ccp
            CCP State:                Open
            Previous State:           Ack Sent
            Time Since Change:        264 hours, 56 minutes and 58 seconds

            Compressor:   STAC-LZS histories 1, check_mode SEQ
            Decompressor: STAC-LZS histories 1, check_mode SEQ

            Max size of compression dictionary:   12494.
            Max size of decompression dictionary: 4424.
```

CCP state

ポイント・ポイント・リンクの現行状態。 『Open』 の場合、このリンクでは圧縮の交渉に成功しています。 Open でない場合は、リンク上では圧縮は実行されていません。

Previous State

現行状態フィールドに表示されている状態の前のポイント・ポイント・リンクの状態

Compressor

交渉された圧縮機能と使用されているオプションを示します。

Decompressor

交渉された解凍機能と使用されているオプションを示します。

Max size of compression dictionary
圧縮 『コンテキスト』 または 『ヒストリー』 に割り振られたデータ・スペースのサイズ。

Max size of decompression dictionary
解凍 『コンテキスト』 または 『ヒストリー』 に割り振られたデータ・スペースのサイズ。

例:

```
PPP x>list control ecp

ECP State:                Open
Previous State:           Ack Sent
Time Since Change:        16 minutes and 40 seconds

Local (transmit) encrypter: DES
Remote (receive) encrypter: DES
```

ECP State:
ポイント・ポイント・リンクの現行状態。 『Open』 の場合、このリンクでは暗号化の交渉に成功しています。 『Open』 でない場合は、リンク上では暗号化は実行されていません。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Previous State:
現行状態フィールドに表示されている状態の前のポイント・ポイント・リンクの状態。

Time Since Change:
上記の 2 つの状態変更の間の経過時間。

Local (transmit) encrypter:
この暗号化アルゴリズムが、この PPP インターフェース上で送信されるデータの暗号化に使用されます。

Remote (receive) encrypter:
この暗号化アルゴリズムが、このインターフェースで受信されたデータの暗号化解除に使用されます。

例:

```
list control lcp

Version:                  1
          Link phase:               Establishing connection (LCP)
          LCP State:                Listen
          Previous State:           Req Sent
          Time Since Change:        1 minute and 57 seconds
          Remote Username:          - No Authentication -
          Last Identification Rx'd
          Time Connected:           - No Connection -

          LCP Option                Local                     Remote
          ----------                -----                     ------
          Max Receive Unit:         2048                      1500
          Async Char Mask:          FFFFFFFF                  FFFFFFFF
          Authentication:           None                      None
          Magic Number:             7A8CBFD7                  None
```

```
Protocol Field Comp:       No                        No
Addr/Cntl Field Comp:      No                        No
32-Bit Checksum:           No                        No
```

Version
ポイント・ポイント・プロトコルの現行バージョンを表示します。

Link phase
リンク上の現行アクティビティーを表示します。これは次の値のいずれかです。

Dead リンク上にはアクティビティーが存在しません。インターフェースはダウンしています。

LCP リンクは LCP ネゴシエーションの最中です。インターフェースを最初に立ち上げるときに、この状態になります。このとき、インターフェースは自己テストを実行している可能性があります。

Authenticate
リンクは初期認証を実行中です。

ECP リンクは暗号化アルゴリズムを交渉中です。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Ready リンクは通常どおり運用可です。 NCP はネゴシエーションを実行し、NCP ネゴシエーションが成功した後、関連のデータ・トラフィックを伝送することができます。

Terminate
リンクは遮断中です。

LCP State
ポイント・ポイント・リンクの現行状態を表示します。これらの状態には、以下のものが含まれます。

OPEN - コネクションが確立され、データを送信できることを示します。この状態では、再試行タイマーは動作しません。

CLOSED - リンクはダウンしており、それをオープンする試みは行われていないことを示します。この状態では、同位からのすべての接続要求はリジェクトされます。

LISTEN - リンクはダウンしており、それをオープンする試みは行われていないことを示します。ただし、CLOSED 状態とは異なり、同位からのすべての接続要求は受け入れられます。

REQUEST-SENT - リンクをオープンする試みが実行されていることを示します。 Configure-request パケットが送信されましたが、Configure-Ack はまだ受信も送信もされていません。このときは、再試行タイマーが動作しています。

ACK-RECEIVED - Configure-request パケットが送信され、Configure-Ack パケットを受信したことを示します。 Configure-Ack パケットが送信されていないので、再試行タイマーはまだ動作しています。

ACK-SENT - Configure-Ack パケットと Configure-request パケットが送信されたが、Configure-Ack パケットを受信していないことを示します。この状態では、常に再試行タイマーが動作しています。

CLOSING - リンクをクローズする試みが実行されていることを示します。 Terminate-request パケットが送信されましたが、Terminate-Ack パケットを受信していません。この状態では、再試行タイマーが動作しています。

Previous State
現行状態フィールドに表示されている状態の前のポイント・ポイント・リンクの状態を表示します。これらの状態は、Current state フィールドで説明したものと同じです。

Time since change
前回のリンク状態変更からの経過時間を表示します。

Remote Username
リンク上で認証が必要とされている場合、このフィールドは同位が提供した名前を示します。

Last Identification Rx'd
LCP に対して定義されているオプションのパケット・タイプは『Identification』 パケットです。このパケットの内容は未定義ですが、通常は、名前、製造業者、モデル番号、あるいは製造業者が提供するその他の情報など、何らかの識別情報を与えるために同位によって提供される人間可読ストリングが想定されます。ルーターがこの種のパケットを受信した場合、最後に受信したパケットの内容がここに表示されます。

Time Connected
同位がこのリンクに接続されていた時間の長さを示します。

LCP Option
これらのフィールドは、LCP がオープン状態のときは、同位と交渉されたオプションの値を示します。 LCP がオープンしていないときは、これらの値は、以降の LCP ネゴシエーションで使用される初期デフォルト値または構成値を表します。

Max Receive Unit
ローカル側とリモート側が送信できるパケット・サイズの最大長を示します。これは PPP パケットのペイロード部分の最大長であり、PPP ヘッダーとトレーラーのバイト数は含まれません。

LCP がオープン状態のときは、この値は同位と交渉された長さを示します。ルーターは、相手側とローカル側で MRU 長さが異なることはサポートしないので、これらの値は同一になります。

Async Character Mask
これは、交渉された非同期制御文字マスクを示します。ルーターは

同期伝送路でも ACCM ネゴシエーションを受け入れます。ただし、これは実際のパケット・データ送信には影響を与えません。 ACCM の詳細については、496ページの **set lcp options** コマンドの項を参照してください。

Authentication
リンクの各側に必要な認証プロトコル (もしあれば) を示します。各側で複数のプロトコルを使用することも可能です。この値は、装置が使用することに合意したプロトコルを示します。

Magic number
リンクのローカル側とリモート側の両方でループバック検出に使用されている現行のマジック番号を表示します。

Protocol compression
PFC が交渉されたかどうかを示します。

Address/Control compression
ACFC が交渉されたかどうかを示します。

32-bit checksum
現在はサポートされていません。 PPP は、受信した場合、このオプションをリジェクトします。

例:

```
list control bcp
BCP State:            Closed
Previous State:        Closed
Time Since Change:     5 hours, 25 minutes and 3 seconds

BCP Option             Local                    Remote
Tinygram Compression   DISABLED                 DISABLED
Source-route Info:
Remote side does not support source-route bridging
```

BCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

Tinygram Compression
リンクのローカル側およびリモート側の Tinygram 圧縮が使用可能か使用不可かを表示します。

Source-route Info
このインターフェースに対応するローカル・ポートおよびリモート・ポートのソース・ルート・ブリッジングが使用可能かどうかを表示します。

例:

```
list control nbcp
NBCP State:               Closed
Previous State:           Closed
Time Since Change:        3 hours, 48 minutes and 24 seconds

NetBIOS Control Protocol Info:
Local  MAC Address = 0x000000000000
Remote MAC Address = 0x000000000000
Remote NetBIOS Names: (0)
```

NBCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

Local MAC Address
ローカル MAC アドレスは、DOS/Win DIALs クライアントによって使用される MAC アドレスです。これは、疑似乱数またはローカル管理アドレス (LAA) (クライアントに LAA を構成した場合) です。

Remote MAC Address
リモート MAC アドレスは、LAN 上で使用するために 2210 DIAL サーバーがこのクライアントに割り当てた MAC アドレスです。

Remote NetBIOS Name
クライアントがアクセスを要求した LAN リソースの NetBIOS ネームのリスト

例:

```
list control nbfcp
NBFCP State:               Closed
Previous State:            Closed
Time Since Change:         4 hours, 5 minutes and 58 seconds

NetBIOS Frame Control Protocol Info:
Local  MAC Address = 0x000000000000
Remote MAC Address = 0x444553540000
Remote NetBIOS Names: (0)

Remote Peer Class:         0
Remote Peer Version Major: 0
Remote Peer Version Minor: 0
```

NBFCP State フィールドは、**list control lcp** コマンドの項で説明したものと同じです。

Local MAC Address
ローカル MAC アドレスは、Win 95/NT ダイヤルアップ・ネットワーキング・クライアントによって使用される MAC アドレスです。これは、疑似乱数またはローカル管理アドレス (LAA) (クライアントに LAA を構成した場合) です。

Remote MAC Address
リモート MAC アドレスは、LAN 上で使用するために 2210 DIAL サーバーがこのクライアントに割り当てた MAC アドレスです。

Remote NetBIOS Name
クライアントがアクセスを要求した LAN リソースの NetBIOS ネームのリスト。

Remote Peer
Remote Peer Class、Version Major、および Version Minor は、NBFCP 同位情報オプションによって 2210 に戻される情報です。

例:

```
list control ipcp
IPCP State:                Listen
Previous State:            Closed
Time Since Change:         1 hour, 57 minutes and 52 seconds

IPCP Option                Local              Remote
-----------                -----              ------
IP Address                 0.0.0.0            10.0.0.152
Compression Slots          None               None
```

```
DHCP State:               BOUND
Lease Server:             10.0.0.111
Leased IP Address:        10.0.0.152
Lease Time:               4 minutes and 0 seconds
Renewal Time:             2 minutes and 0 seconds
Rebind Time:              3 minutes and 30 seconds
Lease Time Elapsed:       1 second
Lease Time Remaining:     3 minutes and 59 seconds

DHCP Client ID:           0100120B0000
```

IPCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

IP Address:
このインターフェースの IP アドレス (Local) およびリモートの交渉されたアドレス (Remote) (もしあれば) を示します。

Compression Slots
使用可能にされている圧縮のタイプを調べるときに参照するために保存された IP ヘッダーの数を示します。

DHCP State
これは RFC 1541 に記述されている プロキシー DHCP です。

Lease Server
このサーバーからリースを獲得しました。

Leased IP address
クライアントにリースされたアドレス。このアドレスは、上記の『Remote IP Address』 と同等でなければなりません。

Lease Time
このアドレスを DHCP サーバーからリースしている時間の長さ。『Lease Time Elapsed』 がこの時間に等しくなると、リースは満了し、IPCP コネクションはクローズされます。

Renewal Time
この時間の後で、プロキシー DHCP はサーバーからのこのリースの延長を試みます。 『Lease Elapsed Time』 がこの時間に等しくなると、プロキシー DHCP はリースの更新を試み、成功した場合は、『Lease Time』、『Lease Elapsed Time』、および 『Lease Time Remaining』をリセットします。

Rebind Time
プロキシー DHCP が、構成された任意の DHCP サーバーから新規リースを取得することを試みる前の時間。 『Lease Elapsed Time』 がこの時間に等しくなると、プロキシー DHCP は新規リースの取得を試み、成功した場合は、『Lease Time』、『Lease Elapsed Time』、および 『Lease Time Remaining』 をリセットします。

Leased Time Elapsed
このリースの経過時間。リースは更新されている可能性があるので、これは必ずしもこの特定のダイヤルイン・セッションの時間を示すものではありません。リースが更新されると、このタイマーは 0 に戻されます。

Leased Time Remaining
このリースの残り時間。このパラメーターは、『Lease Time』 から『Lease Time Elapsed』を差し引いた値に等しくなります。

DHCP client ID
このクライアント (ダイヤルイン・ユーザー) の固有の ID。 DHCP サーバーとの間でやり取りされるすべての DHCP メッセージは、このクライアント ID によって識別されます。

例:

```
list control ipxcp
IPXCP State:          Closed
Previous State:       Closed
Time Since Change:    2 hours, 9 minutes and 9 seconds
```

IPXCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

例:

```
list control atcp
ATCP State:           Closed
Previous State:       Closed
Time Since Change:    6 hours, 27 minutes and 7 seconds

AppleTalk Address Info:
Common network number = 12
Local node ID = 49
Remote node ID = 76
```

ATCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

Common Network Number
ポイント・ポイント・リンクの 2 つの端のネットワーク番号。 (リンクの両端は、同じネットワーク番号を持つように静的に構成する必要があります。)

Local Node ID
リンクのローカル側の固有のノード番号

Remote Node ID
リンクのリモート側の固有のノード番号

例:

```
list control dncp
DNCP State:              Closed
Previous State:          Closed
Time Since Change:       2 hours, 2 minutes and 58 seconds
```

DNCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

例:

```
list control osicp
OSICP State:          Closed
Previous State:       Closed
Time Since Change:    6 hours, 28 minutes and 32 seconds
```

OSICP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

例:

```
list control bvcp
BVCP State:               Open
Previous State:           Ack Sent
Time Since Change:        403 hours, 49 minutes and 2 seconds
```

BVCP 状態フィールドは、**list control lcp** コマンドの項で説明されているものと同じです。

注: コマンド・ワード **bvcp** および頭字語 BVCP は、Banyan VINES 制御プロトコル (BVCP) を表します。

例:

```
list control isrcp
APPN ISRCP State:         Open
Previous State:           Ack Rcvd
Time Since Change:        1 hour, 48 minutes and 5 seconds
```

APPN ISR 制御プロトコル (ISRCP) 状態フィールドは、list control lcp コマンドの項で説明されているものと同じです。

例:

```
list control hprcp
APPN HPRCP State:         Open
Previous State:           Ack Rcvd
Time Since Change:        1 hour, 48 minutes and 10 seconds
```

APPN HPR 制御プロトコル (HPRCP) 状態フィールドは、list control lcp コマンドの項で説明されているものと同じです。

error PPP ソフトウェアによって検出されたすべての誤り状態に関連する情報をリストします。

例:

```
list error
Error Type                Count          Last One
----------                -----          --------
Bad Address:                 0               0
Bad Control:                 0               0
Unknown Protocol:            0               0
Invalid Protocol:            0               0
Config Timeouts:             0               0
Terminate Timeouts:          0               0
```

Bad address

ポイント・ポイント・リンク上で検出された不正なアドレスの合計数を示します。 『Bad addresses』 は、パケットの先頭の HDLC フレーム・バイトを表します。

Bad control

ポイント・ポイント・リンク上で検出された不正な制御パケットの合計数を示します。 『Bad control』 は、HDLC カプセル化 PPP パケットの 0x03 プレフィックス (0xFF の後に続く 『UI』 値) を表します。

Unknown protocol
現行のリンクで検出された不明なプロトコル・パケットの合計数を示します。

Invalid protocol
現行のリンクで検出された無効なプロトコル・パケットの合計数を示します。

Config timeouts
リンクで発生した構成タイムアウトの合計数を示します。

Terminate timeouts
リンクで発生したリンク終了タイムアウトの合計数を示します。

interface
PPP インターフェースの統計をリストします。

例:

```
list interface
Interface Statistic         In              Out
------------------          --              ---
Packets:                     0               0
Octets:                      0               0
```

Packets
このインターフェースで送受信されたパケットの数を示します。

Octets
このインターフェースで送受信されたオクテット数を示します。

lcp リンク制御プロトコルの統計をリストします。

例:

```
list lcp
LCP STATISTIC        IN       OUT
-------------        --       ---
PACKETS:             42       42
OCTETS:              1260     1260
CFG REQ:             0        0
CFG ACK:             0        0
CFG NAK:             0        0
CFG REJ:             0        0
TERM REQ             0        0
TERM ACK             0        0
ECHO REQ:            21       21
ECHO RESP:           21       21
DISC REQ:            0        0
CODE REJ:            0        0
```

Packets
現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された LCP パケットの合計数を示します。

Octets
LCP フレームの場合、現行のポイント・ポイント・インターフェースを介して送受信されたバイトの合計数をオクテットで示します。

CFG REQ
現行のポイント・ポイント・インターフェースを介して送受信された構成要求 (configure-request) LCP パケットの合計数を示します。

CFG ACK
現行のポイント・ポイント・インターフェースを介して送受信された構成確認 (configure-ack (acknowledged)) LCP パケットの合計数を示します。

CFG NAK
現行のポイント・ポイント・インターフェースを介して送受信された構成非確認 (configure-nak (not acknowledged)) LCP パケットの合計数を示します。

CFG REJ
現行のポイント・ポイント・インターフェースを介して送受信された構成リジェクト (configure-reject) LCP パケットの合計数を示します。

TERM REQ
現行のポイント・ポイント・インターフェースを介して送受信された終了要求 (terminal-request) LCP パケットの合計数

TERM ACK
現行のポイント・ポイント・インターフェースを介して送受信された終了確認 (terminal-ack) LCP パケットの合計数

ECHO REQ
現行のポイント・ポイント・インターフェースを介して送受信されたエコー要求 (echo-request) LCP パケットの合計数を示します。

ECHO RESP
現行のポイント・ポイント・インターフェースを介して送受信されたエコー応答 (echo-response) LCP パケットの合計数を示します。

DISC REQ
現行のポイント・ポイント・インターフェースを介して送受信された廃棄要求 (discard-request) LCP パケットの合計数を示します。

CODE REJ
現行のポイント・ポイント・インターフェースを介して送受信された符号リジェクト (code-reject) LCP パケットの合計数を示します。

pap パスワード認証プロトコルの統計をリストします。

例:

```
list pap
PAP Statistics            In                    Out
--------------            --                    ---
Packets:                  0                     0
Octets:                   0                     0
Requests:                 0                     0
Acks:                     0                     0
Naks:                     0                     0
```

Packets
送信または受信された PAP パケットの合計数

Octets
このパケットで送信または受信されたデータのバイト数

Requests
送信または受信された PAP 『要求』 パケットの数。これらは PAP 名前/パスワードの組みが入っているパケットです

Acks PAP 要求に対して送信または受信された Ack (肯定応答) の数 (たとえば、同位が有効な要求パケットを送信した場合、ルーターは Ack で応答します)。

Naks PAP 要求に対して送信または受信された Nak の数 (たとえば、同位が無効な要求パケットを送信した場合、ルーターは Nak で応答します)。

chap チャレンジ/ハンドシェーク認証プロトコルの統計をリストします。

例:

```
list chap
CHAP Statistics            In                      Out
---------------            --                      ---
Packets:                   0                       0
Octets:                    0                       0
Challenges:                0                       0
Responses:                 0                       0
Successes:                 0                       0
Failures:                  0                       0
```

Packets
送信または受信された CHAP パケットの合計数

Octets
パケットで送信または受信されたデータのバイト数

Challenges
送信または受信された CHAP 『チャレンジ』 パケットの数。 CHAP チャレンジ・パケットには、ランダムに生成された暗号化キーが入っており、そのキーおよび保管されているパスワード情報に基づいて適切なレスポンスを生成することを同位に要求します。

Responses
送信または受信された CHAP 『レスポンス』 パケットの数。レスポンス・パケットには、『チャレンジ』 要求に対する同位の応答が入っています。

Successes/Failures
送信または受信された成功 (Success) または不成功 (Failure) パケットの数。装置はチャレンジ・パケットを送信し、同位のレスポンス・パケットを待ちます。次に、レスポンス・パケットを調べて、そのレスポンスが有効であったかどうかを示すために成功または不成功パケットを送信します。

これらのカウンターは、送信された成功または不成功パケットを反映します。認証が失敗と見なされる前に、同位は正常に応答するために数回試行します。

spap Shiva パスワード認証プロトコルの統計をリストします。

例:

```
list spap
SPAP Statistic             In                      Out
-------------              --                      ---
Packets:                   0                       0
Octets:                    0                       0
Requests:                  0                       0
Acks:                      0                       0
Naks:                      0                       0
Dialbacks:                 0                       0
PleaseAuthenticates:       0                       0
Change Passwords:          0                       0
Alerts:                    0                       0
```

Packets
送信または受信された SPAP パケットの合計数

Octets
このパケットで送信または受信されたデータのバイト数

Requests
送信または受信された SPAP 『Request』 パケットの数。これらは SPAP 名前/パスワードの組みが入っているパケットです

Acks SPAP 要求に対して送信または受信された Ack (肯定応答) の数 (たとえば、同位が有効な要求パケットを送信した場合、ルーターは Ack で応答します)。

Naks SPAP 要求に対して送信または受信された Nak の数 (たとえば、同位が無効な要求パケットを送信した場合、ルーターは Nak で応答します)。

Dialbacks
ユーザーが以下のことを行った回数

- コールバック (ローミング・コールバック) を要求して、それが認められた回数
- ダイヤルインし、それらが必須コールバックに構成されていたために、ユーザー・プロファイルに保管されている事前定義された番号にダイヤルしてコールバックされた回数

PleaseAuthenticates
このインターフェース上で送信または受信された SPAP please authenticate パケットの数。 SPAP please authenticate パケットは、相手側が SPAP 認証要求を送ってくるのを待っているときにタイムアウトになった場合に送信されます。

Change Passwords
このインターフェース上で送信または受信されたパスワード変更要求の数

Alerts 送信または受信された SPAP バナーの数

ccp 圧縮制御プロトコルの統計をリストします。

例:

```
list ccp
CCP   Statistic           In                    Out
---------------           --                    ---
Packets:                  24                    25
Octets:                   174                   177
Reset Reqs                0                     0
Reset Acks:               0                     0
Prot Rejects:             0                     0
```

Packets
このインターフェースで送受信されたパケットの数を示します。

Octets
このインターフェースで送受信されたオクテット数を示します。

Reset Reqs
送信または受信された CCP ディクショナリー 『リセット要求』 の数。

Reset Acks
送信または受信された CCP ディクショナリー 『リセット確認』 の数

リセット要求およびリセット確認パケットは、リンクの各端でデータ・ディレクトリーの同期を維持するために、各端の CCP エンティティー間で渡される制御パケットです。

Prot Rejects
同位によって送信された CCP パケットのプロトコル・リジェクトの数を示します (プロトコル・リジェクトの受信は、同位が CCP をサポートしないことを意味しています)。

cdp このインターフェースで送信または受信された圧縮データ・パケットに関連する統計を表示します。

例:

```
list cdp
Compression Statistic      In                      Out
---------------------      --                      ---
Packets:                   31035                   46550
Octets:                    1614885                 2421137
Compressed Octets:         931416                  1521039
Incompressible Packets:    0                       0
Discarded Packets:         0                       0
Copied Packets:            1                       0
Prot Rejects:              0                       -

Compressor (transmit) statistics:
    Recent compression ratio: 1.7:1
Decompressor (receive) statistics:
    Recent compression ratio: 1.7:1
```

Packets
これらのカウンターは、送受信された圧縮データグラムの数を示します。出力側では、カウントには実際に PPP 圧縮データグラムとして送信されたパケットのみが含まれます。圧縮不能であることが検出され、元の未圧縮の形で送信されたパケットは含まれません。

これらのカウンターは、送信または受信された PPP プロトコル・タイプ X'00FD' (CDP) のパケットをカウントします。 STAC 拡張モードまたは MPPC が交渉された場合、圧縮不能パケットを CDP データグラムにカプセル化することができます。このカプセル化の場合は、圧縮不能パケットもこれらのカウントに含まれます。

Octets
これらのカウンターは、圧縮された形で有効に送信または受信されたバイト数を示します。これらのカウントは、圧縮前または解凍後の元のデータグラムの長さを反映します。

Compressed octets
これらのカウンターは、送受信されたすべての圧縮データグラムのバイト数を示します。これらのカウントは、圧縮後または解凍前の実際の CDP パケットの長さです。

Incompressible packets
これらのカウンターは、圧縮不能であったために元の未圧縮の形で送信されたパケットの数を示します。

Discarded packets
これらのカウンターは、正常に解凍できなかったために廃棄された

パケットの数を示します。通常、これらのパケットは、ルーターがリセット要求を送信した直後、ただし同位がそのリセット要求を受信して処理する前に、同位が送信したパケットです。また、ルーターがパケット内のデータに誤りを検出した場合も、パケットは廃棄されます。データの誤りの一例は、不正なシーケンス番号が入っているパケットです。

廃棄されたパケット数が急増する場合は、おそらく伝送路のノイズまたはリンク性能の低下が原因で、パケットが失われているか、破壊されています。

Protocol rejects

このカウンターは、同位から受信した CDP パケットのプロトコル・リジェクトの数を示します。このカウントはゼロでなければなりません。圧縮の使用が交渉済みでなければ、リンクは CDP パケットを送信しないからです。

Compression ratios

比率は、圧縮機能または解凍機能の効率の概略値を表示します。これらの比率は、テキスト・バイト数を対応する圧縮バイト数で割った値に基づいているので、入力側と出力側の両方とも、1 より大きい値が望まれます。数値が高いほど、圧縮効果が高くなります。

出力比率は、元のテキスト・バイト数を圧縮を試みた結果として送信された (パケットが実際に圧縮されたか、あるいは CDP パケットとして送信された) バイト数で割った比率として計算されます。データ・ストリームが十分に圧縮されず、ほとんどのパケットが元の形あるいは拡大 CDP パケットで送信される場合には、圧縮出力比率は低下します。比率が 1.0 以下に低下する場合は、圧縮機能は実際には伝送路の有効帯域幅を増やすどころか、減らしていることになるので、この状態が長く続く場合は、そのインターフェース上の圧縮を使用不可にすべきです。

入力比率は、CDP フレームで受信したバイト数を解凍されたバイト数で割って計算されます。出力比率とは異なり、このカウントには圧縮不能のためテキスト形式で送信されたパケットは含まれません。これはルーターが、受信した非 CDP パケットは、同位がテキスト形式で送信した圧縮不能パケットであるのか、単に同位が圧縮を試みなかったパケットであるのかを判別できないからです。

この計算方法のため、リンクの一端の出力比率は、必ずしも他端の入力比率と一致していません。

compression

このコマンドは list cdp と同じ情報を表示します。

ecp インターフェース上で送信または受信された暗号化制御プロトコルの統計をリストします。

例:

```
PPP
x>list ecp

ECP Statistic             In                    Out
-------------             --                    ---
Packets:                  2                     2
```

```
Octets:                    26                      26
Reset Reqs:                0                       0
Reset Acks:                0                       0
Prot Rejects:              0                       -
Local (transmit) encrypter: DES
Remote (receive) encrypter: DES
```

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Packets
現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された ECP パケットの合計数を示します。

Octets
ECP パケットで送受信された合計バイト数を示します。

Reset Reqs
このインターフェースで送受信されたリセット要求の数を示します。リセット要求は、ECP が EDP パケットを廃棄するたびに送信されます。

注: DES (サポートされる唯一の暗号化アルゴリズム) はリセット要求を送信しないので、この数はゼロになります。

Reset Acks
このインターフェースで送受信されたリセット確認の数を示します。リセット確認 (Reset Ack) パケットは、リセット要求パケットを受信するたびに送信されます。

注: DES (サポートされる唯一の暗号化アルゴリズム) はリセット要求を送信しないので、この数はゼロになります。

Prot Rejects
現行のポイント・ポイント・インターフェースを介して送受信されたプロトコル・リジェクト・パケットの合計数を示します。

Local (transmit) encrypter
このポイント・ポイント・インターフェースで送信されるデータの暗号化には、この暗号化アルゴリズムが使用されます。

Remote (receive) encrypter
このポイント・ポイント・インターフェースで受信したデータの暗号化解除には、この暗号化アルゴリズムが使用されます。

edp インターフェース上で送信または受信された暗号化パケットに関連した統計をリストします。

例:

```
PPP x>list edp

Encryption Statistic       In                      Out
---------------------      --                      ---
Packets:                   20                      30
Octets:                    29164                   44790
Encrypted Octets:          29280                   44880
Discarded Packets:         0                       0
Prot Rejects:              0                       -
```

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

Packets
現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された IP パケットの合計数を示します。

Octets
現行 IP コネクションを介して送受信されたデータ・バイトの合計オクテット数を示します。

Encrypted Octets
このインターフェースで送受信された、暗号化されたオクテット数を示します。

Discarded Packets
正常に暗号化解除できないために廃棄されたパケットの数を示します。

Prot Rejects
現行のポイント・ポイント・インターフェースを介して送受信されたプロトコル・リジェクト・パケットの合計数を示します。

bcp ブリッジング制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list bcp
BCP Statistic           In                  Out
--------------          --                  ---
Packets:                0                   0
Octets:                 0                   0
Prot Rejects:           0                   -
```

brg PPP インターフェースを介して送受信されたブリッジ・パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list brg
BRG Statistic           In                  Out
--------------          --                  ---
Packets:                0                   0
Octets:                 0                   0
Prot Rejects:           0                   -
```

stp スパンニング・ツリー・プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list stp
Spanning Tree Statistic       In            Out
-----------------------       --            ---
Packets:                      0             0
Octets:                       0             0
```

nbcp ポイント・ポイント・インターフェースの NetBIOS 制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list nbcp
NBCP Statistic          In                  Out
---------------         --                  ---
```

```
Packets:                0                       0
Octets:                 0                       0
Prot Rejects:           0                       -
```

nbfcp ポイント・ポイント・インターフェースの NetBIOS フレーム制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list nbfcp
NBFCP Statistic         In                      Out
---------------         --                      ---
Packets:                0                       0
Octets:                 0                       0
Prot Rejects:           0                       -
```

ipcp ポイント・ポイント・インターフェースのインターネット・プロトコル制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list ipcp
IPCP STATISTIC      IN        OUT
--------------      --        ---
PACKETS:            0          0
OCTETS:             0          0
PROT REJECTS:       0
```

ip ポイント・ポイント・リンクを経由する IP パケットに関するすべての情報をリストします。

例:

```
list ip
IP Statistic        In        Out
------------        --        ---
Packets:            349       351
Octets:             128488    129412
Prot Rejects:       0         -
```

Packets
現行のポイント・ポイント・インターフェースを介して送信 (out) および受信 (in) された IP パケットの合計数を示します。

Octets
現行 IP コネクションを介して送受信されたオクテットの合計数を示します。

Prot Rejects
現行のポイント・ポイント・インターフェースを介して送受信されたプロトコル・リジェクト・パケットの合計数を示します。

ipxcp IPX 制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list ipxcp
IPXCP Statistic          In               Out
--------------          --               ---
Packets:                0                0
Octets:                 0                0
Prot Rejects:           0                -
```

ipx ポイント・ポイント・インターフェースの IPX 統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。(520ページを参照してください。)

例:

```
list ipx
IPX Statistic           In        Out
------------            --         ---
Packets:                0          0
Octets:                 0          0
Prot Rejects:           0          -
```

atcp AppleTalk 制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list atcp
ATCP Statistic          In                    Out
---------------         --                    ---
Packets:                0                     0
Octets:                 0                     0
Prot Rejects:           0                     -
```

ap2 ポイント・ポイント・インターフェースの AppleTalk フェーズ 2 の統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list ap2
AP2 Statistic        In         Out
------------         --         ---
Packets:             349        351
Octets:              128488     129412
Prot Rejects:        0
```

dncp DECnet 制御プロトコル・パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list dncp
DNCP Statistic          In                Out
--------------          --                ---
Packets:                0                 0
Octets:                 0                 0
Prot Rejects:           0                 -
```

dn PPP インターフェースを介して送受信された DECnet パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list dn
DN Statistic            In         Out
------------            --         ---
Packets:                0          0
Octets:                 0          0
Prot Rejects:           0          -
```

osicp OSI 制御プロトコルの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list osicp
OSICP Statistic          In                  Out
---------------          --                  ---
Packets:                 0                   0
Octets:                  0                   0
Prot Rejects:            0                   -
```

osi PPP インターフェースを介して送受信された OSI パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list osi
OSI Statistic          In            Out
-------------          --            ---
Packets:               0             0
Octets:                0             0
Prot Rejects:          0             -
```

bvcp Banyan VINES 制御プロトコルに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list bvcp
BVCP Statistic           In                  Out
--------------           --                  ---
Packets:                 0                   0
Octets:                  0                   0
Prot Rejects:            0                   -
```

vines PPP インターフェースを介して送受信された Banyan VINES パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list vines
Vines Statistic          In                  Out
---------------          --                  ---
Packets:                 10                  13
Octets:                  320                 340
Prot Rejects:            0                   -
```

isrcp APPN ISR 制御プロトコル・パケットの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list isrcp
APPN ISRCP Statistic     In                  Out
---------------          --                  ---
Packets:                 3                   3
Octets:                  12                  12
Prot Rejects:            0                   -
```

isr PPP インターフェースを介して送受信された APPN ISR パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list isr
APPN ISR Statistic       In                  Out
-------------            --                  ---
Packets:                 220                 219
Octets:                  1266                1157
Prot Rejects:            0                   -
```

hprcp APPN HPR 制御プロトコル・パケットの統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list hprcp
APPN HPRCP Statistic       In                    Out
---------------            --                    ---
Packets:                   3                     3
Octets:                    12                    12
Prot Rejects:              0                     -
```

hpr PPP インターフェースを介して送受信された APPN HPR パケットに関する統計をリストします。これらのフィールドは、**list ip** コマンドの項で説明されているものと同じです。 (520ページを参照してください。)

例:

```
list hpr
APPN HPR Statistic          In                     Out
-------------               --                     ---
Packets:                    780                    715
Octets:                     131907                 69685
Prot Rejects:               0                      -
```

LLC

LLC コマンドは、LLC 監視プロンプトにアクセスするのに使用します。 LLC コマンドは、この新たに表示されたプロンプトで入力します。各コマンドについての説明は、245ページの『LLC 監視コマンド』 を参照してください。

注: このコマンドは、ソフトウェア・ロードに APPN が含まれている場合にのみ表示されます。

構文:

llc

ポイント・ポイント・プロトコル・インターフェースと GWCON インターフェース・コマンド

PPP インターフェース・トラフィックは、基礎のデータ・リンク・レベルの装置ドライバーによって伝送されます。 PPP リンクの監視に役立つ追加統計を、装置ドライバーの統計から入手できる場合があります。この統計は GWCON 環境から **interface** コマンドを使用して表示します。 (**interface** コマンドの詳細については、 133ページの『第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』 を参照してください。)

この節に示す統計は、ポイント・ポイント構成で使用される以下のインターフェースについて、GWCON 環境から **interface** コマンドを実行すると表示されます。

例: interface 1

```
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
1  1   PPP/0        81620   5D          0         83            0

  Point to Point MAC/data-link on SCC Serial Line interface

  Adapter cable:           V.35 DTE  RISC Microcode Revision:  1
```

```
  V.24 circuit: 105 106 107 108 109 125 141
  Nicknames:    RTS CTS DSR DTR DCD RI  LL
  PUB 41450:    CA  CB  CC  CD  CF  CE
  State:        ON  OFF OFF ON  OFF OFF OFF

 Line speed:              unknown
 Last port reset:         1 minute, 54 seconds ago

Input frame errors:
  CRC error                     0   alignment (byte length)     0
  missed frame                  0   too long (>  2182 bytes)    0
  aborted frame                 0   DMA/FIFO overrun            0
  L & F bits not set            0
Output frame counters:
  DMA/FIFO underrun errors      0   Output aborts sent          0
```

Nt 初期構成時にソフトウェアによって割り当てられたインターフェース番号

Nt' 初期構成時にソフトウェアによって割り当てられたインターフェース番号

注: ダイヤル回線インターフェースの場合、Nt' は Nt と異なっています。ダイヤル回線インターフェースの場合は、Nt' はダイヤル回線で使用される基本インターフェース (ISDN または V.25bis) を示します。

Interface No
インターフェースのタイプとそのインスタンス番号。ポイント・ポイント・インターフェース・タイプは PPP です。

CSR 基本ネットワークのコマンドおよび状況レジスター・アドレス

Vec 割り込みベクトル・アドレス

Self-Test: Passed
ポイント・ポイント・インターフェースが自己テストに成功した合計回数

Self-Test: Failed
ポイント・ポイント・インターフェースが自己テストに失敗した合計回数

Maintenance: Failed
保守障害の合計数

Adapter cable
構成されたアダプター・ケーブルのタイプ (たとえば、V.35 DTE)

V.24 circuit
V.24 で使用される回線。注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

Nicknames
制御信号の注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

PUB 41450
ピン割り当ての注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

State V.24 回線の状態 (オンまたはオフ)。注: 監視出力の記号 - - - は、値または状態が不明であることを示します。

Line speed
構成された回線速度、または想定されるデフォルト値 (回線速度が 0 として構成されている場合)

Last port reset
ポートがリセットされた後の経過時間

CRC error
チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)
長さが 8 ビットの偶数倍でなかったために廃棄された受信パケットの数

Too long (> 2048 bytes)
構成されたフレーム・サイズより大きかったために廃棄されたパケットの数

Aborted frame
送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun
シリアル・インターフェースがシステム・パケット・バッファー・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

Missed frame
フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

L & F bits not set
シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、`L & F bits not set` カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: `L & F bits not set` カウンターはトラフィックによる影響は受けません。

Output Frame Counters:

DMA/FIFO underrun errors
シリアル・インターフェースがデータをシステム・パケット・バッファー・メモリーから速く検索できなかったので、ネットワークへデータを送信できなかった回数

Output aborts sent
高位レベルのソフトウェアの要求によって打ち切られた伝送の数

PPP インターフェースの監視

第35章 マルチリンク PPP プロトコルの使用

マルチリンク PPP プロトコル (MP) を使用すると、複数のリンクから構成される**バーチャル・リンク** を定義することによって、ISDN B チャネルの帯域幅を増やすことができます。得られる MP バンドルの帯域幅は、個々のリンクの帯域幅の合計にほぼ等しくなります。この方式の利点は、単一リンクを介して転送される大きなデータ・パケットを分割し、複数のリンクを介して転送し、受信側ステーションで再び組み立てることができることです。 MP は、ユーザーのネットワークの ISDN 部分のボトルネックをなくすのに役立ちます。 MP は、帯域幅割り当てプロトコルと帯域幅割り当て制御プロトコルの両方を使用して、リンクをバーチャル・リンクに追加したり、バーチャル・リンクから除去したりします。

MP リンクには 2 つのタイプがあります。すなわち、専用のリンクと使用可能にされるリンクです。専用 MP リンクは、特定の MP インターフェースへのリンクとして構成された MP 使用可能ダイヤル回線です。ダイヤル回線が別の MP バンドルに結合しようとした場合、あるいは MP がまったく交渉されない場合、ソフトウェアは呼を終了します。非専用の MP 使用可能ダイヤル回線は、任意の MP バンドルにリンクすることができます。 MP が交渉されない場合、ダイヤル回線はそのダイヤル回線の構成済みプロトコルを使用して、独立したインターフェースとして稼働します。

重要: チャネル化 ISDN T1/E1 インターフェースを基本ネットとするダイヤル回線は、MP バンドルの一部として使用することはできません。

複数の PPP ダイヤル回線からなるマルチリンク PPP インターフェースを、MP バンドルの一部として構成することができます。この場合、それぞれの PPP ダイヤル回線インターフェースが ISDN 基本ネットを使用していることが必要です。

MP インターフェースにも 2 つのタイプがあります。すなわち、専用のリンクを持っているものと、持っていないものです。以下の状態のいずれの場合も、MP インターフェースは専用リンクが必要です。

- リンクが MP インターフェース専用である。
- MP インターフェースが発呼用に構成されている。この場合、専用リンクに着信電話番号と発信者番号を構成する必要があります。
- MP インターフェースが、特定の着呼を受信するように構成されている。この場合、専用リンクには着信電話番号と発信者番号を構成する必要があります。
- MP インターフェースが発信認証を行う必要がある。この場合、すべてのリンクが同じ認証名を使用します。

専用リンクを持たない MP インターフェースは、着信専用インターフェースでなければなりません。これらのインターフェースは、着信ダイヤル回線に似ています。

MP インターフェースは、帯域幅割り当てプロトコル (BAP) と制御プロトコル (BACP) を用いて、ISDN B チャネルを追加したり除去したりして、帯域幅を増やしたり減らしたりすることができます。帯域幅使用率アルゴリズムにより、バンドルにリンクを追加する必要があると判定された場合、利用可能な PPP ダイヤル回線、利用可能な B チャネル、および同位の合意があれば、追加の発呼が行われます。

MP の使用

BAP は、最初に MP インターフェースにアイドル状態の専用 PPP ダイヤル回線を探し、次に MP が使用可能な PPP ダイヤル回線を探します。しかし、別の MP 回線の専用 PPP ダイヤル回線は使用しません。また、MP インターフェースに構成されているリンクの最大数を超えることはありません。

マルチリンク PPP インターフェースの構成

この節では、2 つの ISDN ダイヤル回線をもつマルチリンク PPP インターフェースの例を使用して、マルチリンク PPP インターフェースを構成する方法を示します。

1. 2 つのダイヤル回線およびマルチリンク PPP インターフェースを追加する。

```
*t 6

Config>add dev dial-circuit
Adding device as interface 7
Defaulting Data-link protocol to PPP
Use "net 7" command to configure circuit parameters
Config>add dev dial-circuit
Adding device as interface 8
Defaulting Data-link protocol to PPP
Use "net 8" command to configure circuit parameters
Config>add dev multilink-ppp
Adding device as interface 9
Defaulting Data-link protocol to PPP
Use "net 9" command to configure circuit parameters
Config>
```

2. 各 PPP ダイヤル回線を構成する。 (653ページの『第47章 ダイヤル回線の使用』を参照してください。) この例では、着信側、呼の方向、および LID は、ダイヤル回線の 1 つに設定されています。

```
Config>net 7
Circuit configuration
Circuit config:   7>set dest out
Circuit config:   7>set calls outbound
Circuit config:   7>set net 6
Circuit config:   7>
```

3. 次のように入力して、MP に使用する各ダイヤル回線上の MP を使用可能にする。

```
Circuit config:   7>encapsulator
Point-to-Point user configuration
PPP 7 Config>enable mp

Enabled as a Multilink PPP Link,
Use as a dedicated Multilink PPP link? [No]: yes
Multilink PPP net for this Multilink PPP link [1]? 9
NOTE: PPP configuration will be obtained from the Multilink PPP
      net.  It is NOT necessary to configure PPP for this net!
```

注: このプロンプトからは、専用リンクの PPP パラメーターを構成することはできません。専用リンクは、既存の MP インターフェースの PPP 構成を使用します。

質問 『Use as a dedicated Multilink PPP link?』 に対して 『Yes』 と応答すると、そのリンクは指定されたマルチリンク PPP インターフェース (この例では 9) の専用になります。この場合、このリンクは MP バンドル専用に使用する***必要*** があり、指定された MP インターフェースに結合する***必要*** があります。このリンクは、通常の PPP ダイヤル回線として使用することはできません。

『Use as a dedicated Multilink PPP link?』 に対して 『No』 と応答すると、この PPP ダイヤル回線は任意の MP インターフェースに結合することができます。少なくとも 1 つの PPP ダイヤル回線が、発信 MP インターフェースへの専用リンクであることが***必要*** です。

専用 PPP ダイヤル回線は、すべての PPP パラメーター (LCP オプション、認証、その他) を MP インターフェースから入手します。同じ MP バンドルに結合されている MP 使用可能 PPP ダイヤル回線は、ネゴシエーションにより同じ LCP パラメーターおよび認証名に設定する***必要*** があります。

4. MP インターフェースを構成する。 『Dialout MP link net』 は、専用 PPP ダイヤル回線でなければなりません。

```
Config>net 9
Circuit configuration
MP config:   9>set calls out
Dialout MP link net for this MP Net [0]? 7
MP config:   9>
```

プロトコル BAP、BRS、WAN 復元、WAN 再ルート、およびダイヤル・オンデマンドはすべて、PPP ダイヤル回線上ではなく、MP インターフェース上で実行されます。

第36章 マルチプロトコル PPP プロトコル (MP) の構成および監視

この章では、装置内の特定のマルチリンク PPP インターフェースを構成する方法について説明します。本章には、以下の節が含まれています。

MP 構成プロンプトへのアクセス

`MP config>` プロンプトにアクセスするには、次のようにします。

1. `*` プロンプトで **talk 6** と入力する。
2. **net *n*** と入力する。ただし n は、MP が使用可能にされているダイヤル回線の番号です。

注: ここで構成するのは、マルチリンク PPP インターフェースであって、MP バンドルの一部である PPP ダイヤル回線ではありません。

マルチリンク PPP インターフェースの MP 構成コマンド

表63 は、`MP config >` プロンプトで利用可能なコマンドをリストしています。

表 63. MP 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Disable	オンデマンドの BAP/BACP および帯域幅ネゴシエーションを使用不可にします。
Enable	オンデマンドの BAP/BACP および帯域幅ネゴシエーションを使用可能にします。
Encapsulator	`PPP config >` プロンプトに入り、データ・リンク・プロトコル構成を変更できるようにします。
List	MP インターフェース構成パラメーターを表示します。
Set	MP インターフェースを着信または発信トラフィック用に構成します。アイドル・タイムアウトやその他の MP および BAP パラメーターを設定することもできます。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Disable

disable コマンドは、BAP のネゴシエーションを使用不可にするのに使用します。BAP を使用不可にすると、リンクは必要なときに追加帯域幅を割り振りません。

構文:

disable bap

Enable

enable コマンドは、BAP のネゴシエーションを使用可能にするのに使用します。BAP を使用可能にすると、リンクは必要なときに追加帯域幅を割り振ることができます。

構文:

enable bap

Encapsulator

encapsulator コマンドは、マルチリンク PPP インターフェースの PPP リンク・レイヤー構成にアクセスするのに使用します。

構文:

encapsulator

例:

```
encapsulator
Point-to-Point user configuration
PPP config>
```

List

list コマンドは、現行の MP 構成を表示するのに使用します。

構文:

list

例:

```
list
Idle timer = 0 (fixed circuit)
Outbound calls = allowed
Dialout MP Link net = 7
Max fragment size = 750
Min fragment size = 375
Maximum number of active links = 2
Links associated with this MP bundle:
net number 7
net number 8
BAP enabled
Add bandwidth percentage = 90
Drop bandwidth percentage = 70
Bandwidth test interval (sec) = 15
```

Idle timer

この回線のアイドル・タイマーの設定値 (秒)

設定値 0 は、固定回線を示します。非ゼロの設定値は、回線が指定された秒数の間アイドル状態であるとダウンにされるダイヤル・オンデマンド MP 回線を構成します。ネットワーク通信が再開されると、回線は再起動されます。

Outbound calls
インターフェースを発信用に構成するかどうかを指定します。インターフェースが呼を開始できない場合には、この行は表示されません。

Inbound calls
インターフェースを着信用に構成するかどうかを指定します。インターフェースが着呼を受け入れることができない場合には、この行は表示されません。

Dialout MP link net
発信 MP 回線の最初の発呼を行うように構成された ISDN ダイヤル回線

Max fragment size
MP リンクを介して送信するためにパケットを分割する前に、パケットに含めることができるデータの最大バイト数を指定します。

Min fragment size
これは、パケットが ***Max fragment size*** を超過する場合にソフトウェアが分割する最小サイズ (バイト) です。

Maximum number of active links
MP バーチャル・リンク (***バンドル*** とも呼ばれます) に構成できるリンクの最大数を指定します。

Links associated with this MP bundle
この MP インターフェースに専用のリンクを表示します。

BAP enabled
このインターフェース上で BAP が使用可能かどうかを指定します。

Add bandwidth percentage
BAP が使用可能の場合、ソフトウェアが新規リンクの追加を試みるときの帯域幅使用率

Drop bandwidth percentage
BAP が使用可能の場合、ソフトウェアが MP バンドルからリンクを除去するときの帯域幅使用率

Bandwidth test interval
バンドルにリンクを追加したり、除去したりする必要があるかどうかを調べるために、ソフトウェアが帯域幅使用率をチェックする時間間隔 (秒)

Set

set コマンドは、以下を構成するのに使用します。

- 着信用または発信用の MP インターフェース
- アイドル・タイムアウト
- MP パラメーター
- BAP パラメーター

構文:

set bap parameters
calls

idle

mp parameters

bap parameters

BAP 追加および除去の帯域幅使用率と BAP テスト間隔を指定するようにプロンプトで指示されます。

例:

```
set bap parameters
Add bandwidth % [90]? 80
Drop bandwidth % [70]? 50
Bandwidth test interval (sec) [15]? 25
```

Add bandwidth %

ソフトウェアが新規リンクの追加を試みるときの帯域幅使用率

有効値: 1 ～ 99

デフォルト値: 90

Drop bandwidth %

ソフトウェアが MP バンドルからリンクを除去するときの帯域幅使用率

有効値: 1 ～ 99

デフォルト値: 70

Bandwidth test interval (sec)

バンドルにリンクを追加したり、除去したりする必要があるかどうかを調べるために、ソフトウェアが帯域幅使用率をチェックする時間間隔 (秒)

有効値: 10 ～ 200 秒

デフォルト値: 15

calls このインターフェースが発信専用、着信専用、あるいは両方のタイプの呼のいずれに使用されるのかを指定します。

有効値: 着信、発信、または両方

デフォルト値: 着信

注: 発信または両方を指定した場合、ソフトウェアは最初に発信する専用 MP リンクの番号を要求します。

例:

```
set calls outbound
Dialout MP link net for this MP net []? 4
```

idle MP インターフェースがすべてのリンクの呼を終了する前に、インターフェース上にプロトコル・トラフィックがない状態でいられる期間 (秒数) を指定します。

有効値: 0 ～ 65535

デフォルト値: 0

mp parameters

最大と最小の分割サイズとアクティブ・リンクの最大数を入力するように求めます。

例:

```
set mp parameters
Max frag size [750]? 675
Min frag size [375]? 300
Max number of active links [2]? 4
```

Max frag size

MP リンクを介して送信するためにパケットを分割する前に、パケットに含めることができるデータの最大バイト数を指定します。

有効値: 100 ～ 3 000

デフォルト値: 750

Min frag size

これは、パケットが ***Max fragment size*** を超過する場合にソフトウェアが分割する最小サイズ (バイト) です。

有効値: 100 ～ 3 000

デフォルト値: 375

Max number of active links

MP バーチャル・リンク (***バンドル*** とも呼ばれます) に構成できるリンクの最大数を指定します。

有効値: 1 ～ 64

デフォルト値: 2

MP インターフェース状態の監視

装置内のすべての MP インターフェースの状態を調べるには、 **talk 5** で **configuration** コマンドを使用します (137ページの『Configuration』 を参照してください)。

MP 監視コマンドへのアクセス

MP 監視コマンドにアクセスするには、次のようにします。

1. * プロンプトで **talk 5** と入力する。
2. **net *n*** と入力する。ただし、***n*** は MP インターフェースの番号です。

マルチリンク PPP プロトコル監視コマンド

表64 は、MP インターフェースで利用可能なコマンドを示しています。

表 64. MP 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	BAP、BACP、および MP 統計、誤り、およびその他の情報を表示します。

表 64. MP 監視コマンド (続き)

コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、帯域幅割り当て統計を含めて、MP インターフェースに関する情報を表示するのに使用します。

構文:

list bacp
bap
control bacp
control bap
control mp
mp

注: 以下の例では、この装置上の MP インターフェースは、ネットワーク番号 6 と想定しています。

bacp **list bacp** コマンドは、この MP 回線上で送信または受信された帯域幅割り当て制御パケットの統計をリストします。

例:

```
PPP 6> list bacp

BACP Statistic             In          Out
-------------              --          ---
Packets:                   6           8
Octets:                    60          80
Rejects:                   0           -
```

bap **list bap** コマンドは、この MP 回線上で送信または受信された帯域幅割り当てプロトコル・パケットの統計をリストします。

例:

```
PPP 6> list bap

BAP Statistic               In          Out
-------------               --          ---
Packets:                    3           3
Octets:                     22          37
Call Requests:              1           0
Call Response(ACK):         0           1
Call Resp(NK & FLLNK):      0           0
Call Response(Rej):         0           0
Callback Requests:          0           0
Callback Response(ACK):     0           0
Cllbck Resp(NK & FLLNK):    0           0
Callback Response(Rej):     0           0
Drop Requests:              0           1
Drop Response(ACK):         1           0
Drop Resp(NK & FLLNK):      0           0
Drop Response(Rej):         0           0
Call Status(Success):       1           0
Call Status(Fail):          0           0
```

同位の要求に対するレスポンスは、ACK、NAK、FULL-NAK、および REJECT の 4 種類です。

ACK 同位の要求が受け入れられたことを示します。

NAK (NK)
同位の要求はサポートされますが、この時点では受け入れられないことを示します。後で再試行します。

FULL-NAK (FLLNK)
同位の要求はサポートされますが、資源の状態により、この時点では受け入れられないことを示します。 MP バンドル全体の合計帯域幅が変更されるまでは、この要求を再び送信してはなりません。

REJECT (REJ)
要求はサポートされないことを示します。

control bacp

list control bacp コマンドは、PPP 内部の BACP 状態遷移の現行状態をリストします。この状態情報は、すべての PPP 制御プロトコルで生成されるものと同一です。優先同位に関する情報もリストされます。優先同位は、BAP パケット衝突 (両側が同時に要求を開始した場合) を回避するために使用されます。 BACP ネゴシエーションの際に、それぞれの側がマジック番号を送信し、小さい方のマジック番号をもつ側が優先同位となり、衝突したときには優先されます。通常は、起呼側は**マジック番号** X'1' を選択し、呼の受信側はマジック番号 X'FFFFFFFF' を選択するので、起呼側が優先同位になります。

```
PPP 6> list control bacp

BACP State:                Open

BACP Option                Local                    Remote
----------                 -----                    ------
Magic Number:              FFFFFFFF                 1
Favorite Peer:             NO                       YES
```

control bap

list control bap コマンドは、帯域幅割り当てプロトコルとオンデマンドの帯域幅の状態をリストします。この情報には、BAP 状態、帯域幅の追加および削除のために構成されたオンデマンドの帯域幅パラメーター、現行の帯域幅、および前回の帯域幅ポーリングからの情報が含まれます。

例:

```
PPP 6> list control bap

BAP State:                                      Ready
Bandwidth test interval (sec):                  15
Add bandwidth percentage:                       90
Drop percentage (links-1):                      70
Max # active links in MP bundle:                3
Time since last Bandwidth check (sec):          5
Currently:
    # active links in MP bundle:                1
    Total MP bandwidth (Bytes/sec):             8000
Last Bandwidth Check:
    # active links in MP bundle:                2
    Avg Inbound bandwidth util (%):             12
    Avg Outbound bandwidth util (%):            12
    Drop check: Avg In (%) for links-1:         24
    Drop check: Avg Out (%) for links-1:        24
```

注: 除去比率は links - 1 の現行使用率を考慮しています。

有効な BAP 状態は、以下のとおりです。

Closed
BACP はオープンされていません - BAP が使用可能にされていないか、同位によってサポートされないかのいずれかです。

Ready BACP がオープンされ、処理中のアウトスタンディング要求はありません。

Call Req Sent
ローカル・マシンから送信されたアウトスタンディング発呼要求があります。

Callback Req Sent
ローカルで送信されたアウトスタンディングのコールバック要求があります。

Call Placed
帯域幅を追加するための BAP 要求の結果、起呼されました。

Retry Status Sent
発呼が MP バンドルに結合するのに失敗し、再試行状態が送信されました。

No Retry Status Sent
発呼が成功したか、またはすべての再試行回数を使い尽くして、再試行不能状態が送信されました。

Drop Req Sent
ローカルで送信されたアウトスタンディングの除去要求があります。

構成された bandwidth-on-demand パラメーターには、追加比率、除去比率、MP バンドル内のアクティブ・リンクの最大数、および帯域幅ポーリング間隔が含まれます。

バンドルにリンクを追加するための BAP 要求は、次の条件が両方とも満たされている場合に開始されます。

- 現在のアクティブ・リンク数が、構成されたリンクの最大数より少ない。
- MP バンドル内のすべてのリンクの帯域幅使用率が、その MP バンドルで利用可能な合計帯域幅の追加比率より大きい。

MP からリンクを除去するための BAP 要求は、次の条件が両方とも満たされている場合に開始されます。

- アクティブ・リンクの数が 1 より多い。
- MP バンドル内のすべてのリンクの帯域幅使用率が、その MP バンドルのリンク数マイナス 1 の利用可能な合計帯域幅の除去比率より小さい。

帯域幅のポーリングは、BAP がレディー状態のときにのみ行うことができます。前回のポーリングからリストされた情報は、MP バンドル全体の帯域幅使用率の様子を伝えます。

除去を開始できるときには、次の 2 組の情報が表示されます。

- バンドル全体の帯域幅使用率
- リンク数マイナス 1 の帯域幅使用率

スラッシングを防止するために、リンクを除去するかどうかを判別するときには、2 番目の組の情報が使用されます。

control mp

list control mp コマンドは、アクティブ・リンク数と帯域幅、構成されたリンクの最大数、および廃棄されたパケット数の統計を含めて、この MP 回線の現行状態をリストします。廃棄された MP パケットは、4 つのカテゴリーに分類されます。

M
シーケンス番号が受信されておらず、すべてのリンクの前回受信したシーケンス番号のうちの最小シーケンス番号より小さいためにパケットが廃棄されました。

Timeout
タイムアウト期間中にシーケンス番号を受信しなかったので、パケットが廃棄されました。

Q depth
最大待ち行列の長さを超えたために、パケットが廃棄されました。

Seq order
予期しなかったシーケンス番号を受信したために、パケットが廃棄されました。これは MP がすでに紛失したと宣言された遅延パケットを受信した場合に起こります。

パケットがネットワーク・レイヤーで廃棄された場合は、M、Timeout、または Q depth パケットのいずれかです。これらのカウンターは、パケットが廃棄されると、それに応じて増分されます。

```
PPP 6> list control mp

Current # active links in MP bundle:        2
Max # active links in MP bundle:            3
Total MP bandwidth (Bytes/sec):             16000
Dropped Frags (lost - M):                   0
Dropped Frags (timeout):                    0
Dropped Frags (Q depth):                    0
Dropped Frags (seq order):                  0
```

mp

list mp コマンドは、この MP 回線で送信または受信されたパケットの統計をリストします。表示されるバイト数は、マルチリンク PPP バンドルの解凍がネゴシエーションされた場合は、解凍前のパケットのバイト数です。

```
PPP 6> list mp

MP Statistic                In          Out
------------                --          ---
Bytes (Compressed):         61230       60259
```

第37章 SDLC リレーの使用

この章では、同期データ・リンク制御 (SDLC) リレー・インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『基本構成手順』

DLSw SDLC と SDLC リレーの使い分け方については、 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻バージョン 3.1* の中の 『DLSw の使用と構成』 の章の 『SDLC リレー機能の関係』 を参照してください。

基本構成手順

この節では、SDLC リレー・プロトコルを立ち上げて実行するのに必要な最小構成ステップについて概説します。詳しい構成情報および説明が必要な場合は、本章の構成コマンドの説明個所を参照してください。

注: 新しい構成変更を有効にするためには、ルーターをリスタートする必要があります。

- *番号を追加する。* **add group** コマンドを使用して、1 次または 2 次ポートのグループに番号を追加することが必要です。このコマンドのデフォルト番号は 1 です。
- *ローカル・ポートを追加する。* これは、ローカル・ポートで使用するインターフェースを識別します。またこれにより、選択したインターフェースに対して IP アドレスが構成されないことも保証されます。 **add local-port** コマンドを使用します。
- *リモート・ポートを追加する。* これは、シリアル・ラインのリモート側に直接接続されたポートを識別します。 **add remote-port** コマンドを使用します。

第38章 SDLC リレーの構成

この章では、同期データ・リンク制御 (SDLC) リレーの構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

SDLC リレー構成環境へのアクセス

SDLC リレー (SRLY) 構成環境にアクセスするには、次のようにします。

1. Config> プロンプトで **set data-link srly** と入力する。
2. インターフェース番号を入力する。
3. SRLY インターフェースを構成するために、**network** *interface#* コマンドを入力する。 **network *interface#*** を入力すると、SRLY *interface#* Config> プロンプトが表示されます。

```
Config>network 2
SDLC relay interface user configuration
SRLY 1 Config>
```

4. SRLY プロトコル・パラメーターを構成するために、**protocol sdlc** コマンドを入力する。 **protocol sdlc** を入力すると、SDLC Relay config> プロンプトが表示されます。

```
Config>protocol sdlc
SDLC Relay protocol user configuration
SDLC Relay config>
```

SDLC リレー構成コマンド

この節では、SDLC リレー構成コマンドの要約を示します。この章には、SDLC リレーの **network** パラメーターと **protocol** パラメーターの両方が記載されています。

SDLC リレー構成コマンドでは、SDLC リレー・フレームを転送するインターフェースのルーター・パラメーターを指定することができます。構成コマンドをアクティブにするには、ルーターをリスタートする必要があります。 表65 は、**network sdlc** および **protocol sdlc** の両方のコマンドを示しています。

表 65. SDLC リレー構成コマンドの要約

コマンド	ネットワーク SRLY	プロトコル SDLC	機能
? (Help)	可	可	すべての SDLC リレー構成コマンドをリストするか、または特定のコマンドに関連するオプションをリストします。
Add		可	グループ、ローカル・ポート、およびリモート・ポートを追加します。
Delete		可	グループ、ローカル・ポート、およびリモート・ポートを削除します。

表 65. SDLC リレー構成コマンドの要約 (続き)

コマンド	ネットワーク SRLY	プロトコル SDLC	機能
Disable		可	グループおよびポートを使用不可にします。
Enable		可	グループおよびポートを使用可能にします。
List	可	可	SDLC リレー全体の構成およびグループ特有の構成を表示します。
Set	可		リンク・パラメーターおよびリモート端末パラメーターを設定します。
Exit	可	可	SDLC リレー構成環境を終了して、CONFIG 環境に戻ります。

Add

add コマンドは、グループ番号、ローカル・ポート、およびリモート・ポートを追加するのに使用します。

構文: add

group

local-port

remote-port

group ルーターに追加された 1 次または 2 次ポートのグループに番号を割り当てます。

例: add group

```
Group number: [1]? 1
```

Group number
そのポートに指定するグループ番号

local-port
ローカル・ポートに使用するインターフェースを識別します。

例: add local-port

```
Group number: [1]? 1
Interface number: [0]? 2
(P)rimary or (S)econdary:[S]? p
```

Group number
そのポートのグループ番号。この番号は、以前に構成された **add group** パラメーターの 1 つに一致していなければなりません。

Interface number
ローカル・ポートを示すルーターのインターフェース番号

Primary or Secondary
ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。

remote-port
リモート・ルーターのシリアル・ラインに直接接続されたポートの IP アドレスを識別します。

例: add remote-port

```
Group number: [1]? 1
IP address of remote router:[0.0.0.0]? 128.185.121.97
(P)rimary or (S)econdary:[S]? s
```

Group number
そのポートのグループ番号。この番号は、以前に構成された add group パラメーターの 1 つに一致していなければなりません。

IP address of remote router
リモート・ルーター上のインターフェースの IP アドレスを識別します。

Primary or Secondary
ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。

Delete

delete コマンドは、グループ番号、ローカル・ポート、およびリモート・ポートを削除するのに使用します。

構文: delete

group . . .

local-port . . .

remote-port

group *group#*
SDLC リレーの構成済みポートのグループ (group#) を除去します。

例: `delete group 1`

local-port *interface#*
指定されたインターフェース (interface#) のローカル・ポートを除去します。

例: `delete local-port 2`

remote-port
指定されたグループのリモート・ポートを除去します。

例: `delete remote-port`

```
Group number: [1]? 1
(P)rimary or (S)econdary:[S]? S
```

Group number
リモート・ポートのグループ番号

Primary or Secondary
ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。

Disable

disable コマンドは、リレー・グループ全体または特定のリレー・ポートのリレーを抑制します。

構文: disable

group . . .

port

group *group#*
特定のグループ (group#) との間の SDLC リレー・フレームの転送を抑制します。

例: disable group 1

port 特定のローカル・ポートとの間の SDLC リレー・フレームの転送を抑制します。

例: disable port

```
Group number: [1]? 2
(P)rimary or (S)econdary:[S]? s
```

Group number
使用不可にするポートのグループ番号

Primary or Secondary
ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。

Enable

enable コマンドは、グループ全体または特定のローカル・インターフェース・ポートのデータ転送をオンにするのに使用します。

構文: enable

group . . .

port

group *group#*
指定されたグループ (group#) との間の SDLC リレー・フレームの転送を可能にします。

例: enable group 1

port 指定されたローカル・ポートとの間の SDLC リレー・フレームの転送を可能にします。

例: enable port

```
Group number: [1]? 2
(P)rimary or (S)econdary:[S]? s
```

Group number
使用可能にするポートのグループ番号

Primary or Secondary
ポート・タイプ (1 次 (P) または 2 次 (S)) を指定します。

List (ネットワーク SRLY の場合)

list コマンドは、特定のグループまたはすべてのグループの構成を表示するのに使用します。

構文: list

例: **list**

```
Maximum frame size in bytes = 2048
Encoding:  NRZ
Idle State:  Flag
Clocking:  External
Cable Type:  RS-232 DTE
Speed (bps):  0
Transmit Delay Counter:  0
```

Maximum frame size in bytes
リンクを介して送信できる最大フレーム・サイズ。最大フレーム・サイズは、最大フレームと 15 バイトの SRLY ヘッダーが収まる大きさでなければなりません。

Encoding
シリアル・インターフェースの伝送符号化法。符号化法は、NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) です。

Idle State
データ・リンク・アイドル状態: フラグまたはマーク

Clocking
クロックのタイプ: 内部または外部

Cable Type
シリアル・インターフェースのケーブル・タイプ

Speed (bps)
送信クロックと受信クロックの速度をリストします。

Transmit Delay Counter
連続するフレーム相互間に送信されるフラグの数

List (プロトコル SDLC の場合)

list コマンドは、特定のグループまたはすべてのグループの構成を表示するのに使用します。

構文: list

all

group . . .

all すべてのローカル・ポートの構成を表示します。

例: `list all`

```
                SDLC Relay Configuration

Group Number     Port Status      Net   SDLC Station    IP Address
                                 Number address (hex)
-------------- ----------------- ------ -------------  ------------
    1 (E)      Local   PRMRY (D)   2
    1 (E)      Remote SCNDRY (E)                      128.185.452.11
    2 (D)      Local   PRMRY (D)   1
    2 (D)      Remote SCNDRY (D)                      128.185.450.31
```

Group Number　グループ番号とグループの状態 (使用可能 (E) または使用不可 (D)) を示します。

Port Status　ポートのタイプ (ローカル/リモート 1次/2 次) とその状態 (使用可能 (E) または使用不可 (D)) を示します。

Net Number　ローカル・ポートの装置番号を示します。この番号は、Config list devices コマンドを使用して表示した番号に一致します。

IP Address　リモート・ポートの IP アドレスを示します。

group *group#*
指定されたグループの構成を表示します。

例: `list group 1`

```
                SDLC Relay Configuration

 Group Number     Port Status      Net   SDLC Station    IP Address
                                  Number address (hex)
------------- -----------------  ------ -------------  ------------
    1 (E)      Local   PRMRY (D)   2
    1 (E)      Remote SCNDRY (E)                     128.185.452.11
```

Group Number　グループ番号とグループの状態 (使用可能 (E) または使用不可 (D)) を示します。

Port Status　ポートのタイプ (ローカル/リモート 1次/2 次) とその状態 (使用可能 (E) または使用不可 (D)) を示します。

Net Number　ローカル・ポートの装置番号を示します。この番号は、Config list devices コマンドを使用して表示した番号に一致します。

IP Address　リモート・ポートの IP アドレスを示します。

Set

set コマンドは、SRLY パラメーターを構成するのに使用します。

構文: set

cable

clocking

encoding

frame-size

idle

speed

transmit-delay

cable　シリアル・インターフェースで使用されるケーブルを設定します。オプションは、次のとおりです。

- RS-232 DTE
- RS-232 DCE
- V35 DCE
- V35 DTE
- V36 DTE
- X21 DCE
- X21 DTE

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときに使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときに使用します。

clocking *internal* **or** *external*

SRLY リンクのクロックを構成します。モデムまたは DSU に接続する場合は、クロックを外部として構成します。別の DTE 装置に直接接続する場合は、DCE ケーブルを使用し、クロックを内部として設定し、クロック速度を構成します。内部クロックの場合は、2400 ～ 2048000 ビット/秒の範囲の有効な回線速度を入力する必要があります。

例: `set clocking internal`

encoding *nrz* **or** *nrzi*
SRLY インターフェースの伝送符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) として構成します。 NRZ がデフォルトです。

例: `set encoding nrz`

frame-size
データ・リンク上で送受信できるフレームの最大サイズを構成します。この値を add remote-secondary コマンドで指定した値より大きく設定した場合、この値はその最大値を反映するように変更されます。 IBM 2210 は、この値が変更されることをユーザーに警告するメッセージを生成します。ユーザーは、これが SRAM 構成内で変更されるまで、この ELS メッセージを継続的に受け取ります。有効な入力値を表66 に示します。

注: 最大フレーム・サイズは、最大フレームと 15 バイトの SRLY ヘッダーが収まる大きさでなければなりません。

表 66. Set Frame-Size コマンドのフレーム・サイズの有効値

最小	最大	デフォルト
128	18000	2048

idle flag
SRLY インターフェース上のフレーム転送の送信アイドル状態を構成します。デフォルト設定はフラグ・オプションで、これはフレーム相互間に連続フラグ (16 進 7E) を提供します。

リンクはフラグ・アイドルを透過的に受け取ります。

idle mark
SRLY インターフェース上のフレーム転送の送信アイドル状態を構成します。マーク・オプションは、フレーム間の伝送路をマーキング状態 (OFF, 1) にします。

リンクはマーク・アイドルを透過的に受け取ります。

speed 内部クロックの場合、このコマンドは送信および受信クロック回線の速度を指定します。サポートされる速度の範囲は 2400 ～ 2048000 ビット/秒です。

transmit-delay *value*
転送されるパケット間に遅延を挿入することができます。このコマンドは、フレーム相互間の最小遅延を保証することにより、相手側の旧型で低速のシリアル装置に整合させます。この値は、連続するフレーム間に送信するフラグ・バイト数として指定します。範囲は 0 ～ 15 です。デフォルトは 0 です。

SDLC リレー監視環境へのアクセス

SDLC リレー・インターフェースに関連する情報を監視するには、以下を行って、インターフェース監視プロセスにアクセスします。

1. **status** コマンドを入力して、GWCON の PID を見つける。 (**status** コマンドの出力例については、11ページを参照してください。)

2. OPCON プロンプトで、**talk** コマンドと GWCON の PID を入力する。たとえば、次のように入力します。

```
*talk 5
+
```

GWCON プロンプト (+) がコンソールに表示されます。最初に GWCON に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

3. GWCON プロンプトで **configuration** コマンドを入力して、ルーターに構成されているプロトコルとネットワークを表示する。たとえば、次のように入力します。

```
+ configuration
```

(**configuration** コマンドの出力例については、137ページを参照してください。)

4. **protocol sdlc** コマンドを入力する。たとえば、次のように入力します。

```
+ prot sdlc
SDLC Relay>
```

SDLC リレー・プロンプトがコンソールに表示されます。これで、SDLC リレー監視コマンドを入力して、SDLC リレー・ポートに関する情報を表示することができます。

SDLC リレー監視コマンド

この節では、SDLC リレー監視コマンドの要約を示し、個々のコマンドについて説明します。 SDLC リレー監視コマンドでは、SDLC リレー・フレームを転送するインターフェースのパラメーターを表示することができます。すべての SDLC リレー監視コマンド用の `SDLC Relay>` プロンプトが表示されます。 表67 は、コマンドを示しています。

表 67. SDLC リレー監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Clear-Port-Statistics	指定されたポートの SDLC リレー統計を消去します。
Disable	グループおよびポートを一時的に抑制します。
Enable	グループおよびポートを一時的にオンにします。
List	SDLC リレー全体の構成およびグループ特有の構成を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Clear-Port-Statistics

clear-port-statistics コマンドは、すべてのポートの SDLC リレー統計を廃棄するのに使用します。統計には、転送されたパケットおよび廃棄されたパケットのカウンターが含まれます。

構文:

clear-port-statistics

clear-port-statistics

前回のルーターのリスタートまたは統計の消去以降に収集されたポート統計を消去します。

例:

```
clear-port-statistics
Clear all port statistics? (Yes or No): Y
```

Disable

disable コマンドは、グループ全体または特定のリレー・ポートのデータ転送を抑制します。 SRAM (静的読み取りアクセス・メモリー) は、**disable** 監視コマンドの影響を永続的に保存しません。そのため、ルーターをリスタートすると、このコマンドの影響は消去されます。

構文:

disable group . . .

port

group *group#*

特定のグループ (group#) との間の SDLC リレー・フレームの転送を抑制します。

port *interface# primary-or-secondary*

特定のローカル・ポートとの間の SDLC リレー・フレームの転送を抑制します。

例:

```
disable port
Interface number: [0]? 2
(P)rimary or (S)econdary: [s]? P
```

Interface number

使用不可にするローカル・ポートのインターフェース番号を示します。

Primary or Secondary

ポートが 1 次であるか、2 次であるかを示します。

Enable

enable コマンドは、グループ全体または特定のローカル・インターフェース・ポートのデータ転送をオンにするのに使用します。 SRAM は、**enable** 監視コマンドの影響を永続的に保存しません。そのため、ルーターをリスタートすると、このコマンドの影響は消去されます。

構文:

enable group . . .

port

group *group#*
指定されたグループ (group#) との間の SDLC リレー・フレームの転送を可能にします。

port 指定されたローカル・ポートとの間の SDLC リレー・フレームの転送を可能にします。

例:

```
enable port
Interface number: [0]? 2
(P)rimary or (S)econdary: [s]? P
```

Interface number
使用可能にするローカル・ポートのインターフェース番号を示します。

Primary or Secondary
ポートが 1 次であるか、2 次であるかを示します。

List

list コマンドは、特定のグループまたはすべてのグループの構成を表示するのに使用します。

構文:

list all
group . . .

all すべてのローカル・ポートの構成を表示します。

例:

```
 list all
                SDLC Relay Configuration

Group  Port Status       Net    Packets    IP Address
Num                      Num   fwrd  disc

1 (E)  Local PRMRY (E)    2    2880   57
1 (E)  Remote SCNDRY (E)       4860   13   128.185.452.11
2 (D)  Local PRMRY (D)    1    0      0
2 (D)  Remote PRMRY (D)        0      0    128.185.450.31
```

Group Number
グループ番号とグループの状態 (使用可能 (E) または使用不可 (D)) を示します。

Port Status
ポートのタイプ (ローカル/リモート 1次/2 次) とその状態 (使用可能 (E) または使用不可 (D)) を示します。

Net Number
ローカル・ポートの装置番号を示します。この番号は、Config> **list devices** コマンドを使用して表示した番号と一致します。

Packets (fwrd and disc)
そのポートで転送 (fwrd) および廃棄 (disc) されたパケット数をします。

IP Address
リモート・ポートの IP アドレスを示します。

group *group#*

指定されたグループの構成を表示します。

例:

```
list group 1
             SDLC Relay Configuration

Group  Port Status        Net  Packets    IP Address
Num                       Num  fwrd disc

1 (E)  Local PRMRY (D)    2    2880   57
1 (E)  Remote SCNDRY (E)       4860   13  128.185.452.11
```

SDLC リレー・インターフェースおよび GWCON インターフェース・コマンド

SDLC リレー・インターフェースには独自の監視目的の監視プロセスがありますが、GWCON 環境から **interface** コマンドを使用すれば、ルーターも導入済みネットワーク・インターフェースの完全な統計を表示します。 (**interface** コマンドの詳細については、第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド を参照してください。)

第39章 SDLC インターフェースの使用

この章では、SDLC インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『基本構成手順』
- 557ページの『SDLC 構成要件』
- 『交換 SDLC コールイン・インターフェースの構成』

SDLC 構成コマンドは `SDLC # Config>` プロンプトで入力します。ただし、`#` は network コマンドで指定するインターフェースを識別します。ルーターの構成に加えた変更は、即時には有効にはならず、ルーターがリスタートされたときに、ルーターの静的構成メモリーの一部になります。

基本構成手順

この節では、DLSw または APPN で SDLC を使用できるようにするのに必要な最小構成について概説します。

構成手順を開始する前に、config プロセスから **list device** コマンドを使用して、各種の装置のインターフェース番号のリストを表示します。 Config プロンプトで、**network** *interface number* または **n** *interface number* のいずれかを入力して、構成するインターフェースを選択します。構成コマンドについて詳しい説明が必要な場合は、本章の構成コマンドの説明個所を参照してください。

交換 SDLC コールイン・インターフェースの構成

交換 SDLC コールイン・インターフェースを使用すると、PU タイプ 2.0 装置が交換 SDLC 回線を使用して 2210 にダイヤルインすることが可能になり、ネットワークの接続性オプションが追加されます。インターフェースは PU タイプ 2.0 装置に限られ、DLSw しか実行することができません。

注: 交換 SDLC コールイン・インターフェースを介する APPN は構成できません。

交換 SDLC コールイン・インターフェースを構成するには、次のようにします。

1. V.25bis 基本ネットワークを構成する。

```
Config> set data-link v25bis 2
Config> net 2
V25bis Config>
 (configure the V25bis net)
```

   V25bis の構成についての詳細は、581ページの『第41章 V.25bis ネットワーク・インターフェースの使用』を参照してください。

   注: **encoding type** および **full** 対 **half duplex** といった物理レイヤーのパラメーターはすべて、交換 SDLC ダイヤル回線インターフェース上ではなく、V.25bis インターフェース上で構成します。

2. ダイヤル回線装置を追加する。

```
Config> add device dial
```

3. ダイヤル回線インターフェースのデータ・リンクを SDLC に設定する。この例では、ダイヤル回線はインターフェース 3 です。

```
Config> set data-link sdlc 3
```

4. ダイヤル回線を構成する。

```
Config> net 14
Dial circuit config> set net 2 1
Dial circuit config> encapsulator
sdlc config>
   (configure SDLC)
sdlc config> exit
Dial circuit config> exit
Config>
```

5. DLSw を構成する。

```
Config> prot dls
DLSw protocol user configuration
DLSw config> add sdlc
Interface # [0]? 3
SDLC Address or 'sw' (switched dial-in) [sw]? sw 2
Source MAC address [4000112402C1]? 4000003174d2
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000004 3
Destination SAP in hex [0]? 4 4

XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xfffff) [0]? 00001
For a switched dial-in link station .....
  - PU type is forced to be 2
  - Configured XID block/id num is used to override
     fields in the XID0 from the SDLC station
      - if block/id set to zeroes, XID0 is not modified
      - otherwise configured fields are put into XID0
  - Poll type is not configured (not used)
DLSw config>li sdlc all
Net Addr   Status    Source SAP/MAC   Dest SAP/MAC      PU  Blk/IdNum  PollFrame
 3  FF(sw) Enabled   04 4000003174D2  04 400000000004   2   017/00001  TEST

DSLw config> exit
Config>
```

1 その他のパラメーター値はすべて、ソフトウェアがデフォルト値を取るので、これ以外のダイヤル回線パラメーターは設定できません。デフォルト値についての詳細は、655ページの『Encapsulator』を参照してください。

2 『sw』 という指定は、これが交換 SDLC コールイン・インターフェースであることを示します。

3 宛先 MAC アドレスは、オール 0 であってはなりません。 0 を指定したり、デフォルト値の 0 を受け入れた場合、ソフトウェアは有効なアドレスを入力するように求めるプロンプトを出します。

4 宛先 SAP は 0 であってはなりません。0 を指定したり、デフォルト値の 0 を受け入れた場合、ソフトウェアは有効なアドレスを入力するように求めるプロンプトを出します。

DLSw の構成についての追加情報は、*Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻バージョン 3.1* の 『DLSw の監視』の章の 『DLSw の使用および構成』 の項を参照してください。

SDLC 構成要件

この章で説明した SDLC 特有の構成手順およびコマンドに加えて、DLSw または APPN プロトコルでも SDLC を構成する必要があります。特定の SDLC インターフェース上では、一度に 1 つのプロトコル (DLSw または APPN) しか実行できません。言い換えると、特定の SDLC インターフェース上のリンク・ステーションは、APPN と DLSw 間で分割することはできません。同じ SDLC インターフェースに対する DLSw 構成と APPN 構成が存在する場合は、最初にアクティブになったプロトコルが、その SDLC インターフェースを所有することになります。

第40章 SDLC インターフェースの構成および監視

この章では、SDLC の構成コマンドおよび動作コマンドについて説明します。

本章には、以下の節が含まれています。

構成コマンド・コンソール (SDLC CONFIG>) で行った変更は、ルーターをリスタートすると SRAM 構成の一部になります。

逆に、SDLC 監視プロセス内で入力した SDLC 監視コマンドは、即時に有効になります。ただし、監視コマンドを用いて行った変更は、ルーターの静的構成の一部にはなりません。ルーターをリスタートすると、監視コマンドの影響は、ルーターの静的構成によって上書きされます。監視は、以下のアクションから構成されます。

- 現在ルーターによって使用されているプロトコルおよびネットワーク・インターフェースを監視する。
- SDLC 構成に永続的な影響を与えずに、SRAM 構成をリアルタイムで変更する。
- ルーターのアクティビティーおよび性能に関連する ELS (イベント・ログ・システム) メッセージを表示する。

SDLC 構成環境へのアクセス

ルーターの構成を変更するには、CONFIG プロセスを使用します。新規の構成は、ルーターをリスタートすると有効になります。

構成プロセスに入るには、次のようにします。

1. OPCON (*) プロンプトで **talk 6** (または **t 6**) を入力する。これにより、次の例のような CONFIG> プロンプトが表示されます。

   ```
   MOS Operator Control

   * talk 6

   CONFIG>
   ```

   CONFIG> プロンプトがすぐに表示されない場合は、**Enter** キーをもう一度押してください。 SDLC 構成コマンドは SDLC config> プロンプトで入力します。

2. Config> プロンプトで **set data-link sdlc** コマンドを入力する。プロンプトが出たら、SDLC 装置に関連付けるインターフェースの名前を入力します。

   ```
   Config>set data-link sdlc
   Interface number [0]? 2
   Config>
   ```

3. 次に、**network** コマンドと、前に入力した SDLC インターフェースの番号を入力する。

```
Config>network 2
SDLC 2 Config>
```

構成環境に関する情報は、3ページの『第1章 開始』 を参照してください。

SDLC 構成コマンド

SDLC 構成コマンドを用いて、SDLC インターフェース構成を作成または変更することができます。この節では、ネットワーク構成コンソール内の SDLC Config> プロンプトから出すことができるコマンドの要約を示し、個々のコマンドについて説明します。コマンドとそのパラメーターのデフォルト値は、プロンプトの直後に大括弧で囲んで表示されています。

注: 本章に説明されているコマンドを使用して SDLC を構成するのに加えて、DLSw または APPN プロトコルでも SDLC を構成する必要があります。

2210 は、RS-232、X.21、および V.35 シリアル・インターフェースを介する SDLC 接続をサポートします。 表68 は、SDLC 構成コマンドとその機能をリストしています。

表 68. SDLC 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	SDLC エンド・ステーションを追加します。
Delete	SDLC エンド・ステーションを除去します。
Disable	SDLC リンク・ステーションの 1 つへの接続を防止します。
Enable	SDLC リンク・ステーションの 1 つへの接続を可能にします。
List	SDLC リンク・ステーションの 1 つの構成情報を表示します。
Set	特定のインターフェースおよびリンク・ステーション情報を構成します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、エンド・ステーションを追加するのに使用します。ルーターは、デフォルトでは、1 次エンド・ステーションです。このコマンドを使用しないで、DLSw または APPN で SDLC ステーションを構成した場合、そのエンド・ステーションが追加されます。ソフトウェアは、以下のようなデフォルト値をステーションに割り当てます。

- Maximum BTU は、インターフェースによって許容される最大値
- Tx および Rx ウィンドウは、MOD 8 の場合は 7、MOD 128 の場合は 127

デフォルト値で十分な場合は、SDLC ステーションを追加する必要はありません。

構文:

add station

例:

```
add station
Enter station address (in hex) [C3]?
Enter station name [SDLC_C3]?
Include station in group poll list ([Yes] or No):
Enter max packet size [2009]?
Enter receive window [7]?
Enter transmit window [7]?
```

Enter station address
01 ～ FE の範囲のステーションの SDLC アドレス

Enter station name
SDLC ステーションの名前指定 (最大 8 文字)

Include station in group poll list
このリンクに関するグループ・ポーリング・リストに、このステーションを含めるかどうかを選択します。 SDLC ソフトウェアは、SDLC 2 次ステーションの IBM 3174 グループ・ポーリング機能をサポートします。このパラメーターを有効にするためには、**set link group-poll** コマンドを使用して、グループ・ポーリング・アドレスを追加する必要があります。

Enter max packet size
リモート・リンク・ステーションとの間で送受信できる最大パケット・サイズ。この値は、リンクに指定された最大値より大きくすることはできません。この値は **set link frame-size** コマンドを使用して構成します。

Enter receive window
ルーターがレスポンスを受信せずに送信できるパケットの最大数

Enter transmit window
ルーターがレスポンスを受信せずに送信できる最大パケット数

Delete

delete コマンドは、指定されたエンド・ステーション (ステーション名またはアドレス) を SDLC 構成から除去するのに使用します。ルーターは 1 次エンド・ステーション (デフォルト) と見なされます。

構文:

delete station *name* or *address*

Disable

disable コマンドは、SDLC リンク・ステーションとのコネクションが作成されるのを防止します。

構文:

disable link
station . . .

link インターフェース上のすべての構成済み SDLC リンクへのデータの送受信を防止します。

station *name* **or** *address*
指定されたエンド・ステーション (ステーション名またはアドレス) へのデータの送受信を防止します。

Enable

enable コマンドは、リモート SDLC リンク・ステーションへの接続を可能にします。

構文:

enable link
station

link ルーター内のサブシステム (たとえば、DLSw) が SDLC のファシリティーを使用できるようにします。

station *name* **or** *address*
指定された 2 次リモート・エンド・ステーション (リンク・ステーション名) に接続できます。

List

list コマンドは、1 つまたはすべての SDLC リンク・ステーションの構成情報を表示するのに使用します。

構文:

list link
station *name* or all

link SDLC インターフェースの構成を表示します。

例:

```
list link
Link configuration for: LINK_2   (ENABLED)

Role:          SECONDARY        Type:         POINT-TO-POINT
Duplex:        FULL             Modulo:       8
Idle state:    FLAG             Encoding:     NRZ
Clocking:      EXTERNAL         Frame Size:   2048
Speed:         0                Group Poll:   F3
Cable          V.36 DTE

Timers:     XID/TEST response:  2.0 sec
            SNRM response:      2.0 sec
            Poll response:      0.5 sec
            Inter-poll delay:   0.2 sec
            RTS hold delay:     DISABLED
            Inter-frame delay:  DISABLED
            Inactivity timeout  30.0 sec

 Counters:  XID/TEST retry:  8
             SNRM retry:      6
             Poll retry:      10
```

Link configuration
ルーターの構成に存在する SDLC リンクの名前と状態

Role **set link role** コマンドを使用して構成するリンク・ステーションの役割 (1 次、2 次、または交渉可能)

Type リンクのタイプ（MULTIPOINT または POINT-TO-POINT)

Duplex
二重構成（HALF または FULL)

Modulo
リンクで使用するシーケンス番号の範囲。MOD 8 (0 〜 7) または MOD 128 (0 〜 127)

Idle state
インターフェースがデータを送信していないとき、回線上を送信されるビット・パターン (FLAG または MARK)

Speed インターフェースの物理データ速度。クロックが内部の場合、これは内部クロックによって生成されるデータ速度です。

Group Poll
多地点間リンク構成のグループ・ポーリング機能に使用されるアドレス。グループ組み込みが yes として構成されている 2 次ステーションは、このアドレスから受信した非番号制ポーリングに応答します。このリンクの 2 次ステーションに対してグループ・ポーリング機能を有効にするためには、このアドレスを非空文字にする必要があります。各 2 次ステーションは、グループ・アドレスに加えて、固有のステーション・アドレスも持ちます。

Cable 使用するケーブルのタイプを指定します (RS-232、V.35、V.36、または X.21)。

Encoding
SDLC 伝送符号化法を NRZ (非ゼロ復帰記録) または NRZI (非ゼロ復帰反転) として構成します。

Clocking
インターフェースのクロック (EXTERNAL または INTERNAL)

Frame Size
インターフェースを介して送信できる最大フレーム・サイズ

Timers:
以下にリストするタイマーはすべて 100ms の分解能です。

XID/TEST resp.
XID または TEST フレームを再送する前に、XID または TEST 応答メッセージを待つ最大時間。値 0 は、ルーターは無期限に再試行を継続することを示します。

SNRM response
SNRM(E) を再送する前に、UA 応答メッセージを待つ最大時間

Poll response
再試行の前に、ポーリング・ステーションからのレスポンスを待つ最大時間。

Inter-poll delay
ルーター (1 次の役割をもつように構成) がレスポンスを受信した後、次のステーションをポーリングする前に待つ時間

RTS hold delay
1 次ルーターがフレームの転送後に RTS を low に降下する前に待つ時間の長さ。 RTS 保留遅延パラメーターは、半二重動作に特定のものです。

Interframe delay
フレーム相互間に送信されるフラグの数

Inactivity timeout
アイドル NRM/E 2 次ステーションの場合、インターフェースがステーションを回復状態に変更する前に経過する時間を設定します。 0 (ゼロ) に設定すると、ステーションは無期限にアイドル状態のままになります。

Counters:

XID/TEST retry
タイムアウト前に、応答の受信なしにルーターが XID または TEST フレームを送信する最大回数。値 0 は、ルーターが無期限に再試行することを示します。

SNRM タイムアウトの前に、ルーターがレスポンスを受信せずに SNRM(E) フレームを送信する最大回数。値 0 は、ルーターが無期限に再試行することを示します。

Poll retry
タイムアウトの前に、ルーターがレスポンスを受信せずにステーションをポーリングする最大回数。値 0 は、ルーターは無期限に再試行を継続することを示します。

注: duplex type、**speed**、 **cable type**、**encoding**、 **clocking**、 および **inter-frame delay** といった物理レイヤー・パラメーターは SDLC ダイヤル回線インターフェースには適用されず、**list link** コマンドによって表示されません。

station *all* **または** *address* **または** *link station name*
指定された SDLC リンク・ステーションまたはすべてのリンク・ステーションの情報を表示します。

例:

```
list station c1
 Address   Name     Status   Max BTU   Rx Window   Tx Window
 -------  ------   ------   -------   ---------   ---------
 C1(00)  SDLC_C1    Enabled     2005         7           7
```

例:

```
list station all
 Address   Name      Status     Max BTU  Rx Window  Tx Window
 -------  --------  ----------  -------  ---------  ---------
 C1(00)   SDLC_C1     ENABLED      2005       7          7
 C3(F3)   SDLC_C3     DISABLED     2009       7          7
```

Address
SDLC リンク・ステーションのアドレス。括弧内のアドレスは、そのステーションのグループ・アドレスです。 (00) は、グループ・アドレスが定義されていないことを示します。

Name SDLC リンク・ステーションの文字列での名前指定

Status
SDLC リンク・ステーションの状況（ENABLED または DISABLED)

Max BTU
ステーションのフレーム・サイズ限界。このフレーム・サイズは、

set link frame-size コマンドで構成された最大基本伝送単位 (BTU) パケット・サイズより大きくてはなりません。

Rx Window
受信ウィンドウのサイズ

Tx Window
送信ウィンドウのサイズ

Set

set コマンドは、1 つまたはすべての SDLC リンク・ステーションの特定情報を構成するのに使用します。

構文:

set

- link cable*
- link clocking*
- link duplex* . . .
- link encoding* . . .
- link frame-size
- link group poll* ...
- link idle* . . .
- link inactivity ...
- link inter-frame delay*
- link modulo . . .
- link name
- link poll . . .
- link role* . . .
- link rts-hold
- link snrm
- link speed*
- link type* . . .
- link xid/test
- station *address* . . .

***注:** これらのコマンドは SDLC ダイヤル回線インターフェースでは利用不能です。

link cable *type*
このインターフェースに接続されるケーブルを設定します。オプションとしては、V.36 と次の DCE および DTE タイプである、RS-232、V.35、および X.21 があります。

DTE ケーブルは、ルーターをあるタイプの DCE 装置 (たとえば、モデムまたは DSU/CSU) に接続するときに使用します。

DCE ケーブルは、ルーターが DCE として動作し、直接接続のためのクロックを提供するときに使用します。

link clocking *internal* **or** *external*

SDLC リンクのクロックを構成します。モデムまたは DSU に接続する場合は、クロックを外部として設定します。別の DTE 装置に直接接続する場合は、DCE ケーブルを使用し、クロックを内部として設定し、クロック速度を構成します。内部クロックの場合、回線速度を 2400 〜 2048000 ビット/秒の範囲で設定する必要があります。

link duplex *full* **または** *half*

SDLC 回線を 全二重 *(full-duplex)* または半二重 *(half-duplex)* 信号用に構成します。半二重 は、2210/2216 がデータを転送する前に、RTS を上げて CTS を待つことを意味します。全二重 は、2210/2216 がデータを転送する前に CTS が上がるのを待たないことを意味します。

注: 二重のタイプは、SDLC プロトコル・レベルでの SDLC の動作は制御しません。 2216/2210 は両方向交互モード (SDLC 半二重とも呼ばれます) のみをサポートします。

link encoding *nrz* **または** *nrzi*

SDLC 伝送符号化法を NRZ (非ゼロ復帰記録) または NRZI (非ゼロ復帰反転) として構成します。 NRZ がデフォルトです。

link frame-size

データ・リンク上で送受信できるフレームの最大サイズを構成します。有効な入力値を表69 に示します。

表 69. Link Frame-Size コマンドのフレーム・サイズの有効値

最小	最大	デフォルト
128	18000	2048

リンク・フレーム・サイズは、**set station xxx max packet** コマンドを使用して構成した最大パケット・サイズより大きく設定してください。そうでないと、ルーターは自動的に最大パケット・サイズをリンク・フレーム・サイズとして設定し直し、次のような ELS メッセージを出します。

```
SDLC.054: nt 3 SDLC/0 Stn xx-MaxBTU too large for Link adjusted (4096->2048)
```

例: set link frame-size

link group-poll

リンク上の 2 次ステーションのグループ・ポーリング・アドレスを設定します。 SDLC ソフトウェアは、IBM 3174 グループ・ポーリング機能をサポートします。ステーションをグループ・ポーリング・リストに含めるには、**add station** または **set station group inclusion** コマンドを使用します。

例:

```
set link group-poll
Enter group poll address (in hex) [00:]?f3
Group poll support enabled
```

link idle flag

SDLC フレーム転送の送信アイドル状態を構成します。デフォルト設定はフラグ・オプションで、これはフレーム相互間に連続フラグ (7E) を提供します。

例: set link idle flag

リンクはフラグ・アイドルを透過的に受け取ります。

link idle mark

SDLC フレーム転送の送信アイドル状態を構成します。 mark オプションは、フレーム間の伝送路をマーキング状態 (OFF, 1) にします。

link inactivity *#-of-seconds*

アイドル NRM/E 2 次ステーションの場合、インターフェースがステーションを回復状態に変更する前に経過する時間を設定します。範囲は 0 ～ 7200 秒です。デフォルト値は 30 です。 0 (ゼロ) に設定すると、ステーションは無期限にアイドル状態のままになります。

例:

```
set link inactivity
Enter secondary link station inactivity timeout :[30.0]?
```

link inter-frame delay

転送されるパケット間に遅延を挿入することができます。このコマンドは、フレーム相互間の最小遅延を保証することにより、相手側の旧型で低速のシリアル装置に整合させます。遅延は、連続するフレーム間に送信するフラグ・バイト数として指定します。範囲は 0 ～ 15 フラグで、0 (つまり、フラグなし) がデフォルト値です。

例:

```
set link inter-frame delay
Transmit Delay Counter [0]?
```

link modulo 8 or 128

リンクで使用するシーケンス番号範囲 (MOD 8 (0-7) または MOD 128 (0 - 127)) を指定します。デフォルトは 8 です。

注: この値を変更すると、ウィンドウ・サイズが無効になります。 **set station** コマンドを使用して、受信ウィンドウおよび送信ウィンドウのサイズを変更してください。有効なウィンドウ・サイズは、mod 8 の場合は 0 ～ 7 で、mod 128 の場合は 8 ～ 127 です。

また、コネクションの起動時に、SNRM ではなく SNRME が使用され、監視フレーム・ヘッダーは追加バイト分だけ拡張されます。

link name

構成するリンクの文字ストリングを設定します。このパラメーターは情報としてのみ使用されます。

例:

```
set link name
Enter link name: [LINK_0]?
```

link poll delay

インターフェースを介して送信される各ポーリング間の時間遅延を構成します。

例:

```
set link poll delay
Enter delay between polls [0.2]?
```

link poll retry

コネクションをクローズする前に、インターフェースが 2 次 SDLC リンク・ステーションのポーリングを再試行する回数を構成します。

例:

```
set link poll retry
Enter poll retry count (0 = forever) [10]?
```

link poll timeout

タイムアウトになる前に、インターフェースがポーリング・レスポンスを待つ時間を構成します。

例:

```
set link poll timeout
Enter poll timeout [2.0]?
```

link role *primary* **または** *secondary* **または** *negotiable*

インターフェースを SDLC 1 次、2 次、または交渉可能リンク・ステーションとして構成します (デフォルトは 1 次)。

注:

1. DLSw の場合、***negotiable*** は初期ポーリングに X'FF' (同報通信アドレス) を使用します。

   役割を交渉するのに同報通信アドレスを使用する場合、リンクはデフォルトの SDLC 構成を使用します。

   primary がリンクの役割のときは、リンクは特定アドレスに対して初期ポーリングを行います。

2. APPN ポイント・ポイントまたは交渉可能の場合、初期ポーリングには同報通信アドレスが使用されます。 1 次多地点の場合は、特定のアドレスが使用されます。
3. 交換 SDLC の場合は、装置は 1 次でなければならないので、**link role type** は SDLC ダイヤル回線インターフェースに対しては構成できません。

link rts-hold

フレームの送信後、送信要求 (RTS) を high に保つ時間。この設定値は半二重モード用です。全二重モードでは、この設定値は有効ではありません。

例:

```
set link rts-hold
Enter RTS hold duration after transmit complete [0.0]?
```

link snrm *timeout* **または** *retry*

1 次ステーションに関する以下の SNRM(E) 情報を構成します。

timeout

SNRM(E) を再送する前に、非番号制確認 (UA) レスポンスを待つ時間

retry あきらめる前に、レスポンスを受信せずに SNRM (E) 再送する回数

例:

```
set link snrm timeout
Enter SNRM response timeout [2.0]?
```

例:

```
set link snrm retry
Enter SNRM retry count (0=forever) [6]?
```

link speed
内部クロックの場合、このコマンドは送信および受信クロック回線の速度を指定します。

Example:

```
set link speed
Line Speed [64000]?
```

link type *multipoint* **または** *point-to-point*
SDLC リンクを多地点間リンクまたはポイント・ポイント・リンクとして構成します。

注: 交換 SDLC の場合、リンクは常にポイント・ポイントなので、**link type** は SDLC ダイヤル回線インターフェースに対しては構成できません。

link xid/test *timeout* **または** *retry*
1 次ステーションの以下の XID/test 情報を構成します。

timeout
XID または TEST フレームの再送する前に、XID または TEST フレーム応答を待つ最大時間

retry あきらめる前に、XID または TEST フレームを再送する最大回数。0 (ゼロ) に設定すると、ルーターは無期限に再試行します。

remote-secondary *address* **または** *link_station_name address* **<***argument***>**
リモート・ステーションの SDLC アドレス (02 ～ FE の範囲) を変更します。

例: set remote-secondary SDLC_C1 address ce

station *address* **または** *name* **address**
ステーションの SDLC アドレス (01 ～ FE の範囲) を変更します。

例:

```
set station c1 address
Enter station address (in hex) [C1]?
```

station *address* **または** *link station name* **group-inclusion** *no* **または** *yes*
SDLC 2 次ステーションの場合、このステーションをこのリンクのグループ・ポーリング・リストに含めるかどうかを設定します。これを有効にするためには、**set link group-poll** コマンドを使用して、グループ・ポーリング・アドレスを追加します。

例: set station c1 group-inclusion yes

station *address* **または** *name* **max-packet**
ステーションが受信できるパケットの最大サイズ (デフォルトは 2048)。最大パケット・サイズは、**set link frame-size** コマンドで構成したリンク・フレーム・サイズより大きく設定しないでください。そのように設定すると、ルーターは自動的に最大パケット・サイズをリンク・フレーム・サイズとして設定し直し、次のような ELS メッセージを出します。

```
SDLC.054: nt 3 SDLC/0 Stn xx-MaxBTU too large for Link adjusted (4096->2048)
```

例:

```
set station c1 max-packet
Enter max packet size [2048]?
```

station *address* **または** *name* **name**
SDLC ステーションの名前

例:

```
set station c1 name
Enter station name [SDLC_C1]?
```

station *address* **または** *name* **receive window**
ルーターがレスポンスを送信する前に受信できるフレームの最大数。範囲は 1 ～ 7 で、デフォルトは 7 です。

例:

```
set station c1 receive-window
Enter receive window [7]?
```

station *address* **または** *name* **transmit-window**
ルーターがレスポンス・フレームを受信する前に送信できるフレームの最大数。範囲は 1 ～ 7 で、デフォルトは 7 です。

例:

```
set station c1 transmit-window
Enter transmit window [7]?
```

SDLC 監視環境へのアクセス

監視環境は GWCON プロセスです。 GWCON プロセスに入るには、次のようにします。

1. OPCON (*) プロンプトで **talk 5** (または **t 5**) を入力する。これにより、次の例のような GWCON (+) プロンプトが表示されます。

```
MOS Operator Control

* talk 5
+
```

2. 次に、**network** # コマンドを入力して、以前に SDLC 装置に構成したインターフェースを識別する番号を指定する。

```
+ network 2
SDLC Console
SDLC-2>
```

GWCON (監視) コマンドはすべて + プロンプトで入力します。

監視環境に関する情報は、3ページの『第1章 開始』 を参照してください。

SDLC 監視コマンド

この節では、SDLC コンソールおよび関連のコマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドは、データベースから情報を収集するのに使用します。 571ページの表70 は、SDLC 監視コマンドとその機能をリストしています。

表 70. SDLC 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	SDLC リンク・ステーションを追加します。
Clear	SDLC インターフェースに関するカウンターをクリアします。
Delete	SDLC リンク・ステーションを動的に除去します。
Disable	1 つの SDLC リンク・ステーションへの接続を使用不可にします。
Enable	1 つの SDLC リンク・ステーションへの接続を使用可能にします。
List	SDLC リンク・ステーションの構成およびリンク・ステーション情報を表示します。
Set	特定のインターフェースおよびリンク・ステーション情報を構成します。
Test	ルーターと SDLC リンク・ステーション間のリンクをテストします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、エンド・ステーションを追加するのに使用します。ルーターは、デフォルトでは、1 次エンド・ステーションです。このコマンドを使用しないで、DLSw または APPN で SDLC ステーションを構成した場合、そのエンド・ステーションが追加されます。

構文:

add station

add コマンドの例および詳しい情報は、560ページの『Add』 を参照してください。

Clear

clear コマンドは、インターフェース、1 つのステーション、またはすべてのステーションのカウンターをクリアするのに使用します。ステーションをリストしたい場合は、**list all stations** コマンドを使用します。

構文: clear link

station ...

link *name* **or** *address*
SDLC インターフェースのカウンターをクリアします。

station *name* **or** *address* **or all**
特定のステーションまたはすべてのステーションのカウンターをクリアします。

Delete

delete コマンドは、SRAM 内の SDLC 構成に影響を与えずに、既存の SDLC コネクションを終了するのに使用します。このコマンドは、リンク・ステーションで進行中のすべての SDLC セッションを終了させます。ルーターは、デフォルトでは、1 次エンド・ステーションと見なされます。

構文:

delete station *name* or *address*

Disable

disable コマンドは、SRAM 内の SDLC 構成に影響を与えずに、1 つまたはすべての SDLC リンク・ステーション上のコネクション確立を使用不可にするのに使用します。 **disable** コマンドは、そのステーションへの既存のすべてのコネクションも終了します。

構文: disable

link

station . . .

link すべてのコネクションを終了して、インターフェースに構成されているすべての SDLC リンク・ステーションの接続を防止します。

station *name* **or** *address*
既存のコネクションを終了して、指定されたエンド・ステーション (リンク・ステーション名) への接続を防止します。

Enable

enable コマンドは、SDLC 構成 SRAM に影響を与えずに、リモート SDLC リンク・ステーションと接続を確立できるようにするのに使用します。

構文:

enable link

station . . .

link サブシステム (たとえば、DLSw) が SDLC のファシリティーを使用できるようにします。

station *name* **または** *address*
指定されたエンド・ステーションへの接続を可能にします。

List

list コマンドは、データ・リンク・レイヤーおよびインターフェースに特有の統計を表示するのに使用します。

構文:

list link configuration

link counters

station . . .

link configuration
インターフェース上のすべての構成済み SDLC リンク・ステーションの情報を表示します。

list コマンドの例および詳しい情報は、562ページの『List』 を参照してください。

link counters 前回のルーターのリスタートまたは前回の clear counters 以降の SDLC カウンターの情報を表示します。

I-Frames
送受信された情報フレームの合計数

I-Bytes
送受信された情報バイトの合計数

Re-Xmit
再送されたフレームの合計数

UI-Frames
送受信された非番号制情報フレームの合計数

UI-Bytes
送受信された非番号制情報バイトの合計数

RR 送受信された受信可 (RR) の合計数

RNR 送受信された受信不可 (RNR) の合計数

REJ 送受信されたリジェクトの合計数

UP 送受信された非番号制ポーリング数 (グループ・ポーリング)

station *all* **または** *address* **または** *link station name*

指定された SDLC リンク・ステーションまたはすべてのステーションの状態を表示します。ソフトウェアは、**add station** コマンドを使用して明示的に構成されていないが、プロトコル・レイヤー (DLSw または APPN) で定義されて起動されたために構成に追加されたステーションの横に * を表示します。

インターフェース上の指定された SDLC リンク・ステーション (リンク・ステーション名) の情報を表示します。

Address
SDLC リンク・ステーションのアドレス。括弧内のアドレスは、そのステーションのグループ・アドレスです。 (00) は、グループ・アドレスが定義されていないことを示します。

Name SDLC リンク・ステーションの文字列での名前指定

Status
SDLC リンク・ステーションの状態

Enabled
使用可能であるが、割り当てられていない。

Idle 割り当てられているが、使用されていない。

Connected
接続状態

Disconnected
切断状態

Connecting
接続確立中

Discnectng
切断中

Recovering
一時データ・リンク誤りからの回復を試行中

Max BTU
リモート・ステーションのフレーム・サイズ限界。このフレーム・サイズは、**set link frame-size** コマンドで構成された最大基本伝送単位 (BTU) パケット・サイズより大きくてはなりません。デフォルト値は 2048 バイトです。

Rx Window
受信ウィンドウのサイズ

Tx Window
送信ウィンドウのサイズ

station *name* **または** *address* **counters**
指定されたリンク・ステーションのフレーム送信および受信カウントを表示します。

I-Frames
送受信された情報フレームの数

I-Bytes
送受信された情報バイトの数

Re-Xmit
再送されたフレームの数

UI-Frames
送受信された非番号制情報フレームの数

UI-Bytes
送受信された非番号制情報バイトの数

XID-Frames
送受信された識別交換フレームの数

RR 送受信された受信可フレームの数

RNR 送受信された受信不可フレームの数

REJ 送受信されたリジェクトの数

TEST 送受信されたテスト・フレームの数

SNRM 送受信された通常応答モード設定フレームの数

DISC 送受信された切断フレームの数

UA 送受信された非番号制確認フレームの数

DM 送受信された切断モード・フレームの数

FRMR 送受信されたフレーム・リジェクト・フレームの数

UP 送受信された非番号制ポーリング数 (グループ・ポーリング)

例:

```
list link counters
     I-Frames     I-Bytes     Re-Xmit     UI-Frames     UI-Bytes
     --------     -------     -------     ---------     --------
Send       0           0           0             0            0
Recv       0           0                         0            0

          RR         RNR         REJ           UP
     -------     -------     ----     ---------
Send       0           0          0             0
Recv       0           0          0             0
```

例:

```
list station all

Address    Name      Status    Max BTU   Rx Window     Tx Window
--------   -----     ------    -------   ---------     ---------
 C1(00)    SDLC_C1   IDLE        2048       7             7
 C2(F3)    SDLC_C2   ENABLED     2048       7             7
```

例:

```
list station c1
Address   Name      Status     Max BTU     Rx Window   Tx Window
-------  ------    --------    -------     ---------   ---------
* C1(00) SDLC_C1    ENABLED       2048         7           7
```

例:

```
list station c1 counters
         I-Frames    I-Bytes     Re-Xmit   UI-Frames    UI-Bytes   XID-Frames
         ----------  ----------  --------  ----------  ----------  ----------
 Send            9         384         0           0           0           6
 Recv           29       42792                     0           0           3

            RR          RNR         REJ         TEST        SNRM        DISC
         ----------  ----------  --------  ----------  ----------  ----------
 Send          598           0         0           0           1           0
 Recv          587           0         0           0           0           0

            UA          DM         FRMR        UP
         ----------  ----------  --------  --------
 Send            0           0         0         0
 Recv            1           0         0         0
```

Set

set コマンドは、SRAM 内の SDLC 構成に影響を与えずに、1 つまたはすべての SRAM リンク・ステーションの特定情報を動的に構成するのに使用します。 SDLC 監視環境では、**set** コマンドは、使用不可にされたリンクまたはステーション上でしか実行できません。タイム値はすべて 0.1 秒の分解能で、秒数で入力します。

構文:

set

- link modulo . . .
- link name
- link poll . . .
- link role* . . .
- link rts-hold
- link snrm(e)
- link type* . . .

link xid/test

station . . .

***注:** これらのコマンドは SDLC ダイヤル回線インターフェースではサポートされません。

link modulo

SRAM 構成に影響を与えずに、データ・リンクで使用されるシーケンス番号の範囲を動的に変更します。モジュロ 8 はシーケンス番号範囲 0 ～ 7 を指定し、モジュロ 128 は 0 ～ 127 を指定します。デフォルトは 8 です。

注: この値を変更すると、送信および受信ウィンドウ・サイズが無効になります。 **set station** コマンドを使用して、受信ウィンドウおよび送信ウィンドウのサイズを変更してください。

link name

SRAM 構成に影響を与えずに、リンクの名前を動的に変更します。最大 8 文字を入力できます。このパラメーターは情報としてのみ使用されます。

例:

```
set link name
Enter link name: [LINK_0]?
```

link poll delay または timeout または retry

SRAM 構成に影響を与えずに、以下のポーリング情報を動的に変更します。

delay インターフェースを介して送信される各ポーリング間の遅延を構成します。

timeout
タイムアウトになる前に、インターフェースがポーリング・レスポンスを待つ時間を構成します。

retry コネクションをクローズする前に、インターフェースがリモート SDLC リンク・ステーションのポーリングを再試行する回数を構成します。

例:

```
set link poll delay
Enter delay between polls [0.2]?
```

link role *primary*, *secondary*, **または** *negotiable*

インターフェースを SDLC 1 次、2 次、または交渉可能リンク・ステーションとして構成します。デフォルトは 1 次です。このコマンドの使用は SRAM 構成には影響を与えません。

注:

1. DLSw の場合、***negotiable*** は初期ポーリングに X'FF' (同報通信アドレス) を使用します。

   役割を交渉するのに同報通信アドレスを使用する場合、リンクはデフォルトの SDLC 構成を使用します。

   primary がリンクの役割のときは、リンクは特定アドレスに対して初期ポーリングを行います。

2. APPN ポイント・ポイントまたは交渉可能の場合、初期ポーリングには同報通信アドレスが使用されます。 1 次多地点の場合は、特定のアドレスが使用されます。
3. 交換 SDLC の場合は、装置は 1 次でなければならないので、**link role type** は SDLC ダイヤル回線インターフェースに対しては構成できません。

link rts-hold

フレームの送信後に送信要求 (RTS) を high に保つ時間を、SRAM 構成に影響を与えずに動的に変更します。この設定値は半二重モード用です。全二重モードでは、この設定値は有効ではありません。

例:

```
set link rts-hold
Enter RTS hold duration after transmit complete [0.0]?
```

link snrm *timeout* **または** *retry*

1 次ステーションの場合、SRAM 構成に影響を与えずに、以下の SNRM(E) 情報を動的に変更します。

timeout
SNRM(E) を再送する前に、非番号制確認 (UA) レスポンスを待つ時間

retry あきらめる前に、レスポンスを受信せずに SNRM (E) 再送する回数

例:

```
set link snrm timeout
Enter SNRM response timeout [2.0]?
```

link type multipoint or point-to-point

SRAM 構成に影響を与えずに、SDLC リンクを多地点間リンクまたはポイント・ポイント・リンクに動的に変更します。

注: 交換 SDLC の場合、リンクは常にポイント・ポイントなので、**link type** は SDLC ダイヤル回線インターフェースに対しては構成できません。

link xid/test *timeout* **または** *retry*

1 次ステーションの場合、SRAM 構成に影響を与えずに、以下の XID/テスト情報を動的に変更します。

timeout
テスト・フレームを再送する前に、XID または TEST フレーム・レスポンスを待つ最大時間

retry あきらめる前に、XID または TEST フレームを再送する最大回数。0 (ゼロ) に設定すると、ルーターは無期限に再試行します。

注: 以下のパラメーターの例および説明は、565ページの『Set』 の SDLC 構成の章にあります。

station *address* **または** *name* **address**

ステーションの SDLC アドレスを変更します。

station *address* **または** *name* **max-packet**
このステーションが受信できるパケットの最大サイズ

station *address* **または** *name* **name**
SDLC ステーションの名前

station *address* **または** *name* **receive-window**
ルーターが、応答する前に送信するフレームの最大数

station *address* **または** *name* **transmit-window**
ルーターが、レスポンス・フレームを受信する前に送信するフレームの最大数

Test

指定された数の TEST フレームを指定されたステーションに送信し、レスポンスを待ちます。このコマンドは、接続の整合性をテストするのに使用します。テストを取り消すときは、任意のキーを押します。

注: このコマンドを使用する前に、指定されたリンク・ステーションを使用不可にしてください。

構文:

test station *name* or *address #frames-to-send frame-size*

例:

```
test station c1
Number of frames to send [1]? 5
Frame length [265]?
Starting echo test -- press any key to abort
5 frames sent, 5 frames received, 0 compare errors, 0 timeouts
```

Number of test frames to send
送信するフレームの合計数

Frame length
送信するフレームの長さ。フレームの長さは、指定されたステーションの最大フレーム長より大きくすることはできません。

任意のキーを押せば、テストを打ち切ることができます。

SDLC インターフェースおよび GWCON インターフェース・コマンド

SDLC インターフェースには動作用のコンソール・プロセスがありますが、GWCON 環境から **interface** コマンドを使用すれば、2210 も導入済みインターフェースの完全な統計を表示します。 (interface コマンドの詳細については、133ページの『第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』 を参照してください。)

SDLC インターフェースで表示される統計

interface コマンドを使用すると、SDLC 監視プロセスに入らずに、SDLC 装置の統計を表示することができます。これを行うには、次のように、+ プロンプトで **interface** コマンドとインターフェース番号を入力します。

Nt 初期構成時にソフトウェアによって割り当てられたインターフェース番号を示します。

Nt' 初期構成時にソフトウェアによって割り当てられたインターフェース番号を示します。

注: SDLC インターフェースの場合、Nt' インターフェース番号は、常に Nt インターフェース番号と同じです。

CSR SDLC インターフェースの制御状況レジスターのメモリー・ロケーションを示します。

Self-test passed
SDLC インターフェースが自己テストに合格した合計数を示します。

Self-test failed
SDLC インターフェースが自己テストに合格できなかった合計数を示します。

Maintenance failed
保守障害の数の示します。

以下のパラメーターは、ケーブルが接続されている場合にのみ表示されます。表示される情報は、接続されているケーブルによって決まります。他のケーブルでは、異なるパラメーターが表示されます。

Adapter cable
レベル変換器が使用されているアダプター・ケーブルのタイプを示します。

V.24 circuit
V.24 で使用されている回線を示します。

Nicknames
V.24 回線で使用されている信号を示します。

RS-232
EIA 232 (RS 232) 回線名

State V.24 回線、信号、およびピン割り当て (ON または OFF)

Line speed (configured)
SDLC インターフェースに現在構成されている回線速度を示します。

Last port reset
前回にポートがリセットされた時期を示します。

Input frame errors
入力フレーム誤りタイプ (CRC 誤り、短すぎる、強制終了、配列、長すぎる、DMA/FIFO オーバーラン) および発生した誤りの合計数を示します。

Output frame counters
出力フレームの DMA/FIFO オーバーランおよび送信された出力強制終了の合計数を示します。

Missed frame
フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

L & F bits not set

シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

第41章 V.25bis ネットワーク・インターフェースの使用

V.25bis インターフェースは、ルーターが V.25bis モデムを使用して、交換電話回線を介してシリアル・コネクションを確立できるようにします。この章では、V.25bis インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『始める前に』
- 『構成手順』

注: 着信名を**コネクション・リスト**に割り当て、着信番号をリスト内の各回線に割り当てることができます。着信先名がコールされると、接続されるまで、またはリストが尽きるまで、リスト内の番号が 1 つずつ試されます。

始める前に

ルーター上の V.25bis を構成する前に、以下が用意されていることを確認してください。

- 同期 V.25bis コマンドおよび 1988 ITU/CCITT V.25bis 仕様をサポートする V.25bis モデム。
- モデムが自動的に応答の発信元を検出しない場合は、以下を行う必要があります。
  - リンクの一端のモデムを発呼用に構成する。
  - リンクの他端のモデムを応答用に構成する。
  - 応答側のモデムを自動応答用に設定する。

構成手順

この節では、ルーターを V.25bis 用に構成する方法について説明します。実行する必要があるタスクは、次のとおりです。

1. V.25bis アドレスを追加する。
2. V.25bis パラメーターを構成する。
3. ダイヤル回線を追加する。
4. ダイヤル回線を構成する。

注: V.25bis 構成の変更を有効にするためには、ルーターをリスタートする必要があります。

V.25bis アドレスの追加

各ローカル V.25bis インターフェースおよび各着信先の V.25bis アドレスを追加することが必要です。 V.25bis アドレスには、次のものが含まれます。

- アドレス名。 アドレス名は、アドレスの記述です。最大 23 字までの印刷可能 ASCII 文字列を使用できます。

- *ネットワーク・ダイヤル・アドレス。* ローカル・ポートまたは着信先ポートの電話番号です。接続された V.25bis モデムに有効なフォーマットで、最大 30 文字まで入力できます。詳細については、モデムのマニュアルを参照してください。

  注: CCITT によって定義され、IBM 2210 によってサポートされている電話番号の有効な文字セットには、以下が含まれます。

  – 10 進数の 0 ～ 9
  – コロン (:) -- ″待機トーン″
  – 左かぎ括弧 (<) --″ポーズ″、数字シーケンス間に一定の遅延 (モデムによって異なる) を挿入するのに使用されます。たとえば、PBX または PTN を通す場合などに使用します。
  – 等号 (=) -- ″区切り記号 3″、これは ″国内用″ です。 (モデムのマニュアルを参照してください。)
  – 文字 P -- ″パルス方式でダイヤルを継続″ (一部のモデムではサポートされません。)
  – 文字 T -- ″DTMF 方式でダイヤルを継続″ (一部のモデムではサポートされません。)

V.25bis アドレスを追加するには、Config> プロンプトで **add v25-bis-address** コマンドを入力します。たとえば、次のように入力します。

```
Config>add v25-bis-address
Assign address name [1-23] chars []? remote-site-baltimore
Assign network dial address [1-30 digits][]? 19095551234
```

V.25bis インターフェースの構成

この節では、V.25bis インターフェースを構成する方法について説明します。構成するには、以下を行います。

1. V.25bis 用のシリアル・ライン・インターフェースを設定するために、シリアル・ライン・インターフェースのデータ・リンク・プロトコルを設定する。 Config> プロンプトから **set data-link v25bis** コマンドを使用します。たとえば、次のように入力します。

   ```
   Config>set data-link v25bis
   Interface Number [0]? 2
   ```

2. **network** コマンドに続けてインターフェースの番号を入力して、V.25bis Config> プロンプトを表示する。たとえば、次のように入力します。

   ```
   Config>network 2
   V.25bis Data Link Configuration
   V25bis Config>
   ```

   Config> プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストとを表示することができます。

3. **set local-address** コマンドを使用して、ローカル・ポートのネットワーク・アドレス名を指定する。 **add v25bis-address** コマンドを使用して定義したアドレス名の 1 つを入力する必要があります。たとえば、次のように入力します。

   ```
   V25bis Config>set local-address
   Local network address name  []? remote-site-baltimore
   ```

注: 構成変更を有効にするためには、ルーターをリスタートする必要があります。

オプション V.25bis パラメーター

以下は、ユーザーが設定できるオプション V.25bis パラメーターです。これらのコマンドの詳しい説明は、587ページの『V.25bis 構成コマンド』 を参照してください。

- アクセス不能なアドレスまたはその種の呼を拒否するアドレスへの連続コール回数を制限することができます。これを行うには、**set retries-no-address** および **set timeout-no-answer** コマンドを使用します。
- **set disconnect-timeout** コマンドは、ルーターが前回の呼からの信号を除去した後、発呼を開始するまでに待つ時間を制御します。
- **set command-delay-timeout** コマンドは、ルーターが DTR をオンにした後、発呼するか呼に応答するまでに待つ時間を制御します。
- **set connect-timeout** は、呼を設定するのに許容される秒数を指定します。
- **set duplex** コマンドは、呼の二重方式を設定します。
- **set encoding** コマンドは、呼の符号化を設定します。
- インターフェースの構成を終了したら、**list** コマンドを使用して、構成を表示してみることができます。

ダイヤル回線の追加

ダイヤル回線は、V.25bis シリアル・ライン・インターフェースにマップされます。複数のダイヤル回線を 1 つのシリアル・ライン・インターフェースにマップすることも可能です。

ダイヤル回線を追加するには、Config> プロンプトから **add device dial-circuit** コマンドを使用します。ソフトウェアが、各回線にインターフェース番号を割り当てます。この番号を使用して、ダイヤル回線を構成します。

例:

```
Config>add device dial-circuit
Adding device as interface 6
```

注: ダイヤル回線は、デフォルトではポイント・ポイント・プロトコル (PPP) になります。フレーム・リレー (FR) または SDLC を使用するようにダイヤル回線を構成することも可能です。

ダイヤル回線の構成

この節では、ダイヤル回線の構成方法について説明します。ダイヤル回線コマンドの詳しい説明は、653ページの『第47章 ダイヤル回線の使用』 を参照してください。

注: カプセル化タイプが SDLC の場合、ユーザーが設定できる唯一のダイヤル回線パラメーターは、基本ネット番号です。

ダイヤル回線を構成するには、以下を行います。

1. **network** コマンドに続けてダイヤル回線のインターフェース番号を入力して、Circuit Config> プロンプトを表示する。 Config> プロンプトで **list devices** コマンドを使用すると、追加したダイヤル回線のリストを表示することができます。たとえば、次のように入力します。

```
Config>network 6
Circuit configuration
Circuit Config>
```

2. ダイヤル回線を V.25bis インターフェースにマップする。基本ネットは V.25bis インターフェース番号です。 たとえば、次のように入力します。

```
Circuit Config>set net
Base net for this circuit [0]?  0
```

3. ダイヤル回線を接続するリモート・ルーターのアドレス名を指定する。 **add v25-bis-address** コマンドを使用して定義した名前の 1 つを入力する必要があります。たとえば、次のように入力します。

```
Circuit Config>set destination
Assign destination address name []? newyork
```

4. ダイヤル回線を発信専用、着信専用、または発信と着信の両方として構成する。

   set calls コマンドを使用します。リンクの両側が同時に呼設定を試みた場合に競合を避けるために、リンクの一方の端のダイヤル回線は着信専用に構成し、リンクの他方の端のダイヤル回線は発信専用に構成します。たとえば、次のように入力します。

```
Circuit Config>set calls outbound
Circuit Config>set calls inbound
```

   注: WAN 復元動作または別のダイヤル・オンデマンド・アプリケーションの場合、回線を着信用または発信用のいずれかに設定することが必要です。

5. 回線のタイムアウト期間を指定する。

   set idle コマンドを使用します。この指定された期間、回線上に通信がないと、ダイヤル回線はハングアップします。回線を専用回線として構成する場合は、アイドル・タイマーをゼロに設定します。回線をダイヤル・オンデマンドに構成する場合は、アイドル・タイマーをゼロ以外の値に設定します。範囲は 0 ～ 65535 で、デフォルトは 60 秒です。たとえば、次のように入力します。

```
Circuit Config>set idle
Idle timer (seconds, 0 means always active) [60]? 0
```

   注: WAN 復元動作の場合、アイドル・タイムを 0 に設定する必要があります。

6. オプションで、呼設定と初期パケット送信の間の時間を遅らせることができます。

   set selftest-delay コマンドを使用します。自己テスト遅延を設定すると、初期パケットが廃棄されるのを防止できます。モデムが同期のために余分な時間が必要な場合は、この遅延を調整します。たとえば、次のように入力します。

```
Circuit Config>set selftest-delay
Selftest delay(milli-seconds,0 means no delay)[150]?200
```

7. 着信アドレス名を設定する。

   set inbound コマンドを使用します。このコマンドを使用する必要があるのは、回線が着信と発信の両方に設定されており、ルーターの着信アドレスが、リモート・ルーターがダイヤルする着信アドレスと異なっている場合だけです。たとえば、ルーターの 1 つが PBX、国際、または LATA 間交換局を通す必要がある場合は、番号が異なることになります。たとえば、次のように入力します。

```
Circuit Config>set inbound
Assign destination inbound address name []? newyork
```

add v25-bis-address コマンドを使用して定義した名前の 1 つに一致していることが必要です。

8. **set duplex** コマンドを使用して、回線の二重方式を設定する。
9. **set encoding** コマンドを使用して、回線の符号化方式を設定する。
10. オプションで、ダイヤル回線上で実行されているデータ・リンク・レイヤー・プロトコル (PPP またはフレーム・リレー) の構成プロセスに入ることができます。 **encapsulator** コマンドを使用します。たとえば、次のように入力します。

```
Circuit Config> encapsulator
```

第42章 V.25bis ネットワーク・インターフェースの構成および監視

この章では、V.25bis 構成コマンドと動作コマンド、および GWCON コマンドについて説明します。本章には、以下の節が含まれています。

インターフェース構成プロセスへのアクセス

V.25bis 構成プロセスにアクセスするには、以下の手順を使用します。

1. OPCON プロンプトで、**talk** コマンドと CONFIG の PID を入力する。 (このコマンドの詳細については、第3章 OPCON プロセスおよびコマンド を参照してください。) たとえば、次のように入力します。

   ```
   * talk 6
   Config>
   ```

   talk 6 コマンドを入力すると、CONFIG プロンプト (Config>) がコンソールに表示されます。最初に **CONFIG** に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。 たとえば、次のように入力します。

   ```
   Config> list devices

   Ifc 0 Ethernet                      CSR  81600, CSR2  80C00, vector 94
   Ifc 1 V.25bis                       CSR  81620, CSR2  80D00, vector 93
   Ifc 2 WAN X.25                      CSR  81640, CSR2  80E00, vector 92
   Ifc 3 WAN PPP                       CSR 381620, CSR2 380D00, vector 125
   Ifc 4 WAN Frame Relay               CSR 381640, CSR2 380E00, vector 124
   Ifc 5 Token Ring                    CSR 600000, vector 95
   ```

3. インターフェース番号を記録する。
4. CONFIG **network** コマンドと、構成するインターフェースの番号を入力する。 たとえば、次のように入力します。

   ```
   Config> network 1
   V.25bis Config>
   ```

   これで、V.25bis 構成プロンプトがコンソールに表示されます。

V.25bis 構成コマンド

588ページの表71 は、V.25bis 構成コマンドの要約を示しており、本節の残りの部分で、個々のコマンドについて説明します。これらのコマンドを用いて、V.25bis 構成を表示、作成、または変更することができます。 V.25bis 構成コマンドは、V.25bis Config> プロンプトで入力します。

V.25bis 構成コマンド

表 71. V.25bis 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	V.25bis 構成を表示します。
Set	ローカル・アドレス、接続、切断、および無応答タイムアウト、無応答後の再試行回数、コマンド遅延タイムアウト、および符号化を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、現行の V.25bis 構成を表示するのに使用します。

構文:

list

例:

```
list
          V.25bis Configuration

Duplex                          =  Full
Encoding                        =  NRZ
Local Network Address Name      = v403
Local Network Address           = 15088982403

Non-Responding addresses:
Retries             = 1
Timeout             = 0 seconds

Call timeouts:
Command Delay       = 0 ms
Connect             = 60 seconds
Disconnect          = 2 seconds

Cable type          = V.35 DTE
Speed               = 9600
```

Duplex
ダイヤル接続が確立された場合、インターフェースの二重方式を表示します。

Encoding
ダイヤル接続が確立された場合、インターフェースの伝送符号化法を表示します。符号化法は、NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) です。

Local Network Address Name:
ローカル・ポートのネットワーク・アドレス名を表示します。

Local Network Address:
ローカル・ポートのネットワーク・ダイヤル・アドレスを表示します。

Non-responding addresses:

Retries
ルーターがタイムアウト期間中に無応答アドレスに対して試行する呼の最大数

Timeout
ルーターは、無応答アドレスへの試行の最大数に達した場合、この時間が満了するまで呼設定を試行しません。このタイムアウト期間は、ルーターが最初の発呼を試みた時点で開始します。

Call timeouts:
呼のタイムアウトの回数

Command Delay
ルーターが DTR (データ端末レディー) をオンにした後、発呼するか呼に応答するまでに待つ時間 (ミリ秒)。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) で DTR に応答するのを待ってから、ルーターはコマンドを出します。

Connect
呼を設定するのに許容される秒数。このパラメーターが 0 に設定されている場合、モデムが呼設定タイムアウトを制御します。

Disconnect
ルーターは DTR を除去した後、この時間だけ待ってから、次の呼を開始します。このパラメーターを 0 に設定すると、モデムが CTS および DSR を除去することによって DTR 除去に応答するのを待ってから、ルーターは次の呼を開始します。

Set

set コマンドは、ローカル・アドレス、呼のタイムアウトと遅延、無応答アドレスの再試行とタイムアウト、および HDLC ケーブル・タイプを構成するのに使用します。

構文:

set command-delay timeout . . .
connect-timeout . . .
disconnect-timeout . . .
duplex
hdlc cable . . .
hdlc encoding . . .
hdlc speed . . .
local-address . . .
retries-no-answer . . .
timeout-no-answer . . .

command-delay-timeout *# of milliseconds*
ルーターは DTR (データ端末レディー) をオンにした後、この時間数だけ待ってから、呼を開始したり、呼に応答したりします。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) で DTR に応答するのを待ってから、ルーターはコマンドを出します。範囲は 0 ～ 65535 ミリ秒で、デフォルトは 0 です。

connect-timeout *# of seconds*

呼を設定するのに許容される秒数を設定します。範囲は 0 ～ 65535 秒で、デフォルトは 60 です。このパラメーターを 0 に設定すると、モデムがコネクション・タイムアウトを制御します。最初にこのパラメーターを 0 に設定し、次に ELS イベント V25B.027 を使用して、種々の宛先に接続を確立するための所要時間を調べる必要があります。その後で、このパラメーターを、最長接続時間よりわずかに高い値に設定します。

注: 通常は政府規制により、モデム製造業者は呼設定を最大長にするように制限されています。一部の DSU と相互運用するときは、このパラメーターを変更することが必要になる場合もありますが、この値は最適化のためのものです。

disconnect-timeout *# of seconds*

ルーターが DTR を除去後、次の呼を開始する前に待機する時間 (秒) を指定します。範囲は 0 ～ 65535 秒で、デフォルト値は 2 です。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) で DTR に応答するのを待ってから、ルーターはコマンドを出します。

duplex

回線の二重タイプを指定します。

全二重が構成されている場合、ダイヤル接続が確立された後は、RTS モデム信号は代入されたままになります。

半二重が構成されている場合、ルーターは転送時になると RTS を上げて、モデムが CTS を代入するのを待ちます。 CTS が代入されると、ルーターはデータ・パケットを転送し、転送している間は RTS を除去して、同位装置が応答できるようにします。

交換 SDLC を扱うために V.25bis インターフェースを使用している場合、およびモデムが半二重方式の動作を必要とする場合には、半二重のみを構成してください。

注: PPP またはフレーム・リレー回線の場合は、全二重でなければなりません。

有効値: full または half

デフォルト値: full

hdlc cable *rs232 dte*

このインターフェースに接続されるケーブルのタイプを指定します。このパラメーターを設定した場合、GWCON (+) プロンプトで **interface** コマンドを入力するか、`V.25bis>` 監視プロンプトで **statistics** コマンドを入力すれば、ケーブル・タイプを見ることができます。このパラメーターは、ルーターの動作には影響を与えません。

hdlc encoding

HDLC 伝送符号化法を NRZ (非ゼロ復帰) または NRZI (非ゼロ復帰反転) に設定します。ほとんどの構成は NRZ を使用します。構成された符号化法は、エンド・エンド間の接続で使用されます。

注: NRZI を構成することも可能ですが、DTE とモデム間の交換では (CCITT 勧告の *V.25bis* に記述) NRZ が符号化法として使用されます。

有効値: NRZ または NRZI

デフォルト値: NRZ

hdlc speed

このインターフェースの回線速度を指定します。このパラメーターを設定した場合、GWCON (+) プロンプトで interface コマンドを入力したとき、および `V.25bis>` 監視プロンプトで statistics コマンドを入力したときに、回線速度が表示されます。範囲は 300 ～ 2 048 000 bps です。

注: このコマンドは実際の回線速度には影響を与えませんが、一部のプロトコル (IPX など) が、V.25bis インターフェースにマップされるダイヤル回線のルーティング・コストを計算するのに使用する速度を設定します。

local-address *address name*

ローカル・ポートのネットワーク・ダイヤル・アドレスを表示します。このアドレス名は、`Config>` で **add v25-bis-address** コマンドを使用して定義した名前の 1 つに一致していることが必要です。

例: `set local-address line-1-local`

retries-no-answer *value*

一部の電話サービス提供者は、自動リコール装置に対して、アクセス不能アドレスまたは自動リコールを拒否するアドレスへの連続コール回数を制限しています。このパラメーターは、ルーターがタイムアウト期間中に無応答アドレスに対して試行する呼の最大数を指定します。範囲は 0 ～ 10 で、デフォルトは 1 です。

注: 政府規制により、モデム製造業者がこのパラメーターを変更するのを制限している場合もあります。

timeout-no-answer *# of seconds*

ルーターは、無応答アドレスへの**retries-no-answer** の最大数に達した場合、この時間が満了するまで、次の呼を開始しません。このタイムアウト期間は、あるアドレスにルーターが最初の発呼を試みた時点で開始します。範囲は 0 ～ 65535 秒で、デフォルトは 0 です。このパラメーターを 0 に設定すると、モデムがタイムアウト期間を制御します。

インターフェース監視プロセスへのアクセス

V.25bis のインターフェース監視プロセスにアクセスするには、GWCON (+) プロンプトから、次のコマンドを入力します。

```
+ network #
```

ただし、# は、V.25bis シリアル・ラインの番号です。ダイヤル回線の V.25bis 監視プロセスには直接アクセスできませんが、シリアル・ライン・インターフェースにマップされたダイヤル回線を監視することができます。

注: V.25bis インターフェースには、V.25bis 関連のアクティビティーを監視するのに使用できる ELS トラブルシューティング・メッセージもあります。詳細については、*IBM Nways イベント・ログ・システム メッセージの手引き* を参照してください。

V.25bis 監視コマンド

この節では、V.25bis 動作コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドを用いて、V.25bis インターフェースの呼、回線、パラメーター、および統計を見ることができます。

V.25bis 監視コマンドは、`V.25bis>` プロンプトで入力します。

表 72. V.25bis 監視コマンドの要約

監視コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Calls	前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線で行われた、完了した接続および試行された接続の数をリストします。
Circuits	V.25bis インターフェースに構成されたすべてのデータ回線の状態を示します。
Parameters	V.25bis インターフェースの現行パラメーターを表示します。 (このコマンドは、`V.25bis Config> list` コマンドに似ています。)
Statistics	V.25bis インターフェースの現行統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Calls

calls コマンドは、前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線で行われた、完了した接続および試行された接続の数をリストするのに使用します。

構文:

calls

例:

```
calls
Net Interface  Site Name           In    Out   Rfsd  Blckd
1     PPP/0     v403               2      0      0      0

Unmapped connection indications:    0
```

Net このインターフェースにマップされたダイヤル回線の数

Interface
インターフェースのタイプとそのインスタンス番号

Site Name
ダイヤル回線のネットワーク・アドレス名

In このダイヤル回線で受け入れられたインバウンド接続の数

Out このダイヤル回線によって開始され、完了した接続の数

Rfsd このダイヤル回線によって開始されたが、ネットワークまたはリモート着信ポートによって拒否された接続の数

Blckd ルーターがブロックした接続試行の数。ルーターが接続試行をブロックするのは、ローカル・ポートがすでに使用されている場合、無応答アドレスへの再試行の最大数に達している場合、またはモデムが応答していない場合です。

Unmapped connection indications:
着呼を受け入れるように構成されている使用可能のダイヤル回線がないために、ルーターによって拒否された接続試行の数

Circuits

circuits コマンドは、V.25bis ポートに構成されているすべてのダイヤル回線の状態を示します。

構文:

circuits

例:

```
circuit
Net Interface  MAC/Data-Link    State     Reason      Duration
2   PPP/0      Point to Point   Avail     Rmt Disc     1:02:25
```

Net このインターフェースにマップされたダイヤル回線の数

Interface
インターフェースのタイプとそのインスタンス番号

MAC/DataLink
このダイヤル回線に構成されたデータ・リンク・プロトコルのタイプ

State ダイヤル回線の現行状態

Up - 現在接続されています。

Available - 現在は接続されていませんが、利用可能です。

Disabled - ダイヤル回線は使用不可にされました。

Down - ダイヤル回線がビジーであるか、リンク・レイヤー・プロトコルがダウンしているために、接続に失敗しました。

Reason
現行状態の理由:

nnn_Data - (nnn はプロトコルの名前) プロトコルに送信するデータがあったので、回線は Up です。

Remote Disconnect - リモート着側が呼を切断したので、回線は Down または Available のいずれかです。

Operator Request - 前回の呼が監視コマンドによって切断されたので、回線は Available です。

Inbound - 回線が着呼に応答したので、回線は Up です。

Restoral - WAN 復元動作のため、回線は Up です。

Self Test - 回線は静的として構成されており (アイドル・タイム = 0)、使用可能にされたときに正常に接続されました。

Duration
回線が現行状態にある時間の長さ

Parameters

parameters コマンドは、現行の V.25bis シリアル・ライン構成を表示するのに使用します。これは、`V.25bis Config>` list コマンドで表示される情報と同じです。

構文:

parameters

例:

```
parameters
         V.25bis port Parameters

Local Network Address Name    = v402
Local Network Address         = 15088982402

Non-Responding addresses:
Retries             = 1
Timeout             = 0 seconds

Call timeouts:
Command Delay       = 0 ms
Connect             = 0 seconds
Disconnect          = 0 seconds
```

Local Network Address Name:
ローカル・ポートのネットワーク・アドレス名

Local Network Address:
ローカル・ポートのネットワーク・ダイヤル・アドレス

Non-responding addresses:

Retries
タイムアウト期間中に無応答アドレスに対してルーターが試みる呼の最大数

Timeout
無応答アドレスに対するルーターの再試行が最大数に達すると、この期間が満了するまでルーターは呼の確立を行いません。このタイムアウト期間は、あるアドレスにルーターが最初の発呼を試みた時点で開始します。

Call timeouts:

Command Delay
ルーターが DTR (データ端末レディー) をオンにした後、発呼するか呼に応答するまでに待つ時間 (ミリ秒)。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) で DTR に応答するのを待ってから、ルーターはコマンドを出します。

Connect
呼を設定するのに許容される秒数。このパラメーターが 0 に設定されている場合、モデムが呼設定タイムアウトを制御します。

Disconnect
ルーターは DTR を除去した後、この時間だけ待ってから、次の呼を開始します。このパラメーターを 0 に設定すると、モデムが CTS および DSR を除去することによって DTR 除去に応答するのを待ってから、ルーターは次の呼を開始します。

Statistics

statistics コマンドは、この V.25bis インターフェースの現行統計を表示するのに使用します。

構文:

statistics

例:

```
statistics
        V.25bis port Statistics

  Adapter cable:              RS-232 DTE  RISC Microcode Revision: 1



   V.24 circuit: 105 106 107 108 109 125 141
   Nicknames:    RTS CTS DSR DTR DCD RI  LL
   RS-232        CA  CB  CC  CD  CF  CE
   State:        OFF OFF OFF OFF OFF OFF OFF



  Line speed:             4800
  Last port reset:        24 seconds ago

  Input frame errors:
   CRC error                    0   alignment (byte length)   0
   missed frame                 0   too long (>  2182 bytes)  0
   aborted frame                0   DMA/FIFO overrun          0
   L & F bits not set           0
Output frame counters:
   DMA/FIFO underrun errors     0   Output aborts sent        0
```

Adapter cable:
使用されているアダプター・ケーブルのタイプ。

V.24 circuit:
V.24 仕様で識別された回線番号

Nicknames:
回線の通称名

RS-232
回線の EIA 232 (RS-232 とも呼ばれる) 名

State: 回線の現在の状態: ON、OFF、または "---" （これは、このタイプのインターフェースの状態は未定義であることを意味します。)

Line speed:
送信クロック速度 (概略値)

Last port reset:
ポートがリセットされた後の経過時間

Input frame errors:

CRC error
チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)
長さが 8 の偶数倍でないために廃棄された受信パケットの数

Missed Frame
フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

too long (> nnnn bytes)
構成されたフレーム・サイズ (nnnn) より大きかったために廃棄された受信パケットの数

aborted frame
送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

L & F bits not set
シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

Output frame counters:

DMA/FIFO underrun errors
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーからデータを取り出す速度が遅かったために、パケットをネットワーク上に送信できなかった回数

Output aborts sent
高位レベルのソフトウェアの要求によって打ち切られた伝送の数

V.25bis と GWCON コマンド

V.25bis には独自の監視のための監視プロセスがありますが、GWCON 環境から interface、statistics、および error コマンドを使用すれば、ルーターも構成情報と、装置および回線の完全な統計を表示します。また、GWCON **test** コマンドを使用して、DCE および回線をテストすることもできます。

注: V.25bis シリアル・インターフェースに対して **test** コマンドを出すと、現行の呼は除去され、再ダイヤルされます。

GWCON コマンドについての詳細は、133ページの『第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照してください。

V.25bis インターフェースおよびダイヤル回線の統計

V.25bis シリアル・ライン・インターフェースおよびダイヤル回線の統計を表示するには、GWCON (+) プロンプトから **interface** コマンドを使用します。

V.25bis シリアル・ライン・インターフェースの以下の統計を表示するには、**interface** コマンドに続けて V.25bis シリアル・ライン・インターフェースのインターフェース番号 を入力します。

例: interface 1

```
                            Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
1  1   V.25/0    80000000   44          1          0            0
V.25bis MAC/data-link on SCC Serial Line interface

Adapter cable:       RS-232 DTE       RISC Microcode Revision: 1

    V.24 circuit: 105 106 107 108 109 125
    Nicknames:    RTS CTS DSR DTR DCD R1  LL
    RS-232:       CA  CB  CC  CD  CF  CE
    State:        OFF OFF OFF OFF OFF OFF OFF

Line Speed:               14.400 Kbps
Last port reset:          1 hour, 28 minutes, 25 seconds ago

Input frame errors:
    CRC error                    0   alignment (byte length)   0
    missed frame                 0   too long (>  2182 bytes)  0
    aborted frame                0   DMA/FIFO overrun          0

    Output frame counters:     DMA/FIFO underrun errors     0   Output aborts sent         0
```

ダイヤル回線の以下の統計を表示するには、**interface** コマンドに続けてダイヤル回線のインターフェース番号 を入力します。

例:

```
interface 3
                            Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
3  2   PPP/1        81640   5C          0          5            0
  Point to Point MAC/data-link on V.25bis Dial Circuit interface
```

以下のリストは、シリアル・ライン・インターフェースとダイヤル回線の両方の出力を説明しています。

Nt シリアル・ライン・インターフェース番号またはダイヤル回線インターフェース番号

Nt′ “Nt” がダイヤル回線の場合、これはダイヤル回線がマップされる V.25bis シリアル・ライン・インターフェースの番号です。

Interface
インターフェース・タイプとそのインスタンス番号

CSR 基本ネットのコマンドおよび状況レジスター・アドレス

Vec 割り込みベクトル・アドレス

Self-Test Passed
成功した自己テストの回数

Self-Test Failed
失敗した自己テストの回数

Maintenance: Failed
保守障害の数

Adapter cable:
使用されているアダプター・ケーブルのタイプ

V.24 circuit:
V.24 仕様で識別された回線番号

Nicknames
回線の通称名

RS-232
回線の EIA 232 (RS-232 とも呼ばれる) 名

State 回線の現在の状態 (ON または OFF)

Line speed
送信クロック速度 (概略値)

Last port reset
ポートがリセットされた後の経過時間

Input frame errors:

CRC error
チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)
長さが 8 の偶数倍でないために廃棄された受信パケットの数

Missed Frame
フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

too long (> nnnn bytes)
構成されたフレーム・サイズより大きかったために廃棄された受信パケットの数

DMA/FIFO overrun
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

L & F bits not set
シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビット

がセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

aborted frame
送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

Output frame counters:

DMA/FIFO underrun errors
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーからデータを取り出す速度が遅かったために、パケットを網上に送信できなかった回数

Output aborts sent
高位レベルのソフトウェアの要求によって打ち切られた伝送の数

第43章 V.34 ネットワーク・インターフェースの使用

V.34 インターフェースは、ルーターが標準 AT コマンド・セットをサポートする外付けのモデム または内蔵モデム・アダプターを使用して、交換電話回線を介してシリアル・コネクションを確立できるようにします。 この章では、V.34 インターフェースの使用法について説明します。本章には、以下の節が含まれています。

- 『始める前に』
- 『構成手順』

注: 宛先名を**コネクション・リスト**に割り当て、宛先番号をリスト内の各回線に割り当てることができます。宛先名がコールされると、接続されるまで、またはリストが尽きるまで、リスト内の番号が 1 つずつ試されます。

始める前に

外付けのモデムを使用している場合は、それが Hayes AT コマンド・セットをサポートする非同期モデムであることを確認してください。また、各モデムの最大 DTE 速度も知っている必要があります。

構成手順

この節では、ルーターを V.34 用に構成する方法について説明します。必要な作業には、次のものが含まれます。

1. V.34 アドレスを追加する。
2. V.34 パラメーターを構成する。
3. ダイヤル回線を追加する。
4. ダイヤル回線を構成する。

注: V.34 構成の変更を有効にするためには、ルーターをリスタートする必要があります。

V.34 アドレスの追加

V.34 インターフェースを初めて構成すると、デフォルトの V.34 アドレスが生成されます (『default_address』 と呼ばれます)。 V.34 インターフェース上に構成されたダイヤル回線は、デフォルトでは同じアドレスになるので、V.34 アドレスを変更せずに、いくつかのダイヤルイン・アプリケーションを実行することができます。

ダイヤルアウト・アプリケーションを使用する予定の場合は、V.34 アドレスを追加する (または、default_address を変更する) 必要があります。 V.34 アドレスには、以下のものが含まれています。

- *アドレス名。* アドレス名は、アドレスの記述です。最大 23 字までの印刷可能 ASCII 文字列を使用できます。

- ネットワーク・ダイヤル・アドレス。 ローカル・ポートまたは宛先ポートの電話番号です。最大 31 文字までの、接続されたモデムの有効なダイヤル文字を入力できます。

  注: CCITT によって定義され、IBM 2210 によってサポートされている電話番号の有効な文字セットには、以下が含まれます。

  – 10 進数の 0 ～ 9
  – コロン (:) - ″待機トーン″
  – 左かぎ括弧 (<) - ″ポーズ″、数字シーケンス間に一定の遅延 (モデムによって異なる) を挿入するのに使用されます。たとえば、PBX または PTN を通す場合などに使用します。
  – 等号 (=) - ″区切り記号 3″、これは ″国内用″ です。 (モデムのマニュアルを参照してください。)
  – 文字 P - ″パルス方式でダイヤルを継続″ (一部のモデムではサポートされません。)
  – 文字 T - ″パルス方式でダイヤルを継続″ (一部のモデムではサポートされません。)

V.34 アドレスはインターフェース特有ではないので、Config> プロンプトから追加します。たとえば、次のように入力します。

```
Config>add v34-address
Assign address name [1-23] chars []? remote-site-baltimore
Assign network dial address [1-20 digits][]? 1-909-555-1234
```

V.34 インターフェースの構成

この節では、V.34 インターフェースの構成方法について説明します。構成は、次のようにして行います。

1. V.34 用のシリアル・ライン・インターフェースを設定するために、シリアル・ライン・インターフェースのデータ・リンク・プロトコルを設定する。 Config> プロンプトから **set data-link v34** コマンドを使用します。たとえば、次のように入力します。

   ```
   Config> set data-link v34
   Interface Number [0]? 2
   ```

   注: データ・リンクは自動的に内蔵モデムに設定され、これを変更することはできません。

2. **network** コマンドに続けてインターフェースの番号を入力して、V.34 Config プロンプトを表示する。たとえば、次のように入力します。

   ```
   Config>network 2
   V.34 Data Link Configuration
   V34 System Net Config    2>
   ```

   Config プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。

3. **set local-address** コマンドを使用して、ローカル・ポートのネットワーク・アドレス名を指定する。 **add v34-address** コマンドを使用して定義したアドレス名の 1 つを入力する必要があります。たとえば、次のように入力します。

   ```
   V34 System Net Config   2>set local-address
   Local network address name  []? remote-site-baltimore
   ```

注: 構成変更を有効にするためには、ルーターをリスタートする必要があります。

オプションの V.34 パラメーター

以下のものは、ユーザーが設定することができるオプションの V.34 パラメーターです。これらのコマンドについては、608ページの『V.34 構成コマンド』で詳しく説明しています。

- アクセス不能なアドレスまたは呼を拒否するアドレスへの連続コール回数を制限することができます。これを行うには、**set retries-no-address** および **set timeout-no-answer** コマンドを使用します。
- **set disconnect-timeout** コマンドは、ルーターが前回の呼からの信号を除去した後、発呼を開始するまでに待つ時間を制御します。
- **set command-delay-timeout** コマンドは、ルーターが DTR をオンにした後、発呼するまで、または呼に応答するまでに待つ時間を制御します。
- **set connect-timeout** は、呼を設定するのに許容される秒数を指定します。
- **speed** コマンドは、モデムの最大 DTE 速度を設定します。
- **modem-init-string** コマンドは、ユーザーの要件または外部機器の要件を組み込むことによって、モデムの構成に柔軟性をもたせることができます。
- インターフェースの構成を終了したら、**list** コマンドを使用して構成を表示してみることができます。

ダイヤル回線の追加

ダイヤル回線は、V.34 シリアル・ライン・インターフェースにマップされます。複数のダイヤル回線を 1 つのシリアル・ライン・インターフェースにマップすることも可能です。

V.34 インターフェースは、複数のタイプのダイヤル回線をサポートします。ダイヤル回線を追加するには、`Config>` プロンプトから以下のコマンドを使用します。

- **add device dial-circuit**
- **add device dial-in**
- **add device dial-out**

ソフトウェアが、各回線にインターフェース番号を割り当てます。この番号は、ダイヤル回線を構成するのに使用します。

例:

```
Config> add device dial-circuit
Adding device as interface 6
```

注: ダイヤル回線は、デフォルトではポイント・ポイント・プロトコル (PPP) になります。 **set data-link** コマンドを使用すれば、ダイヤル回線のデータ・リンクをフレーム・リレーに設定することも可能ですが、V.34 上では PPP ダイヤル回線しかサポートされません。

ダイヤル回線の構成

この節では、ダイヤル回線の構成方法について説明します。ダイヤル回線コマンドの詳しい説明は、653ページの『第47章 ダイヤル回線の使用』 を参照してください。
ダイヤル回線を構成するには、次のようにします。

1. **network** コマンドに続けてダイヤル回線のインターフェース番号を入力して、Circuit Config プロンプトを表示する。 Config プロンプトで **list devices** コマンドを使用すると、追加したダイヤル回線のリストを表示することができます。たとえば、次のように入力します。

   ```
   Config>network 6
   Circuit configuration
   Circuit Config>
   ```

2. ダイヤル回線を V.34 インターフェースにマップする。基本ネット (base net) は V.34 インターフェース番号です。たとえば、次のように入力します。

   ```
   Circuit Config>set net
   Base net for this circuit [0]?  0
   ```

3. ダイヤル回線を接続するリモート・ルーターのアドレス名を指定する。 **add v34-address** コマンドを使用して定義した名前の 1 つを入力する必要があります。たとえば、次のように入力します。

   ```
   Circuit Config>set destination
   Assign destination address name []? newyork
   ```

4. ダイヤル回線を発信専用、着信専用、または発信と着信の両方として構成する。

   set calls コマンドを使用します。リンクの両側が同時に呼設定を試みたときの競合を避けるために、リンクの一端のダイヤル回線は着信専用に構成し、リンクの他端のダイヤル回線は発信専用に構成します。たとえば、次のように入力します。

   ```
   Circuit Config> set calls outbound
   Circuit Config> set calls inbound
   ```

   注: WAN 復元動作または別のダイヤル・オンデマンド・アプリケーションの場合、回線を着信用または発信用のいずれかに設定することが必要です。

5. 回線のタイムアウト期間を指定する。

   set idle コマンドを使用します。この指定された期間、回線上に通信がないと、ダイヤル回線は切断されます。回線を専用回線として構成する場合は、アイドル・タイマーをゼロに設定します。回線をダイヤル・オンデマンドに構成する場合は、アイドル・タイマーをゼロ以外の値に設定します。範囲は 0 〜 65535 で、デフォルトは 60 秒です。たとえば、次のように入力します。

   ```
   Circuit Config>set idle
   Idle timer (seconds, 0 means always active) [60]? 0
   ```

   注: WAN 復元動作の場合、アイドル・タイムを 0 に設定する必要があります。

6. オプションで、呼設定から初期パケットが送信されるまでの間の時間を遅らせることができます。

   set selftest-delay コマンドを使用します。自己テスト遅延を設定すると、初期パケットが廃棄されるのを防止できます。モデムの同期化に時間がかかる場合は、この時間を調整してください。たとえば、次のように入力します。

   ```
   Circuit Config>set selftest-delay
   Selftest delay(milli-seconds,0 means no delay)[150]?200
   ```

7. 着信アドレス名を設定する。

set inbound コマンドを使用します。このコマンドを使用する必要があるのは、回線が着信と発信の両方に設定されており、ルーターの着信アドレスが、リモート・ルーターがダイヤルする着信アドレスと異なっている場合だけです。たとえば、ルーターの 1 つが PBX、国際、または LATA 間交換局を通す必要がある場合は、番号が異なることになります。たとえば、次のように入力します。

```
Circuit Config>set inbound
Assign destination inbound address name []? newyork
```

着信アドレス名は、**add v34-address** コマンドを使用して定義した名前の 1 つに一致していることが必要です。

8. オプションとして、ダイヤル回線上で実行されているデータ・リンク・レイヤー・プロトコル (PPP またはフレーム・リレー) の構成プロセスに入ることができます。 **encapsulator** コマンドを使用します。たとえば、次のように入力します。

```
Circuit Config>encapsulator
```

V.34 の使用

第44章 V.34 ネットワーク・インターフェースの構成および監視

この章では、V.34 構成コマンドと動作コマンド、および GWCON コマンドについて説明します。本章には、以下の節が含まれています。

インターフェース構成プロセスへのアクセス

V.34 構成プロセスにアクセスするには、以下の手順を使用します。

1. OPCON プロンプトで、**talk** コマンドと CONFIG の PID を入力する。 (このコマンドの詳細については、第3章 OPCON プロセスおよびコマンド を参照してください。) たとえば、次のように入力します。

   ```
   *talk 6
   Config>
   ```

   talk 6 コマンドを入力すると、コンソールに CONFIG プロンプト (Config) が表示されます。最初に **CONFIG** に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. CONFIG プロンプトで **list devices** コマンドを入力して、ルーターが現在構成されているネットワーク・インターフェース番号を表示する。 たとえば、次のように入力します。

   ```
   Config> list devices
   Ifc 0 Ethernet                      CSR  81600, CSR2  80C00, vector 94
   Ifc 1 V.34 Base Net                 CSR  81620, CSR2  80D00, vector 93
   Ifc 2 WAN X.25                      CSR  81640, CSR2  80E00, vector 92
   Ifc 3 WAN PPP                       CSR 381620, CSR2 380D00, vector 125
   Ifc 4 WAN Frame Relay               CSR 381640, CSR2 380E00, vector 124
   Ifc 5 Token Ring                    CSR 600000, vector 95
   Ifc 6 4-port Modem Adapter          CSR 8001600,CSR2 8000C00,vector 158
   Ifc 7 4-port Modem Adapter          CSR 8001620,CSR2 8000D00,vector 157
   Ifc 8 4-port Modem Adapter          CSR 8001640,CSR2 8000E00,vector 156
   Ifc 9 4-port Modem Adapter          CSR 8001660,CSR2 8000F00,vector 155
   ```

3. V.34 インターフェースは、『V.34 Base Net』 、または 4-port Modem Adapter としてリストされます。 構成するインターフェースのインターフェース番号を記録してください。

4. CONFIG **network** コマンドと、構成するインターフェースの番号を入力する。 たとえば、次のように入力します。

   ```
   Config> network 1
   V.34 System Net Config >
   ```

   これで、V.34 構成プロンプトがコンソールに表示されます。

V.34 構成コマンド

表73 にコマンドの要約を示し、この節の残りの部分で、個々の V.34 構成コマンドについて説明します。これらのコマンドを用いて、V.34 構成を表示、作成、または変更することができます。 V.34 構成コマンドは V.34 Config> プロンプトで入力します。

表 73. V.34 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	V.34 構成を表示します。
Set	ローカル・アドレス、接続、切断、および無応答タイムアウト、無応答後の再試行回数、およびコマンド遅延タイムアウトを設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、現行の V.34 構成を表示するのに使用します。

構文:

list

例:

```
list
         V.34 System Net Configuration:

Local Network Address Name    = v403
Local Network Address         = 1-508-898-2403

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Modem strings:
Initialization string         = at&f&s1l1&d2&c1x3

Speed (bps)                   = 115200
```

Local Network Address Name:
ローカル・ポートのネットワーク・アドレス名を表示します。

Local Network Address:
ローカル・ポートのネットワーク・ダイヤル・アドレスを表示します。

Non-responding addresses:

Retries
ルーターがタイムアウト期間中に無応答アドレスに対して試行する呼の最大数

Timeout
ルーターは、無応答アドレスへの試行の最大数に達した場合、この

時間が満了するまで呼設定を試行しません。このタイムアウト期間は、ルーターが最初の発呼を試みた時点でスタートします。

Call timeouts:

呼のタイムアウトの回数

Command Delay

ルーターが DTR (データ端末レディー) をオンにした後、発呼するか呼に応答するまでに待つ時間 (ミリ秒)。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) を DTR に応答するのを待ってから、ルーターはコマンドを出します。

Connect

呼を設定するのに許容される秒数。このパラメーターが 0 に設定されている場合、モデムが呼設定タイムアウトを制御します。

Disconnect

ルーターは DTR を除去した後、この時間だけ待ってから、次の呼を開始します。このパラメーターを 0 に設定すると、モデムが CTS および DSR を除去することによって DTR 除去に応答するのを待ってから、ルーターは次の呼を開始します。

Modem strings:

接続されたモデムに送信されるコマンド文字列

Initialization string

これは初期化時 (呼が受け入れまたは試行される前) にモデムに送信される最後の AT コマンド文字列です。ほとんどのモデムに適用されるデフォルト文字列が提供されています。

Speed (bps)

これは DTE 速度です。ほとんどのモデムではデフォルト値を適用できますが、場合によっては、正しく動作させるために速度を低く設定したり、モデムがサポートする最大データ速度を達成するために高く設定したりすることが必要になることがあります。

Set

set コマンドは、ローカル・アドレス、呼のタイムアウトと遅延、無応答アドレスの再試行とタイムアウト、および HDLC ケーブル・タイプを構成するのに使用します。

構文:

set

command-delay timeout . . .

connect-timeout . . .

disconnect-timeout . . .

speed . . .

local-address . . .

modem-init-string . . .

retries-no-answer . . .

timeout-no-answer . . .

command-delay-timeout *# of milliseconds*

ルーターは DTR (データ端末レディー) をオンにした後、この時間数だけ待ってから、呼を開始したり、呼に応答したりします。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) で DTR に応答するのを待ってから、ルーターはコマンドを出します。範囲は 0 〜 65535 ミリ秒で、デフォルトは 0 です。

connect-timeout *# of seconds*

呼を設定するために許容される秒数を設定します。範囲は 0 〜 65535 秒で、デフォルトは 60 です。このパラメーターを 0 に設定すると、モデムがコネクション・タイムアウトを制御します。最初にこのパラメーターを 0 に設定し、次に ELS イベント V34B.027 を使用して、種々の宛先に接続を確立するための所要時間を調べる必要があります。その後で、このパラメーターを最長接続時間よりわずかに高い値に設定します。

注: 通常は政府規制により、モデム製造業者は呼設定を最大長にするように制限されています。この値は単に最適化のためのものであり、一部の DSU との相互運用では、このパラメーターを変更することが必要になる場合ことがあります。

disconnect-timeout *# of seconds*

ルーターが DTR を除去後、次の呼を開始する前に待機する時間 (秒) を指定します。範囲は 0 〜 65535 秒で、デフォルト値は 2 です。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) を DTR に応答するのを待ってから、ルーターはコマンドを出します。

speed *# bits per second*

モデムの DTE 速度をビット / 秒で指定します。モデムがサポートする最大速度を使用することが必要です。ただし、モデムによってはサポートされる速度が正しく自動選択されない場合もあります。問題が生じる懸念がある場合は、速度を下げてみてください。

local-address *address name*

ローカル・ポートのネットワーク・ダイヤル・アドレスを表示します。このアドレス名は、`Config>` で **add v34-address** コマンドを使用して定義した名前の 1 つに一致していることが必要です。

modem-init-string *value*

これは、正常に行われたインターフェースの初期化の最後にモデムに送信される AT コマンド文字列です。これを使用して、ユーザーのアプリケーションに適合するようにモデムのパラメーターを調整することができます。

retries-no-answer *value*

一部の電話サービス提供者は、自動リコール装置に制約を付けて、アクセス不能アドレスまたは自動リコールを拒否するアドレスへの連続コール回数を制限しています。このパラメーターは、ルーターがタイムアウト期間中に無応答アドレスに対して試行する呼の最大数を指定します。範囲は 0 〜 10 で、デフォルト値は 1 です。

注: 政府規制により、モデム製造業者がこのパラメーターを変更するのを制限している場合もあります。

timeout-no-answer *# of seconds*

ルーターは、無応答アドレスへの**retries-no-answer** の最大数に達した場合、この時間が満了するまで、次の呼を開始しません。このタイムアウト期間は、あるアドレスにルーターが最初の発呼を試みた時点でスタートします。範囲は 0 ～ 65535 秒で、デフォルトは 0 です。このパラメーターを 0 に設定すると、モデムがタイムアウト期間を制御します。

インターフェース監視プロセスへのアクセス

V.34 のインターフェース監視プロセスにアクセスするには、GWCON (+) プロンプトから、次のコマンドを入力します。

```
+ network #
```

ただし、# は、V.4 インターフェースの番号です。ダイヤル回線の V.34 監視プロセスには直接アクセスできませんが、シリアル・ライン・インターフェースにマップされたダイヤル回線を監視することができます。

注: V.34 インターフェースには、V.34 関連のアクティビティーを監視するのに使用できる ELS トラブルシューティング・メッセージもあります。詳細については、*IBM Nways イベント・ログ・システム メッセージの手引き* を参照してください。

V.34 監視コマンド

この節では、V.34 監視コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドを用いて、V.34 インターフェースの呼、回線、パラメーター、および統計を見ることができます。

V.34 監視コマンドは V.34> プロンプトで入力します。

表 74. V.34 監視コマンドの要約

監視コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Calls	前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線に行われた、完了した接続および試行された接続の数をリストします。
Circuits	V.34 インターフェース上に構成されたすべてのデータ回線の状態を示します。
Reset	接続を切断し、インターフェースをリセットします。
Parameters	V.34 インターフェースの現行パラメーターを表示します。 (このコマンドは、インターフェース構成 "list" コマンドと同じ情報を表示します。)
Statistics	V.34 インターフェースの現行統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Calls

calls コマンドは、このインターフェースにマップされた各ダイヤル回線で行われた、前回にルーター上の統計がリセットされた以降の、完了した接続および試行された接続の数をリストするのに使用します。

構文:

calls

例:

```
calls
Net Interface  Site Name           In    Out   Rfsd  Blckd
1     PPP/0     v403               2      0      0      0

Unmapped connection indications:    0
```

Net このインターフェースにマップされたダイヤル回線の数

Interface
インターフェースのタイプとそのインスタンス番号

Site Name
ダイヤル回線のネットワーク・アドレス名

In このダイヤル回線で受け入れられた着信接続の数

Out このダイヤル回線によって開始され、完了した接続の数

Rfsd このダイヤル回線によって開始されたが、ネットワークまたはリモート着信ポートによって拒否された接続の数

Blckd ルーターがブロックした接続試行の数。ルーターが接続試行をブロックするのは、ローカル・ポートがすでに使用されている場合、無応答アドレスへの再試行の最大数に達した場合、またはモデムが応答しない場合です。

Unmapped connection indications:
着呼を受け入れるように構成されている使用可能のダイヤル回線がないために、ルーターによって拒否された接続試行の数

Circuits

circuits コマンドは、V.34 ポートに構成されているすべてのダイヤル回線の状態を示します。

構文:

circuits

例:

```
circuit
Net Interface  MAC/Data-Link    State     Reason      Duration
2   PPP/0      Point to Point   Avail     Rmt Disc     1:02:25
```

Net このインターフェースにマップされたダイヤル回線の数

Interface
インターフェースのタイプとそのインスタンス番号

MAC/DataLink
このダイヤル回線に構成されたデータ・リンク・プロトコルのタイプ

State ダイヤル回線の現行状態

Up - 現在接続されています。

Available - 現在は接続されていませんが、利用可能です。

Disabled - ダイヤル回線は使用不可にされました。

Down - ダイヤル回線がビジーであるか、リンク・レイヤー・プロトコルがダウンしているために、接続に失敗しました。

Reason
現行状態の理由:

nnn_Data - (nnn はプロトコルの名前) プロトコルに送信するデータがあったので、回線は Up です。

Remote Disconnect - リモート着側が呼を切断したので、回線は Down または Available のいずれかです。

Operator Request - 前回の呼が監視コマンドによって切断されたので、回線は Available です。

Inbound - 回線が着呼に応答したので、回線は Up です。

Restoral - WAN 復元動作のため、回線は Up です。

Self Test - 回線は静的として構成されており (アイドル・タイム = 0)、使用可能にされたときに正常に接続されました。

Duration
回線が現行状態にある時間の長さ

Parameters

parameters コマンドは、現行の V.34 シリアル・ライン構成を表示するのに使用します。これは、`V.34 Config>` list コマンドで表示される情報と同じです。

構文:

parameters

例:

```
parameters
         V.34 port Parameters

Local Network Address Name    = v402
Local Network Address         = 1-508-898-2402

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 0 seconds
Disconnect                    = 0 seconds

Modem strings:
Initialization string         = at&f&s1l1&c1x3
```

Local Network Address Name:
ローカル・ポートのネットワーク・アドレス名

Local Network Address:
ローカル・ポートのネットワーク・ダイヤル・アドレス

Non-responding addresses:

Retries
ルーターがタイムアウト期間中に無応答アドレスに対して試行する呼の最大数

Timeout
ルーターは、無応答アドレスへの試行の最大数に達した場合、この時間が満了するまで呼設定を試行しません。このタイムアウト期間は、あるアドレスにルーターが最初の発呼を試みた時点でスタートします。

Call timeouts:

Command Delay
ルーターが DTR (データ端末レディー) をオンにした後、発呼するか呼に応答するまでに待つ時間 (ミリ秒)。このパラメーターを 0 に設定した場合、モデムが CTS (送信可) を DTR に応答するのを待ってから、ルーターはコマンドを出します。

Connect
呼を設定するために許容される秒数。このパラメーターが 0 に設定されている場合、モデムが呼設定タイムアウトを制御します。

Disconnect
ルーターは DTR を除去した後、この時間だけ待ってから、次の呼を開始します。このパラメーターを 0 に設定すると、モデムが CTS および DSR を除去することによって DTR 除去に応答するのを待ってから、ルーターは次の呼を開始します。

Statistics

statistics コマンドは、この V.34 インターフェースの現行統計を表示するのに使用します。

構文:

statistics

例:

```
statistics
         V.34 port Statistics
  Adapter cable:               RS-232 DTE  RISC Microcode Revision: 1

   V.24 circuit: 105 106 107 108 109 125 141

    Nicknames:    RTS CTS DSR DTR DCD RI  LL
    RS-232        CA  CB  CC  CD  CF  CE
    State:        OFF OFF OFF OFF OFF OFF OFF
   Line speed:              115.200 Kbps
   Last port reset:         24 seconds ago

 Input frame errors:
    CRC error                     0   alignment (byte length)   0
    missed frame                  0   too long (>  2182 bytes)  0
    aborted frame                 0   DMA/FIFO overrun          0
    L & F bits not set            0
```

```
Output frame counters:
   DMA/FIFO underrun errors       0   Output aborts sent        0
```

Adapter cable:
使用されているアダプター・ケーブルのタイプ

V.24 circuit:
V.24 仕様で識別された回線番号

Nicknames:
回線の通称名

RS-232
回線の EIA 232 (RS-232 とも呼ばれる) 名

State: 回線の現在の状態: ON、OFF、または ″---″ （これは、このタイプのインターフェースの状態は未定義であることを意味します。)

Line speed:
送信クロック速度 (概略値)

Last port reset:
ポートがリセットされた後の経過時間

Input frame errors:

CRC error
チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)
長さが 8 の偶数倍でないために廃棄された受信パケットの数

Missed Frame
フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

too long (> nnnn bytes)
構成されたフレーム・サイズ (nnnn) より大きかったために廃棄された受信パケットの数

aborted frame
送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

DMA/FIFO overrun
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

L & F bits not set
シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビット

がセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

Output frame counters:

DMA/FIFO underrun errors
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーからデータを取り出す速度が遅かったために、パケットをネットワークに送信できなかった回数

Output aborts sent
高位レベルのソフトウェアの要求によって打ち切られた伝送の数

V.34 と GWCON コマンド

V.34 には独自の監視用の監視プロセスがありますが、GWCON 環境から interface、statistics、および error コマンドを使用すれば、ルーターも構成情報と、装置および回線の完全な統計を表示します。また、GWCON **test** コマンドを使用して、DCE および回線をテストすることもできます。

注: V.34 シリアル・インターフェースに対して **test** コマンドを出すと、現行の呼は除去され、再ダイヤルされます。

GWCON コマンドについての詳細は、133ページの『第10章 動作/監視プロセス (GWCON - Talk 5) およびコマンド』を参照してください。

V.34 インターフェースおよびダイヤル回線の統計

V.34 シリアル・ライン・インターフェースおよびダイヤル回線の統計を表示するには、GWCON (+) プロンプトから **interface** コマンドを使用します。

V.34 シリアル・ライン・インターフェースの以下の統計を表示するには、**interface** コマンドに続けて V.34 シリアル・ライン・インターフェースのインターフェース番号を入力します。

例:

```
interface 1
                                Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
1  1   V.34/0    80000000   44          1          0
0
V.34 MAC/data-link on SCC Serial Line interface

Adapter cable:       RS-232 DTE       RISC Microcode Revision: 1

   V.24 circuit: 105 106 107 108 109 125
   Nicknames:    RTS CTS DSR DTR DCD R1  LL
   RS-232:       CA  CB  CC  CD  CF  CE
   State:        OFF OFF OFF OFF OFF OFF OFF

Line Speed:               115.200 Kbps
Last port reset:          1 hour, 28 minutes, 25 seconds ago
```

```
Input frame errors:
   CRC error                    0   alignment (byte length)   0
   missed frame                 0   too long (>  2182 bytes)  0
   aborted frame                0   DMA/FIFO overrun          0

   Output frame counters:
    DMA/FIFO underrun errors    0   Output aborts sent         0
```

ダイヤル回線の以下の統計を表示するには、**interface** コマンドに続けてダイヤル回線のインターフェース番号 を入力します。

例:

```
interface 3

                                Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
3  2   PPP/1        81640   5C          0          5            0

  Point to Point MAC/data-link on V.34 Dial Circuit interface
```

以下のリストは、シリアル・ライン・インターフェースとダイヤル回線の両方の出力を説明しています。

Nt シリアル・ライン・インターフェース番号またはダイヤル回線インターフェース番号

Nt′ “Nt” がダイヤル回線の場合、これはダイヤル回線がマップされる V.34 シリアル・ライン・インターフェースの番号です。

Interface
インターフェース・タイプとそのインスタンス番号

CSR 基本ネットのコマンドおよび状況レジスター・アドレス

Vec 割り込みベクトル・アドレス

Self-Test Passed
成功した自己テストの回数

Self-Test Failed
失敗した自己テストの回数

Maintenance: Failed
保守障害の数

Adapter cable:
使用されているアダプター・ケーブルのタイプ

V.24 circuit:
V.24 仕様で識別された回線番号

Nicknames
回線の通称名

RS-232
回線の EIA 232 (RS-232 とも呼ばれる) 名

State 回線の現在の状態 (ON または OFF)

Line speed
送信クロック速度 (概略値)

Last port reset
ポートがリセットされた後の経過時間

Input frame errors:

CRC error
チェックサム誤りが含まれているために廃棄された受信パケットの数

Alignment (byte length)
長さが 8 の偶数倍でないために廃棄された受信パケットの数

Missed Frame
フレームが装置に到着したときに利用可能なバッファーがない場合、ハードウェアはそのフレームを廃棄し、紛失フレーム・カウンターを増分します。

too long (> nnnn bytes)
構成されたフレーム・サイズより大きかったために廃棄された受信パケットの数

DMA/FIFO overrun
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーにデータを送信する速度が遅かったために、ネットワークからデータを受信できなかった回数

L & F bits not set
シリアル・インターフェース上で、ハードウェアは到着するフレームの入力記述子情報をセットします。バッファーが到着したフレーム全体を受け入れることができる場合、ハードウェアはそのフレームの最後のビットと最初のビットの両方をセットして、バッファーが完全なフレームを受け入れたことを示します。いずれかのビットがセットされていない場合、パケットは廃棄され、L & F bits not set カウンターが増分され、バッファーは消去されて再利用できるようになります。

注: L & F bits not set カウンターはトラフィックによる影響は受けません。

aborted frame
送信側によって、または伝送路誤りによって途中廃棄された受信パケットの数

Output frame counters:

DMA/FIFO underrun errors
シリアル・インターフェース・カードがシステム・パケット・バッファー・メモリーからデータを取り出す速度が遅かったために、パケットをネットワークに送信できなかった回数

Output aborts sent
高位レベルのソフトウェアの要求によって打ち切られた伝送の数

第45章 ISDN インターフェースの使用

この章では、IBM 2210 上のサービス総合ディジタル網 (ISDN) インターフェースについて説明します。本章には、以下の節が含まれています。

ISDN の概説

ISDN インターフェース・ソフトウェアにより、ISDN を介してルーターを相互接続することができます。インターフェースを設定して、専用リンクとして機能するようにすることができ、あるいは交換回線接続の開始および受信を行うようにすることもできます。これはオンデマンドで、リスタートから自動的に、あるいはオペレーターがコマンドを出して行うことができます。

I.430、I.431、およびチャネル化 T1/E1 は、交換回線ではありません。これらは固定的な専用回線タイプの接続です。

ISDN アダプターとインターフェース

以下の ISDN アダプターは、14T、24T、24E、および 24M モデル用のものがあります。

- 1 ポート S/T ISDN-BRI
- 4 ポート S/T ISDN-BRI
- 4 ポート U ISDN-BRI
- 1 ポートチャネル化 E1 120 オーム ISDN-PRI
- 1 ポートチャネル化 T1/J1 ISDN-PRI

PRI/チャネル化アダプターには CSU/DSU が内蔵されているので、外付けの CSU/DSU は必要ありません。

インターフェースは、次のとおりです。

- 基本インターフェース (BRI)

  基本インターフェースは、2 つの 64-Kbps (キロビット/秒) ベアラー (B) チャネルと 1 つの 16-Kbps データ (D) チャネルを提供します。 B チャネルは、64-Kbps

ビット・パイプによって区切られた HDLC フレームとして使用されます。 D チャネルは呼設定に使用されます。 D チャネルは X.25 トラフィックにも使用できます。

- 1 次群インターフェース (PRI)

  1 次群インターフェースで提供される機能は、基本インターフェースで提供される機能に似ています。ただし、次のような重要な相違点があります。

  – PRI アダプターは、多地点をサポートしません。 BRI アダプターではサポートします。
  – PRI アダプターは、T1/J1 および E1 サポートを提供します。
    - T1/J1 は、23 の 64-Kbps B チャネルと 1 つの 64-Kbps D チャネルをサポートします。
    - E1 は、30 の 64-Kbps B チャネルと 1 つの 64-Kbps D チャネルをサポートします。
  – チャネル化 T1/E1
    - T1/J1 は最高 24 の 64-Kbps タイム・スロットをサポートします。
    - E1 は最高 31 の 64-Kbps タイム・スロットをサポートします。
    - 64-Kbps のタイム・スロットをまとめて、帯域幅を集合することもできます。

注: talk 6 を使用して BRI から PRI にアップグレードする場合は、最初に ISDN とダイヤル構成を消去し、その後で PRI を起動して、PRI を構成することが必要です。

ダイヤル回線

ダイヤル回線には 4 つのタイプがあります。

- 静的回線 (または、リンク)

  注:

  1. I.430、I.431、およびチャネル化 T1/E1 は専用回線接続なので、ダイヤル回線ではありません。
  2. ISDN は、D チャネルを介した X.25 トラフィックを静的回線とみなしますが、**encapsulator** コマンドを使用して、X.25 回線を PVC または SVC として構成することもできます。

- オンデマンドでダイヤルし、指定されたアイドル時間の後で切れる交換回線
- 割り当てられた 1 次専用回線に障害が生じたときにのみ使用される WAN 復元回線
- ダイヤルイン回線は、リモート・クライアントにネットワーク上の資源へのアクセスを提供するために使用されます。

ダイヤル・オンデマンド・インターフェースを介してブリッジングするときは、スパンニング・ツリーを使用不可にし、MAC フィルターを作成して、すべての不要なトラフィックを除去することをお勧めします。 (MAC フィルターは、特定の MAC アドレスを着信先に指定していないすべてのフレームを廃棄します。) これにより、不要なトラフィックのためにダイヤル回線が接続されたままになるのを防止することができます。

注: FR ダイヤル・オンデマンド・インターフェース上で BAN トラフィックを行う場合は、MAC フィルターを追加する必要はありません。 BAN ソフトウェアは常にフィルターを適用することにより、ダイヤル・オンデマンド回線をハングアップさせないブリッジング・トラフィックは、着信先 MAC アドレスが BAN DLCI MAC アドレスに一致するトラフィックだけになるようにします。

可能な各宛先ごとにダイヤル回線を追加します。複数のダイヤル回線を 1 つの ISDN インターフェースにマップすることも可能です。各ダイヤル回線は、ポイント・ポイント・プロトコル (PPP)、フレーム・リレー、または X.25 (D チャネルのみ) を実行する、通常のシリアル・ライン・ネットワークです。これらのプロトコルは、ダイヤル回線を介して動作するように構成されています。

注: 宛先の名前を**コネクション・リスト**に割り当て (add ISDN address)、宛先の番号をリスト内の各回線に割り当てることができます。宛先の名前がコールされると、接続されるまで、またはリストが尽きるまで、リスト内の番号が 1 つずつ試されます。

ルート可能プロトコルおよびブリッジング機能とルーティング機能は、ISDN インターフェースと直接通信することはできません。これらのプロトコルはダイヤル回線上で実行するように構成する必要があります。この実現では、以下の ISDN ダイヤル回線のプロトコルおよび機能をサポートします。

- APPN
- Banyan VINES
- DECnet
- DLSw
- IP
- IPX
- AppleTalk 2
- ブリッジング (SRB、STP、SR-TB、および SRT)
- 帯域幅予約
- WAN 復元

アドレッシング

電話をかけるには、宛先の電話番号を指定する必要があります。ユーザー自身を交換機に識別するためには、ユーザー自身の電話番号を指定する必要があります。 ISDN の場合、電話番号は被呼側ネットワーク・ダイヤル・アドレスであり、便宜上、ネットワーク・アドレス名と呼ばれる名前 (電話番号を表す) が付けられています。

ISDN インターフェースの設定時に、可能な各宛先のアドレスとユーザー自身の電話番号 (ローカル・ネットワーク・アドレスと呼ばれる) を追加します。ダイヤル回線を構成するときには、ローカル・ネットワーク・アドレスを物理インターフェース構成から入手して、その回線の宛先アドレスを設定します。

回線の競合

ISDN PRI T1/J1 インターフェースは最大 23 のアクティブ・コールをサポートし、ISDN PRI E1 インターフェースは最大 30 のアクティブ・コールをサポートします。ISDN BRI インターフェースは、最大 2 つのアクティブ・コールをサポートします。1S4/1S8/1U4/1U8 モデルで WAN もアクティブになっている場合を除いて、通常は ISDN BRI は 2 つのアクティブ・コールを持つことができます。 ISDN インターフェース上には、サポートされているアクティブ・コール数よりも多くのダイヤル回線を構成することができます。 ISDN インターフェースのすべての呼がアクティブのときに、あるダイヤル回線が呼を試みた場合は、2 通りの可能性があります。 1) そのダイヤル回線の優先順位が、アクティブ・コールをもつ回線より高い場合、低い優先順位のダイヤル回線のアクティブ・コールは打ち切られ、高い優先順位をもつダイヤル回線のコールが試みられます。 2) そのダイヤル回線の優先順位が、アクティブ・コールをもついずれのダイヤル回線の優先順位よりも高くない場合、コールは行われません。ルーターは、ISDN 宛先に接続できないダイヤル回線上のプロトコルによって送信されたパケットを廃棄します。

注: D チャネルを介して X.25 通信を行っている場合、D チャネルは常に X.25 接続に利用可能なので、回線の競合は起こりません。

優先順位についての詳細は、657ページの『Set』 を参照してください。

デマンド回線を介したコスト制御

プロトコルから見ると、ダイヤル・オンデマンド回線は常にアップ状態に見えます。ほとんどのプロトコルは定期的にルーティング情報を送信し、ルーターはルーティング情報が送信されるたびに、ダイヤル・オンデマンド回線を介してダイヤルすることになります。定期的なルーティング更新を制限するには、IP と OSI が静的ルートのみを使用するように構成し、ダイヤル回線を介するルーティング・プロトコル (RIP、OSPF) を使用不可にします。 IPX を使用している場合は、静的ルートとサービスを構成して、ダイヤル回線を介するルーティング・プロトコル (RIP, SAP) を使用不可にします。もう 1 つの選択肢は、RIP と SAP の更新間隔を低い頻度に構成することです。ただし、この場合、ルーティング情報が変更されたときに、RIP と SAP がその変更を同報通信するのを防止することはできません。また、IPX キープアライブ・フィルターも使用可能にしておくことが必要です。これにより、キープアライブ・パケットやシリアル化パケットが連続的にダイヤル・オンデマンド・リンクを起動するのを防止することができます。

呼の検証

この ISDN システムは、専有のライン ID プロトコルを使用して、着呼とダイヤル回線を照合します。この ID プロトコルは、ダイヤル回線構成内のインバウンドとライン ID 名を使用して、呼を発信するダイヤル回線と呼を受信するダイヤル回線を照合します。ライン ID プロトコルは、発呼者が開始し、その呼を受信するダイヤル回線が応答する、短い識別プロトコルです。発呼者がライン ID メッセージを提供しない場合、その呼はリジェクトされることもあります。ライン ID の交換は B チャネルで行われます。

論理 ID (LID) をサポートしないルートに接続する場合は、個々のダイヤル回線構成で構成オプションを使用して、LID 交換を抑制することができます。

```
config> set lid_used
```

着信側では、この変数が設定されている場合、その呼は、任意の着側として構成されているか、宛先フィールドに発呼者の電話番号をもつ最初のダイヤル回線に転送されます。

ISDN 原因符号

この ISDN 実現では、ルーターが ISDN インターフェースを介して接続の確立を試みるのを停止させる原因符号を指定しています。アプリケーションが再試行されると、ルーターは再びこのインターフェースを介して接続の確立を試み、元の問題が解決されていれば、その試みは成功します。再試行中にルーターが同じ原因符号を検出した場合、アプリケーションはそれ以上、このインターフェースを介して接続処理を試みません。

原因符号は、次のように解釈します。

1. cause0 が ″0x5″ でないときは、原因符号を無視する。
2. cause0 が ″0x5″ のときは、cause1 を見る。 cause1 の高位 (最上位) ビットが ON のときは、それを OFF にセットする。
3. 結果を 10 進数に変換し、下表 (*ITU-T 勧告 Q.850* から抜粋) で意味を調べる。

表 75. ISDN Q.931 原因符号

符号	原因
1	未割り当て (割り当てられていない番号)
2	指定された中継ネットワークへのルートなし
3	着側へのルートなし
6	チャネル受付不可
7	呼受付、確立チャネルで呼出通知中
16	通常の呼切断
17	着ユーザー・ビジー
18	ユーザー応答なし
19	相手ユーザー応答なし (ユーザー呼出中)
21	呼リジェクト
22	相手端末番号変更
26	非選択ユーザー切断
27	相手端末故障
28	無効番号フォーマット (アドレス不完了)
29	ファシリティー拒否
30	状態照会（STATUS ENQUIRY) への応答
31	正常、未指定
34	回線/チャネル利用不可
38	ネットワーク障害
41	一時障害

表 75. ISDN Q.931 原因符号 (続き)

符号	原因
42	交換機輻輳
43	アクセス情報廃棄
44	要求回線/チャネル利用不可
47	リソース利用不可、未指定
49	サービス品質利用不可
50	要求ファシリティー未登録
57	伝達能力不許可
58	現在伝達能力不許可
63	サービスまたはオプション利用不可、未指定
65	伝達能力未定義
66	未提供チャネル・タイプ指定
69	要求ファシリティー未定義
70	限定ディジタル情報伝達能力のみ利用可
79	サービスまたはオプション未定義、未指定
81	無効呼番号値
82	識別チャネル未定義
83	呼中断あり、ただしこの呼識別ではない
84	呼識別使用中
85	呼中断なし
86	要求された呼識別の呼が切断された
88	端末属性不一致
91	無効中継ネットワーク選択
95	無効メッセージ、未指定
96	必須情報要素不足
97	メッセージ種別未定義
98	呼状態とメッセージ不一致、またはメッセージ種別未定義
99	情報要素未定義
100	無効通知要素
101	呼状態とメッセージ不一致
102	タイマー満了による回復
111	プロトコル誤り、未指定
127	相互接続、未指定

サンプル ISDN 構成

以下に、いくつかの標準的な ISDN 構成を示します。

ISDN を介するフレーム・リレー構成

図29 は、ISDN ネットワークを介してフレーム・リレー・ネットワークを接続する方法を示しています。この構成では、ダイヤル回線上のデータ・リンクをフレーム・リレーとして設定します。

注: ダイヤル回線は、デフォルトではポイント・ポイント (PPP) プロトコルになります。プロトコルをフレーム・リレーに変更するには、`Config>` プロンプトで **set data-link fr** と入力します。コネクションを使用できるのは、両側のデータ・リンクが一致している場合 (たとえば、FR と FR、あるいは PPP と PPP) だけです。

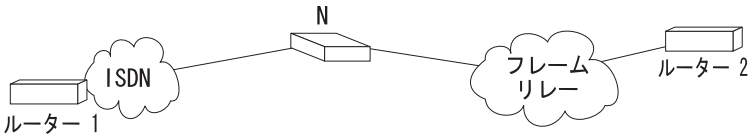


図 29. ISDN を介するフレーム・リレー構成

注: N は、FR 交換機に接続された ISDN TA、または FR 交換機内の ISDN カードのいずれかです。

WAN 復元の構成

図30 は、障害が起きた専用 WAN リンクをバックアップするために (WAN 復元) ISDN 接続を使用する方法を示しています。この例では、ルーター A は通常は WAN リンクを使用してルーター B と通信します。その接続に障害が起きた場合、ISDN ダイヤルアップ・リンクが 2 つのルーターを再接続します。 WAN リンクが回復すると、2 次リンクは自動的に切断します。 WAN 復元用にルーターを構成する方法についての詳細は、763ページの『第57章 WAN 復元の使用』 を参照してください。

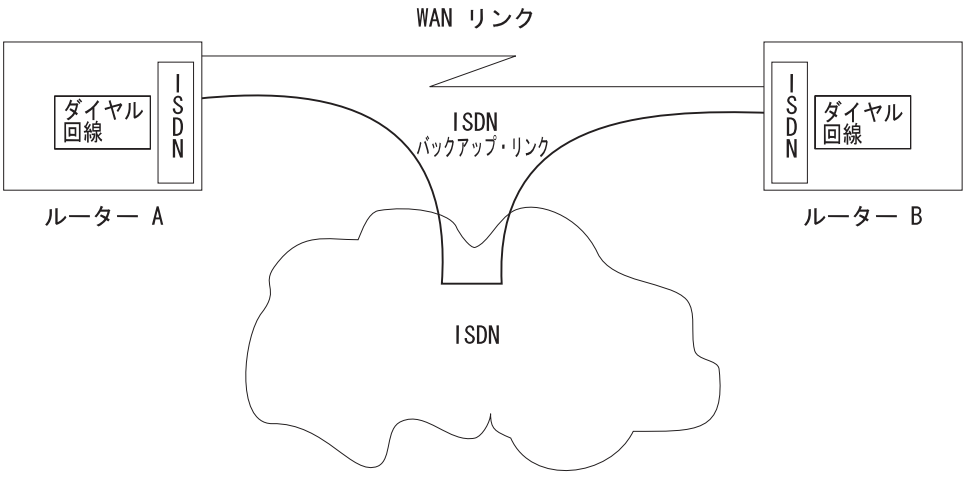


図 30. WAN 復元のための ISDN の使用

WAN 復元の場合、2 次リンクとして使用できるのは、PPP 用に構成されたダイヤル回線だけです。 WAN 再ルートの場合は、PPP ダイヤル回線または FR ダイヤル回線を代替リンクとして使用できます。

チャネル化 T1/E1

チャネル化として構成されている場合、チャネル化/PRI アダプターは分割/チャネル化 T1/J1/E1 サポートを提供します。 56-Kbps または N*64-Kbps のチャネルを使用することができます。これにより、複数の専用回線接続 (たとえば、56-Kbps の V.35 を使用する) を多重化して、1 つの物理接続にまとめることが可能になります。

T1 または E1 の 1 次アダプターをチャネル化として構成するには、次のようにします。

1. ISDN インターフェース用の交換機として 『Channelized』を選択する。
2. ダイヤル回線を構成するときに、この ISDN インターフェース用に使用するタイム・スロットを構成する。詳細については、657ページの『Set』を参照してください。

チャネル化 T1 インターフェースの構成例

```
Config>n 6
ISDN Config>set switch chan
ISDN Config>list


                  ISDN Configuration

Maximum frame size in bytes      = 2048
Switch Variant/Service Type      = Channelized
Available Timeslots: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24


Config>n 7
Circuit config:  7>set net 6
Circuit config:  7>set timeslot 2 3 4 24
Circuit config:  7>list

Base net                        = 6
Idle character                  = 7E
Bandwidth                       = 64 Kbps
Timeslot                        = 2 3 4 24
```

注: これが E1 回線の場合には、利用可能なタイム・スロットは 1 〜 31 になります。

ISDN インターフェースの要件と制約

ルーター

ISDN ソフトウェアは IBM 2210 の以下のモデルを必要とします。

- 127
- 128
- 14T
- 24E - ISDN アダプターが必要

- 24T - ISDN アダプターが必要
- 24M - ISDN アダプターが必要
- 1S4
- 1S8
- 1U4
- 1U8

サポートされる交換機/サービス

ISDN 基本インターフェース (BRI) は、以下の交換機/サービスをサポートします。

- AT&T 5ESS (米国)
- DMS100 (米国)
- USNI1 (米国国内 ISDN1)
- USNI2 (米国国内 ISDN2)
- NET 3 (欧州 ETSI)
- INS-Net 64 (日本)
- VN3 (France Telecom)
- AUS TS 013 (オーストラリア)
- I.430 (634ページの『ISDN I.430 および I.431 交換機』を参照)

ISDN 1 次群速度インターフェース (PRI) は、以下の交換機/サービスをサポートします。

交換機名	有効なコマンド
AT&T 5ESS (米国)	5ESS
AT&T 4ESS	4ESS
Australia (AUSTEL)	AUSPRI
INS-Net 1500 (日本、NTT)	INSPRI
National ISDN 2	USNI2
NET 5 (欧州 ISDN、ETSI)	NET5
Northern Telecom 250 (DMS250)	DMS250
Native I.431	I431 (634ページの『ISDN I.430 および I.431 交換機』を参照)
Channelized T1/E1	CHANNELIZED

ISDN インターフェースの制約事項

- ISDN インターフェースを介して、ルーターのブートまたはダンプを行うことはできません。
- データ通信に D チャネルを使用することはできません。 D チャネルは、D チャネル接続の設定と切断にのみ使用します。
- オプションの ISDN ネットワーク提供者によって提供される X.25 接続性は、D チャネル上ではサポートされません。

ダイヤル回線の構成要件

ISDN を使用する PPP またはフレーム・リレーを構成するときは、以下の要件を考慮する必要があります。

- ISDN インターフェースは、PPP 構成で設定した転送遅延カウンターを強制しません。
- ダイヤル回線では psuedo-serial-ethernet を使用可能にしてはなりません。

始める前に

ISDN の構成を開始する前に、以下の情報が必要です。

- ローカル ISDN ポートの電話番号
- 宛先の電話番号 (内線番号を含む)
- ISDN インターフェースを接続する交換機のタイプ。交換機のリストは、627ページの『サポートされる交換機/サービス』 を参照してください。

注: 交換機のタイプおよびサービス提供者によっては、その他のパラメーター (TEI や SPID など) も必要になることがあります。

構成手順

この節では、ISDN インターフェースと関連のダイヤル回線を構成する方法について説明します。特に実行する必要がある作業は、次のとおりです。

1. ISDN アドレスを追加する。
2. ISDN パラメーターを構成する。
3. ISDN インターフェースを構成する (PRI のみ)。
4. ダイヤル回線を追加する。
5. ダイヤル回線を構成する。

注: 構成変更を有効にするためには、ルーターをリスタートする必要があります。

ISDN アドレスの追加

各 ISDN インターフェースおよび各宛先の ISDN アドレスを追加することが必要です。 ISDN アドレスには、次のものが含まれます。

- *アドレス名*。アドレス名は、アドレスの記述です。最大 23 字までの印刷可能 ASCII 文字列を使用できます。
- *ネットワーク・ダイヤル・アドレス*。ローカル・ポートまたは宛先ポートの電話番号です。句読点を含めて最大 25 桁の数字と 6 文字を入力できます。ルーターは数字のみを使用します。
- *ネットワーク・サブダイヤル・アドレス*。これは任意選択です。これは、インターフェースが PBX に接続した後で解釈される、電話番号の追加部分 (たとえば、内線番号) です。最大 20 桁の数字の他に、11 個のスペースと句読点を含めることができますが、ルーターは数字のみを使用します。

ISDN アドレスを追加するには、Config> プロンプトで **add isdn-address** コマンドを入力します。たとえば、次のように入力します。

```
Config>add isdn-address
Assign address name [23] chars []? baltimore
Assign network dial address [1-15 digits] []? 1-555-0983
Assign network subdial address [1-20 digits] []? 23
```

ISDN アドレスのリストを見たい場合は、Config> プロンプトで **list isdn-address** を入力します。

リストから ISDN アドレスを削除する場合は、Config> プロンプトで **delete isdn-address** コマンドを入力します。

ISDN パラメーターの構成

ISDN Config> プロンプトにアクセスします。 ISDN Config> プロンプトにアクセスするには、Config> プロンプトで、**network** コマンドに続けて ISDN インターフェースのインターフェース番号を入力します。たとえば、次のように入力します。

```
Config>network 3
ISDN user configuration
ISDN Config>
```

Config> プロンプトで **list devices** コマンドを使用すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。構成コマンドについての詳細は、637ページの『ISDN 構成コマンド』 を参照してください。

1. この ISDN インターフェースが接続されている交換機/サービスのタイプを指定する。

   set switch-variant コマンドを使用して、この ISDN インターフェースが接続されているスイッチのタイプを指定します。交換機/サービスのリストは、627ページの『サポートされる交換機/サービス』 を参照してください。たとえば、次のように入力します。

   ```
   ISDN Config>set switch net5
   ```

   これは、交換機で実行されているソフトウェアのタイプです (たとえば、DMS100 は DMS100 Custom ソフトウェアが実行されていることを意味します)。

2. ローカル・ポートのネットワーク・アドレス名を指定する。

   set local-address-name コマンドを使用して、ローカル・ポートのネットワーク・アドレス名を指定します。 **add isdn-address** コマンドを使用して定義したアドレス名の 1 つを使用する必要があります。たとえば、次のように入力します。

   ```
   ISDN Config>: set local-address-name
   Assign local address name []? baltimore
   ```

   注: これは、ISDN 設定メッセージの発番号 (Calling Party Number) フィールドに入れて送られたものです。

3. ローカル・ポートのディレクトリー番号を設定する。

   DN0 は、ISDN サービス提供者が ISDN 設定メッセージの着番号 (Called Party Number) フィールドに入れて提供するものです。このフィールドは着呼にのみ使用されます。 DN0 が構成されていない場合、ルーターは DN0 フィールドを検査せずに、ルーターへのすべての呼に応答します。 DN0 フィールドを追加した場合、

それを削除するときは **remove dn0** コマンドを使用する必要があります。別の set コマンドを使用して、そのフィールドをブランクにすることはできません。

```
ISDN Config>set dn0
Enter DN0 (Directory-Number-0) [ ]?15550983
```

4. BRI の場合のみ、ISDN インターフェースをポイント・ポイント (pp) または マルチポイント (mp) に設定する。

   ポイント・ポイントは、ISDN 回線上の 1 つの ISDN 装置です。マルチポイントは、ISDN 回線を共用する 2 つ以上の ISDN 装置です。交換機の機種によっては、回線上の装置の数に関係なく、回線をマルチポイントとして構成しなければならない場合があります。 ISDN サービス提供者に確認してください。

   ```
   ISDN Config>set multi-point-selection
   Multipoint Selection [MP]? pp
   ```

   注: PRI は構成できません。これは常にポイント・ポイントです。

5. BRI の場合のみ、米国の交換機に接続している場合、サービス提供者がサービス・プロファイル ID (SPID) を必要とすることがあります。

   SPID は、ISDN 装置を固有に識別する最大 20 桁の番号です。 ISDN サービス提供者が SPID を割り当てます。サービス提供者から SPID 番号を入手する必要があります。

   ```
   ISDN Config>set spid
   Enter BChannel Number [1]? 1
   Enter Service Profile ID (SPID) []? 91955555550101
   ```

6. BRI の場合のみ、TEI (端末終端点識別子) を ISDN 交換機の信号 TEI 番号に一致させる。

   サービス提供者に連絡して、交換機がサポートする TEI 信号を確認してください。デフォルトの TEI は auto です。 ISDN インターフェースが接続されている交換機が自動 TEI 信号をサポートしない場合は、TEI を 0 ～ 63 に設定する必要があります。

   5ESS または USNI1 交換機に接続している場合は、各 B チャネルの TEI を設定しなければなりません。 **set tei** コマンドを使用すると、B チャネル番号を求めるプロンプトを出します。

   ```
   ISDN Config>set tei
   TEI [AUTO]? 10
   ```

   注: PRI の場合は、TEI は常に 0 です。

   D チャネルで X.25 を使用している場合には、D チャネルの TEI を別に構成する必要があります。たとえば、次のように入力します。

   ```
   ISDN Config>set tei 2
   TEI  2 []? 21
   ```

7. **set framesize** コマンドを使用して、フレーム・サイズを設定する。たとえば、次のように入力します。

   ```
   ISDN Config>set framesize
   Framesize in bytes (1024/2048/4096/8192) [1024]? 2048
   ```

   注: 1024のフレーム・サイズを選択した場合、PPP は ISDN ダイヤル回線上では動作しません。 PPP の最小サイズは 1500 であるからです。

   ISDN フレーム・サイズの設定については、639ページの『Set』 を参照してください。

任意選択の ISDN パラメーター

この節では、ユーザーが設定できる任意選択の ISDN パラメーターについて説明します。コマンドについての詳しい説明は、637ページの『ISDN 構成コマンド』 を参照してください。

- INS64 を除くすべての ISDN 交換機では、あるアドレスへの発呼数の限界を構成することができます。 **set retries-call-address** コマンドを使用して、応答しない着信先への発呼回数を設定します。また、**set timeout-call-address** コマンドを使用して、呼を再試行する前に待つ時間を設定使用します。

ISDN インターフェースの構成が終了したら、**list** コマンドを使用して、構成を表示してみることができます。

ISDN インターフェースの構成

T1/J1 PRI インターフェース

以下の T1/J1 パラメーターを指定します。

1. T1/J1 PRI インターフェースの場合、伝送路再構成 (line build out) は、ルーターの T1 ポートによって送信される信号の減衰を指定します。サービス提供者によって提供された情報に基づいて、lbo (line build out) を指定します。

   a= -00.0 dB

   b= -07.5 dB

   c= -15.0 dB

   d= -22.5 dB

   たとえば、次のように入力します。

   ```
   set int lbo a
   ```

2. code を B8ZS または AMI に指定する。 B8ZS がデフォルトです。この情報はサービス提供者が提供します。

   たとえば、次のように入力します。

   ```
   set int code AMI
   ```

3. ZBTSI (Zero Byte Time Slot Inversion) を ENABLED または DISABLED に指定する。デフォルトは DISABLED です。この情報はサービス提供者が提供します。

   たとえば、次のように入力します。

   ```
   set int ZBTSI enabled
   ```

4. esf-data-link を指定する。サービス契約に基づいて、次の 1 つを選択します。

   ANSI-T1.403 ANSI-IDLE AT&T-IDLE

   デフォルトは ANSI-T1.403 です。

   たとえば、次のように入力します。

   ```
   set int esf-data-link ansi-idle
   ```

E1 PRI インターフェース

E1 PRI インターフェースの場合、以下のパラメーターを指定します。

1. code を HDB3 または AMI に指定する。 HDB3 がデフォルトです。この情報はサービス提供者が提供します。

   たとえば、次のように入力します。

   ```
   set int code HDB3
   ```

2. crc4 を ENABLED または DISABLED に指定する。デフォルトは ENABLED です。この情報はサービス提供者が提供します。

   たとえば、次のように入力します。

   ```
   set int crc4 enabled
   ```

ダイヤル回線の追加

ダイヤル回線は ISDN インターフェースにマップされます。複数のダイヤル回線を 1 つの ISDN インターフェースにマップすることができます。

ダイヤル回線を追加するには、Config> プロンプトで **add device dial-circuit** コマンドを入力します。ソフトウェアが、各回線にインターフェース番号を割り当てます。この番号を使用して、ダイヤル回線を構成します。たとえば、次のように入力します。

```
Config>add device dial-circuit
Adding device as interface 6
```

構成できるダイヤル回線の数は、構成されるパラメーターの合計数、およびその結果の構成ファイルのサイズによって決まります。

注: ダイヤル回線は、デフォルトではポイント・ポイント (PPP) プロトコルになります。ダイヤル回線プロトコルをフレーム・リレーに変更する場合は、Config> プロンプトで **set data-link fr** コマンドを入力します。回線プロトコルを X.25 に変更する場合は、Config> プロンプトで **set data x25** コマンドを入力します。その他のデータ・リンク・タイプ (SDLC および SRLY) は、ISDN ではサポートされません。

ダイヤル回線の構成

この節では、ダイヤル回線の構成方法について説明します。

1. **network** コマンドに続けてダイヤル回線のインターフェース番号を入力して、Circuit Config> プロンプトを表示する。 Config> プロンプトで **list devices** コマンドを入力すると、ルーター上に構成されているインターフェース番号のリストを表示することができます。たとえば、次のように入力します。

   ```
   Config>network 6
   Circuit configuration
   Circuit Config>
   ```

2. ダイヤル回線を ISDN インターフェースにマップする。 **set net** コマンドを使用します。基本ネットは ISDN インターフェース番号です。たとえば、次のように入力します。

   ```
   Circuit Config>set net
   Base net for this circuit [0]? 3
   ```

   注: ダイヤル回線データ・リンク・タイプが X.25 の場合、または基本ネットの交換機の機種が I.43x またはチャネル化の場合には、以下のステップ (3〜10) は適用されません。

3. ダイヤル回線を接続するリモート・ルーターのアドレス名を指定する。 **add isdn-address** コマンドを使用して定義した名前の 1 つを使用する必要があります。たとえば、次のように入力します。

```
Circuit Config>set destination
Assign destination address name []? baltimore
```

4. ダイヤル回線を発信専用、着信専用、または発信と着信の両方として構成する。

   set calls コマンドを使用します。たとえば、次のように入力します。

```
Circuit Config>set calls outbound
Circuit Config>set calls inbound
Circuit Config>set calls both
```

   注: WAN 復元動作または別のダイヤル・オンデマンド・アプリケーションの場合、回線を着信用または発信用のいずれかに設定することが必要です。

5. 回線のタイムアウト期間を指定する。

   set idle コマンドを使用します。この指定された期間、回線上にトラフィックがないと、ダイヤル回線は切れます。回線を専用回線として構成する場合は、アイドル・タイマーをゼロに設定します。回線をダイヤル・オンデマンドに構成する場合は、アイドル・タイマーをゼロ以外の値に設定します。範囲は 0 ～ 65535 で、デフォルトは 60 秒です。たとえば、次のように入力します。

```
Circuit Config>set idle
Idle timer (seconds, 0 means always active) [0]? 0
```

6. 任意選択で、lid_out_addr を指定することにより、ダイヤル回線の名前を提供することができます。

   2 つのルーター間に複数の回線が構成されている場合 (並列回線)、どちらのダイヤル回線が接続するのかを両方のルーターが知るための手段が必要です。この目的のために、一方の端のルーター (発信側) から lid_out_addr が送信されます。ダイヤル回線を接続するためには、受信側ルーターが、送信側ルーター上の lid_out_address に一致する着信先アドレスを持っていることが必要です。lid_out_addr は、以前に **config>** プロンプトで 『ADD ISDN-ADDRESS』 を使用して追加したアドレス名でなければなりません。

```
Circuit Config>set lid_out_addr  router2
```

7. 任意選択で、ダイヤル回線の相対的な優先順位を設定することができます。

   優先順位フィールドは、利用可能なチャネルがないときに、ある回線を別の回線より優先させることを可能にします。発呼があり、すべてのチャネルが使用中の場合、要求しているダイヤル回線の優先順位を、通信中のすべてのダイヤル回線と照合します。をれより低い優先順位の回線があった場合、その回線は切断され、高い優先順位のダイヤル回線のための呼設定が行われます。

   注: ダウンにされるのは、発信ダイヤル・オンデマンド回線だけです。

   優先順位についての詳細は、657ページの『Set』 を参照してください。

```
Circuit Config>set priority 1
```

8. 任意選択で、呼設定から最初のパケットが送信されるまでの時間を遅らせることができます。 **set selftest-delay** コマンドを使用します。一部の ISDN 交換機は、着側の回線の確立が完了したことを示す信号を受信する前にデータの送信を開始します。自己テスト遅延を設定することにより、最初のパケットが廃棄されるのを防止できます。たとえば、次のように入力します。

```
Circuit Config>set selftest-delay
Selftest delay(milli-seconds,0 means no delay)[150]?200
```

9. 着信アドレス名を設定する。

   set inbound コマンドを使用します。このコマンドは着信回線専用です。たとえば、次のように入力します。

   ```
   Circuit Config>set inbound
   Assign destination inbound address name [ ]? newyork
   ```

   着信アドレス名は、**add isdn-address** コマンドを使用して定義した名前の 1 つに一致していることが必要です。

10. 任意選択で、ダイヤル回線上で実行されているデータ・リンク・レイヤー・プロトコル (PPP またはフレーム・リレー) の構成プロセスに入ることができます。

    encapsulator コマンドを使用します。たとえば、次のように入力します。

    ```
    Circuit Config> encapsulator
    ```

ISDN I.430 および I.431 交換機

日本でサポートされているネイティブ I.430 モード (ドイツでは D64S と呼ばれる) を使用する場合は、ISDN 交換機の機種を I.430 として指定することが必要です。これは ISDN インターフェースを専用回線のように扱います。このモードには、D 信号トラフィックはありません。

ISDN PRI を介して専用回線を稼働している場合は、I.431 交換機を構成する必要があります。

ネイティブ I.430 サポート

各 I.430 または I.431 基本ネットでは、1 つのダイヤル回線しか使用できません。速度は、set bandwidth コマンドを使用して、64-Kbps または 128-Kbps に構成できます。モデル 1S4、1S8、1U4、および 1U8 の場合、WAN と ISDN の両方がアクティブのときには、速度は 64Kbps のみに制限されます。 bandwidth コマンドの構成については、639ページの『Set』を参照してください。

例: Base ISDN Net

```
Config>n 6
ISDN Config>set switch i430
ISDN Config>list all

                                  ISDN Configuration

Maximum frame size in bytes      = 2048
Switch Variant                   = I430 BRI
PS1 detect                       = Enabled
```

例: Dial Circuit

```
Config>n 7 ------------------ DIAL CIRCUIT (CAN ONLY BE ONE FOR I430/I431)
Circuit config:   7>
Circuit config:   7>set net 6
Circuit config:   7>set bandwidth 128
Circuit config:   7>list all

Base net                        = 6
I430 BRI Bandwidth              = 128 kbs
```

ネイティブ I.431 サポート

ネイティブ I.431 サポートを構成する場合は、ダイヤル回線は 1 つしか使用できません。これを基本ネットに接続する必要があります。 I.431 は ISDN PRI T1 アダプター上でのみ動作します。速度は 1.5 Mbps に固定されています。

例: Base ISDN net

```
Config>n 5
ISDN Config>set sw i431
ISDN Config>list all
                  ISDN Configuration

Maximum frame size in bytes      = 2048
Switch Variant                   = I431 PRI
```

例: Dial Circuit

```
Config>n 6
Circuit config:   6>set net 5
Circuit config:   6>list all


Base net                        = 5
```

X.31 サポート

ITU 標準 X.31 は、ISDN を介して X.25 パケットを伝送するためのものです。この標準は、ISDN D チャネル上の X.25 に適用されます。

X.31 は、数カ国のサービス提供者から利用可能です。ルーターに 9600bps X.25 回線を提供します。 D チャネルは常に存在するので、この条件は X.25 PVC または SVC と言えます。

X.31 では、たとえば、パケット・ハンドラーが ISDN サービス提供者によって提供される場合、X.25 パケットおよび LAP/B フレーム (RR、SABME など) が、 ISDN 信号 (Q931/Q921) メッセージとともに D チャネル上で送受信されます。 D チャネルは、ISDN ユーザー端末がリンク・レイヤー・コネクション (SAPI=16) を確立することによって、ISDN 内のパケット・ハンドラー機能にアクセスし、この機能を使用して X.25 レイヤー 3 手順に準拠したパケット通信をサポートできるようにします。最大フレーム転送サイズは 260 バイトです。

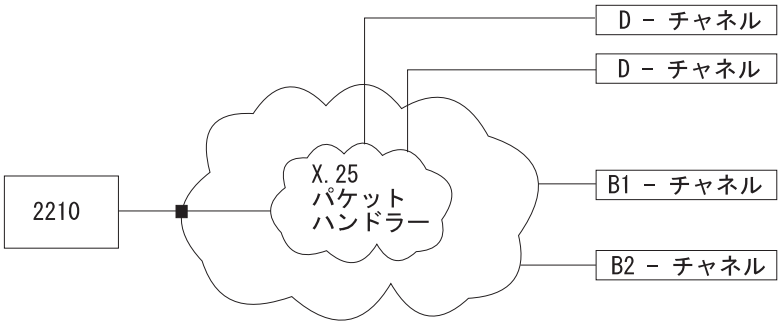


図 31. X.31 サポート

例:

```
Config>n 6
Config>set data x25 6
Circuit config:   6>set net 5
Circuit config:   6>list all


Base net                        = 5
```

マルチポイント ISDN PRI アダプターは、I.431 交換機をサポートしません。 PRI の全ラインを利用するためには、チャネル化を選択し、すべてのタイム・スロットを 1 つのダイヤル回線に割り当てます。

第46章 ISDN インターフェースの構成および監視

この章では、ISDN コマンドおよび GWCON コマンドについて説明します。本章には、以下の節が含まれています。

注: ISDN インターフェースは、ISDN 関連のアクティビティーを監視するのに使用できる ELS メッセージおよび原因符号も提供します。 *イベント・ログ・システム・メッセージの手引き* を参照してください。

ISDN 構成コマンド

表76 は、ISDN 構成コマンドの要約を示しており、それに続く各節で個々のコマンドについて説明しています。これらのコマンドは `ISDN Config>` プロンプトで入力します。

表 76. ISDN 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Disable	BRI の場合にのみ有効です。電源 1 検出を使用不可にします。
Enable	BRI の場合にのみ有効です。電源 1 検出を使用可能にします。
List	ISDN 構成を表示します。
Remove	DN0 エントリーを ISDN 構成から除去します。
Set	フレーム・サイズ、ローカル・アドレス、無応答タイムアウト、無応答後の再試行回数、ISDN 交換機のタイプ、ディレクトリー番号、SPIDS、 TEI、および帯域幅を設定します。
Cause Codes	インターフェースを介して接続を確立するための試行をそれ以上処理するのを停止します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Disable

disable コマンドは、電源 1 検出を使用不可にします。交換機に電源 1 がない場合は、PS1 を使用不可にします。

注: このコマンドは BRI の場合にのみ有効です。

構文:

disable ps1

注: U インターフェース ISDN BRI 上には ps1 検出回線がないので、このフィールドの値は無視されます。

Enable

enable コマンドは、電源 1 検出を使用可能にします。 ISDN 交換機に電源 1 (PS1) がある場合は、インターフェース上の PS1 を使用可能にする必要があります。これにより、インターフェースは、交換機が遮断されて、前回の呼に関するすべての情報が消去されたことを検出してから、接続を再確立するようになります。制限電源モードをサポートする Euro-NET3 交換機の場合は、PS1 を使用可能にしなければなりません。

交換機に電源 1 がない場合は、PS1 を使用可能にしてはなりません。

注: このコマンドは BRI の場合にのみ有効です。

構文:

enable ps1

注: U インターフェース ISDN BRI 上には ps1 検出回線がないので、このフィールドの値は無視されます。

List

list コマンドは、現行の ISDN 構成を表示します。

構文:

list list

例: `list`

```
                                ISDN Configuration
  Local Network Address Name    = line-1-local
  Local Network Address         = 1-508-555-1234
  Local Network Subaddress      = 21
  Maximum frame size in bytes   = 2048
  Outbound call address Timeout = 180  Retries =  2
  Switch-Variant-Model          = US National ISDN-1
  Multipoint Selection          = Point-to-Point
  DN0 (Directory Number 0)      = 5551234
  DN1 (Directory Number 1)      = 5553456
  Service Profile ID (B1)       = 91955555550100
  Service Profile ID (B2)       = 91955555550101
  TEI for B-Channel 1           = Automatic
  TEI for B-Channel 2           = Automatic
  TEI for X.25                      = 21
  PS1 detect                    = Disabled

No circuit address accounting information being kept.
```

Remove

remove コマンドは、**set DN0 entry** コマンドを使用して設定した DN0 エントリーを除去することができます。

構文:

remove DN0-entry...

例: `remove DN0`

Set

set コマンドは、フレーム・サイズ、アドレス、およびタイムアウトを構成します。交換機の機種および TEI 番号も指定します。 PRI の場合、端末終端点識別子 (TEI) は常にゼロ (0) です。

構文:

set framesize...
frame-type[2]
interface
local-address-name...
multipoint-selection[1]...
RAI-type[2]
retries-call-address...
service-profile-id[1]...
timeout-call-address[1]...
switch-variant...
dn0...
dn1...[3]
tei[1]...

framesize 1024 または 2048 または 4096 または 8192

ISDN インターフェースで送受されるフレームの、ネットワーク・レイヤー・部分のサイズを設定します。データ・リンクおよび MAC レイヤーのヘッダーは含まれません。 ISDN フレーム・サイズは、ISDN インターフェースを使用するダイヤル回線に構成したフレーム・サイズ以上の値に設定する必要があります。

PPP ダイヤル回線インターフェースの場合、**set lcp options** コマンドを使用して、PPP MRU を変更することができます。 ISDN フレーム・サイズは、PPP MRU および PPP ヘッダー用のバイトを十分に組み込める大きさであることが必要です。

注: 1024 のフレーム・サイズを選択した場合、PPP は ISDN ダイヤル回線上では動作しません。PPP の最小サイズは 1500 であるからです。

FR ダイヤル回線インターフェースの場合、**set framesize** コマンドを使用して、フレーム・サイズを変更することができます。 ISDN フレーム・サイズは、FR フレーム・サイズ以上の値でなければなりません。

1. BRI のみ
2. チャネル化のみ
3. PRI のみ

ダイヤル回線のフレーム・サイズが ISDN のフレーム・サイズより大きい場合、ルーターの初期化時に、ダイヤル回線のフレーム・サイズが削減されます。

例:

```
set framesize
Framesize in bytes (1024/2048/4096/8192) [1024]? 2048
```

frame type

選択項目は、D4 または ESF です。これは T1 マルチ・フレーム・フォーマットを指定します。非チャネル化モードの場合は、ESF しかサポートされません。フレーム・タイプは、基本 ISDN ネット・メニューのもとで構成します。

例:

```
set frame type
Circuit config: 10>set frame type
```

interface

PRI の場合のみ。 T1 または E1 回線の以下のインターフェース・パラメーターを設定します。

T1 PRI の場合:

lbo ルーターの T1 ポートによって送信される信号の減衰。この情報はサービス提供者によって提供されます。

有効値:

a= -00.0 dB

b= -07.5 dB

c= -15.0 dB

d= -22.5 dB

デフォルト値: a

code この情報はサービス提供者によって提供されます。

有効値: B8ZS または AMI

デフォルト値: B8ZS

ZBTSI ゼロ・バイト・タイム・スロット反転 (Zero Byte Time Slot Inversion)。この情報はサービス提供者によって提供されます。

有効値: 使用可能または使用不可

デフォルト値: 使用不可

esf-data-link

サービス契約。この情報はサービス提供者によって提供されます。

有効値:

ANSI-T1.403

ANSI-IDLE

AT&T-IDLE

デフォルト値: ANSI-T1.403

E1 PRI の場合:

code この情報はサービス提供者によって提供されます。

有効値: HDB3 または AMI

デフォルト値: HDB3

crc4 ルーターの E1 ポートが crc4 符号語を転送し、受信したフレーム内の crc4 符号語を検査するかどうかを指定します。この情報はサービス提供者によって提供されます。

有効値: 使用可能または使用不可

デフォルト値: 使用不可

local-address-name *address name*

これはローカル ISDN ポートのネットワーク・アドレス名です。このアドレス名は、Config> プロンプトで **add isdn-address** コマンドを使用して定義した名前の 1 つに一致していることが必要です。

有効値: 任意の有効なアドレス

デフォルト値: なし

例:

```
set local-address-name
Assign local address name []? line-1-local
```

multipoint-selection mp or pp

BRI の場合のみ。 ISDN 物理バスを、ポイント・ポイント (pp) またはマルチポイント (mp) 構成のいずれかに設定します。ポイント・ポイントは、ISDN 回線上の 1 つの ISDN 装置です。マルチポイントは、ISDN 回線を共用する 2 つ以上の ISDN 装置です。

サービス提供者によっては、回線上の装置の数に関係なく、回線をマルチポイントとして構成することが必要な場合があります。 ISDN サービス提供者に確認してください。

例:

```
set multipoint-selection
Multipoint Selection [PP]? mp
```

RAI type

選択項目は ANSI または Japanese です。これは、D4 フレームを使用している場合、T1 回線上の RAI を示す方法を指定します。 ANSI RAI は、すべてのチャネルのビット 2 の値が 0 であることによって示されます。 Japanese RAI は、フレーム 12 の S ビット位置の値が 1 であることによって示されます。フレーム・タイプは、基本 ISDN ネット・メニューのもとで構成します。

retries-call-address *value*

一部の電話サービス提供者は、自動リコール装置に対して、アクセス不能アドレスまたは自動リコールを拒否するアドレスへの連続コール回数を制限しています。 **Retries-call-address** は、ルーターが一度に試みる呼の最大数を指定します。 **retries-call-address** を 0 に設定すると、ルーターは同時にすべての回線を起動します。

switch-variant を INS64 に設定した場合は、**retries-call-address** のデフォルト値を変更することはできません。 2 に固定されます。

有効値: 0 〜 30

デフォルト値: 23

service-profile-id B-channel# spid#

BRI の場合のみ。各 B チャネルごとにサービス・プロファイル ID (SPID) を設定します。 SPID は、米国で使用され、特定の ISDN 装置を固有に識別します。この ID は、最大 20 桁の長さで、ISDN サービス提供者によって割り当てられます。 SPID は主として、複数の ISDN 装置が単一の ISDN 回線を共用するマルチポイント・バス構成で使用されます。サービス・プロバイダーに問い合わせて、SPID を使用する必要があるかどうかを確認してください。

例:

```
set spid
Enter B-Channel Number [1]? 1
Enter Service Profile ID (SPID) [123]? 91955555550100
```

timeout-call-address # of seconds

ルーターは、無応答アドレスへの **retries-call-address** の最大数に達すると、この時間が満了するまで、次の呼を開始しません。タイムアウト期間は、ルーターがアドレスに向けて最初の発呼を試みた時点で開始します。 **timeout-call-address** を 0 に設定すると、ルーターは呼が設定されるまで再試行します。

switch-variant を INS64 に設定した場合は、 **timeout-call-address** を変更することはできません。 180 に固定されます。

有効値: 0 〜 65535 秒

デフォルト値: 180 秒

例:

```
set timeout-call-address
Outbound call address Time-out (secs) [0]? 180
```

switch-variant

ISDN インターフェースが接続される交換機のモデルを指定します。 ISDN 基本インターフェースまたは ISDN 1 次群インターフェースの交換機の機種/サービス・タイプは、以下のリストから選択することができます。

基本インターフェース (BRI) の有効値:

- 5ESS (米国)
- DMS100 (米国)
- USNI1 (米国の国内 ISDN1)
- USNI2 (米国の国内 ISDN2)
- NET 3 (欧州 ETSI)
- INS 64 (日本)
- VN3 (France Telecom)
- AUS TS 013 (オーストラリア)
- Native I.430

デフォルト値: NET 3

ISDN 1 次群インターフェース (PRI)/チャネル化 T1/E1 の有効値:

- AT&T 5ESS (米国)
- AT&T 4ESS
- Australia (AUSTEL)
- INS-Pri (日本、NTT)
- National ISDN 2
- NET 5 (欧州 ISDN、ETSI)
- Northern Telecom 250
- Native I.431
- Channelized T1/E1

デフォルト値:DMS250

dn0 *directory number 0*

着呼を受け入れるためには、**DN0** が **set local-address-name** コマンドを使用して構成したネットワーク・ダイヤル・アドレス (電話番号) と一致していることが必要です。 DN0 が構成されていない場合は、検査は行われず、すべての着呼が受け入れられます。交換機が呼設定メッセージで発番号を提供しない場合は、DN0 を構成してはなりません。

例:

```
set dn0
Enter DN0 (Directory-Number-0) [ ]? 5088981234
```

dn1 *directory number 1*

DN1 は、交換機 NET3、VN3、および AUS によってサポートされる 2 次ディレクトリー番号です。 DN1 が構成されていない場合は、検査は行われず、すべての着呼が受け入れられます。交換機が呼設定メッセージで発番号を提供しない場合は、DN1 を構成してはなりません。

tei *auto* **または** *none* **または** *value*

BRI または D チャネルを介する X.25 の場合のみ。このコマンドでは、ISDN インターフェースの信号 TEI (端末終端点識別子) を設定します。この設定値は、交換機の信号 TEI と一致していなければなりません。 PRI の場合は、TEI は常にゼロ (0) に設定されます。サービス提供者に問い合わせて、正しい TEI 信号を確認してください。デフォルト値は auto です。交換機が自動 TEI 信号をサポートしない場合にのみ、この設定値を変更します。 TEI の有効な設定値は、auto または 0 〜 63 の値です。 TEI を none に設定すると、ISDN インターフェースは使用不可になります。

USNI-1 および 5ESS 交換機の場合は、各 B チャネルごとに TEI を設定する必要があります。 switch variant をこれらの交換機の 1 つに設定した場合、**set tei** コマンドは B チャネル番号の入力を求めるプロンプトを出します。

例 1:

```
set tei
TEI  [AUTO]? 60
```

例 2:

```
set tei
TEI 0 or TEI 1 [1]? 1
TEI [AUTO]?
```

例 3:

```
set tei 2
TEI []? 21
```

Cause Codes

Cause Code コマンドは、ルーターが 『specified』 (有効値) レスポンスを受信したときに、ISDN インターフェースを介して接続の確立を再試行するのを防止するのに使用します。これらのコマンドは `Cause Config>` プロンプトで入力します。

構文:

cause ? (Help)
add
list
remove
exit

表 77. ISDN Cause Codes コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Add	原因符号エントリーを ISDN 構成に追加します。
List	ISDN 構成の原因符号リストを表示します。
Remove	ISDN 構成から原因符号エントリーを除去します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add **add** コマンドは、原因符号を ISDN 構成に追加するのに使用します。

有効値: 01 ～ FF の間の任意の 16 進値

デフォルト値: なし

構文: cause code add *value*

例: `add FF`

Remove

remove コマンドは、原因符号を ISDN 構成から除去するのに使用します。

有効値: 01 ～ FF の間の任意の 16 進値

デフォルト値: なし

構文: cause code remove *value*

例: `remove FF`

List **list** コマンドは、ISDN 構成の原因符号リストを表示するのに使用します。

構文: cause code list

インターフェース監視プロセスへのアクセス

ISDN のインターフェース監視プロセスにアクセスするには、GWCON (+) プロンプトから、次のコマンドを入力します。

```
+ network #
```

ただし、# は、ISDN インターフェースの番号です。ダイヤル回線の監視プロセスに直接アクセスすることはできませんが、ISDN インターフェースにマップされたダイヤル回線を監視することができます。

ISDN 監視コマンド

以下の節では、ISDN インターフェースの料金計算エントリー、呼、回線、パラメーター、および統計を表示することができる ISDN 動作コマンドについて説明します。これらのコマンドは ISDN> プロンプトで入力します。

表 78. ISDN 監視コマンドの要約

監視コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Calls	前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線に行われた、完了した接続および試行された接続の数をリストします。
Channels	ISDN 1 次群インターフェース上のチャネルの統計をリストします。
Circuits	ISDN インターフェース上に構成されたすべてのデータ回線の状態を示します。
Parameters	ISDN インターフェースの現行パラメーターを表示します。
Statistics	ISDN インターフェースの現行統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Calls

calls コマンドは、前回にルーター上の統計がリセットされた以降に、このインターフェースにマップされた各ダイヤル回線で行われた、完了した接続および試行された接続の数をリストするのに使用します。

構文:

calls

例:

```
calls
Net Interface  Site Name           In    Out   Rfsd  Blckd
  4     PPP/1  v403                2      0      0      0

Unmapped connection indications:    0
```

Net このインターフェースにマップされたダイヤル回線の数

Interface
インターフェースのタイプとそのインスタンス番号

Site Name
ダイヤル回線のネットワーク・アドレス名

In このダイヤル回線で受け入れられた着信接続

Out このダイヤル回線によって開始された、完了した接続の数

Rfsd ネットワークまたはリモート着信ポートによってリジェクトされた、このダイヤル回線によって開始された接続の数

Blckd ルーターがブロックした接続試行。ルーターが接続試行をブロックするのは、すべての利用可能なチャネルが使用中の場合、最大試行回数が使い尽くされてルーターがタイマーのカウントダウンを待っている場合、あるいはレイヤー 1 はアップであるが、レイヤー 2 がダウンの場合です。

Unmapped connection indications:
着呼を受け入れるように構成され、使用可能にされているダイヤル回線がないために、ルーターによってリジェクトされた接続試行の回数

Channels

channels コマンドは、ISDN 1 次群インターフェース上のチャネルの統計をリストします。

構文:

channels

Circuits

circuits コマンドは、ISDN インターフェース上に構成されている 『Up』 または 『Available』 のダイヤル回線の状態を表示します。

構文:

circuits

例:

```
circuit
Net Interface  MAC/Data-Link    State     Reason      Duration
4     PPP/1   Point to Point    Up B1     SelfTest    91:24:03
5     PPP/2   Point to Point    Up B2     Inbound     91:24:00
```

Net このインターフェースにマップされたダイヤル回線の数

Interface
インターフェースのタイプとそのインスタンス番号

MAC/Data-Link
このダイヤル回線に構成されたデータ・リンク・プロトコルのタイプ

State ダイヤル回線の現行状態

Up 現在接続された状態です。

Available
現在は接続されていませんが、利用可能です。

Disabled
ダイヤル回線は使用不可にされています。

Down ダイヤル回線がビジーであるか、リンク・レイヤー・プロトコルがダウンしているために、接続に失敗しました。

Reason
現行状態の理由:

nnn_Data
(nnn はプロトコルの名前です。) プロトコルに送信するデータがあったので、回線はアップです。

Rmt Disc
リモート切断。リモート着側が呼を切断したので、回線はダウンまたは利用可能のいずれかです。

Opr Req
オペレーター要求。前回の呼が監視コマンドによって切断されたので、回線は利用可能です。

Inbound
回線が着呼に応答したので、回線はアップです。

Restoral
WAN 復元動作のため、回線はアップです。

Self Test
回線は静的として構成されており (アイドル・タイム = 0)、使用可能にされたときに正常に接続されました。

Duration
回線が現行状態にある時間の長さ

Parameters

parameters コマンドは、現行の ISDN 構成を表示するのに使用します。

構文:

parameters

例:

```
parameters
ISDN Port parameters:

Local Address Name:        vl233
Local Network Address:     20
Local Network Subaddress:
Frame Size:          2048
TEI 0:               Automatic
TEI 1:               Automatic
X.25 TEI:               21
Switch Variant:      AT&T 5ESS (United States)
Multipoint Selection:    Multipoint
Directory Number 0:      20
Outbound call address Timeout:     180       Retries:     0
```

Statistics

statistics コマンドは、この ISDN インターフェースの現行統計を表示するのに使用します。

構文:

statistics

BRI の例:

```
statistics
Link:   Active    ISDN Firmware:   1.0    Handler State: Running

                     D Channel     B1 Channel     B2 Channel

Total Transmits          32788         230217         164336
Total Receives           32789         164342         208255
Transmit Bytes          196767       22797579        6572177
Receive Bytes           196785        6572411        9517221
Invalid Interrupts           0              0              0

Transmit:     D       B1       B2    Receive:        D       B1       B2

Error         0        0        0    Error           0        5        0
Overflow      0        0        0    Overflow        0        0        0
Underrun      0        0        0    Overrun         0        0        0
Abort         0        0        0    Abort           0        5        0
                                      CRC Error       0        0        0
```

I.430 を使用する BRI の例:

```
statistics
Link:   Active    ISDN Firmware:   0.0    Handler State: Running


Total Transmits          32788
Total Receives           32789
Transmit Bytes          196767
Receive Bytes           196785
Invalid Interrupts           0

Transmit:                          Receive:

Error         0                    Error           0
Overflow      0                    Overflow        0
Underrun      0                    Overrun         0
Abort         0                    Abort           0
                                   CRC Error       0
```

これは、リンクの現在の状態、ファームウェアの改訂、およびダイヤル回線の状態を表示します。また、インターフェース上での送受信に関する統計も表示します。

E1 による PRI の例:

```
  statistics
  Link:   Active    ISDN Firmware:   1.0    Handler State: Running

Transmit    D  Channel     Receive    D  Channel

Packets          68422     Packets          68419
Bytes           411656     Bytes           413592
Overflow            23     Overflow            3
Underrun             0     Too Long            6
                           Abort               4
                           CRC error           8
                           Misaligned          3

Transmit    B  Channels    Receive    B  Channels

Packets        1499094     Packets        1499228
Bytes         59955660     Bytes         59951780
Overflow             0     Overflow            90
Underrun             0     Too Long           171
                           Abort              139
                           CRC error          232
                           Misaligned          72

E1 Status Register         E1 Error Count Registers
```

```
Receive AIS         : Off  CRC6 Errors:        4
Receive RAI         : Off  LCV  Errors:       38
Receive Carrier Loss: Off  FEB  Errors:       11
Receive Loss of Sync: Off  FAS  Errors:       24
```

I.431 を使用する T1 による PRI の例:

```
statistics
Transmit                    Receive

Packets              0      Packets             0
Bytes                0      Bytes               0
Overflow         68480      Overflow            0
Underrun             0      Too Long            0
                            Abort               0
                            CRC error           0
                            Misaligned          0

T1 Status Register          T1 Error Count Registers

Receive AIS         : Off  LCV  Errors:           0
Receive RAI         : Off  CRC6 Errors:           0
Receive Carrier Loss: Off  Sync Errors:    47937328
Receive Loss of Sync: On

T1 PRM Events                  Local       Remote

CRC Error                          0            0
Controlled Slip                    0            0
Line Code Violation                0            0
Frame Sync Bit Error               0            0
Severely Errored Frame             0            0
Payload Looback Active             0            0
PRMs Processed (1/sec)             0            0
```

チャネル化 T1 の例:

```
  statistics
  Link:   Active    ISDN Firmware:   0.0    Handler State: Running

Transmit                    Receive

Packets             44      Packets            40
Bytes             1600      Bytes            1520
Overflow             0      Overflow            0
Underrun             0      Too Long            0
                            Abort               0
                            CRC error           0
                            Misaligned          0

T1 Status Register          T1 Error Count Registers

Receive AIS         : Off  LCV  Errors:           0
Receive RAI         : Off  CRC6 Errors:           0
Receive Carrier Loss: Off  Sync Errors:           0
Receive Loss of Sync: Off
Payload Loopback    : Off
Line    Loopback    : Off

T1 PRM Events                  Local       Remote

CRC Error                          0            0
Controlled Slip                    0            0
Line Code Violation                0            0
Frame Sync Bit Error               0            0
Severely Errored Frame             0            0
Payload Looback Active             0            0
PRMs Processed (1/sec)            46           46
```

ISDN と GWCON コマンド

ISDN には独自の監視用の監視プロセスがありますが、GWCON 環境から **interface**、**statistics**、および **error** コマンドを使用すれば、ルーターも構成情報と、装置および回線の完全な統計を表示します。また、GWCON **test** コマンドを使用して、DCE および回線をテストすることもできます。

注: ISDN インターフェースに対して **test** コマンドを出すと、現行の呼は除去され、再ダイヤルされます。

Interface -- ISDN インターフェースとダイヤル回線の統計

GWCON プロンプト (+) で **interface** コマンドを使用して、ISDN インターフェースおよびダイヤル回線の統計を表示します。

ダイヤル回線の統計を表示するには、**interface** コマンドに続けて、ダイヤル回線のインターフェース番号を入力します。 ISDN インターフェースの場合、情報は D チャネルと B チャネルについて表示されます。 (これは ISDN **statistics** コマンドで表示されるものと同じ情報です。)

例:

```
interface 3

                                Self-Test  Self-Test  Maintenance
 Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
 3  3   ISDN/0          0    0          1          0            0

   ISDN Base Net MAC/data-link on ISDN Basic Rate Interface interface
   Link:   Active    ISDN Firmware:   1.0    Handler State: Running

                       D Channel      B Channels

   Total Transmits            591              0
   Total Receives             601              0
   Transmit Bytes            3981              0
   Receive Bytes             4050              0
   Invalid Interrupts           0              0

   Transmit:    D       B Channels     Receive:      D       B Channels
   Error        0               0      Error         0               0
   Overflow     0               0      Overflow      0               0
   Underrun     0               0      Overrun       0               0
   Abort        0               0      Abort         0               0
                                     CRC Error       0               0
```

ダイヤル回線の以下の統計を表示するには、**interface** コマンドに続けてダイヤル回線のインターフェース番号を入力します。

例:

```
interface 4
                               Self-Test  Self-Test  Maintenance
Nt Nt' Interface      CSR  Vec     Passed     Failed       Failed
4  3   PPP/1           0    0          1          2            0

 Point to Point MAC/data-link on ISDN Basic Rate
Interface
```

下のリストは、ISDN とダイヤル回線の両方の出力を説明しています。

Nt シリアル・ライン・インターフェース番号またはダイヤル回線インターフェース番号

Nt' *Nt* がダイヤル回線の場合、これはダイヤル回線がマップされる ISDN インターフェースのインターフェース番号です。

Interface
インターフェース・タイプとそのインスタンス番号

CSR 基本ネットのコマンドおよび状況レジスター・アドレス

Vec 割り込みベクトル・アドレス

Self-Test Passed
成功した自己テストの回数

Self-Test Failed
失敗した自己テストの回数

Maintenance: Failed
保守障害の数

Configuration -- ルーターのハードウェアおよびソフトウェアに関する情報

ルーターのハードウェアおよびソフトウェアに関する情報を表示するには、 GWCON (+) プロンプトから **configuration** コマンドを入力します。これには、ルーター上に構成されたインターフェースとそのインターフェースの状態を表示するセクションが含まれています。

ダイヤル回線がダイヤル・オンデマンドとして構成されている場合、ダイヤル回線の状態は、接続されているかどうかに関係なく、常に Up として表示されます。この場合、Up は、ダイヤル回線が接続状態または利用可能のいずれかであることを意味しています。

ダイヤル回線が静的回線として構成されている場合には、ダイヤル回線が接続されている場合にのみ、状態は Up と示されます。 (**configuration** コマンドの出力例については、137ページの『Configuration』 を参照してください。)

第47章 ダイヤル回線の使用

この章では、V.25bis、V.34、または ISDN インターフェースにマップされたダイヤル回線インターフェース上のダイヤル回線の使用法について説明します。

ダイヤルインおよびダイヤルアウト・インターフェースは、ダイヤル回線インターフェースの特殊なタイプです。

注:

1. PPP ダイヤル回線インターフェースは、ISDN、V.25bis、または V.34 ネットワークを基本ネットワーク・インターフェースとして使用することができます。
2. FR ダイヤル回線インターフェースは、ISDN または V.25bis ネットワークを基本ネットワーク・インターフェースとして使用することができます。
3. 交換 SDLC コールイン・ダイヤル回線インターフェースは、V.25bis ネットワークを基本ネットワーク・インターフェースとして使用します。
4. BRI の場合、ISDN D チャネルを介して X.25 回線を使用することができます。
5. ダイヤルアウト回線インターフェースは、V.34 ネットワークを基本ネットワーク・インターフェースとして使用します。
6. ダイヤルイン回線は、ISDN または V.34 ネットワークを基本ネットワーク・インターフェースとして使用することができます。

ダイヤル回線の構成方法については、以下を参照してください。

- ISDN インターフェースについては、619ページの『第45章 ISDN インターフェースの使用』 を参照してください。
- V.25bis インターフェースについては、581ページの『第41章 V.25bis ネットワーク・インターフェースの使用』 を参照してください。
- V.34 インターフェースについては、601ページの『第43章 V.34 ネットワーク・インターフェースの使用』を参照してください。

第48章 ダイヤル回線の構成

この節では、ダイヤル回線の構成コマンドおよび動作コマンドについて説明します。

ダイヤル回線構成コマンド

653ページの『第47章 ダイヤル回線の使用』 は、ダイヤル回線構成コマンドの要約を示しています。ダイヤル回線構成コマンドは、Circuit Config> プロンプトで入力します。構成変更を有効にするためには、ルーターをリスタートする必要があります。

Circuit Config> プロンプトにアクセスするには、**network** コマンドに続けて 『ダイヤル回線』 のインターフェース番号を入力します。 (ダイヤル回線番号は、**add device dial-circuit** コマンドを入力したときに割り当てられています。) Config> プロンプトで **list devices** コマンドを入力すると、ユーザーが追加したダイヤル回線のリストを表示することができます。

表 79. ダイヤル回線構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Delete	着呼の設定をダイヤル回線構成から削除します。
Encapsulator	データ・リンク・プロトコル構成を変更することができます。
List	ダイヤル回線構成パラメーターを表示します。
Set	ダイヤル回線を着信用または発信用に構成したり、ダイヤル回線をシリアル・ライン・インターフェースにマップしたり、アドレス、アイドル・タイムアウト、優先順位、lid_out アドレス、着信先、および自己テスト遅延を設定したりします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Delete

delete コマンドは、着呼の設定をダイヤル回線構成から除去するのに使用します。

構文:

delete inbound *destination*

inbound *destination*

INBOUND 着信先および ANY_INBOUND 設定値を、ダイヤル回線構成から除去します。これにより、ダイヤル回線は電話番号が*destination* パラメーターに一致する発呼側からの呼のみを受け入れるようになります。

Encapsulator

encapsulator コマンドは、ダイヤル回線インターフェース上で実行されているリンク・レイヤー・プロトコル (たとえば、 PPP、フレーム・リレー、X.25、ダイヤルアウト、SDLC) の構成プロセスに入るのに使用します。

注: **add device dial-circuit** コマンドによって作成されるダイヤル回線インターフェースのデフォルトは PPP になります。リンク・レイヤー・タイプをフレーム・リレーに変更したい場合は、Config> プロンプトで **set data-link frame-relay** コマンドを使用します。リンク・レイヤー・タイプを SDLC に変更したい場合は、Config> プロンプトで **set data-link sdlc** コマンドを使用します。リンク・レイヤー・タイプを ISDN BRI D チャネル上の X.25 に変更したい場合は、Config> プロンプトで **set data-link x25** コマンドを使用します。

構文:

encapsulator

次の例は、PPP ダイヤル回線またはダイヤル・インターフェースに対して encapsulator コマンドを使用して、PPP 構成プロセスに入ることを示しています。

例:

```
encapsulator
Point-to-Point user configuration
PPP Config>
```

V.25bis を基本ネットとして使用するダイヤル回線を構成する場合は、以下のことに注意してください。

- V.25bis インターフェースのクロックは外部として事前定義されています。モデム (DCE) がクロック速度を制御します。クロック、符号化、およびその他の HDLC パラメーターは、ダイヤル回線構成の一部として構成することはできません。

ISDN に対して PPP またはフレーム・リレーを構成するときは、ダイヤル回線構成の HDLC パラメーターは構成できないので注意してください。物理レイヤー・パラメーターは ISDN インターフェース上で構成します。

PPP プロトコルの構成については、333ページの『第26章 シリアル・ライン・インターフェースの構成』 または 467ページの『第33章 ポイント・ポイント・プロトコル・インターフェースの使用』 を参照してください。

フレーム・リレー・プロトコルの構成については、409ページの『第31章 フレーム・リレー・インターフェースの使用』 または 429ページの『第32章 フレーム・リレー・インターフェースの構成および監視』 を参照してください。

SDLC インターフェースの構成または監視については、555ページの『第39章 SDLC インターフェースの使用』 または 559ページの『第40章 SDLC インターフェースの構成および監視』を参照してください。

ダイヤルインおよびダイヤルアウト・インターフェースの構成については、663ページの『第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用』 を参照してください。

X.25 インターフェースの構成または監視については、345ページの『第28章 X.25 ネットワーク・インターフェースの構成および監視』を参照してください。

Circuit Config> プロンプトに戻るには、**exit** コマンドを使用します。

List

list コマンドは、現行のダイヤル回線構成を表示するのに使用します。

I.430 および I.431 についての詳細は、634ページの『ISDN I.430 および I.431 交換機』を参照してください。

構文:

list

例:

```
list
Base net:       1
Destination name:    remote-site-baltimore
Inbound dst name:    local-1
Outbound calls       allowed
Inbound calls        allowed
Idle timer           = 60 sec
SelfTest Delay Timer = 0 ms
```

Base net:
このダイヤル回線がマップされるシリアル回線インターフェースの名前

Destination name:
発信回線の着呼側ネットワーク・アドレス名と、LID 機構が着呼に対して使用するデフォルトの比較用アドレス

Inbound dst name:
このパラメーターは、他のアドレスのどれにも一致しない着呼を受け入れるように回線が構成されている場合にのみ表示されます。これは、LID 機構が着呼に対して使用する代替の比較用アドレス名です。

Outbound calls allowed
回線が発呼を開始するよう構成されている場合に、このパラメーターを表示します。

Inbound calls allowed
回線が着呼を受け入れるように構成されている場合に、このパラメーターを表示します。

Idle timer
アイドル・タイマーの設定値 (秒) を表示します。範囲は 0 ～ 65535 です。0 は、これが専用回線であることを示します。

SelfTest Delay Timer
自己テスト遅延タイマーの設定値 (ミリ秒) を表示します。範囲は 0 ～ 65535 です。 0 は遅延なしを示します。

Set

set コマンドは、ダイヤル回線をインターフェース (たとえば、ISDN、V.34、または V.25bis) にマップしたり、ダイヤル回線を発信または着信 (あるいは、その両方) 用として構成したり、宛先アドレス、着信アドレス、アイドル・タイムアウト、および自己テスト遅延を設定するのに使用します。

注: ダイヤル回線上で SDLC、I.430、I.431、チャネル化、または X.25 を稼働している場合、以下のパラメーターはソフトウェアが特定のデフォルト値を使用するので、**set** コマンドを使用して変更することはできません。

- Calls - 着信
- Destination - デフォルト・アドレス
- Inbound destination - 宛先着信アドレスなし
- Any_inbound - any_inbound を設定
- Idle - 0
- Lid_out_addr - LID 名なし
- Lid_used - 使用不可
- Priority - 8
- Self_test_delay

構文:

set

any_inbound

bandwidth

calls...

destination...

inbound destination...

idle...

idle-char

lid_out_addr...

lid_used

net...

priority...

selftest-delay...

timeslot . . .

any_inbound
他のどのダイヤル回線にも一致しない着呼は、この回線にマップして、着呼として受け入れることを指定します。

bandwidth *kbps*
I.430 およびチャネル化 T1/E1 回線の帯域幅 (Kbps) を設定します。

有効値:

I.430 の場合: 64 または 128

チャネル化の場合: 56 または 64

デフォルト値: 64

calls [*outbound* **または** *inbound* **または** *both***]**
このダイヤル回線を発信専用、着信専用、または発信と着信の両方に指定します。デフォルトは「両方」です。

destination *address_name*

このパラメーターは、ダイヤル回線が動作するために必要です。これは、このダイヤル回線が接続するリモート・ルーターのネットワーク・ダイヤル・アドレスです。 LID プロトコルは、このパラメーターを着呼に対するデフォルトの比較用アドレスとして使用します。このパラメーターは、Config> プロンプトで **add isdn address** コマンドまたは **add v25-bis address** コマンドを使用して指定したアドレス名と一致していなければなりません。

例: set destination remote-site-baltimore

inbound destination *address_name*

このパラメーターは、ダイヤル回線が発信と着信の両方に設定されており、このルーターのローカル・ダイヤル・アドレスが、リモート・ルーターがダイヤルする宛先ダイヤル・アドレスと異なる場合に設定します。たとえば、ルーターの 1 つが PBX、国際、または LATA 間交換局を通す必要がある場合は、番号が異なることになります。このパラメーターは、LID プロトコルが着呼に適用するデフォルトの比較用アドレスをオーバーライドします。このパラメーターは、Config> プロンプトで **add isdn address** コマンドまたは **add v25-bis address** コマンドを使用して指定したアドレス名と一致していなければなりません。

例: set inbound remote-site-1

idle *# of seconds*

回線のタイムアウト期間を指定します。この指定された期間、回線上にプロトコル・トラフィックがないと、ダイヤル回線は切断されます。範囲は 0 ～ 65535 秒で、デフォルトは 60 秒です。ゼロの設定値はタイムアウト期間がないことを意味し、この回線が専用回線であることを示します。

注:

1. WAN 復元動作の場合は、アイドル・タイムアウトを 0 に設定する必要があります。
2. I.43x、X.25、またはチャネル化回線の場合、ユーザーはこのパラメーターを設定することができません。

idle-char

I.43x またはチャネル化回線に使用されるアイドル文字を指定します。

注: 通常の ISDN 回線の場合は、このパラメーターは構成できません。

有効値: 7E または FF

デフォルト値: 7E

例: set idle-char 7E

lid_out_addr *address_name*

lid_out_addr は、2 つのルーター間のダイヤル回線の名前です。 2 つのルーター間に複数の回線が構成されている場合 (パラレル回線)、どちらのダイヤル回線が接続するのかをルーター間で明確に知る手段が必要です。この目的のために、一方の端のルーター (発信側) から lid_out_addr が送信されます。受信側の他方のルーターは、同じストリングを着呼の宛先名として構成しま

す。 lid_out_addr は、以前に config> プロンプトから **ADD ISDN-ADDRESS** を使用して追加したアドレス名でなければなりません。

lid_used [enabled or disabled]
論理 ID をサポートしない装置への回線の論理 ID 交換を抑制します。

有効値: 使用可能または使用不可

デフォルト値: 使用不可

net # 基本回線番号を、この回線をマップするシリアル・ライン・インターフェースの # に設定します。

注: ダイヤルアウト・インターフェースの場合、インターフェースは V.34 網でなければなりません。

例:

```
Circuit Config> set net
Base net for this circuit [ ]? 2
```

priority
優先順位フィールドは、利用可能なチャネルがないときに、ある回線を別の回線より優先させることを可能にします。発呼要求があり、すべてのチャネルが使用中の場合、要求元のダイヤル・オンデマンド回線の優先順位を、通信中のすべてのダイヤル・オンデマンド回線と照合します。これより低い優先順位の発信ダイヤル・オンデマンド回線があった場合、その回線は切断され、高い優先順位のダイヤル・オンデマンド回線の呼が設定されます。接続の発信側の優先順位のみが考慮されます。ダイヤル・オンデマンドの着呼は、高い優先順位の発呼のためにダウンにされることはありません。ダイヤル・オンデマンドの着呼は、それより低い優先順位の呼をダウンにすることはできません。

selftest-delay *# of milliseconds*
このパラメーターを使用して、呼が設定されてから最初のパケットが送信されるまでの間の時間を遅らせることができます。 selftest-delay を設定することにより、最初のパケットが廃棄されるのを防止できます。範囲は 0 ～ 65535 で、デフォルトは 150 です。

V.25bis ダイヤル回線の場合、モデムの同期化に時間がかかる場合は、この設定値を調整します。

ISDN ダイヤル回線の場合、一部の ISDN 交換機は着側の回線の設定が完了したことが通知される前にデータ転送を開始するので、ダイヤル・オンデマンド・リンクでは、この設定値を調整することが必要になることがあります。

timeslot *list of slots*
このダイヤル回線で使用するスロットまたはスロットのリストを指定します。回線で使用できるスロットの番号は、サービス提供者が割り当てます。リストの指定は、スロット番号をブランクで区切って示します。

注: このパラメーターは、チャネル化 T1/E1 回線の場合にのみ使用できます。

有効値:

チャネル化 T1 の場合: 1 ～ 24

チャネル化 E1 の場合: 1 〜 31

デフォルト値: なし

例: `set timeslot 1 4 5 8`

第49章 LAN へのダイヤルイン・アクセス (DIALs) サーバーの使用

DIAL サーバーを使用すると、リモート・ユーザーが LAN にダイヤルインし、LAN アダプターによってローカル接続されている場合と同じ方法で LAN の資源にアクセスすることが可能になります。同様に、DIAL サーバーを使用すると、LAN に接続されたユーザーがダイヤルアウトして WAN の資源 (電子掲示板、FAX 装置、インターネット・サービス提供者 (ISP)、およびその他のオンライン・サービス) にアクセスすることも可能になり、ワークステーション上にアナログ電話回線とモデムを装備する必要がなくなります。

DIAL サーバーは、同時にダイヤルイン・ユーザーとダイヤルアウト・ユーザーの両方として構成することができます。 IBM DIAL ダイヤルイン・クライアントは、リモート・ワークステーション上で稼働し、ダイヤルイン機能を提供します。 664ページの図32 は、ダイヤルイン機能をサポートする DIAL サーバーとして使用される装置の例を示しています。

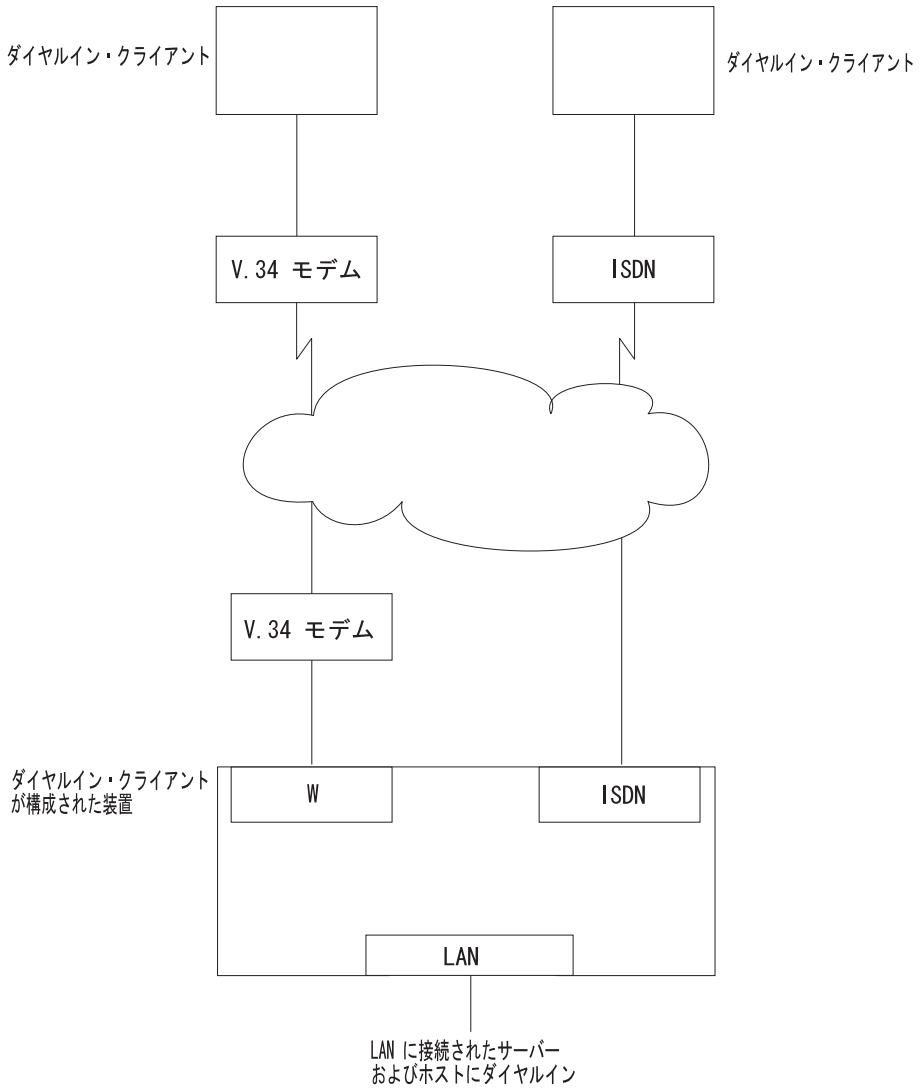


図 32. ダイヤルインをサポートする DIAL サーバーの例

IBM DIAL ダイヤルアウト・クライアントは、ネットワークに接続されたワークステーション上で稼働し、ダイヤルアウト機能を提供します。 665ページの図33 は、ダイヤルアウト機能をサポートする DIAL サーバーとして使用されている 2210 の例を示しています。

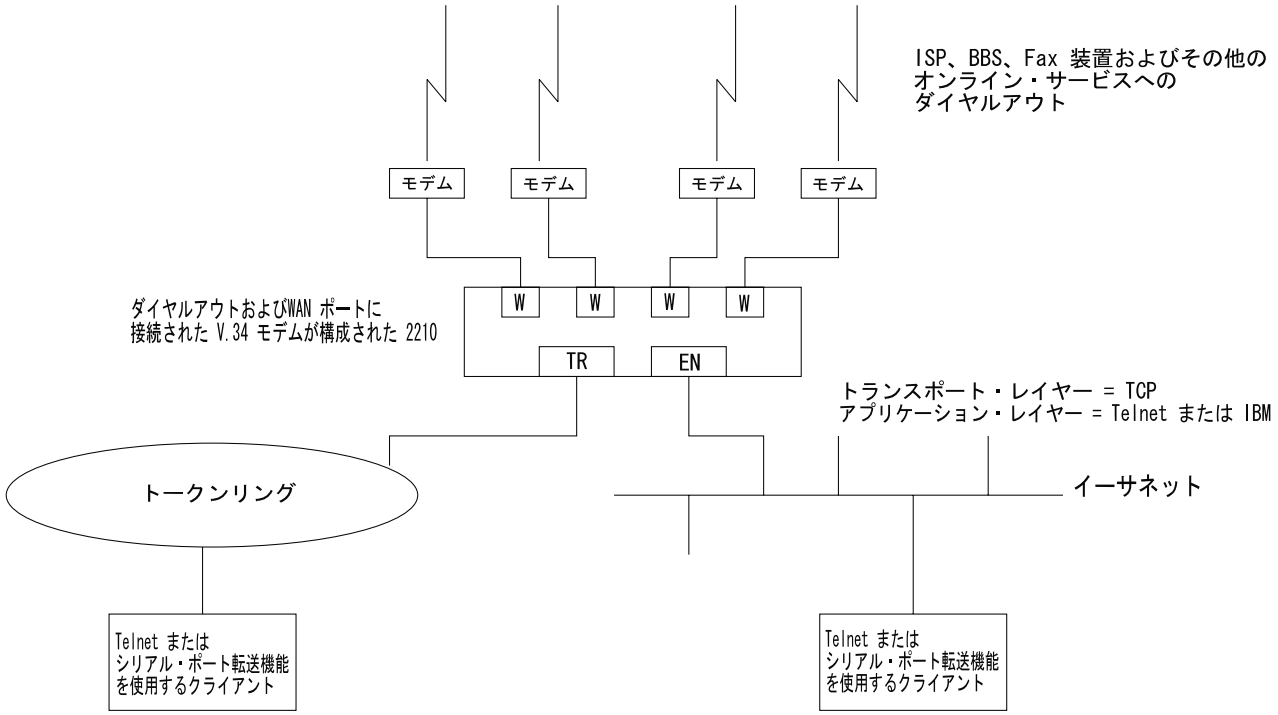


図 33. ダイヤルアウトをサポートする DIAL サーバーの例

ダイヤルイン・アクセスを使用する前に

ダイヤルイン・アクセスを使用する前に、以下の要件を満たしていることが必要です。

- ワークステーションで、IBM DIAL ダイヤルイン・クライアントまたは別の PPP ダイヤルイン・クライアント (以下では、***ダイヤルイン・クライアント*** または ***PPP ダイヤルイン・クライアント*** と呼びます) が稼働している。
- クライアント・マシンのプロトコル構成が完了している。
- 単一ユーザー・ダイヤルインに使用する 2210 の WAN ポートに、ISDNインターフェース、内蔵モデム・インターフェース、または外付け V.34 モデムが接続されている。
- LAN に DIAL サーバーが完全に構成されている。

ダイヤルイン・アクセスの構成

この節では、DIAL サーバー上のダイヤルイン機能とダイヤルアウト機能両方を構成する方法について説明します。ダイヤルイン・アクセスを使用するためのクライアントの構成方法は、ワークステーションが使用するクライアントに付属の資料に記載されています。

ダイヤルイン・インターフェースの構成

2210 上のダイヤルイン・インターフェースは、ダイヤル回線の特殊なタイプです。通常のダイヤル回線の設定値のほとんどは、単一ユーザー・ダイヤルイン・アプリケ

ーションには該当しないので、***ダイヤルイン*** という名前の新しい装置タイプを追加して、このダイヤル回線用の適切なデフォルト値を設定することができます。ダイヤルイン装置を追加すると、IBM DIAL ダイヤルイン・クライアントを含めた大多数の PPP ダイヤルイン・クライアントに適用できる PPP カプセル化機能構成のデフォルト値も設定されます。これらのデフォルト値については、『ダイヤルイン・インターフェースのダイヤル回線パラメーターのデフォルト値』、および 『ダイヤルイン回線のダイヤル回線 PPP カプセル化機能パラメーター』で説明します。

注: DIALs 機能は、ダイヤルイン回線でしか使用可能にできません。ダイヤルイン回線は、基本ネットがV.34 または ISDN ネットの場合にのみサポートされます。

ダイヤルイン・インターフェースのダイヤル回線パラメーターのデフォルト値

注: この節で説明するパラメーターは、指定変更してはなりません。指定変更すると、ダイヤルイン機能が正しく動作しなくなります。パラメーターの詳しい説明は、653ページの『第47章 ダイヤル回線の使用』を参照してください。

ダイヤルイン・インターフェースを追加すると、以下のデフォルト値が設定されます。

- ***Idle time*** は 0 に設定されます。標準回線は、アイドル・タイマーが意味をもたない回線として定義されていることに注意してください。これは、自動的にダイヤルアウトする固定回線ではありません。この回線がダイヤルアウトするのは、PPP コールバックがネゴシエーションされた場合、あるいはこの回線でマルチリンク PPP が使用可能にされている場合だけです。 475ページの『Shiva パスワード認証プロトコル (SPAP)』および 527ページの『第35章 マルチリンク PPP プロトコルの使用』を参照してください。
- ***Inbound calls*** は許可されます。 PPP ダイヤルイン・クライアントは Nways ダイヤル回線によって実現された LID 交換を使用しないので、任意の着信を設定することができます。
- ***Outbound calls*** は許可されます。

  注: ダイヤルイン回線の 『発信』 は、ダイヤルアウト回線と同じではありません。668ページの『ダイヤルアウト・インターフェースを構成する前に』を参照してください。

- 『default_address』 に対してデフォルトの宛先アドレスが設定されます。このアドレスは、V.34 アドレスまたは ISDN アドレスのリストに追加されます。これらの呼は着信であり、発呼はコールバックまたはマルチリンク PPP 交換の結果だけになるので、宛先アドレスは無意味になります。ただし、このアドレスは、回線パラメーター用として必要です。このアドレスは削除してはなりません。削除すると、回線が使用不能になります。

ダイヤルイン回線のダイヤル回線 PPP カプセル化機能パラメーター

注: 以下のパラメーターについての詳しい説明は、467ページの『第33章 ポイント・ポイント・プロトコル・インターフェースの使用』を参照してください。

ダイヤルイン・インターフェースを追加すると、以下のデフォルト値が設定されます。

- SPAP、CHAP、および PAP に対する認証は使用可能です。
- PPP MRU は 1522 に設定されます。この MRU サイズは、IBM DIAL ダイヤルイン・クライアントの Windows 3.1、OS/2、および DOS バージョンで必要です。これらのクライアントを使用していないことが明らかでない限り、この設定値を変更しないでください。
- PPP カプセル化機能上の DIAL を自動的に使用可能にします。これにより、NetBIOS 制御プロトコル、NetBIOS フレーム制御プロトコル、残り時間、SPAP 認証、コールバック、LCP 識別、およびクライアントへの IP 静的ルートの自動追加と削除など、LAN へのダイヤルイン・アクセス ユーザーにとって重要な機能がオンになります。 DIALs 機能についての詳細は、467ページの『第33章 ポイント・ポイント・プロトコル・インターフェースの使用』を参照してください。

ダイヤルイン・インターフェースの追加

ダイヤルイン・インターフェースを追加するには、次のようにします。

1. 2210 の利用可能な WAN インターフェースの 1 つで、V.34 または ISDN 基本ネットを構成する。構成についての詳細は、601ページの『第43章 V.34 ネットワーク・インターフェースの使用』、および 619ページの『第45章 ISDN インターフェースの使用』を参照してください。
2. **talk 6** コマンドを入力して、`Config >` プロンプトにアクセスする。
3. `Config >` プロンプトで **add device dial-in** と入力して、ダイヤルイン・インターフェースを追加する。ダイヤルイン回線をいくつ追加するかを尋ねられます。このコマンドは、新しいネットを作成し、それぞれのネット番号を報告し、基本ネットの番号の入力を求め、マルチリンク PPP の場合は使用可能にするように指示するプロンプトを出します。

   例: 現在の最大ネットは 1 、そして基本ネット 1 に 2 ダイヤルイン・ネットを追加したいと想定します。

図34 は、ダイヤルイン・インターフェースの定義例です。

図 34. ダイヤルイン・インターフェースの追加

```
*talk 6
Config>add device dial-in
Enter the number of PPP Dial-in Circuit interfaces [1]? 2
Adding devices as interfaces 2-3
Defaulting data-link protocol to PPP

Base net for this circuit [0]? 1
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.

Base net for this circuit [0]? 1
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.

Use "set data-link" command to change the data-link  protocol
Use "net " command to configure dial circuit parameters.
Config>li dev
Ifc 0     Ethernet                        Slot: 1    Port 1
Ifc 1     8-port ISDN Primary T1/J1       Slot: 4    Port 1
Ifc 2     PPP Dial-in Circuit
Ifc 3     PPP Dial-in Circuit
```

ダイヤルアウト・インターフェースを構成する前に

2210 上でダイヤルアウト・インターフェースを構成し、それを使用する前に、以下の要件を満たしていることが必要です。

- DIAL サポートを備えた IBM Nways ソフトウェアが 2210 にロードされている。
- 2210 上の利用可能な WAN ポートに接続する場合は、外付け V.34 モデム、内蔵モデム、または ISDN インターフェース。構成については、601ページの『第43章 V.34 ネットワーク・インターフェースの使用』を参照してください。
- ワークステーションが、2210 DIAL サーバーへのアクセスをもつ LAN に接続されている。
- クライアントに telnet、telnet 転送機能、または IBM DIAL ダイヤルアウト・クライアントなどのソフトウェアが導入されている。ダイヤルアウト・クライアントが正しく機能するためには、クライアントに IP が正しく構成されていることが必要です。

ダイヤルアウト・インターフェースの構成

以下のステップでは、装置上のダイヤルアウト・インターフェースの構成方法について説明します。

1. V.34 モデムを、ダイヤルアウト・インターフェースとして使用する WAN ポートに接続する。
2. 2210 DIAL サーバーのコンソールに接続する。
3. * プロンプトで **talk 6** と入力する。
4. V.34 インターフェースを設定する。詳細については、601ページの『第43章 V.34 ネットワーク・インターフェースの使用』を参照してください。
5. **add device dial-out** コマンドを使用して、ダイヤルアウト・インターフェースを追加する。インターフェースの入力を求められたら、利用可能な V.34 インターフェース番号を入力します。

   注:

   a. V.34 基本ネット上に複数の回線を構成することができます。ただし、同時にアクティブにできる回線は 1 つだけです。

   b. ソフトウェアは、***default_address*** と呼ばれる V.34 アドレスを定義します。このアドレスはダイヤルアウトに必要なので、削除しないでください。これがないと、ダイヤルアウトは機能しなくなります。
6. PPP 認証サーバーを構成し (IBM DIAL ダイヤルアウト・クライアントを使用している場合)、474ページの『PPP 認証プロトコル』で説明しているように、PPP ユーザーを追加する。追加される PPP ユーザーは、ダイヤルアウトが使用可能でなければなりません。 telnet を使用するダイヤルアウトは認証の必要がないので、telnet セッションの場合は認証を構成しないでください。
7. グローバル・ダイヤルアウト・パラメーターを構成する。 **feature dial** と入力して (72ページの『Feature』を参照)、ダイヤルイン・アクセス構成環境に入ります。

   この環境で、ダイヤルアウト非活動タイマー、ダイヤルアウト・サーバー名、モデム・プール、およびその他のパラメーターを構成することができます。
8. 装置をリスタートする。

モデム・プールの構成

モデム・プールとは、ユーザーからは 1 つのモデムに見えるモデムのグループとして定義されます。ユーザーのダイヤルアウトが必要になると、このプールの中の最初の利用可能なモデムが使用されます。モデム・プールは、同じポート名をもつダイヤルアウト・インターフェースのグループを定義することによって、2210 DIAL サーバー内に作成されます。デフォルトでは、すべてのダイヤルアウト・インターフェースは 『ALL_PORTS』 という名前になり、これがモデム・プールを形成します。ダイヤルアウト・インターフェースを個別に命名すれば、ユーザーはダイヤルアウトに使用する特定のモデムを選択することが可能になります。

モデム・プールを構成するには、次のようにします。

1. `*` プロンプトで **talk 6** と入力する。
2. **net *n*** と入力する。ここで、***n*** は、668ページのステップ 4 で定義したダイヤルアウト・インターフェースの番号です。これにより、このインターフェースの構成環境に入ります。
3. `Circuit Config>` プロンプトで **encapsulator** と入力する (655ページの『Encapsulator』を参照してください)。これにより、ダイヤルアウト構成環境に入ります。
4. `Dial-out Config>` プロンプトで **set portname** と入力する。ポートの番号 (最大 30 文字) の入力を求めるプロンプトが出ます。既存のポート名を指定すると、モデムはその名前のプールに追加されます。
5. 2210 をリスタートする。

DIAL の構成

この節では、DIAL サーバーを構成するのに使用されるコマンドを示します。その他の関連のコマンドは、以下に記載されています。

- 56ページの『Add』
- 72ページの『Feature』
- 80ページの『Set』
- 154ページの『ELS 構成環境への出入り』

動的ホスト構成プロトコル (DHCP)

動的ホスト構成プロトコル (DHCP) は、ネットワーク上のホストに構成パラメーターを提供するために開発されたものです。 DHCP は、他の構成パラメーターとともに、ネットワーク・アドレスをホストに割り当てる機構を備えています。

プロキシー DHCP 機能は、ダイヤルイン PPP ユーザーに代わって、クライアントとしての役目を果たします。これによって、装置はダイヤルイン・セッションの期間、あるいはリース期間が満了するまでの間、IP アドレスをリースすることができます。 DHCP サーバーから割り当てられた IP アドレスが、PPP IPCP を通してダイヤルイン・クライアントに通知されます (IPCP の説明は、480ページの『IP 制御プロト

コル』を参照してください)。ダイヤルイン・クライアント・ソフトウェアは、IP アドレスを割り当てるために DHCP が使用されたことは知らないので、DHCP を起動する必要はまったくありません。

プロキシー DHCP を使用するためには、少なくとも 1 つの DHCP サーバーが構成されており、ルーターからアクセス可能であることが必要です。

プロキシー DHCP では、ダイヤルイン・ユーザーに割り当てられるアドレスは、直接接続された LAN の同じサブネット内に存在することが必要です。標準的な構成では、プロキシー ARP サブネット・ルーティングを使用可能にし、ルーターがダイヤルイン・クライアントに代わってローカル・ネットワーク上のホストへの ARP 要求に応答できるようにすることが必要です。

基本 DHCP の設定

最も基本的な構成では、ルーターと同じネットワーク上に 1 つの DHCP サーバーが存在し、リースされるダイヤルイン・アドレスがこの LAN と同じサブネット内にあることが必要です。

クライアントはダイヤルインするときに、DHCP サーバーから IP アドレスをリースし、クライアントとの IPCP ネゴシエーションに使用します。

1. 2210 と DHCP を同じ LAN に接続する。
2. DHCP サーバーを構成し、開始する (IP アドレスをリースするためのサーバーの設定方法については、DHCP サーバーの資料を参照してください。リースする IP アドレスは、直接接続された LAN のサブネット内に存在しなければならず、またプロキシー ARP が 2210 上で使用可能にされていなければならないことを覚えておいてください。)
3. プロキシー DHCP の標準的な設定では、Client-Specified、Userid、および Interface IP Address Negotiation オプションを使用不可にします。

```
Dials
Config>list ip
DIALs client IP address specification:
Client : disabled
UserID : disabled
Interface : disabled
DHCP Proxy : enabled
```

これは、要するに、ユーザーは IP アドレスを DHCP サーバーから入手する必要があることを示しています。ルーターは、ユーザーが自分のアドレスを指定することを許可しないだけでなく、Userid または Interface セクションに IP アドレスが構成されていても、それを無視します。

4. DHCP サーバーを追加する (`Dials Config>` **`add dhcp 10.0.0.111`**)
5. ダイヤルイン・クライアント・ソフトウェアを *Server assigned* に設定する。

   注:

   a. *Server assigned* 構成は、ダイヤルイン・クライアントの実現によって異なります。

   b. クライアント・ソフトウェアは、そのアドレスを DHCP から入手するように構成してはなりません。クライアントのアドレスは、初期構成要求時にアドレス 0.0.0.0 を IPCP に送信することによって入手する必要があります。
6. この設定では、DHCP GATEWAY ADDRESS はデフォルトの 0.0.0.0 にします。

DHCP サーバーへの複数のホップ

構成された DHCP サーバーは、接続されたルーターから到達可能な IP アドレスに存在しなければなりません。リモート・アクセス・ボックスからサーバーに常に PING できることが必要です。

DHCP サーバーが複数ホップ離れた場所にある場合、サーバーは応答の送信先のアドレスを知っている必要があり、また、どのプールから IP アドレスを割り当てるかを示すことが必要です。 DHCP サーバーを利用して多数のサブネットにアドレスを提供できるようにするために、IP を割り当てるプールは重要であり、どのアドレス・プールから選択するかについて何らかの指示をする必要があります。この目的のために、DHCP ゲートウェイ・アドレス (*giaddr*) が使用されます (この用語は RFC 2131 の定義に準拠しています)。 *giaddr* は、2210 にローカルのアドレス (たとえば、トークンリングまたはイーサネット LAN ポートなど) でなければなりません。また、*giaddr* は DHCP サーバーが応答に使用するアドレスなので、DHCP サーバー自体からこのアドレスに PING できることも確認する必要があります。

複数 DHCP サーバー・ネットワーク

冗長度のために、複数の DHCP サーバーを構成することも可能です。複数のサーバーを構成した場合、プロキシー DHCP クライアントはすべてのサーバーにアドレスを尋ね、最初に受信した応答を受け入れます。 DHCP サーバーのいずれかが 2 ホップ以上離れていたり、プール内のアドレスに対応していないサブネットに接続されている場合には、*giaddr* を構成する必要があります。 『DHCP サーバーへの複数のホップ』を参照してください。

複数の DHCP サーバーがアドレスを提供する可能性があるので、各サーバーに構成するアドレス・プールはオーバーラップしないようにすることが重要です。さらに、DHCP サーバーが応答および検索を行う *giaddr* は 1 つしかないので、各アドレス・プールは相互に同じサブネット内に存在することが必要です。

動的ドメイン・ネーム・サーバー (DDNS)

ドメイン・ネーム・サーバー (DNS) は、IP アドレスをホスト名にマップするもので、通常は静的な性質を持っています。動的 DNS 機能というのは、DDNS DHCP サーバーおよび DNS サーバーとともに使用すると、DHCP が IP アドレスとホスト名のマッピングを用いて DNS サーバーを動的に更新することができる機能をいいます。この機能は、プロキシー DHCP と一緒にしか使用できません。

2210 上の DNS を使用可能にし、ユーザー・プロファイルにホスト名を構成すると (474ページの『PPP 認証プロトコル』を参照)、このホスト名がオプション 81 (DDNS) として DHCP サーバーに渡されます。 DDNS に対して DHCP サーバーが正しく構成されている場合、DHCP サーバーは、ルーターにリースされた IP アドレスと、ルーターが送信したホスト名を使用して、DDNS サーバーを更新します。これによって、他のユーザーはホスト名を使用してダイヤルイン・クライアントにアクセスすることが可能になり、クライアントは動的に選択された IP アドレスを知っている必要はありません。

第50章 ダイヤルイン・アクセス・インターフェースの構成

この章では、ダイヤルイン・アクセス・インターフェースの構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

- 680ページの『ダイヤルイン・インターフェースの監視』
- 680ページの『ダイヤルアウト・インターフェースの監視』

ダイヤルイン・アクセス・インターフェースの監視は、他のインターフェースの監視と同様です。インターフェース監視プロンプトにアクセスするには、次のようにします。

1. * プロンプトで **talk 5** と入力する。
2. **net *n*** と入力する。ここで、***n*** は、ダイヤルイン・インターフェースの番号です。

DIAL グローバル構成コマンド

DIAL (DIAL Config>) グローバル・パラメーター構成環境にアクセスするには、Config> プロンプトで **feature dials** と入力します。 表80 は、利用可能なコマンドをリストしています。

表 80. DIAL グローバル構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	DHCP (動的ホスト構成プロトコル) サーバーを、DHCP サーバーのリストに追加します。
Delete	DHCP サーバーをリストから削除します。
Disable	IP アドレス・ネゴシエーション、ダイヤルアウト・プロトコル、SPAP バナー、および動的 DNS を使用不可にします。
Enable	IP アドレス・ネゴシエーションのタイプ、ダイヤルアウト・プロトコル、SPAP バナー、および動的 DNS を使用可能にします。
List	グローバル DIALs パラメーターとその値をリストします。
Set	許容時間、DHCP ゲートウェイ・アドレス、NetBIOS ネーム・サーバー・アドレス、ローカル割り当て MAC アドレス、動的ネーム・サーバー・アドレス、ダイヤルアウト非活動タイマー、およびダイヤルアウト・サーバー名を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Add

add コマンドは、サーバーのリストに新しいプロキシー DHCP サーバーを追加するのに使用します。リストには DHCP サーバーの IP アドレスが入っており、この IP アドレスがダイヤルイン・クライアントにリースされます。冗長度のために、複数のサーバーを追加することも可能です。サーバーの最大数は 20 です。

構文:

add dhcp-server *ipaddress*

例:

```
DIALs Config> add dhcp-server
DIALs Proxy DHCP server address [0.0.0.0]? 10.0.0.1
```

Delete

delete コマンドは、サーバーのリストから既存のプロキシー DHCP サーバーを削除するのに使用します。

構文:

delete dhcp-server *ip address*

例:

```
DIALs Config> delete dhcp-server
Enter the address to be deleted [0.0.0.0]? 10.0.0.1
```

Disable

disable コマンドは、IP アドレス・ネゴシエーション、ダイヤルアウト・プロトコル、SPAP バナー、および動的 DNS を使用不可にするのに使用します。

構文:

disable dynamic-dns

dial-out

ip-address-negotiation . . .

spap-banner

dial-out ***type***

telnet または IBM DIAL ダイヤルアウト・クライアントとのダイヤルアウトを使用不可にします。以下のものを指定することができます。

dials すべての IBM DIAL ダイヤルアウト・クライアントを使用不可にします。

telnet すべての telnet クライアントを使用不可にします。

両方のタイプのクライアントを使用不可にするためには、各タイプごとに disable dial-out コマンドを入力する必要があります。両方のタイプのクライアントを使用不可にすると、2210 上のダイヤルアウトが使用不可になります。

IP-address-negotiation ***type***

各種の IPCP アドレス・ネゴシエーション方式を使用不可にします。以下のいずれも指定できます。

- クライアントは、使用するアドレスを指定することができます。これは ″userid″ インターフェースおよび ″dhcp-proxy″ より優先されます。
- Userid - ルーターは認証されたユーザー・プロファイルで IP アドレスを調べます。アドレスが非ゼロの場合、そのアドレスがクライアントに提供されます。これは ″interface″ および ″dhcp-proxy″ より優先されます。

- Interface - ルーターはインターフェースの IPCP 設定値を調べます。アドレスが非ゼロに構成されている場合、そのアドレスがクライアントに提供されます。これは ″dhcp-proxy″ より優先されます。
- DHCP-proxy - ルーターは DHCP サーバーに IP アドレス・リースを照会します。リースを取得できない場合、IPCP は失敗します。

これらの方式についての説明は、480ページの『IP 制御プロトコル』を参照してください。

dynamic-dns
ユーザーのホスト名の DHCP オプション 81 を送信するのを使用不可にします。詳細については、671ページの『動的ドメイン・ネーム・サーバー (DDNS)』を参照してください。

spap-banner
SPAP バナーを SPAP によって認証されたリモート・ユーザーに送信するのを使用不可にします。

注: \n を入力すると、バナーの改行文字がクライアントに表示されます。

Enable

enable コマンドは、IP アドレス・ネゴシエーション、ダイヤルアウト・プロトコル、SPAP バナー、および動的 DNS を使用不可にするのに使用します。

構文:

enable ip-address-negotation . . .
dynamic-dns
ip-address-negotiation . . .
spap-banner

dial-out *type*
telnet または IBM DIAL ダイヤルアウト・クライアントとのダイヤルアウトの使用を使用可能にします。デフォルトでは、両方のタイプのクライアントが使用可能になります。以下のものを指定することができます。

dials すべての IBM DIAL ダイヤルアウト・クライアントを使用可能にします。

telnet すべての telnet クライアントを使用可能にします。

IP-address-negotiation *type*
各種の IPCP アドレス・ネゴシエーション方式を使用可能にします。以下のいずれも指定できます。

- Client-specified - クライアントは、使用するアドレスを指定することができます。これは 『userid』、『interface』、および 『dhcp-proxy』 より優先されます。
- Userid - ルーターは認証されたユーザー・プロファイルで IP アドレスを調べます。アドレスが非ゼロの場合、そのアドレスがクライアントに提供されます。これは 『interface』 および 『dhcp-proxy』 より優先されます。

- Interface - ルーターはインターフェースの IPCP 設定値を調べます。アドレスが非ゼロに構成されている場合、そのアドレスがクライアントに提供されます。これは 『dhcp-proxy』 より優先されます。
- DHCP-proxy - ルーターは DHCP サーバーに IP アドレス・リースを照会します。リースを取得できない場合、IPCP は失敗します。

これらの方式についての説明は、480ページの『IP 制御プロトコル』を参照してください。

dynamic-dns

ユーザーのホスト名の DHCP オプション 81 を送信するのを使用可能にします。詳細については、671ページの『動的ドメイン・ネーム・サーバー (DDNS)』を参照してください。

spap-banner

SPAP バナーを SPAP によって認証されたリモート・ユーザーに送信するのを使用可能にします。このコマンドは、バナーの内容を入力するように求めるプロンプトを出します。詳細については、475ページの『Shiva パスワード認証プロトコル (SPAP)』を参照してください。

List

list コマンドは、現行の構成を表示するのに使用します。ポイント・ポイント・コンソールから、各ネットの DHCP 状態およびリース時間を監視することができます。508ページの例を参照してください。

構文:

list all

dhcp-servers

dial out

dynamic-dns

ip-address-negotiation

name-servers

spap-banner

time-allowed

例:

```
DIALs config>li all
DIALs client IP address specification:
Client     :  enabled
UserID     :  enabled
Interface  :  enabled
DHCP Proxy :  disabled


Note: Proxy DHCP is currently disabled
Configured DHCP servers:            1.1.1.1          2.2.2.2
DHCP Gateway (giaddr): 0

Dynamic DNS: Disabled

Primary Domain Name Server    (DNS) : none
Primary NetBIOS Name Server  (NBNS) : none
Secondary Domain Name Server  (DNS) : none
```

```
Secondary NetBIOS Name Server (DNS) : none

Time allowed for connections: unlimited

SPAP BANNER is :Welcome to my world.

Box-level dial-out settings

Inactive timer:                            15
Transport Protocols enabled for dial-out:  TELNET DIALs
Server name:                               2210_DIALS_SERVER
```

この例は、以下のことを示しています。

DIALs client IP address specification
IP アドレス・ネゴシエーション方式とそれらが使用可能かどうかを表示します。このセクションの表示およびボックス・レベルのダイヤルアウト設定値が入っているセクションを、**list ip-address-negotiation** コマンドへの応答として受け取ります。

Configured DHCP servers
現在 DHCP サーバーとして構成されている IP アドレスのリストを表示します。このセクションには、DHCP ゲートウェイとして使用されているインターフェースもリストされます。このセクションの表示は、**list dhcp-servers** コマンドへの応答として受け取ります。

Dynamic Name Servers
動的 DNS が使用可能かどうかを表示します。このセクションの表示は、**list dynamic-dns** コマンドへの応答として受け取ります。

primary domain server (dns)
この行とその下の数行は、構成されている 1 次および 2 次ネーム・サーバーを表示します。このセクションの表示は、**list name-servers** コマンドへの応答として受け取ります。

time allowed
このユーザーの最大時間 (分) を表示します。このセクションの表示は、**list time-allowed** コマンドへの応答として受け取ります。

spap banner
spap バナーの内容を表示します。このセクションの表示は、**list spap-banner** コマンドへの応答として受け取ります。

Set

set コマンドは、許容時間、DHCP ゲートウェイ・アドレス、NetBIOS ネーム・サーバー・アドレス、動的ネーム・サーバー・アドレス、ダイヤルアウト非活動タイマー、およびダイヤルアウト・サーバー名を設定するのに使用します。

構文:

set dhcp-gateway-address
dial-out . . .
dns . . .
laa

nbns . . .

time-allowed

dhcp-gateway-address *interface# ipaddress*

DHCP ゲートウェイに対応する IP アドレスを設定します。 DHCP はアドレスを以下の目的で使用します。

1. DHCP の応答先のアドレス
2. DHCP が割り当てる IP アドレスが入っているアドレス・プールの指示

DHCP サーバーが LAN インターフェースに直接接続されていない場合、このアドレスは、DHCP サーバーに直接接続された LAN インターフェースのうちの 1 つのアドレスとして構成する必要があります。詳細については、669ページの『動的ホスト構成プロトコル (DHCP)』、および RFC 1541 の『giaddr』 の定義を参照してください。

dial-out *parameter*

ダイヤルアウト・ネットの非活動タイマーまたはサーバー名を設定します。 ***Parameter*** は、以下のいずれかです。

inactivity-timer

ダイヤルアウト・ネットのダイヤルアウト非活動タイマーを設定します。これは、ユーザーがデータ・トラフィックなしに接続していられる時間 (分) として定義されます。たとえば、非活動タイマーが 5 分に設定されている場合、5 分間データの送受信がないと、その接続は除去され、モデムが利用可能になります。デフォルト値は 0 です。これは非活動タイマーは使用不可にされており、接続は無期限に保持されることを意味しています。

servername

ダイヤルアウト・サーバーの名前を設定します。最大長さ 30 文字までの任意の文字列を使用することができます。デフォルト値は『2210_DIALS_SERVER』 です。これは、IBM DIALs ダイヤルアウト・クライアントが 『Chooser』アプリケーションを使用してダイヤルアウト・サーバーを見つけるときに表示される名前です。このパラメーターは、telnet ダイヤルアウト・クライアントに対しては意味を持ちません。

dns *type ipaddress*

1 次および 2 次ドメイン・ネーム・サーバー (DNS) を構成します。 ***Type*** は、以下のいずれかです。

primary

使用するダイヤルイン・クライアントの 1 次 DNS サーバーの IP アドレスを設定します。一部のダイヤルアウト・クライアントでは (特に、Windows 95)、この値は IPCP 時にネゴシエーションされます。

secondary

使用するダイヤルイン・クライアントの 2 次 DNS サーバーの IP アドレスを設定します。一部のダイヤルアウト・クライアントでは (特に、Windows 95)、この値は IPCP 時にネゴシエーションされます。

laa *#MAC_addresses MAC_address_base*

ローカル管理アドレス (LAA) テーブルの MAC アドレスおよび基本アドレスの数を設定します。 LAA アドレスを使用するのは、レイヤー 2 トンネル・ネットだけです。

#MAC_addresses

MAC_Address_Base から始まる LAA テーブルに追加する MAC アドレスの数を指定します。

有効値: 0 ～ 256

デフォルト値: 0

MAC_address_base

LAA テーブルの基本 MAC アドレスを指定します。

有効値: 任意の有効な MAC アドレス

デフォルト値: 000000000000

例:

```
DIALs config>set laa
    Number of Mac Addresses:  [0]? 20
    Locally Administered Mac Address Base (hex) [000000000000]? 002210aaaaaa
    DIALs config>
```

nbns ***type ipaddress***

1 次および 2 次 NetBIOS ネーム・サーバーを構成します。 ***Type*** は、以下のいずれかです。

primary

1 次 NetBIOS ネーム・サーバーの IP アドレスを設定します。

secondary

2 次 NetBIOS ネーム・サーバーの IP アドレスを設定します。

time-allowed

PPP ダイヤルイン・ユーザーおよびダイヤルアウト・ユーザーに許容される時間を設定します。このパラメーターは、ユーザーが接続を維持できる最大時間 (分) を定義します。デフォルト値は 0 で、これはユーザーが無期限に接続していられることを意味します。

ダイヤルアウト・インターフェース構成コマンド

ダイヤルアウト・インターフェース・パラメーター環境にアクセスするには、次のようにします。

1. `*` プロンプトで **talk 6** と入力する。
2. `Config >` プロンプトで **net *n*** と入力する。
3. `Circuit config: n>` プロンプトで **encapsulator** と入力する。

680ページの表81 は、`dial-out config>` プロンプトから利用可能なコマンドをリストしています。

表 81. ダイヤルアウト・インターフェース構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Set	モデムに対応するポート名を定義します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Set

set コマンドは、モデムのポート名を定義するのに使用します。

構文:

set portname *name*

portname

モデムに対応するポートの名前を定義します。この名前は、***モデム・プールを定義するために使用します。*** 名前の長さは最大 30 文字までです。

デフォルト値: ALL_PORTS

例: `dial-out config>`**set portname localcalls**

ダイヤルイン・インターフェースの監視

ダイヤルイン・インターフェースの監視は、他の PPP ダイヤル回線の監視と同様です。詳細については、483ページの『第34章 ポイント・ポイント・プロトコル・インターフェースの構成および監視』を参照してください。

ダイヤルアウト・インターフェースの監視

表82 は、ダイヤルアウト・インターフェースを監視するのに使用できるコマンドをリストしています。

表 82. ダイヤルアウト・インターフェース監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Clear	このダイヤルアウト・インターフェースの統計をリセットします。
List	ダイヤルアウト・インターフェースの現在の状態、このインターフェース上で送受信されたバイト数、およびクライアントの現行パラメーターをリストします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

Clear

clear コマンドは、このインターフェースによって送受信されたオクテット数の統計をリセットするのに使用します。

構文:

clear

例:

```
clear
Statistics reset.
```

List

list コマンドは、ダイヤルアウト・インターフェースの現在の状態を表示するのに使用します。 **list** コマンドは常に、ダイヤルアウト・ネットの現在の状態、その状態に変更されてから経過した時間、および送受信したバイト数を表示します。

構文:

list

非アクティブ・インターフェースの例:

```
list
Dial-out Settings for current session:

Dial-out state is DOWN
Time since change           = 52 minutes and 34 seconds

Dial-out Octets transmitted = 0
Dial-out Octets received    = 0

Session down, no valid settings
```

注: クライアントが telnet を使用してダイヤルアウト・ポートに接続している場合、サーバーは認証を行わなかったので、ユーザー名は存在しません。

アクティブ・インターフェースの例:

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change           = 3 seconds

Dial-out Octets transmitted = 14
Dial-out Octets received    = 765

Current user                = not available
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = TELNET
Options negotiated:
        Will Suppress Go Ahead
        Wont' Echo characters
```

アクティブ IBM DIAL ダイヤルアウト・クライアントの例:

```
list
Dial-out Settings for current session:

Dial-out state is UP
```

```
Time since change           = 12 seconds

Dial-out Octets transmitted = 11
Dial-out Octets received    = 756

Current user                = ebooth
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = DIALs
```

第51章 レイヤー 2 トンネル伝送プロトコル (L2TP)

レイヤー 2 トンネル伝送プロトコル (L2TP) は、UDP/IP のようなパケット方式データ・ネットワークを経由して PPP をトンネル伝送するための、標準トラック IETF 提案の標準プロトコルです。 L2TP はコネクション型です。

注: L2TP は、1x4 モデルではサポートされません。

L2TP の概説

L2TP は、多数の個別の自立走行式プロトコル・ドメインが、モデム、アクセス・サーバー、および ISDN ルーターを含む共通のアクセス・インフラストラクチャーを共用することを可能にします。 L2TP は、PPP リンク・レイヤー (たとえば、HDLC および非同期 HDLC) のトンネル伝送を許します。このようなトンネルを使用すると、接続するダイヤルアップ・サーバーの場所とネットワークへのアクセスを提供する場所とを分離することが可能になります。

従来、インターネット上のダイヤルアップ・ネットワーク・サービスは、登録済み IP アドレスに対してのみ提供されています。 L2TP は、インターネット上の複数プロトコルおよび未登録 IP アドレスを認める新しいクラスのバーチャル・ダイヤルアップ・アプリケーションを定義しています。このクラスのネットワーク・アプリケーションは、既存のインターネット・インフラストラクチャーを利用して PPP 経由で私設アドレス IP、IPX、および AppleTalk ダイヤルアップをサポートするのに便利です。

このようなマルチプロトコル・バーチャル・ダイヤルアップ・アプリケーションに対するサポートは、アクセスおよびコア・インフラストラクチャーへの巨額の投資を共有することができ、またエンド・ユーザーはローカル・コールを使用してサービスにアクセスできるなどの理由で、エンド・ユーザー、企業、およびインターネット・サービス提供者にとって有益です。

L2TP は、既存のインターネット・インフラストラクチャー内の非 IP プロトコル・アプリケーションへの現行投資も確実に利用できます。

図35 は、ISDN を使用した L2TP ネットワークの例を示しています。このネットワークでは、L2TP ネットワーク・アクセス集線装置 (LAC) と L2TP ネットワーク・サーバー (LNS) 間で、任意の媒体タイプを使用することができます。

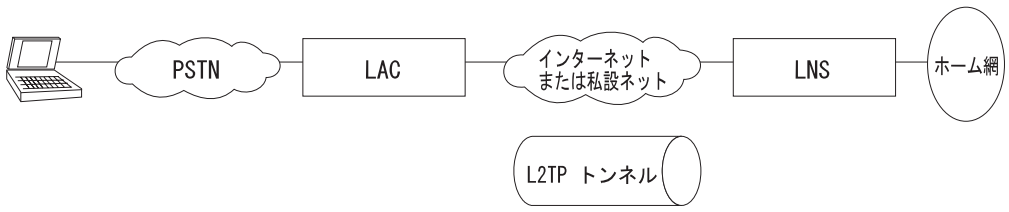


図 35. L2TP ネットワークの例

L2TP の用語

L2TP を説明するために、以下の用語が使用されています。

属性値ペア (AVP)
メッセージ・タイプと本文を符号化するための統一方式。この方式により、L2TP の拡張性が最大化され、相互運用も可能になります。

L2TP アクセス集線装置 (LAC)
PPP 動作と L2TP プロトコルの両方を処理できる、1 つまたは複数の公衆電話網 (PSTN) または ISDN 回線に接続された装置。 LAC は、L2TP を運用する媒体を実装しています。 L2TP は、トラフィックを 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) に渡します。 L2TP は PPP ネットワークによって運ばれたプロトコルをトンネル伝送することができます。

L2TP ネットワーク・サーバー (LNS)
LNS は、PPP エンド・ステーションとして使用できる任意のプラットフォーム上で稼働します。 LNS は、L2TP プロトコルのサーバー側の処理を担当します。 L2TP は単一媒体にのみ依存して L2TP トンネル伝送を行うので、LNS は 1 つの LAN または WAN インターフェースしか持つことができませんが、LAC がサポートする任意の PPP インターフェースからの着呼を終了させることができます。

ネットワーク・アクセス・サーバー (NAS)
ユーザーの要求時に一時的にネットワーク・アクセスを提供する装置。このアクセスは、PSTN または ISDN 回線を使用するポイント・ポイントです。

セッション (コール)
L2TP は、ダイヤル・ユーザーと LNS 間でエンド・エンド PPP 接続が試みられると、セッションを作成します。セッションのデータグラムは、LAC と LNS 間のトンネルを介して伝送されます。 LNS と LAC は、LAC に接続された各ユーザーの状態情報を維持します。

トンネル
トンネルは LNS と LAC の組み合わせで定義されます。トンネルは、LAC と LNS 間で PPP データグラムを伝送します。 1 つのトンネルによって多数のセッションを多重化することができます。同じトンネルを介して動作する制御接続が、すべてのセッションとトンネル自体の確立、解放、および保守を制御します。

サポートされる機能

L2TP は UDP/IP を介して実行され、以下の機能をサポートします。

- 単一ユーザー・ダイヤルイン・クライアントのトンネル伝送
- 小規模ユーザー (たとえば、認証済みユーザー・プロファイルに基づいて単一の静的ルートを設定するルーター) のトンネル伝送
- LAC から LNS への着呼
- 1 つのトンネルでの複数の呼
- PAP および CHAP のプロキシー認証
- プロキシー LCP

- プロキシー LCP が LAC で使用されない場合の LCP のリスタート
- トンネル・エンドポイント認証
- プロキシー PAP パスワードを転送するための隠れ AVP
- ローカル rhelm (つまり、user@rhelm) 索引テーブルを使用したトンネル伝送
- AAA サブシステム内の PPP ユーザー名索引を使用したトンネル伝送

注: Rhelm トンネル伝送では、*name@rhelm* フォーマットのユーザー名が必要です。この方式のトンネル伝送では、ソフトウェアは 2 つのテーブルを使用して、ダイヤルイン・ユーザーのトンネル伝送の宛先を解決する必要があります。このトンネル伝送方式の利点は、ユーザーは rhelm を定義するだけで済み、その rhelm に一致するすべてのユーザー名が同じ宛先にトンネル伝送されます。

ユーザー・ベースのトンネル伝送の場合は、1 つのテーブルで解決されます。この方式では、各ユーザーを個別に固有の宛先にトンネル伝送することができます。

- LNS 用の BRS (PPP エンドポイントとして)
- **delete interface** コマンドを使用して L2TP 装置を削除する機能
- 動的に L2TP 装置を再構成する機能
- 順序制御、待ち行列化、再送、およびフロー制御チャネルの確立。 L2TP はデータ・チャネルの順序制御、待ち行列化、およびフロー制御も行います。

タイミングに関する考慮事項

ルートされたネットワークを介した PPP パケットのトンネル伝送は、その性質上、タイミングに関するいくつかの問題を考慮する必要があります。 L2TP では、LAC と LNS の間にはトンネル伝送の同位がタイムアウトになるほどの遅延はないものと想定しています。同位間の待ち時間が PPP 状態遷移タイムアウト (通常は 3 秒) に達したり、それを超過する状態が繰り返される場合には、接続性が妨げられる可能性があります。 LAC と LNS 間の待ち時間がこのように悪いときには、PPP 状態遷移を人為的にアクティブに維持したとしても、接続が全般的に非常に悪く、適正が接続が得られなくなります。接続の両側に PPP タイムアウトを延長する機能が備わっている場合は、これを使用すると、接続が非常に悪いときでも接続できることがあります。

待ち時間の他に、LAC/LNS の組みと LAC/クライアントの組みの間の帯域幅の不一致も問題の原因になることがあります。たとえば、LAC と LNS の実際の帯域幅が PPP クライアントの帯域幅より大幅に少ない場合、LAC は LNS にパケットを送信するのに長時間かかる可能性があります。一方、LNS と LNS ホーム・ネットワーク上のホストとの間の接続が、ダイヤルイン・クライアントに比べて極端に速い場合、LNS は LAC にデータを送信するのに過剰な負担がかかる可能性があります。 L2TP は、このような状況に対処するために、一連の内部および外部フロー制御を実装しています。

LCP に関する考慮事項

プロキシー LCP を使用している場合、LAC が LCP との交渉 (ネゴシエーション) を担当し、PPP は LNS で処理を継続します。 LAC は LCP オプションを LNS に転送するので、LNS は交渉の結果を知ることができます。 LNS は、クライアントと LAC 間で交渉されるパラメーターに対して柔軟であることが必要です。 LNS に受け入れられないパラメーターがあった場合、L2TP はトンネルを介してクライアントに *LCP 構成要求* を送って LCP と再交渉します。

LNS が柔軟性を保つという要件は、MRU に関しては特に重要です。 IBM LNS では、構成済みの MRU は、プロキシー LCP に許される最大値です。 LAC からのプロキシー LCP メッセージの値が、LNS に構成された MRU 値より大きい場合、L2TP は LCP と再交渉して、MRU を構成済み MRU に等しくしようと試みます (LAC からの他の LCP オプションは変更せずに)。

L2TP の構成

L2TP を構成するには、次のようにします。

1. **feature** コマンドを使用して、L2TP 機能にアクセスする。

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. L2TP を使用可能にする。

```
Layer-2-Tunneling config> enable l2tp
```

3. 必要な L2TP ネットワークを追加する。 LAC だけに限定される場合は、L2TP ネットを追加する必要はありません。

```
Layer-2-Tunneling
Config>ADD L2-NETS
Additional L2 nets:  [0]? 10
Add unnumbered IP addresses for each L2 net? [Yes]: yes
Adding device as interface 31
Defaulting Data-link protocol to PPP
Adding device as interface 32
Defaulting Data-link protocol to PPP
Adding device as interface 33
Defaulting Data-link protocol to PPP
Adding device as interface 34
Defaulting Data-link protocol to PPP
Adding device as interface 35
Defaulting Data-link protocol to PPP
Adding device as interface 36
Defaulting Data-link protocol to PPP
Adding device as interface 37
Defaulting Data-link protocol to PPP
Adding device as interface 38
Defaulting Data-link protocol to PPP
Adding device as interface 39
Defaulting Data-link protocol to PPP
Adding device as interface 40
Defaulting Data-link protocol to PPP
```

4. 必要な L2TP トンネルを構成する。

   AAA ローカル・リストを使用してトンネルを構成する場合は、次のように指定します。

```
Config>add tunnel-profile
Enter name:  []? lns.org
Enter hostname to use when connecting to this peer: []? lac.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1
```

```
     PPP user name: lns.org
     Tunnel Server: 11.0.0.1
     Hostname: lac.org

User 'lns.org' has been added
Config>
```

上の例を使用して、LAC 上のトンネル認証、および 『user@lns.org』 形式の『rhelm』 トンネル伝送を構成することができます。

トンネル認証を特定の RADIUS サーバーで実行するように設定することも可能です。 847ページの『認証、許可、および会計 (AAA) セキュリティー』を参照してください。

AAA ローカル・リストまたは RADIUS を使用して、LAC 上の PPP ユーザー名に基づいてトンネル伝送する場合は、次のように指定します。

```
Config>add ppp-user
Enter name:  []? peter
Password:
Enter again to verify:
Will 'peter' be tunneled? (Yes, No): [No] Y
Enter hostname to use when connecting to this peer: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

     PPP user name: peter
     Tunnel Server: 11.0.0.1
     Hostname: lac.org

Is information correct? (Yes, No, Quit): [Yes]

User 'peter' has been added
Config>
```

5. **set** コマンドを使用して、種々の L2TP パラメーターを構成する (必要な場合)。
6. encapsulator コマンドを使用して、すべての L2 ネットの PPP パラメーターを構成する (必要な場合)。

   ```
   Layer-2-Tunneling Config>encapsulator
   PPP-L2TP Config>
   ```

   PPP の構成が完了したら、**exit** を押して、L2TP 構成環境に戻ります。
7. **enable** コマンドを使用して、L2TP 機能を使用可能にする。
8. **set laa** コマンドを使用して、ローカル割り当て MAC アドレスを構成する。677ページの『Set』を参照してください。

第52章 L2TP の構成および監視

この章では、L2TP の構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

- 693ページの『L2TP 監視プロンプトへのアクセス』
- 694ページの『L2TP 監視コマンド』

L2TP 構成コマンド

表83 は、L2TP 構成コマンドの要約を示しており、この節の残りの部分で、これらのコマンドについて説明します。コマンドは L2TP Config> プロンプトで入力します。

表 83. L2TP 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Add	L2TP ネットワークまたは同位を追加します。
Delete	L2TP 同位を構成から削除します。
Disable	L2TP および L2TP の機能を使用不可にします。
Enable	L2TP または L2TP の機能を使用可能にします。
Encapsulator	すべての L2TP ネットの PPP パラメーターを構成できるようにします。
List	各種の L2TP 構成に関する情報を表示します。
Set	バッファー、呼受信ウィンドウ、およびその他の L2TP パラメーターを設定することができます。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、 L2TP 同位 (LAC または LNS) または L2 ネットを追加するのに使用します。このルーターで終端する各並行 PPP セッションごとに 1 つの L2 ネットが必要です。トンネル伝送 PPP セッションの終端は、トンネルの LNS エンドポイントです。

構文: add
L2-nets

686ページの『L2TP の構成』 に、**add** コマンドの例が示されています。

L2-nets

注: このコマンドは、すべて小文字で入力できます。分かりやすくするために、最初の文字は大文字で示してあります。

L2TP 構成に L2 ネットを追加します。このルーターで転送される各並行 PPP セッションごとに 1 つの L2 ネットが必要です。このルーターを LAC としてのみ使用する場合は、バーチャル L2 ネットは必要ありません。このコマ

ンドを入力すると、追加するネットの数および各 L2 ネットの非番号制 IP アドレスを追加するかどうかを尋ねるプロンプトが出ます。

追加するネットの数は、今回 L2TP が自動的に追加するネットの数を指しています。これらのネットは、既存の L2 ネットに追加されます。

各 L2 ネットの非番号制 IP アドレスを追加すると、各 L2 ネットの IP ルーティング・テーブルに非番号制 IP エントリーが自動的に追加されます。非番号制 IP アドレスが、推奨される運用方式です。 L2 ネットで番号制アドレスが必要とされる場合は、IP プロトコル構成環境で変更することができます (*Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視解説書 第 1 巻 バージョン 3.1* の 『IP の構成』 の章を参照してください)。

Disable

disable コマンドは、L2TP の機能を使用不可にするか、あるいは L2TP 自体を使用不可にするのに使用します。

構文: disable

- call-rcv-window
- force-chap-challenge
- hiding-for-pap-attributes
- L2tp
- proxy-auth
- proxy-lcp
- tunnel-authentication

call-rcv-window

L2TP は、順序制御および輻輳 (ふくそう) 制御を行うために、各呼のパケットを待ち行列化することができます。各呼にはそれぞれ独自の待ち行列 (または、ウィンドウ) があり、フロー制御アルゴリズムを正しく機能させるためには、そのサイズを同位に転送する必要があります。 *call-rcv-window* を使用不可にすると、各セッションのすべてのフロー制御がオフになります。 LAC と LNS 間の接続が高品質で、十分な帯域幅があり、パケット再配列が頻繁に行われないことが明らかであれば、これを設定しても構いません。

force-chap-challenge

クライアントの LNS CHAP 再チャレンジを使用不可にします。 PPP クライアントによる CHAP 再チャレンジが困難な場合に、CHAP 再チャレンジを使用不可にすることが必要になります。

hiding-for-pap-attributes

LAC と LNS 間のプロキシー PAP 情報の暗号化を使用不可にします。

L2tp

注: このコマンドは、すべて小文字で入力できます。分かりやすくするために、最初の文字は大文字で示してあります。

このルーター上の L2TP を使用不可にします。

proxy-auth

LAC からLNS への PPP プロキシー認証の送信を使用不可にします。

proxy-lcp
LAC からLNS への LCP 情報の送信を使用不可にします。

tunnel-authentication
すべてのトンネルの共有の秘密に基づく同位の認証を使用不可にします。

Enable

enable コマンドは、L2TP の機能を使用可能にするか、あるいは L2TP 自体を使用可能にするのに使用します。

構文:

enable
- force-chap-challenge
- hiding-for-pap-attributes
- L2tp
- proxy-auth
- proxy-lcp
- tunnel-authentication

force-chap-challenge
LNS がプロキシー CHAP を受信しても、クライアントの LNS CHAP 再チャレンジを使用可能にします。クライアントがこのような再チャレンジを問題なく扱えることが分かっている場合には、セキュリティーの観点から、これを使用可能にすることが望まれます。

hiding-for-pap-attributes
LAC と LNS 間のプロキシー PAP 情報の暗号化を使用可能にします。

L2tp

注: このコマンドは、すべて小文字で入力できます。分かりやすくするために、最初の文字は大文字で示してあります。
このルーター上の L2TP を使用可能にします。

proxy-auth
LAC からLNS への PPP プロキシー認証の送信を使用可能にします。

proxy-lcp
LAC からLNS への LCP 情報の送信を使用可能にします。

tunnel authentication
すべてのトンネルの共有の秘密に基づく同位の認証を使用可能にします。

Encapsulator

encapsulator コマンドは、L2 ネットの PPP パラメーターを構成するのに使用します。

構文: encapsulator

List

list コマンドは、種々の L2TP 構成パラメーターの状態を表示するのに使用します。

構文: list

```
Layer-2-Tunneling Config>list
GENERAL ADMINISTRATION
------- --------------
  L2TP                                = Enabled
  Maximum number of tunnels           = 20
  Maximum number of calls (total)     = 50
  Buffers Requested                   = 300

CONTROL CHANNEL SETTINGS
------- ------- --------
  Tunnel Auth                         = Enabled
  Tunnel Rcv Window                   = 4
  Retransmit Retries                  = 6
DATA CHANNEL SETTINGS
---- ------- --------
  Force CHAP Challenge (extra security)= Disabled
  Hiding for PAP Attributes           = Disabled
  Call Rcv Window                     = 6

MISCELLANEOUS
-------------
  SEND PROXY-LCP FROM LAC             = Enabled
  SEND PROXY-AUTH FROM LAC            = Enabled
```

Set

set コマンドは、L2TP 動作パラメーターを構成するのに使用します。

構文: set buffers

call-rcv-window

max-calls

max-tunnels

transmit-retries

tunnel-rcv-window

buffers

要求された内部 L2TP バッファーの数を指定します。要求を満たすのに十分なメモリーがない場合、リブートするとバッファーの一部だけが利用可能になります。 L2TP がアクティブのときにメモリーの量を確認するには、**memory** コマンドを使用します (697ページの『Memory』を参照してください)。

有効値: 1 ～ 1000

デフォルト値: モデルによって異なります。

モデル	値
12x	100
14x または **24x**	150
1Sx または **1Ux**	80

call-rcv-window

受信ウィンドウとして使用するパケットの数を指定し、call-rcv-window を使用

可能にします。データ・チャネルのフロー制御が使用可能にされている場合、ルーター上のプロトコルが使用するため、および開始メッセージを使用して同位に通信するのに使用するための、受信ウィンドウ・サイズを指定する必要があります。構成された値は、このルーターによって開始されるすべての呼に適用されます。

有効値: 0 ～ 100

デフォルト: 6

max-calls

LAC または LNS として同時にアクティブにできるすべてのトンネルを経由する呼の最大数を指定します。

有効値: 1 ～ 500

デフォルト値: モデルによって異なります。

モデル	x4x	12x	1Sx/1Ux	
デフォルト値	50	40	30	

max-tunnels

LAC または LNS として同時にアクティブにできるトンネルの最大数を指定します。

有効値: 1 ～ 100

デフォルト値: モデルによって異なります。

モデル	x4x	12x	1Sx/1Ux	
デフォルト値	20	15	10	

transmit-retries

セッションまたはトンネルが非アクティブとして宣言されて遮断される前に、制御チャネル上でパケットが再送される回数を指定します。

有効値: 2 ～ 100

デフォルト値: 6

tunnel-rcv-window

高信頼制御接続トランスポートの受信ウィンドウ・サイズを指定します。このトランスポートでは、トンネルまたはセッションの設定、切断、および保守のために必要なメッセージを送受信します。

有効値: 1 ～ 100

デフォルト値: 4

L2TP 監視プロンプトへのアクセス

L2TP 監視プロンプトにアクセスするには、次のようにします。

1. OPCON (*) プロンプトで **talk 5** と入力する。
2. GWCON (+) プロンプトで **feature layer-2-tunneling** コマンドを入力する。

L2TP 監視コマンド

この節では、L2TP 監視コマンドの要約を示し、個々のコマンドについて説明します。コマンドは Layer-2-Tunneling Console> プロンプトで入力します。

表84 は、L2TP 監視コマンドを要約しています。

表 84. L2TP 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。13ページの『ヘルプの入手』 を参照してください。
Call	進行中の各呼に関する統計と情報を表示します。
Kill	呼またはトンネル伝送を即時に終了します。
Memory	現在の L2TP バッファーの割り当てと使用状況を表示します。
Start	別の同位とのトンネル伝送を開始します。
Stop	呼またはトンネル伝送を停止し、各同位が必要な管理を実行できるようにします。
Tunnel	既存の各トンネルに関する統計と情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Call

call コマンドは、呼の統計と情報を表示するのに使用します。

構文: call errors

physical-errors

queue

state

statistics

errors この呼で発生した一般伝送誤りを表示します。

例:

```
Layer-2-Tunneling Console> call errors
CallID │ Serial # │ ACK-timeout │ Dropped pkts
 56744 │        1 │           0 │        0
```

CallID この呼に対応するローカル識別子。

Serial #
この呼をログ記録するのに使用された番号

ACK-timeout
同位からタイムアウト通知を受信した回数

Dropped pkts
この呼における紛失を宣言されたパケットの数。これは、受信するはずであったが、同位によって紛失として通知されたパケットです。

physical-errors
呼で発生したデータ誤りを表示します。

例:

```
Layer-2-Tunneling Console> call physical-errors
CallID | Serial# | CRC    |framing| HW     | buffer|timeout| align-| time since
       |         | Errors| Errors|overrun|overrun| Errors| ment  | updated
 56744 |       1 |     0 |     0 |     0 |     0 |     0 |     0 |
```

CallID この呼に対応するローカル識別子

Serial #
この呼をログ記録するのに使用された番号

CRC Errors
CRC が一致しなかったパケットの数

framing errors
フレーム誤りをもつパケットの数

HW overrun
ハードウェア・オーバーランが発生した回数

buffer overrun
バッファー・オーバーランが発生した回数

timeout errors
インターフェースがタイムアウトになった回数

alignment
配列誤りが発生した回数

time since updated
前回の誤りのポーリングからの経過時間

queue 各呼の待ち行列に関する情報を表示します。

例:

```
Layer-2-Tunneling Console> call queue
CallID | Serial # |Tx Win|Rx Win|   Ns   |   Nr   |Rx Q|Tx Q|priority| out Q
 56744 |        1 |    4 |    4 |    100 |   200  |  0 |  0 |      0 |     0
```

CallID この呼に対応するローカル識別子

Serial #
この呼をログ記録するのに使用された番号

Tx Win
同位のデータの最大受信ウィンドウ

Rx Win
ローカル最大送信ウィンドウ

Ns この呼で送信される次のパケット・シーケンス番号

Nr この呼で受信が期待されている次のパケット・シーケンス番号

Rx Q 受信待ち行列の現在のパケット数

Tx Q 送信待ち行列の現在のパケット数

priority
L2TP による送信を待っている優先順位 PPP パケットの数

out Q L2TP による送信を待っている通常の PPP パケットの数

state 各呼の現在の状態を表示します。

例:

```
Layer-2-Tunneling Console> call state
CallID │ Serial # │ Net # │    State    │ Time Since Chg │ PeerID │ TunnelID
 56744 │        1 │     2 │ Established │   00:00:00     │  345   │ 45678
```

CallID この呼に対応するローカル識別子

Serial #
この呼をログ記録するのに使用された番号

Net # この呼に対応する装置番号。 LNS の呼の場合、これは L2 ネットです。 LAC の呼の場合、これは最初の呼を受信した PPP 装置です。

State 現在の呼の状態。有効な呼の状態は、次のとおりです。

Established
トンネル・ネットワーク・トラフィックの伝送準備完了

Idle 呼はアイドル状態です。

Wait Cs Answer
通信リンクがオープンするのを待っています。

Wait Reply
同位からの応答を待っています。

Wait Tunnel
トンネルの確立を待っています。

Time since chg
前回の状態変更からの経過時間

PeerID
同位の呼 ID

TunnelID
この呼に対応するローカル・トンネル

statistics
各呼のデータ伝送に関する統計を表示します。

例:

```
Layer-2-Tunneling Console> call statistics
CallID │ Serial # │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │ ATO
 56744 │        1 │      34 │     1056 │      45 │     1567 │   10  │ 34
```

CallID この呼に対応するローカル識別子

Serial #
この呼をログ記録するのに使用された番号

Tx Pkts
この呼の送信されたパケット数

Tx Bytes
この呼の送信されたバイト数

Rx Pkts
この呼の受信されたパケット数

Rx Bytes
この呼の受信されたバイト数

RTT この呼の現行の算定一巡時間

ATO この呼の現行の算定適応タイムアウト

Kill

kill は、トンネルを即時に終了するのに使用します。このコマンドは、トンネルのすべてのローカル資源を解放して、強制的に接続を終了させます。トンネルの終了は同位に通知されません。

注: このコマンドを使用するのは、**stop** コマンドではトンネルを終了させることができない場合だけに限ってください。

構文: kill tunnel *tunnelid*

tunnel *tunnelid*
トンネルを終了することを指定します。

Memory

memory コマンドは、L2TP の現在のメモリーの使用状況を表示するのに使用します。

構文: memory

例:

```
Layer-2-Tunneling Console> mem
Number of layer-2-tunneling buffers: Requested = 2000, Total = 1200, Free
= 1000
```

この例では、ユーザーは 2000 のバッファーを構成しましたが、1200 しか割り当てることができませんでした。現在、200 のバッファーが使用中で、1000 が空いています。

Start

start コマンドは、別の同位とのトンネル伝送を開始するのに使用します。

構文: start (パラメーターを付けないと、ホスト名の入力を求められます。)

tunnel *hostname*

hostname
L2TP がトンネルを確立する相手のホストの名前

Stop

stop コマンドは、トンネル伝送を停止するのに使用します。トンネルを終了する前に、必要な終結処置を完了させます。

構文: stop tunnel *tunnelid*

tunnel *tunnelid*
終了させるトンネルを指定します。

Tunnel

tunnel コマンドは、すべてのトンネルに関する統計と情報を表示するのに使用します。

構文: tunnel　call
errors
peer
queue
state
statistics
transport

calls　すべてのトンネルと、各トンネル内の各呼の状態を表示します。

errors　トンネル上で発生した誤りを表示します。

例:

```
Layer-2-Tunneling Console> tunnel errors
Tunnel ID │ Type │ACK-timeouts
 96785    │ L2TP │    0
```

Tunnel ID
この呼に対応するローカル識別子

Retransmissions
トンネル上で再送されたパケットの数

peer　トンネルとそのトンネルに対応する同位を表示します。

例:

```
Layer-2-Tunneling Console> tunnel peer
Tunnel ID │ Type │ Peer ID │ Peer Hostname
 96785    │ L2TP │   89777 │ mypeer
```

Tunnel ID
この呼に対応するローカル識別子

Peer ID
このトンネルに割り当てられた同位のトンネル識別子

Peer Hostname
ローカル・データベースに表示される同位のホスト名

queue　各トンネルの待ち行列に関する情報を表示します。

例:

```
Layer-2-Tunneling Console> tunnel queue
Tunnel ID │ Type │ Rx Win │ Tx Win │   Ns   │   Nr   │ Rx Q │ Tx Q
 96785    │ L2TP │      4 │      4 │      5 │      6 │    0 │    0
```

Tunnel ID
この呼に対応するローカル識別子

Rx Win
受信ウィンドウを構成するパケットのローカル最大数

Tx Win
同位の受信ウィンドウを構成するパケットの最大数

Ns 送信する次のパケットのシーケンス番号

Nr 受信する次のパケットのシーケンス番号

Rx Q 現在受信待ち行列にあるパケットの数

Tx Q 現在送信待ち行列にあるパケットの数

state すべてのトンネルの現在の状態を表示します

例:

```
Layer-2-Tunneling Console> tunnel state
Tunnel ID │ Type │ Peer ID │     State     │ Time Since Chg │ # Calls │ Flags
 96785    │ L2TP │  89777  │ Established   │   00:00:00     │       1 │  0
```

Tunnel ID
この呼に対応するローカル識別子

Peer ID
このトンネルに割り当てられた同位のトンネル識別子

State 現在のトンネルの状態。有効なトンネル状態は、次のとおりです。

Established	トンネルは確立されました。
Idle	トンネルはアイドル状態です。
Wait Ctrl Reply	ホストは同位からの応答を待っています。
Wait Ctrl Conn	ホストは同位からの接続確立表示を待っています。

Time since chg
前回の状態変更からの経過時間

 # Calls
このトンネル上のアクティブの呼の数

Flags このトンネル上の接続メッセージを制御するのに使用されたフラグ

statistics
トンネルに関連する統計を表示します。

例:

```
Layer-2-Tunneling Console> tunnel statistics
Tunnel ID │ Type │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │ ATO
 96785    │ L2TP │      4  │      78  │      5  │     89   │   10  │ 31
```

Tunnel ID
この呼に対応するローカル識別子

Tx Pkts
送信されたパケット数

Tx Bytes
送信されたバイト数

Rx Pkts
受信されたパケット数

Rx Bytes
受信されたバイト数

RTT トンネル制御接続メッセージの現行の算定一巡時間

ATO　トンネル制御接続メッセージの現行の算定適応タイムアウト

transport

トンネルに関する UDP 情報を表示します。

例:

```
Layer-2-Tunneling Console> tunnel transport
Tunnel ID │ Type │ Peer IP Address │ UDP Src │ UDP Dest
 96785    │ L2TP │  11.0.0.102     │  1056   │   1089
```

Tunnel ID

この呼に対応するローカル識別子

Peer IP address

このトンネルの同位の IP アドレス

UDP Src

このトンネルの UDP 発信ポート

UDP Dest

このトンネルの UDP 着信ポート

第4部 機能の概要、構成、および使用

第53章 帯域幅予約および優先待ち行列の使用

この章では、フレーム・リレーおよび PPP インターフェースで現在利用可能な帯域幅予約システムおよび優先待ち行列機能について説明します。本章には、以下の節が含まれています。

- 『帯域幅予約システム』
- 705ページの『フレーム・リレー上の帯域幅予約』
- 707ページの『優先待ち行列』
- 709ページの『BRS とフィルター』
- 714ページの『サンプル構成』

帯域幅予約システム

帯域幅予約システム (BRS) は、あるネットワーク接続上で需要 (トラフィック) が供給 (スループット) を超えた場合、どのパケットを廃棄するかを決めることができます。帯域幅の使用率が 100% に達した場合、BRS はユーザーの構成に基づいて、廃棄するトラフィックを判別します。

帯域幅予約は、指定されたクラスのトラフィック用として伝送帯域幅を ″予約″ します。各クラスに、接続の帯域幅の最小比率が割り振られています。 704ページの図36 および 704ページの図37 を参照してください。

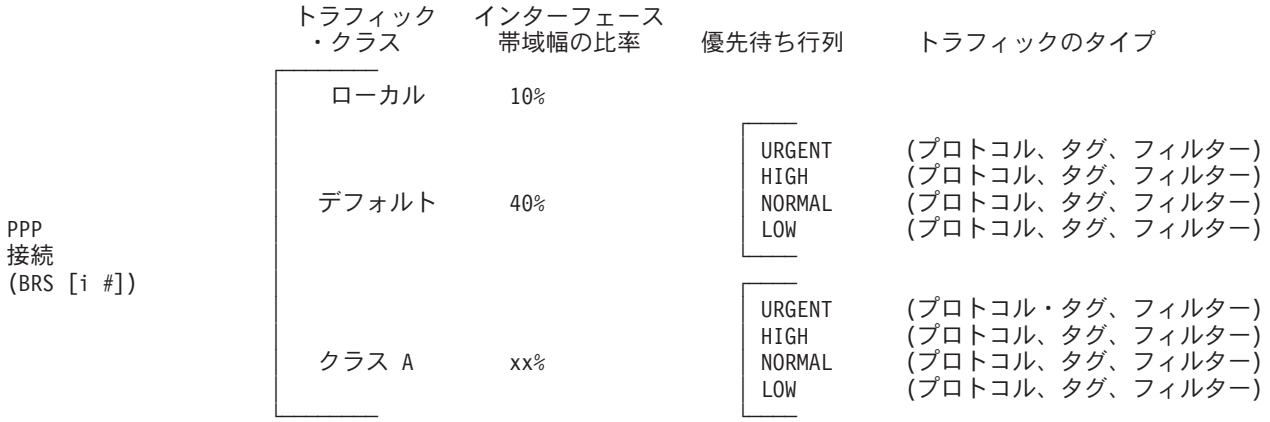
PPP インターフェースでは、トラフィック・クラス (t-classes) を定義し、各トラフィック・クラスに PPP インターフェースの帯域幅の比率を割り振ります。少なくとも 2 種類のトラフィック・クラスがあります。

1. LOCAL クラス。ルーターによってローカルで発信されたパケット (たとえば、IP RIP パケット) のための帯域幅が割り振られます。
2. DEFAULT クラス。その他のすべての通信は、最初はこのクラスに割り当てられます。

ユーザーは、追加のトラフィック・クラスを作成し、トラフィック・クラス内の優先待ち行列に、プロトコル、フィルター、およびタグを割り当てることができます。 704ページの図36 を参照してください。

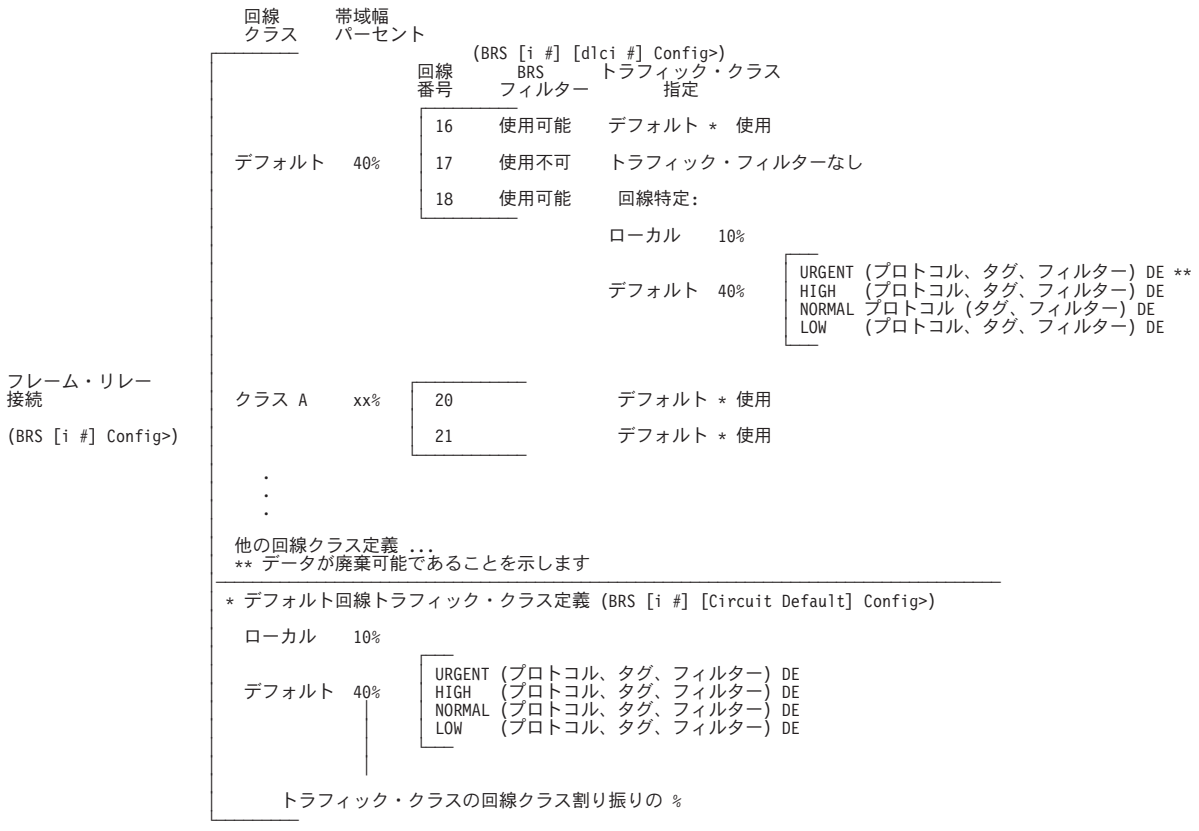
フレーム・リレー・インターフェースでは、回線クラス (c-classes) を定義し、各回線クラスに、フレーム・リレー・インターフェースの帯域幅の比率を割り振ります。少なくとも 1 つの回線クラス (DEFAULT 回線クラス) が存在し、すべての回線が最初はこのクラスに割り当てられます。ユーザーは追加の回線クラスを作成し、それらの回線クラス (c-classes) に回線を割り当てることができます。各フレーム・リレー回線では、トラフィック・クラス (t-classes) を定義し、各トラフィック・クラスに、そのフレーム・リレーの帯域幅の比率を割り振ることができます。フレーム・リレー回線のトラフィック・クラス・サポートは、PPP インターフェースのトラフィック・クラス・サポートと同様です。フレーム・リレーの回線クラスとトラフィック・クラスの関係については、704ページの図37 を参照してください。

BRS および優先待ち行列の使用



注: すべてのプロトコルが、最初は DEFAULT トラフィック・クラスの NORMAL 優先待ち行列に割り当てられます。ユーザーは、トラフィック・クラス内の優先待ち行列に、プロトコル、フィルター、またはタグを割り当てることができます。

図 36. PPP BRS トラフィック・クラスとトラフィック・クラス優先待ち行列の関係



注: すべてのプロトコルが、最初は DEFAULT トラフィック・クラスの NORMAL 優先待ち行列に割り当てられます。ユーザーは、トラフィック・クラス内の優先待ち行列に、プロトコル、フィルター、またはタグを割り当てることができます。

図 37. フレーム・リレー BRS 回線クラスとトラフィック・クラスの関係

これらの予約される比率は、そのネットワーク接続の帯域幅の最小*配分* です。ネットワークが容量いっぱいで稼働している場合、あるクラスのメッセージは、そのクラスに割り振られた構成済み帯域幅までしか送信できません。この場合、他の帯域幅伝送が満たされるまで、追加の伝送は保留されます。トラフィック量の少ないパスの場合は、他にトラフィックがなければ、パケット・ストリームは許容最小値を最大 100% 超過するまで帯域幅を使用できます。

帯域幅予約は、実際には一種の*安全機能* です。一般的には、装置は回線速度の 100% を超える速度は使用しないようにすべきです。このような状態になる場合は、より高速の回線が必要と考えられます。ただし、トラフィックの “バースト性” により、要求された伝送速度が短時間 100% を超えてしまうことがあります。そのような場合には、帯域幅予約を使用可能にすることにより、優先順位の高いトラフィックが確実に送達される (つまり、廃棄されない) ようにすることができます。

帯域幅予約は、次の接続タイプ上で実行されます。

- フレーム・リレー (シリアル・ラインまたはダイヤル回線インターフェース)
- PPP (シリアル・ラインまたはダイヤル回線インターフェース)

フレーム・リレー上の帯域幅予約

帯域幅予約は、2 つのレベルで帯域幅を予約することができます。

- インターフェース・レベルでは、インターフェースの帯域幅の比率を回線クラス (*c-classes*) に割り当てることができます。各回線クラスには、1 つまたは複数の回線が含まれます。
- 回線レベルでは、トラフィック・クラスを定義し、回線の帯域幅の比率を割り振ることができます。

パケットは、そのパケットのプロトコル・タイプと構成済み BRS フィルターに基づいてフィルターに掛けられ、BRS t-classes に待ち行列化されます。次に、パケットは DLCI 番号に基づいて BRS c-class に待ち行列化されます。

帯域幅予約のために実際に利用可能な帯域幅の量は、インターフェースと回線をどのように構成したかによって決まります。

- フレーム・リレー CIR 監視を使用可能にした場合、回線に利用可能な帯域幅は、認定情報速度 (CIR)、認定バースト・サイズ、および超過バースト・サイズに従って厳密に割り振られます。
- CIR 監視を使用不可にした場合、インターフェースの帯域幅の最高 100 % までを回線に利用可能です。

オーファン回線および BRS が明示的に使用可能にされていない回線は、デフォルトの BRS 待ち行列環境を使用します。つまり、パケットはデフォルトの t-class と優先順位、およびデフォルトの c-class に基づいて待ち行列化されます。

特定インターフェースの回線クラスの予約カウンターを表示するための帯域幅予約監視コマンドがいくつかあります。

- clear-circuit-class
- counters-circuit-class

- last-circuit-class

BRS の監視についての詳細は、721ページの『第54章 帯域幅予約の構成および監視』を参照してください。

インターフェースは、帯域幅監視コマンド用のプロンプトに表示されるものです。たとえば、BRS [i 5] は、インターフェース 5 のプロンプトです。

BRS 回線クラスを使用したくない場合は、デフォルト c-class 内のすべての回線を除去し、その他に回線クラスを作成しないようにします。

待ち行列化のサポート

フレーム・リレー上の帯域幅予約を使用すると、インターフェースおよび回線の帯域幅予約が使用可能にされていない場合でも、各回線は輻輳 (ふくそう) 状態のときにフレームを待ち行列化することができます。

廃棄可能性

フレーム・リレー・ネットワークは、PVC 上の CIR を超過した転送データを廃棄することがあります。ルーターは、DE ビットをセットすることにより、一部のトラフィックを廃棄可能と見なすように指示することができます。該当する場合、フレーム・リレー・ネットワークは廃棄可能としてマーク付けされたフレームを廃棄します。これによって、廃棄可能のマークが付いていないフレームがネットワークを通過できるようになることがあります。ユーザーは、プロトコル、フィルター、またはトラフィック・クラスへのタグを割り当てるときに、そのプロトコル、フィルター、またはタグ・トラフィックが廃棄可能かどうかを指定することができます。トラフィックを廃棄可能として構成する方法については、728ページを参照してください。

トラフィック・クラス処理のためのデフォルト回線定義

フレーム・リレー・インターフェースには、多数の回線を定義することができます。 BRS では、各回線のトラフィック・クラス定義を完全に構成する必要はなく、デフォルトの 1 組のトラフィック・クラスとプロトコル、フィルター、およびタグ割り当てを定義し (デフォルト回線定義と呼ばれます)、インターフェース上の任意の回線がこれを使用できるようにします。回線上で BRS を初期に使用可能にすると、回線はデフォルト回線定義を使用するように初期設定されます。回線がトラフィック・クラスの扱いに関するデフォルト回線定義を使用できない場合には、**add-class**、 **change-class**、 **assign**、**deassign**、 **tag**、および **untag** コマンドを使用して、その回線に特定した定義を作成することができます。

回線が回線特定の定義を使用しているときに、それに代えてデフォルト回線定義を使用するように設定したい場合は、その回線の BRS プロンプトで **use-circuit-defaults** コマンドを使用することができます。

トラフィック・クラスの扱いに関するデフォルト回線定義は、BRS フレーム・リレー・インターフェース・プロンプトで **set-circuit-defaults** を使用して定義します。このコマンドは BRS 回線デフォルト・プロンプトを表示します。そこから、トラフィック・クラスの追加、変更、および削除、プロトコル、フィルター、およびタグ

の割り当てと割り当て解除、ならびに BRS タグの作成を行うことができます。トラフィック・クラスのデフォルト回線定義を変更すると、デフォルト回線定義を使用しているすべての回線のトラフィック・クラスの扱いが動的に更新されます。

優先待ち行列

帯域幅予約は、指定されたトラフィック・クラス (*t-classes*) に対して、接続の総帯域幅の比率を割り振ります。 BRS t-class は、同じ名前によって識別されたパケットの集りです。たとえば、“ipx” という名前のクラスは、すべての IPX パケットを表します。

優先待ち行列を用いて、各帯域幅 t-class に以下の優先順位の設定値の 1 つを割り当てることができます。

- Urgent
- High
- Normal (通常、デフォルト設定)
- Low

Urgent 優先順位が割り当てられたすべてのパケットが、そのクラス内で最初に送信されます。これらのパケットの後に、High、Normal、そして Low の順でそれぞれのメッセージが送信されます。 Urgent パケットがすべて転送されると、High パケットの転送が始まり、そのすべてが送信されるまで (または、新たな Urgent メッセージが待ち行列に入れられるまで) 続けられます。 Urgent、High、または Normal パケットが残っていないときにのみ、Low 優先順位のパケットが転送されます。優先順位の設定値が指定されていない場合、設定値はデフォルトの Normal になります。

また、各帯域幅 t-class の各優先順位ごとに、待ち行列で待っているパケットの数を設定することもできます。 BRS **queue-length** コマンドは、各 BRS 優先待ち行列に待ち行列化できる出力バッファーの最大数、およびルーターの入力バッファーが不足しているときに各 BRS 優先待ち行列に待ち行列化できる出力バッファーの最大数を設定します。 PPP とフレーム・リレーの両方の優先待ち行列の長さを設定できます。

重要： 待ち行列の長さの値を高く設定し過ぎると、ルーターの性能が大きく低下する可能性があります。

BRS の場合、PPP およびフレーム・リレー WAN 接続の優先待ち行列の長さを設定することができます。 **queue-length** コマンドの説明は、738ページの『Queue-length』を参照してください。

ある帯域幅 t-class の優先順位の設定値は、他の帯域幅クラスでは無効です。ある帯域幅クラスが他の帯域幅クラスより優先されるということはありません。

帯域幅予約なしの優先待ち行列

帯域幅予約なしで優先待ち行列が構成されている場合、最高の優先順位のトラフィックが最初に送達されます。高優先順位のトラフィックが大量にある場合には、低

い優先順位のトラフィックは見過ごされる可能性がありますが、優先待ち行列と帯域幅予約を組み合わせれば、パケット転送をすべてのタイプのトラフィックに割り振ることができます。

トラフィック・クラスの構成

add-class コマンドを使用してトラフィック・クラスを作成し、次に **assign** コマンドを使用して、そのクラスにトラフィックのタイプを割り当てます。トラフィックは、そのプロトコル・タイプ に基づいて、あるいは特定のタイプのプロトコル・トラフィック を識別する (たとえば、SNMP IP パケット) フィルターに基づいて、トラフィック・クラスに割り当てられます。

サポートされるプロトコル・タイプは、次のとおりです。

- IP
- ARP
- DNA
- VINES
- IPX
- OSI
- AP2
- ASRT
- SNA/APPN-ISR
- APPN-HPR
- HPR/IP

BRS フィルター

帯域幅予約を使用すると、特定のプロトコル・トラフィックを、同じプロトコル・タイプを使用する他のトラフィックとは異なる扱いにすることができます。たとえば、SNMP IP トラフィックを、他の IP トラフィックとは異なるトラフィック・クラスおよび優先順位に割り当てるといったことが可能です。この例では、特定のプロトコル・トラフィックを ″フィルターする″ (つまり、固有に識別する) ので、SNMP は BRS フィルターです。 IP、ASRT (ブリッジング)、および APPN-HPR プロトコル・トラフィックを帯域幅予約によって ″フィルターする″ ことが可能であり、以下のフィルターがサポートされています。

- IP トンネル伝送
- IP 経由の SDLC トンネル伝送 (SDLC リレー)
- Rlogin
- Telnet
- SNA/APPN-ISR
- APPN-HPR
- SNMP
- IP マルチキャスト
- DLSw

- MAC フィルター
- NetBIOS
- Network-HPR
- High-HPR
- Medium-HPR
- Low-HPR
- XTP
- TCP/UDP ポート番号またはソケット

BRS とフィルター

以下の節では、BRS を各種のフィルターと共に使用する方法について説明します。

MAC アドレス・フィルターとタグ

MAC Address フィルターは、タグ を使用して、帯域幅予約と MAC フィルター (MCF) の共同作業で処理されます。たとえば、帯域幅予約を使用しているユーザーは、ブリッジ・トラフィックにタグを割り当てることによって、それを分類することができます。

タグ付けプロセスは、MAC フィルター構成コンソールでフィルター項目を作成し、それにタグ番号を割り当てることによって行われます。このタグ番号は、このタグに対応するすべてのパケットのトラフィック・クラスを設定するのに使用されます。タグ値は、現在は 1 〜 64 の範囲でなければなりません。 MAC フィルターについての詳細は、747ページの『第55章 MAC フィルターの使用』を参照してください。

注: タグは、ブリッジされるパケットに**のみ**適用されます。 PPP またはフレーム・リレー接続では、最高 5 つのタグ付けされた MAC フィルターを帯域幅予約フィルターとして割り当てることができ、それらを TAG1 〜 TAG5 として指定します。 TAG1 が最初に探索され、次に TAG2 というようにして TAG5 まで続けられます。 1 つの MAC フィルター・タグは、MCF に設定された任意の数の MAC アドレスから構成することができます。

MAC フィルター構成プロセスでタグ・フィルターを作成したら、BRS タグ構成コマンドを使用して、BRS タグ名 (TAG1、TAG2、TAG3、TAG4、または TAG5) を MAC フィルター・タグ番号に割り当てることができます。次に、BRS assign コマンドでその BRS タグ名を使用して、対応する MAC フィルターを帯域幅トラフィック・クラスと優先順位に割り当てます。

タグは、IP トンネルの例に見られるように、“グループ” とも呼ばれます。 IP トンネルのエンドポイントは、任意の数のグループに属することができます。パケットは、MAC アドレス・フィルターのタグ付け機能によって、特定のグループに割り当てられます。 MAC フィルターについての追加情報は、747ページの『第55章 MAC フィルターの使用』 および 751ページの『第56章 MAC フィルターの構成および監視』を参照してください。

BRS および優先待ち行列の使用

帯域幅予約と待ち行列優先順位をタグ付きパケットに適用するには、次のようにします。

1. `filter config>` プロンプトで MAC フィルター構成コマンドを使用して、ブリッジを通過するパケットのタグを設定する。詳細については、747ページの『第55章 MAC フィルターの使用』 を参照してください。
2. 帯域幅予約 **tag** コマンドを使用して、帯域幅予約のタグを参照する。
3. 帯域幅予約 **assign** コマンドを使用して、BRS タグを t-class に割り当てる。**assign** コマンドは、その BRS t-class 内の待ち行列優先順位も指定するように求めるプロンプトを出します。

TCP/UDP ポート番号フィルター

パケットの UDP または TCP ポート番号と (オプションで) ソケットに基づいて、一定範囲の TCP または UDP ポートからの TCP/IP パケットを、BRS t-class と優先順位に割り当てることができます。最高 5 つの UDP/TCP ポート番号フィルターを指定することができます。フィルターに、個々の TCP または UDP ポート番号、一定範囲の TCP または UDP ポート番号、あるいはソケット識別子 (ポート番号と IP アドレスの組み合わせ) を指定します。そのフィルターを、BRS トラフィック・クラスとそのクラス内の優先順位に割り当てることができます。

UDP/TCP ポート・フィルターが使用可能のとき、BRS は各 TCP または UDP パケットを調べて、宛先または発信元ポート番号が、フィルターに指定したポート番号の 1 つに一致しているかどうかをチェックします。また、ユーザーが IP アドレスを BRS UDP/TCP フィルターの一部として定義しており、宛先または発信元 IP アドレスが、ユーザーの定義したフィルター・アドレスと一致している場合には、BRS はパケットを、そのポート番号フィルターのトラフィック・クラスと優先順位に割り当てます。

たとえば、ポート番号フィルターを 25 ～ 29 の範囲の UDP ポート番号に構成し、そのフィルターをトラフィック・クラス 'A' の優先順位 'normal' に割り当てるといったことができます。この場合、BRS は、発信元または宛先ポート番号が 25 ～ 29 のすべての UDP パケットを、トラフィック・クラス 'A' の Normal 優先順位待ち行列に入れます。

また、TCP ポート番号フィルターを IP アドレス 5.5.5.25 の TCP ポート番号に構成し、そのフィルターをトラフィック・クラス 'B' の優先順位 'urgent' に割り当てるといったこともできます。この場合、BRS は、発信元または宛先ポート番号が 50 で、宛先または発信元 IP アドレスが 5.5.5.25 のすべての TCP パケットを、トラフィック・クラス 'B' の Urgent 優先待ち行列に入れます。

IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィックのための IP バージョン 4 優先順位ビット処理の使用

BRS は通常、ポート番号によって IP TCP トラフィックと UDP トラフィックを区別します。しかし、BRS は、IP 保護トンネルを通して伝達されたり、2 次 UDP または TCP フラグメントに入れて伝達される IP トラフィックのように、2 度カプセル化されたトラフィックのポートは識別することができません。その結果、BRS はこの種のトラフィックをフィルターに掛けることができません。 IP バージョン 4 優先

順位ビット処理を使用すると、BRS は、IP 保護トンネルを通して伝達されたり、2 次 TCP または UDP フラグメントに入れて伝達されるカプセル化 SNA トラフィックを引き続きフィルターに掛けることが可能になります。

APPN/HPR トラフィックは IP を介してルートされるときに、APPN-HPR の各伝送優先順位 (network、high、medium、および low) が、3 つの IP バージョン 4 優先順位ビットの特定の値にマップされます。

- HPR ネットワーク伝送優先順位は、IPv4 優先順位値 '110'b にマップされます。
- HPR high 伝送優先順位は、IPv4 優先順位値 '100'b にマップされます。
- HPR medium 伝送優先順位は、IPv4 優先順位値 '010'b にマップされます。
- HPR low 伝送優先順位は、IPv4 優先順位値 '001'b にマップされます。

BRS に対して IPv4 優先順位フィルターが使用可能にされており、IP パケット内の優先順位ビットが APPN/HPR トラフィック用に使用される値の 1 つに一致している場合、そのパケットは、対応する HPR 伝送優先順位が割り当てられている BRS t-class の優先順位待ち行列に入れられます。たとえば、IP パケットの優先順位値が '110'b で、BRS HPR-Network フィルターが t-class A、優先順位レベル normal に割り当てられている場合、パケットは t-class A の normal 優先順位待ち行列に入れられます。 BRS HPR 伝送優先順位フィルターは構成されていないが、APPN-HPR フィルターは構成されている場合には、パケットは APPN-HPR フィルターが割り当てられている優先順位待ち行列と t-class に入れられます。

以下の 3 種類のトラフィックは、IPv4 優先順位値 '011'b にマップされます。

- APPN/HPR が IP を介してルートされるときに送信される APPN/HPR XID トラフィック
- DLSw トラフィック
- TN3270 トラフィック

複数のタイプのトラフィックが 1 つの値にマップされるので、IPv4 優先順位ビットに基づくフィルターが使用可能にされている場合には、BRS はトラフィックを区別することができません。そのため、優先順位値 '011'b を持つ IP パケットを検出すると、BRS は以下の順序で BRS フィルターを評価して、フィルターが使用可能にされているかどうかを調べます。構成されている BRS フィルターが見つかると、パケットはその BRS フィルターが割り当てられている優先順位待ち行列と t-class に入れられます。

- SNA/APPN-ISR (APPN/HPR XID 交換に使用される)
- DLSw
- Telnet

パケットが BRS によってフィルターに掛けられる優先順位値の 1 つを持っているが、適用できる BRS フィルター・タイプが構成されていない場合、パケットは IP プロトコルが割り当てられている優先順位待ち行列と BRS t-class に入れられます。

TN3270 トラフィックが、クライアントによって、BRS が使用可能な広域ネットワークを介して 2216 に送信される場合、クライアントが優先順位ビットを '011'b に設定していない限り、BRS はクライアントからのトラフィックに優先順位を付けることはできません。

さまざまな場合に、IPv4 優先順位ビット処理を構成する必要があります。

BRS および優先待ち行列の使用

1. BRS では、BRS が IPv4 優先順位ビットに基づいてフィルター処理する必要があるかどうかを構成します。 BRS は、IP 保護トンネル・パケット、または TCP および UDP 2 次フラグメント・パケットに対してのみ、このタイプのフィルター処理を実行します。
2. DLSw、IP 経由 HPR、および TN3270 を構成する場合、これらのプロトコル・タイプのそれぞれについて、2216 が発信するパケットに対して IPv4 優先順位ビットを設定する必要があるかどうかを指定します。

IPv4 優先順位ビット・フィルター処理を使用するためには、以下のステップを実行します。

1. BRS の IPv4 優先順位フィルターをアクティブにする。
2. 各種のカテゴリーの SNA トラフィックに対して BRS t-classes を構成し、プロトコルとフィルターを割り当てる。これは、IP 保護トンネルを通して伝達されない、あるいはフラグメント化されない SNA トラフィックの場合と同様の方法で行います。
3. DLSw、IP 経由 HPR、および TN3270 プロトコルを構成するときに、IPv4 優先順位ビットの設定値を使用可能にする。

ブリッジ・トラフィックの SNA および APPN フィルター

SNA/APPN-ISR フィルターは、ブリッジされる SNA および APPN-ISR トラフィックを、BRS トラフィック・クラスに割り当てることができます。 SNA および APPN-ISR トラフィックは、宛先または発信元 SAP が 0x04、0x08、または 0x0C で、その LLC (802.2) 制御フィールドが非番号制情報 (UI) フレームでないことを示しているブリッジ・パケットとして識別されます。

注: フレーム・リレー BAN パケットが、このカテゴリーに入ります。

APPN-HPR フィルターは、ブリッジされる HPR トラフィックを BRS t-class に割り当てることができます。 HPR トラフィックは、宛先または発信元 SAP が X'04'、X'08'、X'0C'、または X'C8' で、その LLC (802.2) 制御フィールドが非番号制情報 (UI) フレームであることを示してブリッジ・パケットとして識別されます。

Network-HPR、High-HPR、Medium-HPR、および Low-HPR フィルターは、さらに HPR ブリッジ・パケットを HPR 伝送優先順位に従ってフィルターに掛けるすることができます。たとえば、Network 伝送優先順位を持つ HPR トラフィックをある t-class と優先順位に割り当て、その他のすべての HPR ブリッジ・トラフィックを異なる t-class または優先順位に割り当てたい場合、Network-HPR フィルターを該当する t-class と優先順位に割り当て、その APPN-HPR フィルターを使用して、残りの HPR トラフィックを異なる t-class または優先順位に割り当てることができます。

IP を介してルーティングされる APPN-HPR トラフィックは、network、high、medium、および low HPR 伝送優先順位に割り当てられた UDP ポート番号を使用してフィルターに掛けられます。 XID 交換には、追加の UDP ポート番号が使用されます。 IP を介する APPN-HPR をサポートするのに使用される UDP ポート番号はすべて構成可能です。

IP ネットワークの中間ルーターで APPN が使用可能にされていない場合は、BRS Config> コマンド・プロンプトから、IP 経由 HPR 用の UDP ポート番号を構成する

ことができます。装置で APPN が使用可能にされている場合には、BRS は APPN Config> コマンド・プロンプトで構成された値を使用します。

その他のフィルターも、トラフィックを割り当てるのに役立つ場合があります。たとえば、DLSw フィルターは、TCP 接続を介して送信される SNA-DLSw トラフィックを BRS t-class に割り当てることができます。

SNA/APPN-ISR および APPN-HPR フィルターは、上記以外の SAP をチェックしたい場合に、MAC フィルターを使用してスライディング・ウィンドウ・フィルターを作成し、そのフィルターにタグを付けます。次に、タグ付けされた MAC フィルターを BRS t-class に割り当てます。

フィルターの優先順位

1 つのパケットが複数の BRS フィルター・タイプに一致することもあり得ます。たとえば、SNA が入っている IP トンネル伝送ブリッジ・パケットは、IP トンネル伝送フィルターと SNA/APPN-ISR フィルターに一致します。パケットが BRS フィルター・タイプに一致するかどうかを判別する際のフィルターの評価順序は、次のとおりです。

1. ブリッジ・パケットの MAC フィルター・タグの一致 (IP/ASRT)
2. ブリッジングの NetBIOS (IP/ASRT)
3. ブリッジングの SNA/APPN-ISR (IP/ASRT)
4. HPR-Network (IP/ASRT/APPN-HPR)
5. HPR-High (IP/ASRT/APPN-HPR)
6. HPR-Medium (IP/ASRT/APPN-HPR)
7. HPR-Low (IP/ASRT/APPN-HPR)
8. APPN-HPR (IP/ASRT)
9. UDP/TCP ポート番号フィルター (IP)
10. IP トンネル伝送 (IP)
11. SDLC リレー (IP)
12. DLSw (IP)
13. マルチキャスト (IP)
14. SNMP (IP)
15. Rlogin (IP)
16. Telnet (IP)
17. XTP (IP)

注: 括弧内は、フィルターが適用されるプロトコルです。

サンプル構成

フレーム・リレー回線のトラフィック・クラス処理にデフォルト回線定義を使用する場合

注:

1 機能 BRS を構成します。

2 インターフェース 1 の BRS を使用可能にします。

3 回線 16、17、18 の BRS を使用可能にします。これらの回線では、トラフィック・クラス処理のデフォルト回線定義が使用されます。

4 トラフィック・クラス処理のデフォルト回線定義を定義するために set-circuit-defaults メニューにアクセスします。

5 トラフィック・クラスを追加し、そのトラフィック・クラスにプロトコルとフィルターを割り当てます。

6 回線 16 の BRS 定義をリストおよび表示します。回線 16 はデフォルト回線定義を使用しているので、デフォルト回線定義で定義されたトラフィック・クラスと、プロトコルおよびフィルター割り当てが表示されます。

7 固有のクラス CIRC171 を作成して、回線 17 がトラフィック・クラス処理にデフォルト回線定義ではなく、回線特定の定義を使用するように変更します。このクラスに、プロトコル、フィルター、またはタグを割り当てることができます。

8 デフォルト回線定義を変更して DEF1 および DEF2 トラフィック・クラスがそれぞれ帯域幅の 10% を予約するようにし、これらの変更が、回線 16 には反映されているが、回線 17 には反映されていない (回線 17 は現在、回線特定の定義を使用しているので) ことを表示します。

9 回線 17 がトラフィック・クラス処理に回線特定の定義ではなく、デフォルト回線定義を使用するように変更します。

```
t 6
 Gateway user configuration
 Config>feature brs      1
 Bandwidth Reservation User Configuration
 BRS Config>interface 1     2
 BRS [i 1]Config>enable
 Please restart router for this command to take effect.
 BRS [i 1] Config>circuit 16    3
 BRS [i 1][dlci 16] Config>enable
 Defaults are in effect for this circuit.
 Please restart router for this command to take effect.
 BRS [i 1] [dlci 16] Config>exit
 BRS [i 1]Config>circuit 17
 BRS [i 1][dlci 17] Config>enable
 Defaults are in effect for this circuit.
 Please restart router for this command to take effect.
 BRS [i 1] [dlci 17] Config>exit
 BRS [i 1]Config>circuit 18
 BRS [i 1][dlci 18] Config>enable
 Defaults are in effect for this circuit.
 Please restart router for this command to take effect.
 BRS [i 1][dlci 18] Config>
 *restart
 Are you sure you want to restart the gateway? (Yes or [No]): yes



 *t 6
 Gateway user configuration
 Config>feature brs
```

```
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS[i 1] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1
maximum queue length 10, minimum queue length 3
total bandwidth allocated 10%
total circuit classes defined (counting one default) 1


class DEFAULT has 10% bandwidth allocated
  the following circuits are assigned:
      16  using defaults.
      17  using defaults.
      18  using defaults.

default class is DEFAULT

BRS [i 1] Config>?
 ENABLE
 DISABLE
 SET-CIRCUIT-DEFAULTS
 CIRCUIT
 ADD-CIRCUIT-CLASS
 DEL-CIRCUIT-CLASS
 CHANGE-CIRCUIT-CLASS
 DEFAULT-CIRCUIT-CLASS
 ASSIGN-CIRCUIT
 DEASSIGN-CIRCUIT
 QUEUE-LENGTH
 LIST
 SHOW
 CLEAR-BLOCK
 EXIT
 BRS [i 1] Config>set-circuit-defaults     4
 BRS [i 1] [circuit defaults] Config>?
 ADD-CLASS
 DEL-CLASS
 CHANGE-CLASS
 DEFAULT-CLASS
 TAG
 UNTAG
 ASSIGN
 DEASSIGN
 LIST
 EXIT
 BRS [i 1] [circuit defaults] Config>add    5
 Class name [DEFAULT]?DEF1
 Percent bandwidth to reserve [10]? 5
 BRS [i 1] [circuit defaults] Config>add
 Class name [DEFAULT]? DEF2
 Percent bandwidth to reserve [10]? 5
 BRS [i 1] [circuit defaults] Config>assign ip
 Class name [DEFAULT]?DEF1
 Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
 Frame Relay Discard Eligible <NO/YES>[NO]?
 BRS [i 1] [circuit defaults] Config>assign asrt
 Class name [DEFAULT]? DEF2
 Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
 Frame Relay Discard Eligible <NO/YES>[NO]?
 BRS [i 1] [circuit defaults] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, default circuit
 total bandwidth allocated 60%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.

 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
```

```
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [circuit defaults] Config>exit
BRS  [i 1] Config>circuit 16     6
BRS  [i 1][dlci 161] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 16 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS  [i 1] [dlci 16] Config>show

BANDWIDTH RESERVATION currently in RAM
interface number 1, circuit number 16 using defaults.
maximum queue length 10, minimum queue length 3
4 current defined classes:
  class LOCAL has 10% bandwidth allocated
  class DEFAULT has 40% bandwidth allocated
  class DEF1 has 5% bandwidth allocated
  class DEF2 has 5% bandwidth allocated

protocol and filter assignments:

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   DEF1                 NORMAL            NO
ARP                  DEFAULT              NORMAL            NO
DNA                  DEFAULT              NORMAL            NO
VINES                DEFAULT              NORMAL            NO
IPX                  DEFAULT              NORMAL            NO
OSI                  DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEF2                 NORMAL            NO

BRS [i 1] [dlci 16] Config>exit
```

```
BRS [i 1] Config>circuit 17
 BRS [i 1] [dlci 17] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, circuit number 17 using defaults.
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 60%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible

 class DEF1 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol IP with priority NORMAL is not discard eligible


 class DEF2 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ASRT with priority NORMAL is not discard eligible

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 1] [dlci 17] Config>add-class    7
 This circuit is currently using circuit defaults...
 Are you sure you want to override the defaults ?(Yes or [No]): yes
 Class name [DEFAULT]? CIRC171
 Percent bandwidth to reserve [10]? 5
 BRS[i 1] [dlci 17] Config>assign vines
 Class name [DEFAULT]? CIRC171
 Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
 Frame Relay Discard Eligible <NO/YES>[NO]?
BRS [i 1] [dlci 17] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, circuit number 17
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 65%
 total classes defined (counting one local and one default) 5


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible


 class DEF1 has 5% bandwidth allocated
   the following protocols and filters assigned:
     protocol IP with priority NORMAL is not discard eligible


 class DEF2 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ASRT with priority NORMAL is not discard eligible


 class CIRC171 has 5% bandwidth allocated
```

```
    the following protocols and filters are assigned:
      protocol VINES with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 17] Config>show

  BANDWIDTH RESERVATION currently in RAM
  interface number 1, circuit number 17
  maximum queue length 10, minimum queue length 3
  5 current defined classes:
    class LOCAL has 10% bandwidth allocated
    class DEFAULT has 40% bandwidth allocated
    class DEF1 has 5% bandwidth allocated
    class DEF2 has 5% bandwidth allocated
    class CIRC171 has 5% bandwidth allocated


  protocol and filter assignments:

  Protocol/Filter      Class              Priority    Discard Eligible
  ---------------      -----              --------    ----------------
  IP                   DEF1                 NORMAL            NO
  ARP                  DEFAULT              NORMAL            NO
  DNA                  DEFAULT              NORMAL            NO
  VINES                CIRC171              NORMAL            NO
  IPX                  DEFAULT              NORMAL            NO
  OSI                  DEFAULT              NORMAL            NO
  AP2                  DEFAULT              NORMAL            NO
  ASRT                 DEF2                 NORMAL            NO

  BRS [i 1] [dlci 17] Config>exit
  BRS [i 1] Config>set-circuit-defaults
  BRS [i 1] [circuit defaults] Config>change DEF1     8
  Percent bandwidth to reserve [5]? 10
  BRS [i 1] [circuit defaults] Config>change DEF2
  Percent bandwidth to reserve [5]? 10
  BRS [i 1] [circuit defaults] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, default circuit
  total bandwidth allocated 70%
  total classes defined (counting one local and one default) 4


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol VINES with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible

  class DEF1 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [circuit defaults] Config>exit
BRS [i 1] Config>circuit 16
  BRS [i 1] [dlci 16] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
```

```
  interface number 1, circuit number 16 using defaults.
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 70%
  total classes defined (counting one local and one default) 4


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol VINES with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible

  class DEF1 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 16] Config>exit
BRS [i 1] Config>circuit 17
  BRS [i 1[ [dlci 17] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 17
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 65%
  total classes defined (counting one local and one default) 5


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible


  class DEF1 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible


  class CIRC171 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol VINES with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 17] Config>use-circuit-defaults     9
  This circuit is currently NOT using circuit defaults...
  Are you sure you want to delete current definitions and use defaults ? (Yes or
  [No]): yes
  Defaults are in effect for this circuit.
```

```
Please restart router for this command to take effect.
BRS [i 1] [dlci 17] Config>
*restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
*t 6
Gateway user configuration
Config>feature brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1]Config>circuit 17
BRS [i 1] [dlci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL


BRS [i 1] [dlci 17] Config>show

BANDWIDTH RESERVATION currently in RAM
interface number 1, circuit number 17 using defaults.
maximum queue length 10, minimum queue length 3
4 current defined classes:
  class LOCAL has 10% bandwidth allocated
  class DEFAULT has 40% bandwidth allocated
  class DEF1 has 10% bandwidth allocated
  class DEF2 has 10% bandwidth allocated

protocol and filter assignments:

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   DEF1                 NORMAL            NO
ARP                  DEFAULT              NORMAL            NO
DNA                  DEFAULT              NORMAL            NO
VINES                DEFAULT              NORMAL            NO
IPX                  DEFAULT              NORMAL            NO
OSI                  DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEF2                 NORMAL            NO

BRS [i 1] [dlci 17] Config>exit
```

第54章 帯域幅予約の構成および監視

この章では、帯域幅予約システム (BRS) の構成コマンドおよび監視コマンドについて説明します。

本章には、以下の節が含まれています。

帯域幅予約構成の概説

ルーター上で帯域幅予約構成コマンドにアクセスし、帯域幅予約を構成するには、以下のようにします。

1. OPCON (*) プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **feature brs** と入力する。
3. BRS Config> プロンプトで **interface #** と入力する。
4. BRS [i 0] Config> プロンプトで **enable** と入力する。

   これはインターフェース・プロンプト・レベルで、この例では、インターフェース番号はゼロになっています。構成する各インターフェースごとに、ステップ 3 とステップ 4 を繰り返す必要があります。

   フレーム・リレー・インターフェースの BRS を構成している場合は、ステップ 4a を続けてください。

   それ以外のインターフェースの BRS を構成している場合は、直接、ステップ 5 に進んでください。

   a. BRS [i 0] Config> プロンプトで **circuit** # と入力する。ただし、# は構成する回線の番号です。
   b. BRS [i 0] [dlci 16] Config> プロンプトで **enable** と入力する。これは回線プロンプト・レベルで、この例では、回線 (DLCI) 番号は 16 です。
   c. BRS [i 0] [dlci 16] Config> プロンプトで **exit** と入力して、インターフェース・レベル・プロンプトに戻る。
   d. BRS t-classes を定義したい各回線ごとに、ステップ 4a ～ 4c を繰り返してください。
5. ルーターを リスタート する。
6. 使用可能にした特定のインターフェースに対して帯域幅予約を構成するために、ステップ 1 ～ 3 を繰り返してください。
7. PPP インターフェースの BRS を構成している場合は、BRS[i 0]Config> プロンプトで、 724ページの表87 にリストされている構成コマンドを使用して、トラフィック・クラスを構成し、そのトラフィック・クラスにプロトコル、フィルター、およびタグを割り当てます。 FR インターフェースの BRS を構成している場合は、ステップ 8 ～ 10 に従ってください。

8. FR インターフェースの BRS を構成している場合は、724ページの表86 にリストされているコマンドを使用して、回線クラスを構成し、その回線クラスに回線を割り当てることができます。
9. デフォルトの回線定義を使用したい場合は、BRS[i 0]Config> プロンプトで **set-circuit-defaults** コマンドを入力します。これにより BRS[i 0][circuit defaults] プロンプトが表示されるので、ここで 724ページの表87 からの該当するコマンドを使用して、トラフィック・クラスを構成し、そのトラフィック・クラスにプロトコル、フィルター、およびタグを割り当てることができます。トラフィック・クラス処理のデフォルト回線定義を定義する作業が完了したら、″exit″ と入力して、BRS[i 0] Config> プロンプトに戻ります。
10. トラフィック・クラス処理のデフォルト回線定義を使用できない FR 回線がある場合には、**circuit** *permanent-virtual-circuit circuit_number* と入力します。これで回線プロンプトにアクセスできるので、ここから 724ページの表87 にリストされたコマンドを使用して、トラフィック・クラス処理の回線特定の定義を作成します。

注: t-class および c-class 構成変更を有効にするために、ルーターをリスタートする必要はありません。

talk 6 (t 6) コマンドは、構成プロセスにアクセスします。

feature brs コマンドは、BRS 構成プロセスにアクセスします。このコマンドは、機能名 (brs) または機能番号 (1) を使用して入力できます。

interface # コマンドは、帯域幅予約を構成する特定のインターフェースを選択します。 BRS クラスを構成する前に、**enable** コマンドを使用して、インターフェース上の BRS を使用可能にしておく必要があります。 721ページのステップ 4 のプロンプトは、選択されたインターフェースの番号がゼロであることを示しています。

circuit # コマンドは、BRS トラフィック・クラスを構成する FR インターフェース上の回線を選択します。回線の BRS t-classes を構成する前に、**enable** コマンドを使用して、回線上の BRS を使用可能にしておく必要があります。 721ページのステップ 4.b のプロンプトは、インターフェース 0 上の回線 16 が選択されたことを示しています。

選択したインターフェースおよび回線の帯域幅予約を使用可能にした後、ルーターをリスタートした上で、回線クラス (フレーム・リレーのみ) およびトラフィック・クラスを構成することが必要です。

種々のレベルの BRS プロンプトから Config> プロンプトが表示されるまで **exit** コマンドを入力することによって、いつでも Config> プロンプトに戻ることができます。

帯域幅予約の構成コマンド

この節では、帯域幅予約の構成コマンドについて説明します。使用できるコマンドは、表示されているBRS 構成プロンプト (BRS Config>、BRS [i x] Config>、or BRS [i x] [dlci y] Config>、または BRS [i x] [circuit defaults] Config>) によって異なります。

表 85. 帯域幅予約構成コマンドの要約 (BRS Config> プロンプトから利用可能)

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Activate-IP-precedence-filtering	保護 IP トンネルを介して送信される、または 2 次 TCP または UDP フラグメントに入れて送信される APPN および SNA パケットの BRS IPv4 優先順位フィルターを起動します。 DLSw、IP 経由 HPR、および TN3270 を構成する場合は、IPv4 優先順位ビットの設定値を構成することも必要です。
Deactivate-IP-precedence-filtering	IPv4 優先順位フィルター処理を停止します。
Enable-hpr-over-ip-port-numbers	IP 経由 APPN-HPR トラフィックの BRS フィルター処理を使用可能にし、IP 経由 HPR パケットを識別するのに使用する UDP ポート番号を構成できるようにします。 **注:** APPN がロード・イメージに存在する場合は、このコマンドはサポートされません。BRS は APPNから、IP 経由 HPR が構成されているかどうかを確認し、構成されている場合には、APPN サポートから、IP 経由 HPR に使用される UDP ポート番号を確認します。
Disable-hpr-over-ip-port-numbers	IP 経由 APPN-HPR トラフィックの BRS フィルター処理を使用不可にします。 **注:** APPN がロード・イメージに存在する場合は、このコマンドはサポートされません。BRS は APPNから、IP 経由 HPR が構成されているかどうかを確認します。
Interface	帯域幅予約を構成するインターフェースを選択します。 **注:** このコマンドは、他の構成コマンドを使用する前に入力する必要があります。 724ページの表86 および 724ページの表87 を参照してください。

表 85. 帯域幅予約構成コマンドの要約 (BRS Config> プロンプトから利用可能) (続き)

コマンド	機能
List	帯域幅予約をサポートするインターフェースをリストし、各インターフェースについて、帯域幅予約が使用可能か使用不可かを示します。
Exit	直前のコマンド・レベルに戻ります。 13 ページの『下位レベル環境の終了』 を参照してください。

表 86. フレーム・リレー・インターフェースの BRS [i #] Config> プロンプトから利用可能な構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add-circuit-class	帯域幅 c-class の名前とその帯域幅の比率を設定します。
Assign-circuit	指定された回線を指定された帯域幅 c-class に割り当てます。
Change-circuit-class	帯域幅 c-class に構成された帯域幅の量を変更します。
Circuit	BRS 回線レベル・プロンプト (`BRS [i x][dlci y] Config>`) にアクセスします。ここから 表87 にリストされたコマンドを使用して、フレーム・リレー回線上の帯域幅予約を構成することができます。
Clear-block	現行インターフェースに関連した構成データを SRAM から消去します。回線クラス構成データおよびトラフィック・クラスのデフォルト回線定義が消去されます。
Deassign-circuit	指定された回線をデフォルトの c-class に復元します。
Default-circuit-class	デフォルト帯域幅 c-class の名前とそのインターフェース帯域幅の比率を設定します。
Del-circuit-class	指定された帯域幅 c-class を削除します。
Disable	インターフェース上の帯域幅予約を使用不可にします。
Enable	インターフェース上の帯域幅予約を使用可能にします。
List	c-classes と割り当てられた回線定義を SRAM から表示します。
Queue-length	優先待ち行列内のパケット数の最大値と最小値を設定します。
Set-circuit-defaults	`BRS [i x] [circuit defaults] Config>` コマンド・プロンプトにアクセスし、表87 から該当するコマンドを使用して、トラフィック・クラス処理のデフォルト回線定義を作成できるようにします。
Show	現在定義されている c-classes と、割り当てられている回線を、SRAM から表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

次の表は、PPP インターフェースの `BRS [i x] Config>` プロンプト、フレーム・リレー回線の `BRS [i x] dlci [y] Config>` プロンプト、および `BRS [i x] [circuit defaults] Config>` プロンプトから利用可能な BRS 回線コマンドをリストしています。

表 87. BRS トラフィック・クラス処理コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add-class	指定された量の帯域幅をユーザー定義のトラフィック・クラスに割り振ります。

表 87. BRS トラフィック・クラス処理コマンド (続き)

コマンド	機能
Assign	プロトコルまたはフィルターを、構成されたトラフィック・クラスに割り当てます。
Change-class	帯域幅 t-class に対して構成された帯域幅の量を変更します。
Clear-block	PPP インターフェースまたはフレーム・リレー回線のトラフィック・クラスとプロトコル、フィルター、およびタグ割り当て構成データを、SRAM から消去します。 **注:** このコマンドは BRS [i x] [circuit defaults] Config> プロンプトからは使用できません。
Deassign	指定されたパケットまたはフィルターの待ち行列化を、デフォルトの t-class と優先順位に復元します。
Default-class	デフォルトの t-class と優先順位を必要な値に設定し、すべての未割り当てプロトコルを新しいデフォルト t-class に割り当てます。
Del-class	以前に構成した帯域幅 t-class を削除します。
Disable	PPP インターフェースまたはフレーム・リレー回線上の帯域幅予約を使用不可にします。 **注:** BRS [i x] [circuit defaults] Config> プロンプトからは、BRS を使用可能または使用不可にすることはできません。
Enable	PPP インターフェースまたはフレーム・リレー回線上の帯域幅予約を使用可能にします。 **注:** BRS [i x] [circuit defaults] Config> プロンプトからは、BRS を使用可能または使用不可にすることはできません。
List	SRAM に保管されている構成済み t-classes とプロトコル、フィルター、およびタグ割り当てをリストします。
Queue-length	優先待ち行列内のパケット数の最大値と最小値を設定します。 **注:** このコマンドは、BRS [i x] [circuit defaults] Config> プロンプトではサポートされません。
Show	RAM に保管されている現在定義済みの t-classes とプロトコル、フィルター、およびタグ割り当てを表示します。 **注:** このコマンドは、BRS [i x] [circuit defaults] Config> プロンプトではサポートされません。
Tag	MAC フィルター機能の構成時にタグ付けされた MAC フィルターに、BRS タグ名 (TAG1-TAG5) を割り当てます。
Untag	BRS タグ名 (TAG1-TAG5) と MAC フィルター機能の構成時にタグ付けされた MAC フィルターとの関係を除去します。
Use-circuit-defaults	ユーザーがトラフィック・クラス処理の circuit-specific 定義を削除して、circuit-defaults 定義を使用することができるようにします。このコマンドは、フレーム・リレーの BRS [i x] dlci [y] Config> プロンプトでのみ有効です。 **注:** デフォルトを有効にするためには、ルーターを リスタートする必要があります。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

該当するコマンドを使用して、ポイント・ポイント・プロトコル (PPP) およびフレーム・リレーの帯域幅予約を構成してください。フレーム・リレーの場合は、回線とネットワーク・インターフェースを構成することが必要です。 PPP の場合は、ネットワーク・インターフェースを構成するするだけで済みます。

注:

1. BRS インターフェース・メニュー内から **clear-block**、 **disable**、**enable**、 **list**、および **show** コマンドを出すと、選択されたインターフェースに構成されている帯域幅予約情報に影響を与えたり、リストしたりします。 BRS 回線メニュー内からこれらのコマンドを出した場合は、パーマネント・バーチャル・サーキット (PVC) に構成されているフレーム・リレー帯域幅予約情報にのみ影響を与えたり、リストしたりします。
2. 帯域幅予約コマンドを使用する前に、次のことを念頭に入れてください。
   - 他の構成コマンドを使用する前に、**interface** コマンドを使用して、インターフェースを選択しておくことが必要です。 (BRS 構成は、これを強制的に要求します。)
   - *Class-name* パラメーターは、大文字小文字の区別をします。
   - 現行の *class-names* を見たい場合は、**list** または **show** コマンドを使用します。
   - インターフェースまたは回線上の帯域幅予約を使用可能にした後は、回線およびトラフィック・クラスを追加/削除/変更したり、回線またはプロトコルを動的に割り当てたりすることができます。有効にするためにルーターをリスタートする必要があるコマンドは、enable、disable、use-circuit-defaults、および clear-block コマンドだけです。
3. t-class および c-class 構成変更を有効にするために、ルーターをリスタートする必要はありません。

Activate-IP-precedence-filtering

activate-ip-precedence-filtering コマンドは、保護 IP トンネルを介して送信される、または 2 次 TCP または UDP フラグメントに入れて送信される APPN および SNA パケットの BRS IPv4 優先順位フィルターを起動するのに使用します。 DLSw、IP 経由 HPR、および TN3270 を構成する場合は、IPv4 優先順位ビットの設定値を構成することも必要です。詳細については、710ページの『IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィックのための IP バージョン 4 優先順位ビット処理の使用』を参照してください。

構文:

activate-ip-precedence-filtering

Add-circuit-class

注: フレーム・リレーの構成時にのみ使用されます。

add-circuit-class コマンドは、インターフェース・レベルで、ユーザー定義の帯域幅 c-class に割り当てられた回線グループが使用する指定量の帯域幅を割り振るのに使用します。

構文:

add-circuit-class *class-name %*

Add-class

add-class コマンドは、指定量の帯域幅をユーザー定義の帯域幅 t-class に割り振るのに使用します。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。 『Yes』 と応答すると、回線はトラフィック・クラス処理に回線特定の定義を使用するように変更され、コマンドの使用が認められます。 『No』 と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、BRS [i x][circuit defaults]Config> コマンド・プロンプトに行く必要があります。

構文:

add-class [*class-name* or *class#*] *%*

例:

```
BRS [i 1] [dlci 17] Config>add-class
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults ?(Yes or [No]): y
Class name [DEFAULT]? CIRC17
Percent bandwidth to reserve [10]?5
BRS [i 1] [dlci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17
maximum queue length 10, minimum queue length 3
total bandwidth allocated 65%
total classes defined (counting one local and one default) 5


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
   protocol DNA with default priority is not discard eligible
   protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible
    protocol ASRT with default priority is not discard eligible


class DEF1 has 5% bandwidth allocated
  protocol IP with priority NORMAL is not discard eligible.


class DEF2 has 5% bandwidth allocated
 protocol ARP with priority NORMAL is not discard eligible.


class CIRC171 has 5% bandwidth allocated
  no protocols or filters are assigned to this class.

assigned tags:

default class is DEFAULT with priority NORMAL
```

Assign

assign コマンドは、指定されたタグ、プロトコル・パケット、またはフィルターを、そのクラス内の特定の t-class と優先順位に割り当てるのに使用します。 4 つの優先順位タイプは、次のとおりです。

- Urgent
- High
- Normal (デフォルト優先順位)
- Low

構文:

assign [*protocol-class* または TAG または *filter-class*] [*class-name* or *class#*]

assign コマンドは、フレーム・リレーのフレームの廃棄可能性 (DE) ビットを設定するのにも使用できます。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。 『Yes』 と応答すると、回線はトラフィック・クラス処理に回線特定の定義を使用するように変更され、コマンドの使用が認められます。 『No』 と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

例:

```
assign IPX test
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]? low
protocol IPX maps to class test with priority LOW Discard eligible <yes/no> [N]?
```

Assign-circuit

注: フレーム・リレーの構成時にのみ使用されます。

assign-circuit コマンドは、インターフェース・レベルで、指定された回線 (DLCI) を指定された帯域幅 c-class に割り当てるのに使用します。

注: **circuit** コマンドを使用して DLCI 上の BRS を使用可能にし、ルーターをリスタートしてからでなければ、このコマンドを用いて回線に回線クラスを割り当てることはできません。

構文:

assign-circuit *# class name*

Change-circuit-class

注: フレーム・リレーの構成時にのみ使用されます。

change-circuit-class コマンドは、インターフェース・レベルで、指定された c-class に割り当てられた回線グループが使用する帯域幅の比率を変更するのに使用します。

構文:

change-circuit-class *class-name %*

Change-class

change-class コマンドは、帯域幅 t-class に構成された帯域幅の量を変更するのに使用します。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。 『Yes』 と応答すると、回線はトラフィック・クラス処理に回線特定の定義を使用するように変更され、コマンドの使用が認められます。 『No』 と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

構文:

change-class [*class-name* or *class#*] *%*

Circuit

注: フレーム・リレーの構成時にのみ使用されます。

circuit コマンドは、フレーム・リレーのパーマネント・バーチャル・サーキット (PVC) の DLCI を構成するのに使用します。このコマンドは、BRS インターフェース構成プロンプト (`BRS [i #] Config>`) からしか出せません。

構文:

*ci***rcuit** *permanent-virtual-circuit-#*

add-class、**assign**、 **default-class**、**del-class**、 **deassign**、または **change-class** コマンドを使用する前に、回線上の BRS を使用可能にし、ルーターを リスタートしておく必要があります。たとえば、次のようにします。

```
BRS [i 1] Config> circuit
Circuit to reserve bandwidth:  [16]

BRS [i 1 ] [dlci 16] Config> enable
```

フレーム・リレー回線に対して **enable** コマンドを出し、ルーターをリスタートすると、その回線に対して以下の構成コマンドが利用可能になります。

add-class	deassign	enable	tag
assign	default-class	exit	untag
change-class	del-class	list	clear-block
disable	show	use-circuit-defaults	

Clear-block

clear-block コマンドは、現行の帯域幅予約構成データを SRAM から消去するのに使用します。

構文:

clear-block

- このコマンドを PPP のインターフェース・プロンプトから入力すると、そのインターフェースのすべての BRS 構成データが消去されます。
- このコマンドをフレーム・リレーのインターフェース・プロンプトから入力すると、そのインターフェースまたはインターフェース上の回線は使用可能でなくなり、すべての回線クラス構成データとトラフィック・クラス処理のデフォルト回線定義が消去されます。ただし、個々の回線のトラフィック・クラス構成データは消去されず、インターフェース上の BRS を再び使用可能にすれば利用可能です。
- 回線のトラフィック・クラス構成データを消去するためには、最初にインターフェース・レベル・プロンプトから **circuit** コマンドを入力し、次に回線レベル・プロンプトから **clear-block** コマンドを入力します。各回線のトラフィック・クラス構成データを消去した後で、インターフェース・レベル・プロンプトから **clear-block** コマンドを入力して、回線クラス構成データを消去します。この変更は、ルーターをリスタートするまで有効になりません。

例:

```
clear-block
You are about to clear BRS configuration information for this interface
Are you sure you want to do this (Yes or No): y
BRS [i 1] Config>
```

Deactivate-IP-precedence-filtering

deactivate-ip-precedence-filtering コマンドは、IPv4 優先順位フィルター処理を停止にするのに使用します。

構文:

deactivate-ip-precedence-filtering

Deassign

deassign コマンドは、指定されたプロトコル・パケットまたはフィルターの待ち行列化を、デフォルトの t-class と優先順位に復元するのに使用します。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。 『Yes』 と応答すると、回線はトラフィック・クラス処理に回線特定の定義を使用するように変更され、コマンドの使用が認められます。 『No』 と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

構文:

deassign [*prot-class* or *filter-class*]

Deassign-circuit

注: フレーム・リレーの構成時にのみ使用されます。

deassign-circuit コマンドは、インターフェース・レベルで、指定された回線の待ち行列化をデフォルト c-class に復元するのに使用します。

構文:

deassign-c #

Default-circuit-class

注: フレーム・リレーの構成時にのみ使用されます。

default-circuit-class コマンドは、インターフェース・レベルで、デフォルト帯域幅 c-class のユーザー定義名と、そのクラスの回線 (帯域幅 c-class に割り当てられていないオーファンを含む) に割り振られる帯域幅の比率を設定するのに使用します。

構文:

default-circuit-class *class-name %*

Del-circuit-class

注: フレーム・リレーの構成時にのみ使用されます。

del-circuit-class コマンドは、インターフェース・レベルで、指定された帯域幅 c-class を削除するのに使用します。

構文:

del-circuit-class *class-name*

Default-class

default-class コマンドは、デフォルト t-class と優先順位を必要な値に設定するのに使用します。以前に値が指定されていない場合、システム・デフォルト値が使用されます。そうでない場合は、最後に指定された値が使用されます。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。 『Yes』 と応答すると、回線はトラフィック・クラス処理に回線特定の定義を使用するように変更され、コマンドの使用が認められます。 『No』 と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

BRS と優先待ち行列の構成

構文:

default-cl [*class-name* or *class#*] *priority*

Del-class

del-class コマンドは、指定されたインターフェースまたは回線から、以前に構成された帯域幅 t-class を削除するのに使用します。

注: 現在、トラフィック・クラスの処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。 『Yes』 と応答すると、回線はトラフィック・クラス処理に回線特定の定義を使用するように変更され、コマンドの使用が認められます。 『No』 と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

構文:

del-class [*class-name* or *class#*]

Disable

disable コマンドは、インターフェース上 (インターフェース・プロンプトから入力した場合) または回線上 (回線プロンプトから入力した場合) の帯域幅予約を使用不可にするのに使用します。この変更は、ルーターをリスタートするまで有効になりません。

帯域幅予約が使用不可にされたかどうかを確認するには、**list** コマンドを入力します。

構文:

disable

Disable-hpr-over-ip-port-numbers

disable-hpr-over-ip-port-numbers コマンドは、IP 経由 HPR トラフィックの BRS フィルター処理を使用不可にするのに使用します。

構文:

disable-hpr-over-ip-port-numbers

IP 経由 HPR トラフィックの BRS フィルター処理が使用不可にされたかどうかを確認するには、**list** コマンドを入力します。

注: APPN がロード・イメージに含まれている場合は、`APPN Config>` コマンド・プロンプトで、IP 経由 HPR トラフィックを使用するかどうかを構成します。

Enable

enable コマンドは、インターフェース上 (インターフェース・プロンプトから入力した場合) または回線上 (回線プロンプトから入力した場合) の帯域幅予約を使用可能にするのに使用します。この変更は、ルーターを リスタートするまで有効になりません。

構文:

enable

注:

- PPP インターフェース上の BRS を構成するときは、インターフェース・プロンプトで **enable** コマンドを出し、ルーターをリスタートした後で、トラフィック・クラスを構成し、トラフィック・クラスにプロトコルとフィルターを割り当てます。
- 回線上で BRS を初期に使用可能にすると、回線はデフォルト回線定義を使用するように初期設定されます。インターフェース・プロンプトおよびトラフィック・クラスを定義したい各回線の回線プロンプトで、**enable** コマンドを出します。その後、ルーターを リスタートしてから、インターフェースの回線クラスおよび各回線のトラフィック・クラスを構成します。たとえば、次のように入力します。

```
t 6
Gateway user configuration
Config>f brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1] Config>enable
Please  restart router for this command to take effect
BRS [i 1] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1
maximum queue length 10, minimum queue length 3
total bandwidth allocated 10%
total circuit classes defined (counting one default) 1


class DEFAULT has 10% bandwidth allocated
  no circuits are assigned to this class.

default class is DEFAULT

BRS [i 1] Config>circ 16
BRS [i 1] [dlci 16] Config>enable
Defaults are in effect for this circuit.
Please  restart router for this command to take effect.
BRS [i 1] [dlci 16] Config>ex
Please  restart router for this command to take effect.
BRS [i 1] [dlci 16] Config>
*rest
Are you sure you want to  restart the gateway? (Yes or [No]): y
```

Enable-hpr-over-ip-port-numbers

enable-hpr-over-ip-port-numbers コマンドは、IP 経由 APPN-HPR トラフィックの BRS フィルター処理を使用可能にし、IP 経由 HPR パケットを識別するのに使用する UDP ポート番号を構成するのに使用します。

注: APPN がロード・イメージに含まれている場合は、APPN Config> コマンド・プロンプトで、IP 経由 HPR を使用可能にし、IP 経由 HPR トラフィックに使用する UDP ポート番号を指定します。

構文:

enable-hpr-over-ip-port-numbers

例:

```
BRS Config> enable-hpr-over-ip-port-numbers
XID exchange port number [12000]?
HPR net  trans prio port number [12001]?
HPR high trans prio port number [12002]?
HPR medium trans prio port number [12003]?
HPR low    trans prio port number [12004]?
```

XID exchange port number

このパラメーターは、XID 交換に使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12000

Network priority port number

このパラメーターは、network 優先順位トラフィックに使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12001

High exchange port number

このパラメーターは、high 優先順位トラフィックに使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12002

Medium exchange port number

このパラメーターは、medium 優先順位トラフィックに使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12003

Low exchange port number

このパラメーターは、low 優先順位トラフィックに使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12004

Interface

interface コマンドは、帯域幅予約構成コマンドが適用されるシリアル・インターフェースを選択するのに使用します。*帯域幅予約は、PPP (ポイント・ポイント・プロトコル) およびフレーム・リレー・インターフェースを稼働するルーター上でサポートされます。*

構文:

interface *interface#*

注:

1. 新しいインターフェースに対する帯域幅予約コマンドを入力する場合は、他の帯域幅予約構成コマンドを使用する***前に*** このコマンドを入力する必要があります。帯域幅予約プロンプトを終了した後で、前に構成したインターフェースの帯域幅予約を変更するためにこのプロンプトに戻りたい場合には、再びこのコマンドを最初に入力する必要があります。
2. WAN 復元が使用されており、1 次インターフェースに BRS が構成されている場合、2 次インターフェースにも BRS を構成する必要があります。通常、WAN 復元が使用されている場合には、2 次インターフェースは 1 次インターフェースと同じアイデンティティーを取りますが、 BRS の場合はそうではないので、1 次インターフェースと 2 次インターフェースの両方で BRS を構成することが必要です。

特定のインターフェース上の帯域幅予約を使用可能にするには、`BRS Config>` プロンプトで、その特定プロトコルまたは機能をサポートするインターフェースの番号を入力します。これにより、この章で説明している BRS **enable** 構成コマンドを使用できるようになります。インターフェース番号を使用可能にした後、2210 を リスタートして、このコマンドを有効にしてからでないと、インターフェースに他の構成変更を加えることはできません。

注:

1. フレーム・リレー・インターフェースの BRS を構成している場合は、ルーターをリスタートする前に、**circuit** コマンドを使用して回線を選択し、それらの回線の帯域幅予約を使用可能にすることができます。

List

list コマンドは、現在定義されている帯域幅クラスとそれぞれに保証されている比率を表示するのに使用します。

list コマンドと **show** コマンドは似ています。 **list** コマンドは現行の SRAM 定義を表示し、**show** コマンドは現行の RAM 定義を表示します。

構文:

list *interface#*

list コマンドを出すプロンプトに応じて、さまざまな出力が表示されます。 **list** コマンドは、次のプロンプトから出すことができます。

- BRS [i 1] [dlci 16] Config>
- BRS [i 1] Config>
- BRS Config>
- BRS [i 1] [circuit defaults] Config>

注: このコマンドをフレーム・リレー回線プロンプト (BRS [i x] [dlci y] Config>) から使用すると、回線がトラフィック・クラス処理のデフォルト回線定義を使用しているのか、回線特定の定義を使用しているのかが示されます。回線がデフォルト回線定義を使用している場合、デフォルト回線定義に現在定義されているトラフィック・クラス、プロトコル、フィルター、およびタグが表示されます。ただし、デフォルト回線定義を変更したい場合には、BRS[i x] [circuit defaults] Config> プロンプトに行かないと変更できません。

PPP インターフェースの BRS インターフェース・レベル・プロンプト (BRS [i 0]) およびフレーム・リレー・インターフェースの BRS 回線レベル・プロンプト (BRS [i 0] [dlci 16] Config>) では、**list** コマンドは、構成された帯域幅の比率、および割り当てられたプロトコルとフィルターをリストします。

フレーム・リレーの BRS インターフェース・レベル・プロンプトでは、**list** コマンドは、回線クラス、それぞれに構成された帯域幅の比率、および割り当てられた回線をリストします。

例 1

```
BRS Config>list
 Bandwidth Reservation is available for 2 interfaces.

 Interface   Type            State
 ---------   ----            -----
         1   FR              Enabled
         2   PPP             Enabled

 The use of HPR over IP port numbers is disabled

 BRS Config>interface 1
 BRS [i 1] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 10%
 total circuit classes defined (counting one default) 1


 class DEFAULT has 10% bandwidth allocated
   the following circuits are assigned:
        17
        16  using defaults.
        18  using defaults.

 default class is DEFAULT

 BRS [i 2] Config>exit
 BRS Config>interface 2
 BRS [i 2] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 2
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 50%
 total classes defined (counting one local and one default) 2


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.
```

```
 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol IP with default priority
     protocol ARP with default priority
     protocol DNA with default priority
     protocol VINES with default priority
     protocol IPX with default priority
     protocol OSI with default priority
     protocol AP2 with default priority
     protocol ASRT with default priority

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 2] Config>
```

例 2

```
 BRS [i 1] [dlci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
   protocol ASRT with priority NORMAL is not discard eligible
   filter NETBIOS with priority NORMAL is not discard eligible


class CLASS1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
   protocol IP with priority NORMAL is not discard eligible
   protocol ARP with priority NORMAL is not discard eligible
   protocol DNA with priority NORMAL is not discard eligible
   protocol VINES with priority NORMAL is not discard eligible
   protocol IPX with priority NORMAL is discard eligible
   protocol OSI with priority NORMAL is not discard eligible
   protocol AP2 with priority NORMAL is not discard eligible
```

例 3

```
 BRS [i 1] [circuit defaults] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, default circuit
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 70%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.



 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible
     protocol ASRT with default priority is not discard eligible


 class DEF1 has 10% bandwidth allocated
   protocol IP with priority NORMAL is not discard eligible.


 class DEF2 has 10% bandwidth allocated
  protocol ARP with priority NORMAL is not discard eligible.

 assigned tags:
```

```
default class is DEFAULT with priority NORMAL

 BRS [i 1] [circuit defaults] Config>
```

例 4

```
BRS Config>list
 Bandwidth Reservation is available for 2 interfaces.

 Interface   Type            State
 ---------   ----            -----
         1   FR              Enabled
         2   PPP             Enabled

 The use of HPR over IP port numbers is enabled.

    Transmission Type   Port Number
    -----------------   -----------
        XID exchange        12000
        HPR network         12001
        HPR high            12002
        HPR medium          12003
        HPR low             12004
```

Queue-length

queue-length コマンドは、各 BRS 優先待ち行列に待ち行列化できるパケットの数を設定するのに使用します。各 BRS クラスには、そのプロトコル、フィルター、およびタグに割り当てられた優先順位値があり、各優先待ち行列に、このコマンドで指定したパケット数を保管することができます。

構文:

queue-length *maximum-length minimum-length*

このコマンドは、各 BRS 優先待ち行列に待ち行列化できるバッファーの最大数、およびルーターの入力バッファーが不足しているときに各 BRS 優先待ち行列に待ち行列化できる最大数を設定します。

PPP インターフェースに対して **queue-length** を出すと、このコマンドは、そのインターフェースに定義されている各 BRS t-class の各優先待ち行列の queue-length 値を設定します。

フレーム・リレー・インターフェースに対して **queue-length** を出すと (プロンプト BRS [i 0] Config> で)、このコマンドは、そのインターフェースの各パーマネント・バーチャル・サーキットに対して定義されている各 BRS t-class の各優先待ち行列のデフォルト queue-length 値を設定します。

フレーム・リレー PVC に対して **queue-length** を出すと (プロンプト BRS [i 0] [dlci 16] Config> などで)、このコマンドは、その PVC に定義されている各BRS t-class の各優先待ち行列の待ち行列長さ値を設定します。これらの値は、そのフレーム・リレー・インターフェースに設定されているデフォルトの待ち行列長さ値をオーバーライドします。

重要： このコマンドは、その使用が不可欠のとき以外は、使用しないでください。待ち行列長さのデフォルト値は、ほとんどのユーザーに推奨できる値です。待ち行列の長さの値を高く設定し過ぎると、ルーターの性能が大きく低下する可能性があります。

Set-circuit-defaults

set-circuit-defaults コマンドは、トラフィック・クラス処理のデフォルト回線定義を定義するのに必要なコマンドにアクセスするのに使用します。これらのデフォルト回線定義は、同じトラフィック・クラスと、プロトコル、フィルター、およびタグ割り当てを使用できる、インターフェース上のすべてのフレーム・リレー回線で使用できます。

構文:

set-circuit-defaults

Show

show コマンドは、RAM に保管されている現行の定義済み帯域幅クラスを表示するのに使用します。

構文:

show *interface#*

show コマンドを出すプロンプトに応じて、さまざまな出力が表示されます。 **show** コマンドは、次のプロンプトから出すことができます。

- BRS [i *x*] Config> - インターフェース番号 *x* のインターフェース・レベル・プロンプト。
- BRS [i *x*] [dlci *y*] Config> - フレーム・リレー・インターフェース番号 *x* 上の回線 *y* の回線レベル・プロンプト。次の例は、回線レベル・プロンプトからの show コマンドの出力を示しています。

```
BRS [i 1] [dlci 17] Config>show

Protocol/Filter      Class             Priority    Discard Eligible
---------------      -----             --------    ----------------
IP                   CLASS1              NORMAL            NO
ARP                  CLASS1              NORMAL            NO
DNA                  CLASS1              NORMAL            NO
VINES                CLASS1              NORMAL            NO
IPX                  CLASS1              NORMAL            YES
OSI                  CLASS1              NORMAL            NO
AP2                  CLASS1              NORMAL            NO
ASRT                 DEFAULT             NORMAL            NO
NETBIOS              DEFAULT             NORMAL            NO
```

PPP のインターフェース・プロンプトおよびフレーム・リレーの回線プロンプトでは、トラフィック・クラス情報が表示されます。フレーム・リレーのインターフェース・プロンプトでは、回線クラス情報が表示されます。

注:

1. このコマンドをフレーム・リレー回線プロンプト (BRS [i x] [dlci y] Config>) から使用すると、回線がトラフィック・クラス処理のデフォルト回線定義を使用しているのか、回線特定の定義を使用しているのかが示されます。回線がデフォルト回線定義を使用している場合、デフォルト回線定義に現在定義されているトラフィック・クラス、プロトコル、フィルター、およびタグが表示されます。ただし、デフォルト回線定義を変更したい場合には、BRS[i x] [circuit defaults] Config> プロンプトに行かないと変更できません。

2. このコマンドは BRS [i x] [circuit defaults] Config> プロンプトからは使用できません。

Tag

tag コマンドは、MAC フィルター機能の構成時にタグ付けされた MAC フィルター項目を、次に利用可能な BRS タグ名に割り当てるのに使用します。 BRS タグ名は、TAG1、TAG2、TAG3、TAG4、および TAG5 です。 assign コマンドで BRS タグ名を指定して、タグを BRS トラフィック・クラスに割り当てます。

構文:

tag *mac_filter_tag#*

list コマンドを使用すると、どの MAC フィルター・タグが BRS タグ名に割り当てられており、どの BRS タグ名が帯域幅トラフィック・クラスに割り当てられているかがリストされます。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。 『Yes』 と応答すると、回線はトラフィック・クラス処理に回線特定の定義を使用するように変更され、コマンドの使用が認められます。 『No』 と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、BRS [i x][circuit defaults]Config> コマンド・プロンプトに行く必要があります。

Untag

untag コマンドは、MAC フィルター・タグ番号と BRS タグ名の関係を除去するのに使用します。タグを除去できるのは、対応する BRS タグ名が帯域幅トラフィック・クラスに割り当てられていないときだけです。

構文:

untag *mac_filter_tag#*

list コマンドを使用すると、どの MAC フィルター・タグが BRS タグ名に割り当てられており、どの BRS タグ名が帯域幅トラフィック・クラスに割り当てられているかがリストされます。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。 『Yes』 と応答すると、回線はトラフィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。 『No』 と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、BRS [i x][circuit defaults]Config> コマンド・プロンプトに行く必要があります。

Use-circuit-defaults

use-circuit-defaults コマンドは、インターフェース・レベルで、回線特定の定義を削除して、トラフィック・クラス処理のデフォルト回線定義を使うようにするのに使用します。回線デフォルト値を使用することの確認を求めるプロンプトが出ます。

構文:

use-circuit-defaults

注:

1. このコマンドは、フレーム・リレーの構成時にのみ使用されます。
2. デフォルトを有効にするためには、ルーターを リスタートする必要があります。

例:

```
BRS [i 1] [dlci 17]
Config>use-circuit-defaults
This circuit is currently NOT using circuit defaults...
 Are you sure you want to delete current definitions and use defaults ? (Yes or
 [No]): y
 Defaults are in effect for this circuit.
 Please  restart router for this command to take effect.
 BRS [i 1] [dlci 17] Config>
 *rest
 Are you sure you want to  restart the gateway? (Yes or [No]): y
```

帯域幅予約監視プロンプトへのアクセス

帯域幅予約監視コマンドにアクセスし、ルーター上の帯域幅予約を監視するには、以下のようにします。

1. OPCON プロンプト (*) で **talk 5** と入力する。
2. GWCON プロンプト (+) で **feature brs.** と入力する。
3. BRS> プロンプトで **interface #** と入力する。ただし、# は監視するインターフェースの番号です。これにより、インターフェース・レベル・プロンプト BRS [i x]> が表示されます。ただし、x はインターフェース番号です。
4. フレーム・リレーの場合のみ、インターフェース・プロンプトで **circuit #** と入力して、このインターフェース上の監視する回線を指定する。

   これにより、回線レベル・プロンプト BRS [i x] [dlci y]> が表示されます。ただし、x はインターフェース番号で、y は回線番号です。
5. プロンプトで、該当する監視コマンドを入力する。 (742ページの『帯域幅予約監視コマンド』 を参照してください。)

   talk 5 (t 5) コマンドは、監視プロセスにアクセスします。

   feature brs コマンドは、BRS 監視プロセスにアクセスします。このコマンドは、機能名 (brs) または機能番号 (1) を使用して入力できます。

   interface # コマンドは、帯域幅予約を監視する特定のインターフェースを選択します。

   circuit # コマンドは、フレーム・リレーのパーマネント・バーチャル・サーキット (PVC) の DLCI を選択します。

   BRS> プロンプトで **exit** コマンドを入力すれば、いつでも GWCON プロンプトに戻ることができます。

帯域幅予約監視プロンプト (BRS>) にアクセスしたら、表88 に説明されている特定の監視コマンドのどれでも入力できます。

帯域幅予約監視コマンド

この節では、帯域幅予約監視コマンドの要約を示し、個々のコマンドについて説明します。 表88 は、帯域幅予約監視コマンドを示しています。使用できるコマンドは、BRS 監視プロンプト (BRS>、BRS [i x]>、または BRS [i x] [dlci y]>) によって異なります。

表 88. 帯域幅予約監視コマンドの要約

コマンド	FR でのみ使用	機能
? (Help)		このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13 ページの『ヘルプの入手』を参照してください。
Circuit	yes	フレーム・リレーのパーマネント・バーチャル・サーキット (PVC) の DLCI を選択します。フレーム・リレーの帯域幅予約トラフィックを監視するには、回線プロンプト・レベルにあることが必要です。
Clear		現在の t-class カウンターをクリアし、それらを **last** t-class カウンターとして保管します。 カウンターはクラス別にリストされます。
Clear-circuit-class	yes	現在の c-class カウンターをクリアし、それらを **last** c-class カウンターとして保管します。カウンターはクラス別にリストされます。
Counters		現在の t-class カウンターを表示します。
Counters-circuit-class	yes	現在の c-class カウンターを表示します。
Interface		監視するインターフェースを選択します。 **注:** このコマンドは、他の帯域幅予約監視コマンドを使用する前に入力する必要があります。
Last		最後に保管された t-class カウンターを表示します。
Last-circuit-class	yes	最後に保管された c-class カウンターを表示します。
Exit		直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Circuit

注: フレーム・リレーを監視するときにのみ使用します。

circuit コマンドは、監視するフレーム・リレー PVC の DLCI を選択するのに使用します。このコマンドは、BRS インターフェース監視プロンプト (BRS [i #]>) からしか出せません。

構文:

circuit *permanent-virtual-circuit-#*

フレーム・リレー回線を選択した後、回線プロンプトで次のコマンドを使用することができます。

```
CLEAR
COUNTERS
LAST
EXIT
```

Clear

clear コマンドは、現行の帯域幅予約 t-class カウンターを保管して **last** コマンドを用いて検索できるようにし、値をクリアするのに使用します。カウンターは、帯域幅トラフィック・クラスに基づいて保持されます。

構文:

clear

Clear-Circuit-Class

注: フレーム・リレーを監視するときにのみ使用します。

clear-circuit-class コマンドは、現行の帯域幅予約 c-class カウンターを保管して **last-circuit-class** コマンドを用いて検索できるようにし、値をクリアするのに使用します。カウンターは、回線クラスに基づいて保持されます。

構文:

clear-circuit-class

Counters

counters コマンドは、PPP インターフェースまたはフレーム・リレー回線に対して構成されたトラフィック・クラスの帯域幅予約トラフィックを説明する統計を表示するのに使用します。

構文:

counters

例: **counters**

```
Bandwidth Reservation Counters
Interface 1

Class         Pkt Xmit     Bytes Xmit     Bytes Ovfl
LOCAL                0              0              0
DEFAULT              1             30              0
CLASS 1              1             56              0
CLASS 2              0              0              0

TOTAL                2             86              0
```

注: Bytes Ovfl 欄は、優先待ち行列の最大 queue-length に達したか、あるいは優先待ち行列が最小待ち行列長さ限界値にあるときに、受信バッファーが不足しているインターフェースからパケットが来たためにパケットを待ち行列化できなかったかのいずれか理由で転送できなかったパケットのバイト数をリストしています。

Counters-Circuit-Class

注: フレーム・リレーを監視するときにのみ使用します。

counters-circuit-class コマンドは、フレーム・リレー回線に対して構成されたトラフィック・クラスの統計を表示するのに使用します。

構文:

counters-circuit-class

例: **counters-circuit-class**

```
Bandwidth Reservation Circuit Class Counters
Interface 1


Class         Pkt Xmit     Bytes Xmit     Bytes Ovfl
DEFAULT             25           3402             26
CIRCLASS1            1             56              0
CIRCLASS2            0              0              0

TOTAL               26           3458             26
```

Interface

interface コマンドは、帯域幅予約監視コマンドが適用されるシリアル・インターフェースを選択するのに使用します。*帯域幅予約は、PPP (ポイント・ポイント・プロトコル) およびフレーム・リレー・インターフェースを稼働するルーター上でサポートされます。*

構文:

interface *interface#*

注: 新しいインターフェースに対する帯域幅予約コマンドを入力する場合は、他の帯域幅予約監視コマンドを使用する前にこのコマンドを入力する必要があります。帯域幅予約監視プロンプト (BRS>) を終了した後で、帯域幅予約を監視するためにこのプロンプトに戻りたい場合には、再びこのコマンドを最初に入力する必要があります。

特定のインターフェースの帯域幅予約を監視するには、BRS> 監視プロンプトで、そのインターフェースの番号を入力します。これにより、この章で説明している帯域幅予約監視コマンドを使用できるようになります。

Last

last コマンドは、最後に保管された t-class 統計を表示するのに使用します。 t-class 統計は、**counters** コマンドの場合と同じフォーマットで表示されます。

構文:

last

Last-Circuit-Class

注: フレーム・リレーを監視するときにのみ使用します。

last-circuit-class コマンドは、最後に保管された回線クラス統計を表示するのに使用します。 c-class 統計は、**counters-circuit-class** コマンドの場合と同じフォーマットで表示されます。

構文:

last-circuit-class

第55章 MAC フィルターの使用

この章では、処理時にパケットに適用するパケット・フィルターを指定するための、媒体アクセス制御 (MAC) の使用法について説明します。本章には、以下の節が含まれています。

- 『MAC フィルターと DLSw トラフィック』
- 748ページの『MAC フィルター・パラメーター』

フィルターとは、ブリッジするときのパケットの処理方法を決めるために、パケットに適用される 1 組の規則です。 MAC フィルターは、ブリッジされるトラフィックにのみ適用されます。

注: MAC フィルターはトンネル・トラフィックに対して適用できます。

フィルター・プロセスでは、ブリッジング時にパケットは処理されるか、フィルターされるか、またはタグ付けされます。アクションは、次のとおりです。

- **処理** - パケットは、影響を受けずにブリッジを通過することを許されます。
- **フィルター** - パケットは、ブリッジを通過することを許されません。
- **タグ付け** - パケットは、ブリッジを通過することを許されますが、構成可能パラメーターに基づいて 1 ～ 64 の範囲の番号でマーク付けされます。

MAC フィルターは、次の 3 つのオブジェクトから構成されます。

1. フィルター項目 - パケット内のアドレス・フィールドまたは任意のウィンドウのデータに適用される 1 つの規則です。この規則を適用した結果は、真 (一致する) または偽 (一致しない) のいずれかの状態です。
2. フィルター・リスト - 1 つまたは複数のフィルター項目のリストが入っています。
3. フィルター - 1 組のフィルター・リストが入っています。

MAC フィルターと DLSw トラフィック

MAC フィルターを実現することにより、DLSw ネットワークの着信 LLC トラフィックをフィルター処理することができます。

LLC に対するフィルターを設定するときは、*Bridge Net* 番号を、そのフィルターのインターフェース番号として使用します。 Bridge Net 番号は、ルーターに構成したインターフェースの数に 2 を加算して決めます。インターフェースのリストを見たい場合は—hConfig> プロンプトで **list devices** コマンドを入力するか、または + プロンプトで **configuration** を入力します。

次の例では、Bridge Net 番号は 7 です。

```
Ifc 0 Ethernet                      CSR  81600, CSR2  80C00, vector 94
Ifc 1 WAN X.25                      CSR  81620, CSR2  80D00, vector 93
Ifc 2 WAN X.25                      CSR  81640, CSR2  80E00, vector 92
Ifc 3 WAN PPP                       CSR 381620, CSR2 380D00, vector 125
Ifc 4 WAN Frame Relay               CSR 381640, CSR2 380E00, vector 124
Ifc 5 Token Ring                    CSR 600000, vector 95
```

たとえば、この Bridge Net に対してフィルターを設定した場合、ルーターは除外フィルターに一致するフレームを廃棄しません。代わりに、これらのフレームをブリッジに転送します。

MAC フィルター・パラメーター

フィルターを作成するときには、次のパラメーターの一部または全部を指定することができます。

- 発信元 MAC アドレスまたは宛先 MAC アドレス
- パケット内の照合データ
- フィルターに掛けるパケットのフィールドに適用されるマスク
- インターフェース番号
- 入出力指定
- 組み込み/除外/タグ指定
- タグ値 (タグ指定されている場合)

フィルター項目パラメーター

次のパラメーターは、アドレス・フィルター項目 (address-filter-item) を構成するのに使用されます。

- アドレス・タイプ: SOURCE または DESTINATION
- タグ: *tag-value*
- アドレス・マスク: *hex-mask*

各フィルター項目 (filter-item) は、パケット内のタイプと照合されるアドレス・タイプ (SOURCE または DESTINATION のいずれか) を指定します。

アドレス・マスクは、16 進法で入力される数字の列で、パケットのアドレスと比較するのに使用されます。マスクは、指定された MAC アドレスと比較する前に、パケットの SOURCE または DESTINATION MAC アドレスに適用されます。

アドレス・マスクは、MAC アドレスと長さが等しいことが必要であり、指定の MAC アドレスと等しいかどうかを比較する前に MAC アドレス内のバイトとの論理積を取るバイトを指定します。マスクが指定されていない場合は、オール 1 と想定されます。

フィルター・リスト・パラメーター

次のパラメーターは、フィルター・リスト (filter-list) を構成するのに使用されます。

- 名前: an *ASCII-string*
- フィルター項目リスト: *filter-item 1 . . . filter-item n*
- アクション: INCLUDE、EXCLUDE、TAG(*n*)

フィルター・リストは、1 つまたは複数のフィルター項目で構成されます。各フィルター・リストには、固有の名前が与えられます。

パケットにフィルター・リストを適用するということは、リストに追加された順序で各フィルター項目を比較することを表します。リスト内のいずれかのフィルター項目が TRUE 条件を戻した場合、フィルター・リストはそれに指定されているアクションを戻します。

フィルター・パラメーター

次のパラメーターは、フィルターを構成するのに使用されます。

- フィルター・リスト名: *ASCII-string 1 . . . ASCII-string n*
- インターフェース番号: *IFC-number*
- ポート方向: INPUT または OUTPUT
- デフォルト・アクション: INCLUDE、EXCLUDE、または TAG
- デフォルト・タグ: *tag-value*

フィルターの構成は、1 組のフィルター・リスト名をインターフェース番号に対応付け、INPUT または OUTPUT を指定することによって行います。フィルターをパケットに適用するということは、対応付けられたフィルター・リストのそれぞれを、指定された番号のインターフェースで受信 (INPUT) または送信 (OUTPUT) されたパケットに適用することを意味しています。

フィルターがパケットを INCLUDE 条件と評価した場合、そのパケットは転送されます。フィルターがパケットを EXCLUDE 条件と評価した場合、そのパケットは廃棄されます。フィルターが TAG 条件と評価した場合、対象のパケットはタグを付けて転送されます。

各フィルターの追加パラメーターとして、デフォルト・アクションがあります。これは、フィルター・リストのすべてが一致しなかった結果として取られる処置です。このデフォルト値 INCLUDE ですが、 INCLUDE、EXCLUDE、または TAG のいずれに設定しても構いません。デフォルト・アクションが TAG の場合は、タグ値も指定します。

MAC フィルター・タグの使用

以下に、MAC フィルター・タグの使用法のいくつかをリストします。

- MAC アドレス・フィルターは、タグを使用して、帯域幅予約と MAC フィルター機能 (MCF) が共同で処理します。また、帯域幅予約を使用しているユーザーは、ブリッジ・ トラフィックなどにタグを割り当てることによって、それを分類することができます。
- タグ付けプロセスは、MAC フィルター構成コンソールでフィルター項目を作成し、それにタグを割り当てます。次に、このタグを使用して、このタグに関連したすべてのパケットを対象にした帯域幅クラスを設定します。タグ値は、現在は 1 〜 64 の範囲でなければなりません。
- MAC フィルター構成プロセスでタグ付きフィルターを作成したら、帯域幅予約 (BRS) **tag** 構成コマンドを使用して、MAC フィルター・タグ番号に BRS タグ名 (TAG1、TAG2、TAG3、TAG4、または TAG5) を割り当てます。次に、この BRS タグ名を BRS **assign** 構成コマンドで使用して、対応する MAC フィルターを、帯域幅トラフィック・クラスと優先順位に割り当てます。

- 最高 5 つのタグ付き MAC アドレスを、1 ～ 5 の値に設定できます。 TAG1 が最初に探索され、次に TAG2 という具合で、TAG5 まで続けられます。

タグによって、IP トンネルの 『グループ』 を参照するすることもできます。 MAC アドレス・フィルターのタグ付け機能を使用して、パケットを特定のグループに割り当てることによって、IP トンネルのエンドポイントを任意の数のグループに所属させることができます。

第56章 MAC フィルターの構成および監視

この章では、MAC フィルターの構成および監視プロンプトにアクセスする方法、および利用可能なコマンドの使用法について説明します。本章には、以下の節が含まれています。

MAC フィルター構成プロンプトへのアクセス

MAC フィルター構成コマンドにアクセスするには、CONFIG プロセスから **feature** コマンドを使用します。 **feature** コマンドを使用すると、プロトコルおよびネットワーク・インターフェースの構成プロセスの外部の特定機能の構成コマンドにアクセスできます。

feature コマンドの後に疑問符を入力すると、使用しているソフトウェア・リリースで利用可能な機能のリストを入手することができます。たとえば、次のように入力します。

```
Config> feature ?
WRS
BRS
MCF
Feature name or number [MCF]?
```

MAC フィルター構成プロンプトにアクセスするには、**feature** コマンドに続けて *feature number* (3) または *short name* (MCF) を入力します。たとえば、次のように入力します。

```
Config> feature mcf
MAC Filtering user configuration
Filter config>
```

MAC フィルター構成プロンプトにアクセスしたら、特定の構成コマンドの入力を開始することができます。 MAC フィルター構成プロンプトから **exit** コマンドを入力すれば、いつでも CONFIG プロンプトに戻ることができます。

MAC フィルター構成コマンド

この節では、MAC フィルター構成コマンドの要約を示します。これらのコマンドは `Filter config>` プロンプトで入力します。

以下のコマンドを使用して、MAC フィルター機能を構成します。

表 89. MAC フィルター構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Attach	フィルター・リストをフィルターに追加します。

表 89. MAC フィルター構成コマンドの要約 (続き)

コマンド	機能
Create	フィルター・リスト、あるいは INPUT または OUTPUT フィルターを作成します。
Default	指定されたデフォルト・アクションを EXCLUDE、INCLUDE、または TAG に設定します。
Delete	フィルター・リストに関連するすべての情報を除去します。また、create filter コマンドを使用して作成されたフィルターも削除します。
Detach	フィルター・リストをフィルターから除去します。
Disable	MAC フィルター全体を使用不可にするか、または特定のフィルターを使用不可にします。
Enable	MAC フィルター全体を使用可能にするか、または特定のフィルターを使用可能にします。
List	ユーザーによって構成されたすべてのフィルター・リストおよびフィルターの要約をリストします。また、このフィルターに追加されたフィルター・リストのリスト、およびフィルターに関するすべての後続情報も生成します。
Move	指定のフィルターに追加されたフィルター・リストを配列し直します。
Reinit	ルーターの残りの部分に影響を与えずに、更新された構成から MAC フィルター・システム全体を再初期化します。
Set-Cache	フィルターのキャッシュ・サイズを変更します。
Update	特定のフィルター・リストの情報を追加または削除します。該当するサブコマンドのメニューが表示されます。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Attach

attach コマンドは、フィルター・リストをフィルターに追加するのに使用します。

フィルターの構成は、1 組のフィルター・リストをインターフェース番号に関連付けることによって行います。フィルター・リストは、1 つまたは複数のフィルター項目で構成されます。

構文:

attach *filter-list-name filter-number*

Create

create コマンドは、フィルター・リスト、あるいは INPUT または OUTPUT フィルターを作成するのに使用します。

構文:

create list *filter-list-name*

filter [input or output] *interface-number*

list *filter-list-name*

フィルター・リストを作成します。リストには、ユーザーが選択した最大 16 文字の固有の文字列 (Filter-list-name) の名前を付けます。この名前は、作成しているフィルター・リストを識別するのに使用します。また、この名前は、そのフィルター・リストに関連した他のコマンドでも使用されます。

filter [input or output] *interface-number*
フィルターを作成し、それをインターフェース番号で指定されたインターフェース上の INPUT または OUTPUT 方向に対応するネットワークに置きます。デフォルトでは、このフィルターはフィルター項目を付加せずに作成され、デフォルト・アクションは INCLUDE であり、ENABLED にされます。

Default

default コマンドは、指定されたフィルター番号を持つフィルターのデフォルト・アクションを EXCLUDE、INCLUDE、または TAG に設定するのに使用します。

構文:

default exclude *filter-number*
include *filter-number*
tag *tag-number filter-number*

exclude *filter-number*
指定されたフィルター番号のフィルターのデフォルト・アクションを EXCLUDE に設定します。

include *filter-number*
指定されたフィルター番号のフィルターのデフォルト・アクションを INCLUDE に設定します。

tag *tag-number filter-number*
指定されたフィルター番号のフィルターのデフォルト・アクションを TAG に設定し、関連のタグ値をタグ番号に設定します。

Delete

delete コマンドは、フィルター・リストに関連するすべての情報を除去し、割り当てられた名前を新規フィルター・リストの名前として解放するのに使用します。ユーザーがすでに作成したフィルターにフィルター・リストが付加されている場合、このコマンドは何も削除せずに、コンソールにエラー・メッセージを表示します。また、このリストに属するすべてのフィルター項目も削除されます。

create filter コマンドを使用して作成されたフィルターも、このコマンドで削除されます。

構文:

delete list *filter-list*
filter *filter-number*

list *filter-list*
フィルター・リストに関連するすべての情報を除去し、割り当てられた文字列を新規フィルター・リストの名前として解放します。フィルター・リストは、以前に **create list** コマンドで入力された文字列でなければなりません。

ユーザーがすでに作成したフィルターにフィルター・リストが付加されている場合、このコマンドは何も削除せずに、コンソールにエラー・メッセージを表示します。このコマンドが使用されると、このリストに属しているすべてのフィルター項目も削除されます。

filter *filter-number*
create filter コマンドを使用して作成されたフィルターを削除します。

Detach

detach コマンドは、フィルター・リスト名 (filter-list パラメーター) をフィルター (filter-number パラメーター) から削除するのに使用します。

構文:

detach *filter-list-name filter-number*

Disable

disable コマンドは、MAC フィルター全体を使用不可にするか、または特定のフィルターを使用不可にするのに使用します。

構文:

disable all

filter *filter-number*

all MAC フィルター全体を使用不可にします。ただし、前に使用可能にされたフィルターは、ENABLED として設定されたままになります。

filter *filter-number*
特定のフィルターを使用不可にします。 filter-number パラメーターは、**list filters** コマンドで表示された番号に対応します。

Enable

enable コマンドは、MAC フィルター全体を使用可能にするか、または特定のフィルターを使用可能にするのに使用します。

構文:

enable all

filter *filter-number*

all MAC フィルター全体を使用可能にします。ただし、フィルター自体は DISABLED に設定されたままになる場合もあります。

filter *filter-number*
特定のフィルターを使用可能にします。 filter-number パラメーターは、**list filters** コマンドで表示された番号に対応します。

List

list コマンドは、ユーザーによって構成されたすべてのフィルター・リストとフィルターの要約をリストするのに使用します。フィルターに付加されたすべてのフィルター・リストのリストは表示されません。その他に、次の情報が表示されます。

- フィルター・システムの状態 (ENABLE, DISABLE) が入っているリスト
- 構成済みフィルター・リスト・レコードの集合
- 個々の構成済みフィルター・レコード

さらに、各フィルターについて、次の情報が表示されます。

- フィルター番号
- インターフェース番号
- フィルターの方向 (INPUT、OUTPUT)
- フィルターの状態 (ENABLE、DISABLE)
- フィルターのデフォルト・アクション (TAG、INCLUDE、EXCLUDE)

また、このコマンドは、フィルターに付加されたフィルター・リストのリスト、およびフィルターに関するすべての後続情報も生成します。

構文:

list all
filter *filter-number*

all 構成されたすべてのフィルター・リストおよびフィルターの要約を表示します。

filter *filter-number*
指定されたフィルターに付加されたフィルター・リストのリスト、およびそのフィルターに関するすべての後続情報を生成します。

Move

move コマンドは、指定されたフィルター (filter-number パラメーターによって示される) に追加されたフィルター・リストを配列し直すのに使用します。 Filter-list-name1 によって示されるリストは、Filter-list-name2 によって示されるリストの直前に移動されます。

構文:

move *filter-list-name1 filter-list-name2 filter-number*

Reinit

reinit コマンドは、ルーターの残りの部分に影響を与えずに、更新された構成から MAC フィルター・システム全体を再初期化するのに使用します。

構文:

reinit

Set-Cache

set-cache コマンドは、デフォルトのキャッシュ・サイズ (16) を 4 〜 32768 の範囲の数に変更するのに使用します。

構文:

set-cache *cache-size filter-number*

Update

update コマンドは、特定のフィルター・リストを情報を追加または削除するのに使用します。必要なフィルター・リスト名を指定してこのコマンドを使用すると、その特定フィルター・リストの `Filter filter-list-name Config>` プロンプトが表示されます。こうして表示された新たなプロンプトから、指定されたリストの情報を変更することができます。

新たに表示されたプロンプト・レベルを使用して、フィルター・リストにフィルター項目を追加または削除します。フィルター・リストにフィルター項目を指定する順序は重要です。それによって、フィルター項目がパケットに適用される順序が決まるからです。

構文:

update *filter-list-name*

更新サブコマンド

この節では、MAC フィルター構成サブコマンドの要約を示します。これらのサブコマンドは `Filter filter-list-name config>` プロンプトで入力します。

表 90. 更新サブコマンドの要約

サブコマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	発信元または宛先 MAC アドレス・フィルターまたはウィンドウ・フィルターを追加します。フィルター項目をフィルター・リストに追加します。
Delete	フィルター項目をフィルター・リストから削除します。
List	ユーザーによって構成されたすべてのフィルター・リストとフィルターの要約をリストします。また、このフィルターに付加されたフィルター・リストのリスト、およびフィルターに関するすべての後続情報も生成します。
Move	指定されたフィルターに付加されたフィルター・リストを配列し直します。
Set-Action	INCLUDE、EXCLUDE、または TAG (タグ番号オプション付き) 条件を評価するように、フィルター項目を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

以下のサブコマンドを使用して、フィルター・リストを更新します。

Add

add サブコマンドは、フィルター項目をフィルター・リストに追加するのに使用します。このサブコマンドでは特別に、発信元または宛先 MAC アドレスと比較するための 16 進数を追加したり、あるいはパケット・データと比較するためのマスク付きの一連のウィンドウ・データを追加したりすることができます。

フィルター・リストにフィルター項目を指定する順序は重要です。それによって、フィルター項目がパケットに適用される順序が決まるからです。

add サブコマンドを使用するたびに、フィルター・リスト内にフィルター項目が作成されます。最初に作成されたフィルター項目にはフィルター項目番号 1 が割り当てられ、次の項目には番号 2 が割り当てられるというようになります。 **add** サブコマンドを正常に入力すると、ルーターは追加されたばかりのフィルター項目の番号を表示します。

最初の一致が見つかると、フィルター項目の適用は停止され、フィルター・リストの指定のアクションに基づいて、フィルター・リストは INCLUDE、EXCLUDE、または TAG に評価します。フィルター・リストのどのフィルター項目にも一致しない場合には、フィルターのデフォルト・アクション (INCLUDE、EXCLUDE、または TAG) が戻されます。

構文: add

source *hex-MAC-addr hex-Mask*

destination *hex-MAC-addr hex-Mask*

window MAC *offset-value hex-data hex-mask*

window INFO *offset-value hex-data hex-mask*

source *hex-MAC-addr hex-Mask*

発信元 MAC アドレスと比較するための 16 進数を追加します。***hex-MAC-addr*** は、最大 16 桁の偶数の 16 進数で、前に 0x を付けずに入力する必要があります。

hex-mask パラメーターは hex-MAC-address と同じ長さであることが必要であり、パケット内の指定された MAC アドレスと論理 AND されます。デフォルトの hex-mask 引き数は、すべてが 2 進数の 1 になります。

hex-MAC-addr パラメーターは、標準または非標準のビット配列で指定することができます。標準ビット配列は、単に 16 進数として指定します (たとえば、000003001234)。また、一連の 16 進数を 2 桁ずつハイフン (-) で区切って表すこともできます (たとえば、00-00-03-00-12-34)。

非標準ビット配列は、一連の 16 進数を 2 桁ずつコロン (:) で区切って指定します (たとえば、00:00:C9:09:66:49)。フィルター項目の MAC は、標準表記と非標準表記を区別するために、常にハイフン (-) またはコロン (:) のいずれかを使用して表示します。

destination *hex-MAC-addr hex-Mask*

照合の対象がパケットの発信元 MAC アドレスではなく、宛先 MAC アドレスであることを除いて、add source サブコマンドと同様に機能します。

window MAC *offset-value hex-data hex-mask*
マスク付き 16 進数をパケット・データに照合するための指定のオフセット (フレームの先頭から計算された) を使用して、スライディング・ウィンドウ・フィルター項目を追加します。

window INFO *offset-value hex-data hex-mask*
オフセットが情報フィールドの先頭から計算されることを除いて、**add window mac** コマンドと同様です。

Delete

delete サブコマンドは、フィルター項目をフィルター・リストから除去するのに使用します。フィルター項目を削除するには、その項目を追加したときに割り当てたフィルター項目番号を指定します。

delete サブコマンドが使用されたときに生じた番号順のすき間は埋められます。たとえば、フィルター項目 1、2、3、および 4 が存在し、フィルター項目 3 が削除された場合、フィルター項目 4 の番号が 3 に変更されます。

構文:

delete *filter-item-number*

List

list サブコマンドは、すべてのフィルター項目レコードのリストを印刷出力するのに使用します。各 MAC アドレス・フィルター項目に関する次の情報が表示されます。

- 標準形式および非標準形式の MAC アドレスとアドレス・マスク
- フィルター項目番号
- アドレス・タイプ (発信元または宛先)
- フィルター・リストのアクション

構文:

list canonical
noncanonical
mac-address canonical
mac-address noncanonical
window

canonical
フィルター・リスト内のすべてのフィルター項目レコードのリストを印刷出力して、項目番号、アドレス・タイプ (SRC、DST)、標準形式 MAC アドレス、および標準形式アドレス・マスクを表示します。フィルター・リストのアクションも示されます。

mac-address canonical
フィルター・リスト内のすべてのフィルター項目レコードのリストを印刷出

力して、項目番号、アドレス・タイプ (SRC、DST)、標準形式 MAC アドレス、および標準形式アドレス・マスクを表示します。また、フィルター・リストのアクションも示されます。

noncanonical
フィルター・リスト内のすべてのフィルター項目レコードのリストを印刷出力して、項目番号、アドレス・タイプ (SRC、DST)、非標準形式 MAC アドレス、および非標準形式アドレス・マスクを表示します。フィルター・リストのアクションも示されます。

mac-address noncanonical
フィルター・リスト内のすべてのフィルター項目レコードのリストを印刷出力して、項目番号、アドレス・タイプ (SRC、DST)、非標準形式 MAC アドレス、および非標準形式アドレス・マスクを表示します。フィルター・リストのアクションも示されます。

window
フィルター・リスト内のすべてのスライディング・ウィンドウ・フィルター項目レコードのリストを印刷出力して、項目番号、基底、オフセット、データ、およびマスクを表示します。フィルター・リストのアクションも示されます。

Move

move サブコマンドは、フィルター・リスト内のフィルター項目を配列し直します。番号が *filter-item-name1* によって指定されているフィルター項目は、*filter-item-name2* の直前に移動され、番号が付け直されます。

構文:

move *filter-item-name1 filter-item-name2*

Set-Action

set-action サブコマンドは、INCLUDE、EXCLUDE、または TAG (タグ番号オプション付き) 条件を評価するように、フィルター項目を設定することができます。フィルター・リストのフィルター項目の 1 つが、フィルター対象と見なされるパケットのコンテンツに一致している場合、フィルター・リストは指定された条件に評価します。デフォルト設定値は INCLUDE です。

構文:

set-action [INCLUDE or EXCLUDE or TAG] *tag-number*

MAC フィルター監視プロンプトへのアクセス

MAC フィルター監視コマンドにアクセスするには、GWCON プロセスから **feature** コマンドを入力します。 **feature** コマンドを使用すると、プロトコルおよびネットワーク・インターフェースの監視プロセスの外部の特定ルーター機能の監視コマンドにアクセスできます。

MAC フィルターの構成

feature コマンドの後に疑問符を入力すると、使用しているソフトウェア・リリースで利用可能な機能のリストを入手することができます。たとえば、次のように入力します。

```
+ feature ?
WRS
BRS
MCF
```

MAC フィルター監視プロンプトにアクセスするには、**feature** コマンドに続けて、機能番号 (3) または短縮名 (MCF) を入力します。たとえば、次のように入力します。

```
+ feature mcf
MAC Filtering user monitoring
Filter>
```

MAC フィルター監視プロンプトにアクセスしたら、特定の監視コマンドの入力を開始することができます。 MAC フィルター監視プロンプトから **exit** コマンドを入力すれば、いつでも GWCON プロンプトに戻ることができます。

MAC フィルター監視コマンド

この節では、MAC フィルター監視コマンドの要約を示します。これらのコマンドは `Filter>` プロンプトで入力します。

表 91. MAC フィルター監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Clear	list filter コマンドでリストされた "フィルター単位" 統計を消去します。
Disable	MAC フィルターをグローバルに使用不可にするか、または "フィルター単位" で使用不可にします。
Enable	MAC フィルターをグローバルに使用可能にするか、または "フィルター単位" で使用可能にします。
List	現在ルーターで実行されている各フィルターの統計および設定値の要約をリストします。
Reinit	ルーターの残りの部分に影響を与えずに、更新された構成から MAC フィルター・システム全体を再初期化します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

以下のコマンドを使用して、MAC フィルター機能を監視します。

Clear

clear コマンドは、フィルター統計を消去するのに使用します。

構文:

clear all

filter *filter-number*

all **list all** コマンドによってリストされた統計を消去します。

filter *filter-number*
list filter コマンドによってリストされた統計を消去します。

Disable

disable コマンドは、MAC フィルターをグローバルに使用不可にするのに使用します。このコマンドは、各フィルターを個別には使用不可にしません。

このコマンドは、フィルター番号によって指定されたフィルターも使用不可にします。このフィルターは、構成レコードを変更せずに、使用不可にされます。引き数が指定されていない場合、MAC フィルターはグローバルに使用不可にされます。

構文:

disable all
filter *filter-number*

all MAC フィルターをグローバルに使用不可にします。このコマンドは、各フィルターを個別には使用不可にしません。

filter ***filter-number***
フィルター番号によって指定されたフィルターを使用不可にします。このフィルターは、構成レコードを変更せずに、使用不可にされます。フィルター番号が指定されていない場合、MAC フィルターはグローバルに使用不可にされます。

Enable

enable コマンドは、MAC フィルターをグローバルに使用可能にするのに使用します。このコマンドは、各フィルターを個別には使用可能にしません。

このコマンドは、フィルター番号によって指定されたフィルターも使用可能にします。このフィルターは、構成レコードを変更せずに、使用可能にされます。引き数が指定されていない場合、MAC フィルターはグローバルに使用可能にされます。

構文:

enable all
filter *filter-number*

all MAC フィルターをグローバルに使用可能にします。このコマンドは、各フィルターを個別には使用可能にしません。

filter *filter-number*
フィルター番号によって指定されたフィルターを使用可能にします。このフィルターは、構成レコードを変更せずに、使用可能にされます。フィルター番号が指定されていない場合、MAC フィルターはグローバルに使用可能にされます。

List

list コマンドは、現在ルーターで実行されている各フィルターの統計および設定値の要約をリストするのに使用します。 **list all** コマンドを使用すると、各フィルターの以下の情報が表示されます。

- デフォルト・アクション
- キャッシュ・サイズ
- デフォルト・タグ
- 状態 (使用可能/使用不可)
- INCLUDE、EXCLUDE、または TAG としてフィルターされたパケットの数

さらに、指定のフィルターに対する **list filter** コマンドでは、次の情報も表示されます。

- list all コマンドによって表示されるすべての情報
- 現在このフィルターで実行されているすべてのフィルター・リスト。以下のものが含まれます。
  - リスト名
  - リスト・アクション
  - リスト・タグ
  - 各フィルター・リストによってフィルターされたパケットの数

構文:

list all

filter *filter-number*

all 現在ルーターで実行されている各フィルターの統計および設定値をリストします。

filter *filter-number*
各フィルターの統計および設定値に加えて、現在このフィルターで実行されているすべてのフィルター・リストの統計および設定値を生成します。

Reinit

reinit コマンドは、ルーターの残りの部分に影響を与えずに、更新された構成から MAC フィルター・システム全体を再初期化するのに使用します。

構文:

reinit

第57章 WAN 復元の使用

本章には、以下の節が含まれています。

WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの概説

WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローは、機能が似ているので混同する可能性があります。ここでは、いずれの機能がユーザーにとって便利であるかを判断し、それを構成するのに必要な情報を見つけるのに役立つ事柄を概説します。

3 つの機能のすべての構成コマンドを、「WAN 復元の構成」の章に収めてあります。WAN 再ルートおよびダイヤル・オン・オーバーフローに関する追加情報は、787ページの『第59章 WAN 再ルート機能』 を参照してください。

WAN 復元

WAN 復元は、最も基本的な機能です。 WAN 復元を使用する場合は、1 次リンクと 2 次リンクを構成します。 1 次リンクに障害が起きた場合、2 次リンクがスタートし、1 次の特性を引き継ぎます。 2 次リンクは 1 次リンクからのプロトコル定義を使用するので、2 次リンクにプロトコル定義を構成する必要はありません。

WAN 復元の場合:

- 1 次リンクと 2 次リンクが組みになっています。
- 1 つの 1 次リンクのみが特定の 2 次リンクを使用するように構成できます。
- 2 次リンクではプロトコル定義 (たとえば、プロトコル・アドレス) を構成しません。
- 1 次リンクは PPP シリアル・インターフェースでなければなりません。PPP ダイヤル回線インターフェースは使用できません。
- 2 次リンクは、PPP ダイヤル回線またはマルチリンク PPP インターフェースでなければなりません。
- **enable wrs** コマンドを使用して、WRS 機能を使用可能にする必要があります。
- **enable secondary-circuit** コマンドを使用して、1 次/2 次の組みを使用可能にする必要があります。

注: 1 次リンクに BRS が構成されており、その 1 次リンクが WAN 復元の 1 次/2 次の組みの片方である場合、2 次リンクにも BRS を構成する必要があります。通常は、WAN 復元が構成されている場合には、2 次リンクは 1 次リンクと同じ

機能を引き継ぎます。しかし BRS については、これは該当しません。そのため、BRS は 1 次リンクと 2 次リンクの両方で構成する必要があります。

WAN 再ルート

WAN 再ルートは、より拡張された機能です。 WAN 再ルートを使用する場合は、1 次リンクと代替リンクを構成します。 1 次リンクに障害が起きた場合、代替リンクがスタートします。ルーティング・プロトコル (たとえば、RIP または OSPF) は、新たに利用可能になったリンクを検出し、パケットの転送に使用されるルートを調整します。

WAN 再ルートの場合:

- 1 次リンクと代替リンクが組みになっています。
- 複数の 1 次リンクが同じ代替リンクを使用するように構成できます。
- 代替リンクでプロトコル定義を構成する必要があります。
- 1 次リンクには、ルート可能プロトコル (たとえば、IP、IPX) を構成できる任意のリンクを使用できます。たとえば、1 次リンクには、LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線を使用することができます。 1 次リンクに使用できないインターフェース・タイプの例としては、SDLC シリアル・インターフェース、SRLY シリアル・インターフェース、および V.25bis や ISDN のような基本ネットがあります。
- 代替リンクは、ルート可能プロトコル (たとえば、IP、IPX) を構成できる任意のリンクを使用することができ、代替リンクのデータ・リンク・タイプは、1 次リンクのデータ・リンク・タイプと一致している必要はありません。たとえば、代替リンクには、LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線などを使用できます。代替リンクに使用できないインターフェース・タイプの例としては、SDLC シリアル・インターフェース、SRLY シリアル・インターフェース、および V.25bis や ISDN のような基本ネットがあります。
- 1 次リンクがダイヤル回線である場合は、代替リンクは、ダイヤル・オンデマンド・ダイヤル回線 (ダイヤル回線で 'set idle 0' を構成する必要がある) であってはなりません。 I.430、I.431、およびチャネル化 T1/E1 ダイヤル回線は、暗黙的に固定されているので、WRS 1 次として使用できます。

  注: I.430/I.431 およびチャネル化 T1/E1 ダイヤル回線は、明示的に構成することなく、WRS 1 次として使用することができます。
- 代替リンクは、ダイヤル・オンデマンド・ダイヤル回線 (ダイヤル回線で 'set idle 0' を構成する必要がある) であってはなりません。
- **enable wrs** コマンドを使用して、WRS 機能を使用可能にする必要があります。
- **enable alternate-circuit** コマンドを使用して、1 次/代替の組みを使用可能にする必要があります。
- オプションで、1 次リンクへの復帰を制御するための安定化時間および復帰開始時刻と終了時刻も構成できます。
- 代替リンクが X.25 の場合、WAN 再ルートを使用可能にしたルーターの X.25 インターフェースを構成するときは **national-personality set disconnect-procedure**

active コマンドを使用し、他方のルーターの X.25 インターフェースを構成するときは **national-personality set disconnect-procedure passive** コマンドを使用することが必要です。

ダイヤル・オン・オーバーフロー

ダイヤル・オン・オーバーフローは WAN 再ルートに似ていますが、 1 次リンクに障害が起きなくても、代替リンクをスタートさせることができます。 1 次リンクの使用状況を監視し、限界値を超えると、代替リンクがスタートします。また、すべてのプロトコルが代替リンクで起動されるわけではありません。 IP だけが代替リンクで起動され、その他のプロトコルは、1 次リンクがダウンしない限り、引き続き 1 次リンクを使用します。

1 次リンクがダウンすると、WAN 再ルートが引き継ぎ、代替インターフェース上に構成されているプロトコルが、代替インターフェース上のルートを検出し、そのルートを使用し始めることができます。

ダイヤル・オン・オーバーフローの場合:

- ダイヤル・オン・オーバーフローは、WAN 再ルートの組み合わせである 1 次/代替の組みを使用します。
- ダイヤル・オン・オーバーフローを使用するためには、WAN 再ルートの組みを構成する必要があり、WAN 再ルート構成のすべての制約が適用されます。
- ダイヤル・オン・オーバーフローに使用される WAN 再ルートの組みの 1 次リンクは、フレーム・リレーでなければなりません。
- ダイヤル・オン・オーバーフローを使用するためには、OSPF ルーティング・プロトコルを使用することが必要です。
- **enable dial-on-overflow** コマンドを使用して、追加限界値と廃棄限界値、帯域幅監視間隔、および最小代替アップ・タイムを構成する必要があります。
- 安定化時間 (Stabilization time)、復帰開始時刻 (start-time-of-day-revert-back) および復帰停止時刻 (stop-time-of-day-revert-back) は、ダイヤル・オン・オーバーフローの動作には影響を与えません。

WAN 再ルートについての詳細は、787ページの『第59章 WAN 再ルート機能』 を参照してください。

始める前に

WAN 復元を構成する前に、以下の用意が必要です。

1. 1 次シリアル・インターフェース (専用回線) が PPP 用に構成されている。ルーター上の任意のシリアル・インターフェースを使用できます。
2. 対応するダイヤル回線をもつインターフェースがルーター上に構成されている。ISDN インターフェース、V.25bis インターフェース、または V.34 インターフェースを基本ネットとして使用することができます。

3. 2 次ダイヤル回線が、1 次インターフェースがダウンしたときにダイヤルするように構成されている。ダイヤル回線をこのように構成するには、ダイヤル Circuit Config> プロンプトで **set idle** コマンドを使用して、アイドル・タイマーをゼロに設定します。
4. リンクの一方の端の 2 次ダイヤル回線が発信専用に構成されている。 Circuit Config> プロンプトで **set calls outbound** コマンドを使用して構成します。

   注: 2 次インターフェースにはプロトコル・アドレスを構成しないでください。 2 次リンク (ダイヤル回線) がアクティブになると、1 次インターフェースのプロトコル割り当てが使用されます。
5. リンクの他方の端の 2 次ダイヤル回線が受信専用に構成されている。 Circuit Config> プロンプトで **set calls inbound** コマンドを使用して構成します。

WAN 復元の構成手順

この節では、WAN 復元を構成するのに必要な手順について説明します。構成を開始する前に、Config> プロンプトで **list device** コマンドを使用して、種々の装置のインターフェース番号をリストしてください。

以下のステップに従って、ルーター上の WAN 復元を構成します。

1. Config> プロンプトで **feature wrs** コマンドを入力して、WRS Config> プロンプトを表示する。たとえば、次のように入力します。

   ```
   Config>feature wrs
   WAN Restoral user configuration
   WRS Config>
   ```
2. 1 次インターフェースに 2 次ダイヤル回線を割り当てる。このダイヤル回線は、1 次インターフェースをバックアップします。たとえば、次のように入力します。

   ```
   WRS Config>add secondary-circuit
   Secondary interface number  [0]? 3
   Primary interface number  [0]? 1
   ```
3. 追加した 2 次ダイヤル回線上の WAN 復元を使用可能にする。たとえば、次のように入力します。

   ```
   WRS Config>enable secondary-circuit
   Secondary interface number  [0]? 3
   ```
4. ルーター上の WAN 復元をグローバルに使用可能にする。たとえば、次のように入力します。

   ```
   WRS Config>enable wrs
   ```
5. ルーターをリスタートして、構成変更を有効にする。

2 次ダイヤル回線の構成

ダイヤル回線を構成するには、以下の手順で行います。

1. ダイヤル回線インターフェース番号を調べる。これを行うには、次のように入力します。

   ```
   Config> list device
   ```

   PPP ダイヤル回線インターフェースがリストされない場合は、次のように入力して、ダイヤル回線インターフェースを追加します。

```
Config> add device dial-circuit

Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
```

2. Config> プロンプトから次のように入力して、2 次インターフェース (ダイヤル回線) が1 次インターフェース (PPP) と同じデータ・リンク・タイプを持つように構成する。

```
Config> set data PPP
Interface Number [0]? 3
```

3. **network** *interface#* を入力して、ダイヤル回線構成プロンプト (Circuit Config>) にアクセスする。

```
Config> network 3
```

4. ダイヤル回線の基本ネット・インターフェースを選択する。基本ネットは V.25bis、ISDN、または V.34 です。

```
Circuit Config> set net 2
```

5. ダイヤル回線アイドル・タイマーを 0 (0 = 固定) に設定するために、次のように入力する。

```
Circuit Config> set idle 0
```

6. バックアップ・コネクションの一方の端 (たとえば、ルーター A) を受信用に設定するために、次のように入力する。

```
Circuit Config> set calls inbound
```

7. バックアップ・コネクションの他方の端 (たとえば、ルーター B) を発信用に設定するために、次のように入力する。

```
Circuit Config> set calls outbound
```

注:

1. **set calls both** コマンドは使用しないでください。これらを個別に設定することにより、着信と発信の接続試行が衝突するのを防止できます。
2. ダイヤル回線には、転送プロトコル (たとえば、IP、IPX など) アドレスは構成しないでください。 2 次インターフェース (ダイヤル回線) がアクティブになると、1 次インターフェースのプロトコル割り当てが使用されます。
3. ISDN の構成方法については、619ページの『第45章 ISDN インターフェースの使用』 を参照してください。
4. V.25bis の構成方法については、581ページの『第41章 V.25bis ネットワーク・インターフェースの使用』 を参照してください。
5. V.34 の構成方法については、601ページの『第43章 V.34 ネットワーク・インターフェースの使用』を参照してください。

第58章 WAN 復元の構成および監視

この章では、WAN 復元の構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの構成コマンド

WAN 復元構成コマンドを用いて、WAN 復元インターフェース構成を作成または変更することができます。この節では、WAN 復元構成コマンドの要約を示し、個々のコマンドについて説明します。

表92 は、WAN 復元構成コマンドとその機能をリストしています。これらのコマンドは WRS Config> プロンプトで入力します。 WRS Config> にアクセスするには、Config> プロンプトで **feature wrs** と入力します。

表 92. WAN 復元構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	1 次から 2 次へ (WAN 復元の場合) または 1 次から代替へ (WAN 再ルートの場合) のマッピングを追加します。
Disable	WRS、個々の 2 次回線マッピング、または代替回線マッピングを使用不可にします。
Enable	WRS、個々の 2 次回線マッピング、または代替回線マッピングを使用可能にします。
List	現行の復元構成を表示します。
Remove	add によって作成された 1 次から 2 次へのマッピングまたは 1 次から代替へのマッピングを除去します。
Set	安定化 (stabilization) タイマーおよび復帰時刻 (time-of-day-revert-back) タイマーの値を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、2 次または代替ダイヤル回線、あるいは 1 次シリアル・リンクの専用リンク・インターフェースを識別するのに使用します。

構文:

add alternate-circuit

secondary-circuit

alternate-circuit

add alternate-circuit コマンドは、WAN 再ルートのために、代替インター

フェースを 1 次インターフェースに結合します。複数の 1 次リンクを単一の代替インターフェースに割り当てることができます。代替リンク・タイプは、1 次リンク・タイプと同じである必要はありません (たとえば、代替リンク・タイプが PPP ダイヤル回線で、1 次リンク・タイプがフレーム・リレー専用回線であっても構いません)。

例:

```
WRS Config>add alt
Alternate interface number  [0]? 6
Primary interface number  [0]? 1
```

Alternate interface number
これは、以前に代替インターフェースに割り当てたインターフェース番号です。任意の LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線を、代替インターフェースとして使用できます。デフォルトは 0 です。

Primary interface number
これは、装置が追加されたときに、割り当て済みの1次インターフェースのインターフェース番号です。 1 次インターフェースは、以前に定義された任意の LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線を使用できます。デフォルトは 0 です。

secondary-circuit

add secondary-circuit コマンドは、WAN 復元のために、2 次インターフェースを 1 次インターフェースに結合します。両方のインターフェースとも、以前に構成されていることが必要です。 1 つの 2 次インターフェースを 1 次に (または、その逆に) 割り当てることしかできません。

例:

```
WRS Config>add secondary-circuit
Secondary interface number  [0]? 4
Primary interface number  [0]? 1
```

Secondary interface number
これは、以前に装置が追加されたときに、2 次インターフェースに割り当てられたダイヤル回線インターフェース番号です。任意の PPP ダイヤル回線またはマルチリンク PPP インターフェースを、2 次インターフェースとして使用できます。デフォルトは 0 です。

Primary interface number
これは、以前に装置が追加されたときに割り当てられた 1 次インターフェースのインターフェース番号です。 1 次インターフェースには、PPP を実行する任意の定義済み専用回線を使用できます。デフォルトは 0 です。

Disable

disable コマンドは、WAN 復元機能、WAN 復元における 1 次/2 次の組み合わせ、WAN 再ルートにおける 1 次/代替の組み合わせ、または 1 次/代替の組みに対するダイヤル・オン・オーバーフローを使用不可にするのに使用します。

構文:

disable alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit *interface#*

WAN 再ルートの 1 次/代替の組み合わせを使用不可にします。

例:

```
WRS Config> disable alternate-circuit
Alternate interface number  [0]? 6
```

Alternate interface number

これは、以前に **add alternate-circuit** コマンドを使用して構成された代替インターフェースの番号です。デフォルトは 0 です。

dial-on-overflow *alt-intfc#*

指定された代替リンクを使用するすべての 1 次/代替の組みに対するダイヤル・オン・オーバーフローを使用不可にします。

例:

```
WRS Config> disable dial-on-overflow
alternate interface number  [0]? 6
```

Alternate interface number

これは、以前に **add alternate-circuit** コマンドを使用して構成された代替インターフェースの番号です。デフォルトは 0 です。

secondary-circuit *interface#*

WRS コンソールから次の **enable secondary-circuit** コマンドが出されるまで、関連の 2 次インターフェースによる特定の 1 次インターフェースの復元を使用不可にします。両方のインターフェースとも構成済みであり、WRS 構成内で相互が結合されていることが必要です。

例:

```
WRS Config> disable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number

これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

wrs ルーター上の WAN 復元機能をグローバルに使用不可にします。これは、WAN 再ルートおよびダイヤル・オン・オーバーフローも使用不可にされることを意味しています。

Enable

enable コマンドは、WAN 復元機能、WAN 復元における 1 次/2 次の組み合わせ、WAN 再ルートにおける 1 次/代替の組み合わせ、または 1 次/代替の組みに対するダイヤル・オン・オーバーフローを使用可能にするのに使用します。

構文:

enable alternate-circuit

dial-on-overflow

secondary-circuit

wrs

alternate-circuit *interface#*

代替回線を使用可能にします。

例:

```
WRS Config>enable alternate-circuit
Alternate interface number  [0]? 6
```

Alternate interface number

これは、以前に **add alternate-circuit** コマンドを使用して構成された代替インターフェースの番号です。デフォルトは 0 です。

dial-on-overflow

ダイヤル・オン・オーバーフローを使用可能にし、ダイヤル・オン・オーバーフローの動作方法を制御するパラメーターを設定できるようにします。

例:

```
WRS>enable dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate
interface.
Primary interface number  ]0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!
```

Primary interface number

これは、ダイヤル・オン・オーバーフローを使用可能にする 1 次インターフェースのインターフェース番号です。デフォルトは 0 です。

add-threshold

帯域幅の追加のために代替インターフェースを起動する時期を決めます。この値は、1 次インターフェースに構成された回線速度の比率として表すことが必要です。デフォルトは 90% です。

drop-threshold

帯域幅の追加のための代替インターフェースが不要になる時期を決めます。この値は、1 次インターフェースに構成された回線速度の比率として表すことが必要です。デフォルトは 60% です。

bandwidth monitoring interval

add-threshold および *drop-threshold* のために 1 次インターフェースの帯域幅を監視する頻度を決めます。デフォルトは 15 秒です。

Minimum time to keep alternate up

この時間枠には、ローカル・ルーター上の IP トラフィックを代替インターフェースに再ルートするときに、ルーターが新規ルートを確立できる十分な時間を含める必要があります。デフォルトは 5 分です。

secondary-circuit *interface#*

指定された 2 次リンクによる 1 次リンクの復元を使用可能にします。

例:

```
WRS Config>enable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number
これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

wrs ルーター上の WAN 復元の機能を使用可能にします。これは、WAN 再ルートおよびダイヤル・オン・オーバーフローも構成されている場合には、それらも使用可能になることを意味しています。

List

list コマンドは、その機能のグローバル構成情報を表示したり、WAN 復元の 1 次/2 次の組み、WAN 再ルートの 1 次/代替の組み、およびダイヤル・オン・オーバーフローに関する構成情報を表示するのに使用します。

構文:

list

例:

```
 WRS Config>list
 WAN Restoral is enabled.
 Default Stabilization Time:       0 seconds
 Default First Stabilization Time: 0 seconds

                                                  Secondary
Primary Interface          Secondary Interface    Enabled
 -----------------------  ----------------------  --------
  4 - WAN PPP              7 - PPP Dial Circuit       No
                                          Alt.     1st  Subseq TOD Revert Back
 Primary Interface  Alternate Interface  Enabled  Stab  Stab  Start    Stop
 -----------------  ---------------------  -------  ----  ----  -------  -------

  1 - WAN Frame Re   2 - WAN Frame Relay      Yes    dflt  dflt  Not Set  Not Set


 Dial-on-overflow is enabled.
 Primary    add-       drop-      test       minimum
 Interface  threshold  threshold  interval   alt up time
 ---------  ---------  ---------  ---------  -----------
      1         29%        20%      15 sec.   300 sec.
```

Remove

remove コマンドは、代替インターフェースあるいは 2 次 (バックアップ) インターフェースの 1 次インターフェースへのマッピングを削除するのに使用します。

構文:

remove alternate-circuit
secondary-circuit

alternate-circuit *alternate-interface# primary-interface#*
WAN 再ルートの代替 (バックアップ) インターフェースの 1 次インターフェースへのマッピングを除去します。両方のインターフェースとも割り当て済みであり、 **add alternate-circuit** コマンドを使用して相互が結合されていることが必要です。

Alternate-interface#

これは、以前に **add alternate-circuit** コマンドを使用して構成された代替インターフェースの番号です。デフォルトは 0 です。

Primary-interface#

これは、除去される代替に以前に結合された 1 次インターフェースのインターフェース番号です。デフォルトは 0 です。

例:

```
WRS Config> remove alternate-circuit
Alternate interface number  [0]? 3
Primary interface number  [0]? 1
```

secondary-circuit *secondary-interface# primary-interface#*

WAN 復元の 2 次 (バックアップ) インターフェースの 1 次インターフェースへのマッピングを除去します。両方のインターフェースとも割り当て済みであり、 **add secondary-circuit** コマンドを使用して相互が結合されていることが必要です。

Secondary-interface#

これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

Primary-interface#

除去される 2 次インターフェースにバインド済みの、 1 次インターフェースのインターフェース番号です。デフォルトは 0 です。

例:

```
WRS Config> remove secondary-circuit
Secondary interface number  [0]? 3
Primary interface number  [0]? 1
```

Set

set コマンドは、WAN 再ルートのパラメーターを設定するのに使用します。

構文:

set ?

default

first-stabilization

stabilization

start-time-of-day-revert-back

stop-time-of-day-revert-back

default

set default コマンドは、安定化 (stabilization) 期間および最初の安定化 (first-stabilization) 期間が構成されていないリンクで使用されるデフォルト値を設定するのに使用します。

first-stabilization

最初の安定化時間 (first-stabilization time) が構成されていないリンクで使用されるデフォルトの最初の安定化時間の値を設定します。

```
WRS Config>set default first
Default first primary stabilization time (0 - 3600 seconds) [0]? 20
```

stabilization

安定化時間 (stabilization time) が構成されていないリンクで使用されるデフォルトの安定化時間の値を設定します。

```
WRS Config>set default stab
Default primary stabilization time (0 - 3600 seconds)  [0]? 30
```

first-stabilization

1 次リンクがアップにならない場合、この 1 次リンクのルーティングを代替リンクに切り替える前の、ルーター初期化の秒数を設定します。

例:

```
WRS Config>set first
Primary interface number  [0]? 1
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?
```

Primary interface number

これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

First primary stabilization time

この 1 次インターフェースの安定化時間。デフォルトは 1 です。

stabilization

1 次リンクがアップであることが最初に検出された後、ルーティングを 1 次に戻す前に必要な秒数を設定します。 1 次リンクがこの秒数だけアップ状態に保たれるまでは、ルーティングは代替リンクを介して継続されます。

例:

```
WRS Config>set first
Primary interface number  [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

これは、安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Primary stabilization time

1 次インターフェースの安定化時間。デフォルトは 1 です。

start-time-of-day-revert-back

ルーターが 1 次ルートに戻すことができる最も早い時刻。ルーターは、復帰開始時刻 (start-time-of-day-revert-back) と復帰停止時刻 (stop-time-of-day-revert-back) の間の任意の時刻に、1 次に戻すことができます。1 次への復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。 デフォルトは 0 です。

例:

```
WRS Config>set start
Primary interface number  [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number

これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Time-of-day-revert-back-window start

この時刻は、復帰ウィンドウの開始時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インター

フェースに戻すことができます。 1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。 デフォルトは 1 です。

stop-time-of-day-revert-back

この時刻は、復帰ウィンドウの終了時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに戻すことができます。 1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。 デフォルトは 1 です。

例:

```
WRS Config>set stop
Primary interface number  [0]? 1
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured) [0]?5
```

Primary interface number

これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Time-of-day-revert-back-window stop

この時刻は、復帰ウィンドウの終了時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに戻すことができます。 1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。デフォルトは 1 です。

WAN 復元インターフェース監視プロセスへのアクセス

WAN 復元インターフェース監視プロセスにアクセスするには、GWCON (+) プロンプトから、次のコマンドを入力します。

```
+ feature wrs
```

WAN 復元監視コマンド

WAN 復元 (WRS) 監視コマンドを用いて、WAN 復元の 1 次/2 次の組み、WAN 再ルートの 1 次/代替の組み、およびダイヤル・オン・オーバーフローの状態を監視することができます。監視インターフェースを通して行われた WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの動作状態の変更は、ルーターのリスタートを経ると維持されません。

WRS プロンプトにアクセスするには、GWCON (+) プロンプトで **feature wrs** と入力します。 表93 は、WRS コマンドとその機能をリストしており、後続の節で個々のコマンドについて説明しています。

表 93. WAN 復元監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Clear	**list** コマンドを使用して表示した監視統計を消去します。

表 93. WAN 復元監視コマンド (続き)

コマンド	機能
Disable	WRS を使用不可にするか、または個々の 2 次、代替、またはダイヤル・オン・オーバーフローを使用不可にします。
Enable	WRS を使用不可にするか、または個々の 2 次、代替、またはダイヤル・オン・オーバーフローを使用可能にします。
List	代替または 2 次回線の 1 つまたはすべてに関する監視情報を表示します。
Set	安定化 (stabilization) および復帰時刻タイマー (time-of-day-revert-back-timers) の値を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Clear

clear コマンドは、**list** コマンドを使用して表示された 、WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの統計を消去するのに使用します。

構文:

clear

注: このコマンドは *Longest restoral period* は消去しますが、*Most recent restoral period* は消去しません。画面の表示については、**list** コマンドの項に示されている例を参照してください。

Disable

disable コマンドは、WAN 復元機能を完全に使用不可にする、特定の 1 次インターフェースに対応する 2 次インターフェースによる復元を使用不可にする、代替インターフェースを使用不可にする、またはダイヤル・オン・オーバーフローを使用不可にするのに使用します。

構文:

disable alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit

WAN 再ルートの 1 次/代替の組みを使用不可にします。同じ代替を使用する複数の組みが存在することもあります。このコマンドは、指定された代替回線を使用するすべての組みを使用不可にします。

例:

```
WRS>disable alternate-circuit
Alternate circuit number  [0]? 6
```

Alternate circuit number

これは、代替回線の番号です。デフォルトは 0 です。

dial-on-overflow

指定された 1 次/代替の組みのダイヤル・オン・オーバーフローを、その組みに対する WAN 再ルートの使用可能/使用不可状態を変更せずに、使用不可にします。ダイヤル・オン・オーバーフローがルーティングを実行中の場合は、次の監視インターバルが満了した時点で終了されます。

secondary-circuit

特定の 1 次インターフェースに対応する 2 次インターフェースによる復元を、次の **restart**、**reload**、または **enable secondary-circuit** コマンドまで使用不可にします。両方のインターフェースとも構成済みであり、WRS 構成内で相互が結合されていることが必要です。

通常は、**talk 5** (GWCON) の **disable** コマンドによりインターフェースは非アクティブにされ、非アクティブのままになりますが、 WAN 復元の 2 次の場合は、そうではありません。 2 次インターフェースに適用される **disable** コマンドは、インターフェース自体は使用不可にしません。現行の呼だけを使用不可にします (つまり、アクティブの呼が切断されます)。 2 次回線を使用不可にするためには、WAN 復元監視プロンプトで **disable secondary-circuit** と入力し、トップ・レベルの GWCON プロンプトで 2 次インターフェースを使用不可にすることが必要です。

例:

```
WRS>disable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number

これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

wrs WRS を使用不可にすると、ルーター上の WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローが、次の **restart**、**reload**、または **enable WRS** コマンドまで使用不可になります。

Enable

enable コマンドは、WAN 復元インターフェースを使用可能にする、1 次リンクの 2 次回線による復元を使用可能にする、代替回線を使用可能にする、またはダイヤル・オン・オーバーフローを使用可能にするのに使用します。

構文:

enable alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit

指定された代替を使用するすべての組みに対して、WAN 再ルートの 1 次/代替の組み合わせを使用可能にします。

例:

```
WRS> enable alternate-circuit
Alternate circuit number  [0]? 3
```

Alternate circuit number
これは、代替回線のインターフェース番号です。デフォルトは 0 です。

dial-on-overflow
ダイヤル・オン・オーバーフローを使用可能にし、ダイヤル・オン・オーバーフローを制御するパラメーターを設定できるようにします。オプションで、ただちに IP プロトコルを代替に切り替える (追加限界値を超えたときのように) ことも可能です。

例:

```
WRS> dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate interface.
Primary interface number  [0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!

Do you want to switch IP traffic to the alternate now?(Yes or [No]):
WRS>
```

secondary-circuit
指定された 2 次リンクによる 1 次リンクの復元を使用可能にします。

例:

```
WRS> enable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number
これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

wrs ルーター上の WAN 復元の機能を使用可能にします。 WAN 復元、WAN 再ルート、またはダイヤル・オン・オーバーフローを行うためには、この機能を使用可能にすることが必要です。

Set

set コマンドは、WAN 再ルートのパラメーターを設定するのに使用します。

構文:

set ? default / first-stabilization / stabilization / start-time-of-day-revert-back / stop-time-of-day-revert-back

default
set default コマンドは、安定化 (stabilization) 期間および最初の安定化 (first-stabilization) 期間が構成されていないリンクで使用されるデフォルト値を設定するのに使用します。

例:

```
WRS Config>set default ?
FIRST-STABILIZATION
STABILIZATION
```

first-stabilization

最初の安定化時間 (first-stabilization time) が構成されていないリンクで使用されるデフォルトの最初の安定化時間の値を設定します。

```
WRS Config>set default first
Default first primary stabilization time (0 - 3600 seconds) [0]? 20
```

stabilization

安定化時間 (stabilization time) が構成されていないリンクで使用されるデフォルトの安定化時間の値を設定します。

```
WRS Config>set default stab
Default primary stabilization time (0 - 3600 seconds)  [0]? 30
```

first-stabilization

1 次リンクがアップにならない場合、この 1 次リンクのルーティングを代替リンクに切り替える前の、ルーター初期化の秒数を設定します。

例:

```
WRS Config>set first
Primary interface number  [0]? 1
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?
```

Primary interface number

これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

First primary stabilization time

この 1 次インターフェースの安定化時間。デフォルトは 1 です。

stabilization

1 次リンクがアップであることが最初に検出された後、ルーティングを 1 次に戻す前に必要な秒数を設定します。 1 次リンクがこの秒数だけアップ状態に保たれるまでは、ルーティングは代替リンクを介して継続されます。

例:

```
WRS Config>set first
Primary interface number  [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

これは、安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Primary stabilization time

1 次インターフェースの安定化時間。デフォルトは 1 です。

start-time-of-day-revert-back

ルーターが 1 次ルートに戻すことができる最も早い時刻。ルーターは、復帰開始時刻 (start-time-of-day-revert-back) と復帰停止時刻 (stop-time-of-day-revert-back) の間の任意の時刻に、1 次に戻すことができます。1 次への復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。 デフォルトは 0 です。

例:

```
WRS Config>set start
Primary interface number  [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number
これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Time-of-day-revert-back-window start
この時刻は、復帰ウィンドウの開始時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに戻すことができます。 1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。 デフォルトは 1 です。

stop-time-of-day-revert-back
この時刻は、復帰ウィンドウの終了時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに戻すことができます。 1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。 デフォルトは 1 です。

例:

```
WRS Config>set stop
Primary interface number  [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]? 5
```

Primary interface number
これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Time-of-day-revert-back-window stop
この時刻は、復帰ウィンドウの終了時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに戻すことができます。 1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。デフォルトは 1 です。

List

list コマンドは、WAN 復元の 1 次/2 次の組みの 1 つまたはすべて、あるいは WAN 再ルートの 1 次/代替の組みの 1 つまたはすべてに関する情報を表示するのに使用します。

構文:

list all
alternate-circuit
secondary-circuit
summary

all 各 2 次インターフェースについて、要約情報を表示し、続いて特定の情報を表示します。

例:

```
list all
WAN Restoral/Re-route is enabled with 2 circuits configured
    Total restoral attempts =          7 completions   =          7
    Total packets forwarded =         39
```

```
    Longest completed restoral period in hrs:min:sec     0:03:27

    Total overflow attempts =         20 completions   =         19
    Longest completed overflow period in hrs:min:sec     0:05:00

   Primary       Secondary    Restoral  Restoral   Current/Longest
Net Interface  Net Interface  Enabled    Active       Duration
-------------  -------------  --------  --------   --------------------
  4  PPP/0       7  PPP/1       No         No       00:03:27/ 00.06.00

                               Re-route/ Re-route/         Recent
   Primary       Alternate    Overflow  Overflow     Reroute/Overflow
Net Interface  Net Interface  Enabled    Active          Duration
-------------  -------------  --------  --------   --------------------
  1   FR/0       2   FR/1     Yes/Yes    No /No     00:00:56/ 00:05:00
```

Total restoral attempts
1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

Completions
復元の試みに成功した (2 次がアップになり、使用された) 回数

Total packets forwarded
2 次インターフェースを介して転送されたパケットの合計数。これは両方向の合計数で、restart または clear restoral-statistics コマンドが出されるまでの、すべての正常な復元期間における累計です。

Longest Completed Restoral Period
このフィールドは、現行の使用期間はカウントせずに、復元が動作していた最長時間を時間、分、秒数で表示します。

Total Overflow Attempts
オーバーフローが原因での試行回数

Completions
オーバーフローが原因での試行に成功した (2 次リンクがアップになり、使用された) 回数

Longest Completed Overflow Period
現行の使用時間はカウントせずに、1 つのオーバーフローが動作していた最長時間を時間、分、秒数で表示します。

Primary Net Interface
対応する2 次インターフェースによってバックアップされているインターフェース

Secondary Net Interface
対応する 1 次インターフェースをバックアップするのに使用されるダイヤル回線

Restoral Enabled
この 1 次インターフェースの復元が現在使用可能になっていることを示します。

Restoral Active
復元がアクティブかどうか (Yes または No) を示します。

Current/Longest Duration
現行の時間と、2 次ネット・インターフェースがアップであった最長時間を時間、分、秒数で表示します。

Primary Net Interface
対応する代替インターフェースによってバックアップされるインターフェース

Alternate Net Interface
対応する 1 次インターフェースのバックアップとして使用されるインターフェース

Re-route/Overflow Enabled
再ルートおよびオーバーフローが使用可能であるかどうか (Yes または No) を示します。

Re-route/Overflow Active
再ルートおよびオーバーフローがアクティブかどうか (Yes または No) を示します。

Recent Re-route Overflow Duration
代替ネットワーク・インターフェースの最新の再ルートおよびオーバーフローの時間数を、時間、分、秒数で示します。

Alternate-circuit
代替回線の合計数を提供します。監視オペレーターは、WAN 再ルートの状態、および各代替インターフェースと対応の 1 次マッピングに関する統計を検索することができます。

例:

```
WRS>li alt 7
Primary    1:FR/0 Frame Relay SCC Serial Line
Alternate  7:PPP/1 Point to Point V.25bis Dial Circuit
reroute Enabled, currently inactive
overflow Enabled, currently inactive
Primary first stabilization time: default (0 seconds)
Primary stabilization time: default (0 seconds)
Time-of-day revert back not configured: start = 0, stop = 0
Restored 0 times (0 attempts)
Overflow 0 times (0 attempts)
```

Primary Interface
この代替インターフェースによってバックアップされるインターフェース

Alternate Interface
対応する 1 次インターフェースをバックアップするのに使用されるダイヤル回線

Reroute Enabled
この 1 次インターフェースの再ルートが現在使用可能になっているかどうかを示します。

Overflow Enabled
この 1 次インターフェースのオーバーフローが現在使用可能になっているかどうかを示します。

Primary first stabilization
1 次リンクがアップにならない場合、この 1 次リンクのルーティングを代替リンクに切り替える前の、ルーター初期化の秒数

First stabilization
1 次リンクがアップであることが最初に検出された後、ルーティング

を 1 次に戻す前に必要な秒数。 1 次リンクがこの秒数だけアップ状態に保たれるまでは、ルーティングは代替リンクを介して継続されます。

Time-of-day revert back
ルーターが 1 次ルートに戻すことができる時刻。ルーターは、復帰開始時刻 (start-time-of-day-revert-back) と復帰停止時刻 (stop-time-of-day-revert-back) の間の任意の時刻に、1 次に戻すことができます。 1 次への復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にのみ実行されます。 デフォルトは 0 です。

Restored times
1 次インターフェースを再ルートするための試行回数

Overflow times
ダイヤル・オン・オーバーフローの試行回数

secondary-circuit
各 2 次回線の合計数を提供します。監視オペレーターは、WAN 復元の状態、および各 2 次インターフェースと対応の 1 次とのマッピングに関する統計を検索することができます。

例:

```
list secondary-circuit
Secondary interface number  [0]? 1

                                                  Secondary
Primary Interface          Secondary Interface    Enabled
-------------------        -------------------    ---------
1  PPP/0  Point to Poi     3  PPP/1  Point to Poi    Yes

Router primary interface state = Up
Router secondary interface state = Available
Restoral Statistics:

  Primary restoral attempts =       6   completions =    5
  Restoral packets forwarded =    346
    Most recent restoral period in hrs:min:sec          00:08:20
```

Primary Interface
この対応する 2 次インターフェースによってバックアップされているインターフェース

Secondary Interface
対応する 1 次インターフェースをバックアップするのに使用されるダイヤル回線

Secondary Enabled
この 1 次インターフェースの復元が現在使用可能になっているかどうかを示します。

Router Primary Interface State
1 次インターフェースの状態が、次のいずれかであることを示します。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。

Disabled - オペレーターがリンクを使用不可にしたことを示します。

Not present - リンクは構成されているが、ハードウェアに問題があることを示します。

Router Secondary Interface State

対応する 2 次インターフェースの状態が、次のいずれかであることを示します。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。これは、Config> プロンプトまたはオペレーター・コンソールで、2 次の基本ネットが使用不可にされている場合にも起こります。

Available - リンクが待機モードにあることを示します。

Testing - リンクが接続確立中であることを示します。

復元の統計:

Primary Restoral Attempts

1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

Restoral Packets forwarded

このフィールドには、転送されたパケットの合計数が表示されます。

Most Recent Restoral Period

これは、前回の使用時または現行の復元の使用時の、2 次がアップであった時間数を示します。

summary

各 2 次回線の合計数を提供します。

例:

```
list summary
WAN Restoral is enabled with 3 circuit(s) configured

  Total restoral attempts =      3 completions =      2
  Total packets forwarded =    346
  Longest restoral period in hrs:min:sec   00:08:20

Primary Interface and State      Secondary Interface and State
---------------------------   ----------------------------------
 1  PPP/0  - Up                3  PPP/1  - Available
```

Total restoral attempts

1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

Completions

復元の試みに成功した (2 次がアップになり、使用された) 回数

Total packets forwarded

2 次インターフェースを介して転送されたパケットの合計数。これは両方向の合計数で、restart または clear restoral-statistics コマンドが使用されるまでの、すべての復元期間における累計です。

Longest restoral period

このフィールドは、現行の使用期間はカウントせずに、復元が使用された最長時間を時間、分、秒数で表示します。

Primary Interface and State

対応する 2 次によってバックアップされるインターフェース。有効な状態は、次のとおりです。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。

Disabled - オペレーターがリンクを使用不可にしたことを示します。

Not present - リンクは構成されているが、ハードウェアに問題があることを示します。

Secondary Interface and State

対応する 1 次をバックアップするのに使用されているダイヤル回線。有効な状態は、次のとおりです。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。これは、`Config>` プロンプトまたはオペレーター・コンソールで、2 次の基本ネットが使用不可にされている場合にも起こります。

Testing - リンクが接続確立中であることを示します。

Available - リンクが待機モードにあることを示します。

第59章 WAN 再ルート機能

この章では、WAN 再ルート機能について説明します。本章には、以下の節が含まれています。

- 『WAN 再ルートの概説』
- 789ページの『WAN 再ルートの構成』

重要

1Sx および 1Ux モデルでは、ルーターの WAN ポートと ISDN B チャネルが両方ともアクティブの場合にのみ、WAN 再ルートを利用可能です。

WAN 再ルートの概説

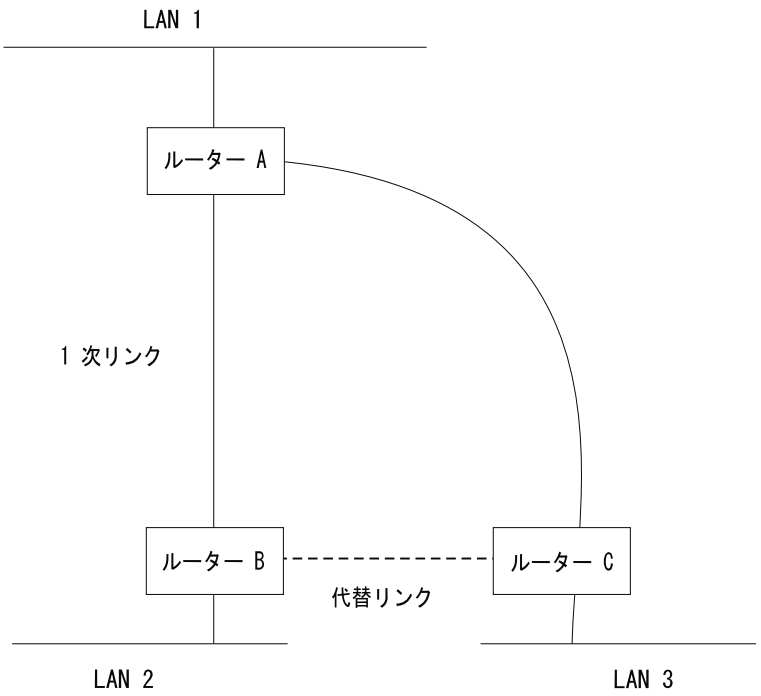
WAN 再ルートは、代替ルートを設定することによって、1 次リンクに障害が起きたときに、ルーターが自動的に代替ルートを通る着信先への新しい接続を開始できるようにします。 WAN 復元の説明、および WAN 再ルートとダイヤルオン・オーバーフローを合わせて使用する方法については、763ページの『WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの概説』を参照してください。

WAN 再ルート・プロセスは、次のとおりです。

1. 1 次リンクの障害を検出する。
2. 代替リンクに切り替える。
3. 1 次リンクの回復を検出する。
4. 1 次リンクに戻す。

代替リンクは、ルート可能プロトコル (たとえば、IP、IPX) を構成できる任意のリンクを使用することができ、代替リンクのデータ・リンク・タイプは、1 次リンクのデータ・リンク・タイプと一致している必要はありません。たとえば、代替リンクには、LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線などを使用できます。代替リンクに使用できないインターフェース・タイプの例としては、SDLC シリアル・インターフェース、SRLY シリアル・インターフェース、および V.25bis や ISDN のような基本ネットがあります。

注: 1 次リンクまたは代替リンクがダイヤル回線の場合、そのダイヤル回線はダイヤル・オンデマンド用に構成することはできません。



ルーター A と B の間の 1 次リンクに障害が起きた場合、WAN 再ルートは、ルーター B と C の間に代替リンクを確立します。これにより、ルーター A と B は、ルーター C を介して通信できるようになります。

図 38. WAN 再ルート. 通常は、ルーター A と B の間、およびルーター A と C の間にコネクションがあります。

ダイヤル・オン・オーバーフロー

ダイヤル・オン・オーバーフローでは、1 次リンクのトラフィック速度が指定の限界値に達すると、IP トラフィック用の代替インターフェースを使用することができます。これは、1 次インターフェースが必ずしもダウンしなくても、代替リンクが起動されることを意味しています。 1 次インターフェースのトラフィックが指定の限界値に達すると、ルーターは代替リンクを起動します。ダイヤル・オン・オーバーフローを使用するためには、WAN 再ルートが構成されており、1 次インターフェースがフレーム・リレーであることが必要です。ダイヤル・オン・オーバーフローで代替インターフェースに切り替えることができる唯一のプロトコルは、IP です。また、ダイヤル・オン・オーバーフローを使用する場合は、RIP の代わりに、OSPF を IP ルーティング・プロトコルとして使用する必要があります。

ダイヤル・オン・オーバーフローの構成については、769ページの『WAN 復元、WAN 再ルート、およびダイヤル・オン・オーバーフローの構成コマンド』 を参照してください。

帯域幅の監視

WAN 再ルートの構成時に、ダイヤル・オン・オーバーフローの帯域幅監視のインターバルを指定することができます。 1 次インターフェースの送受信の帯域幅が監視されます。 1 次インターフェースの帯域幅が*追加* 限界値に達すると、代替インターフ

ェースを起動するための WAN 再ルート要求が生成されます。 WAN 再ルートが代替インターフェースの起動に成功すると、IP は 1 次インターフェースを介したルーティングを停止し、代替インターフェースを介してルーティングを開始します。

WAN 再ルートが代替ルートの起動に成功しない場合、1 次インターフェースの帯域幅使用率が除去 限界値を下回るまで、代替インターフェースの起動を定期的に試みます。

1 次インターフェースの送受信の帯域幅使用率が除去 限界値に達し、構成された最小アップ・タイムが満了すると、代替インターフェースは除去されます。これにより、IP は代替インターフェースを介したルーティングを停止し、1 次インターフェースの使用を開始します。

追加限界値および除去限界値は、1 次リンクに構成された回線速度の比率として指定します。構成された回線速度は、必ずしもリンクの実際の速度と一致するとは限りません。リンク上の各方向のトラフィックの量は、別々に計算されます。いずれかの方向のトラフィックが指定の比率より大きい場合、限界値を超過することになります。

WAN 再ルートの構成

以下に示すのは、WAN 再ルートを構成するのに必要なステップです。次の節に、これらのタスクを実行する方法の例を示します。

WAN 再ルートを構成するには、以下の作業が必要です。

1. 1 次リンクを構成する。
2. 代替リンクを構成する。
3. 代替リンクを 1 次リンクに割り当てる。 1 次リンクの安定化 (stabilization) 期間も指定できます。

   安定化時間が終わった後 (構成されている場合) に行われる 1 次リンクへの復帰時刻 (time-of-day revert-back) を指定することができます。これにより、ユーザーが希望する時刻まで 2 次をアップに維持し、オフ・ピーク時に 1 次に復帰させるといったことが可能になります。

   注: 1 次リンクと代替リンクは、異なるデータ・リンク・タイプであっても構いません。 1 次リンクおよび代替リンクには、以下のものを使用できます。
   - LAN インターフェース
   - PPP シリアル・インターフェース
   - フレーム・リレー・シリアル・インターフェース
   - X.25 シリアル・インターフェース
   - PPP ダイヤル回線
   - フレーム・リレー・ダイヤル回線

サンプル WAN 再ルート構成

790ページの図39 は、ISDN を介するフレーム・リレー・ダイヤル回線を代替リンクとして使用している WAN 再ルートを示しています。ルーター A とルーター C 間

のフレーム・リレー DLCI に障害が起きた場合、WAN 再ルートはダイヤル回線を使用してルーター D を経由する代替コネクションを確立します。支局から本局への 1 次リンクの 1 つに障害が起きた場合、WAN 再ルートは別の支局を経由して本局に接続する代替ルートを確立します。

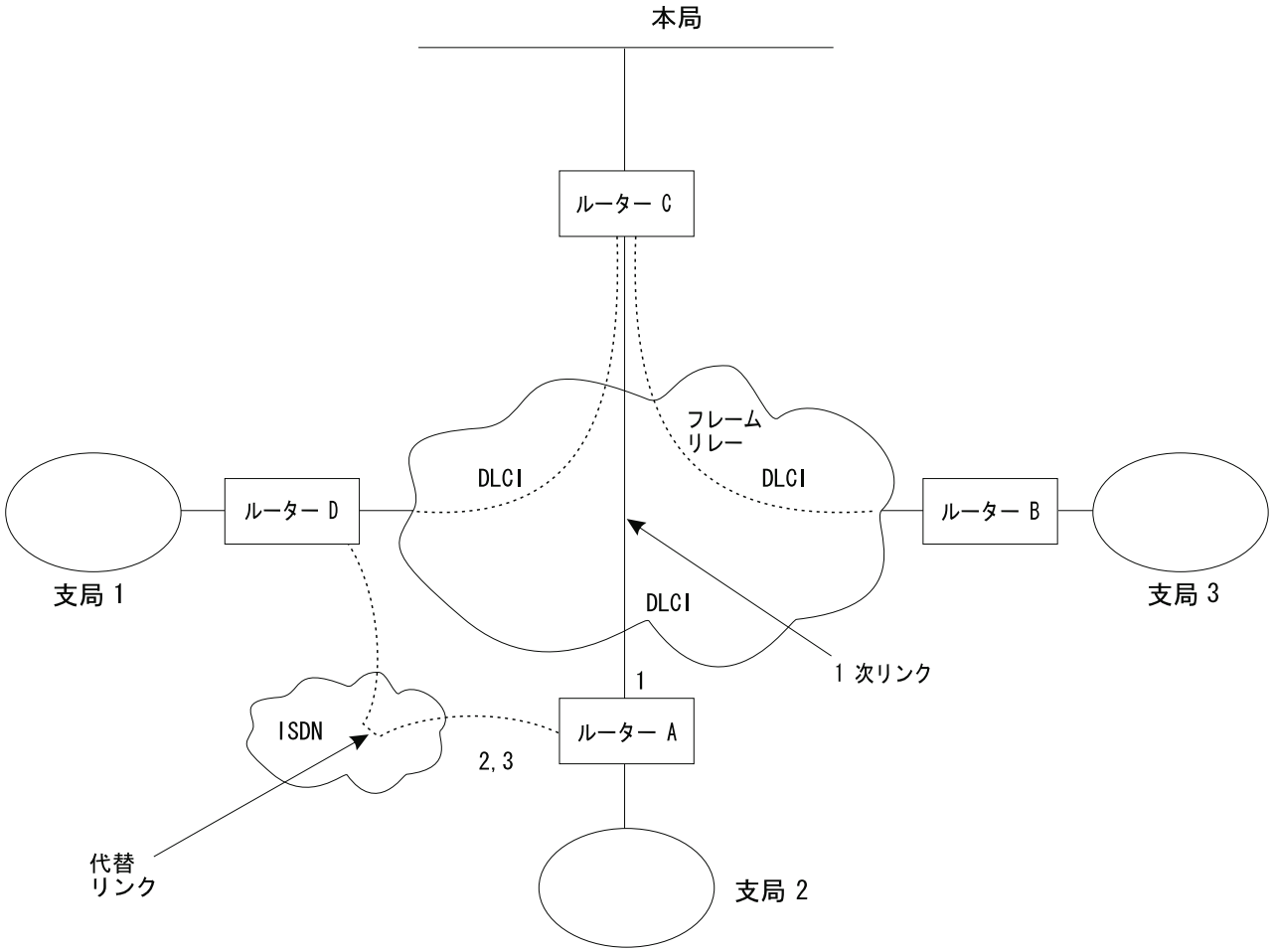


図 39. サンプル WAN 再ルート構成. 支局はフレーム・リレーを使用して本局に接続。

以下の節では、図39 のルーター A 上の WAN 再ルートを設定する方法について説明します。以下のタスクが必要になります。

- 1 次フレーム・リレー・インターフェース (1) を構成して、そのフレーム・リレー・インターフェースに必要な PVC または必要な PVC グループを設定するか、あるいは No-PVC 機能を使用可能にする。
- ISDN インターフェース (2) およびそのフレーム・リレー・ダイヤル回線 (3) を構成する。
- ダイヤル回線を、1 次フレーム・リレー・インターフェースの代替リンクとして割り当て、ダイヤル回線の config プロンプトで 'set idle 0' コマンドを出す。
  - オプションで、以下のものも指定できます。
  - 1 次リンクの安定化 (stabilization) 期間
  - 1 次リンクの復帰時刻 (time-of-day revert-back) ウィンドウ

これらのタスクについて、以下で詳しく説明します。

フレーム・リレー・インターフェースの構成

ルーター A 上に WAN 再ルート用のフレーム・リレー・インターフェースを構成するには、1 次フレーム・リレー・インターフェース上のルーター A と C 間に PVC を追加します。

他のルーターへの接続が失われたときに、1 次 FR インターフェースが自身をダウンとして宣言するようにさせるには、3 通りの方法を選択できます。

1. No-PVC 機能を使用可能にする。この機能が使用可能のとき、アクティブの PVC がないと、FR インターフェースはダウンします。
2. ある PVC を必須として構成するが、その PVC を必須 PVC グループの中に含めない。この場合、その PVC が非アクティブになると、FR インターフェースはダウンします。
3. 1 組の PVC を必須として構成し、必須 PVC グループに含める。この場合、必須 PVC グループのすべての PVC が非アクティブになると、FR インターフェースはダウンします。

フレーム・リレー・インターフェースの構成は、以下の手順で行います。

1. インターフェース上のデータ・リンクをフレーム・リレーに設定する (まだ行っていない場合)。

   ```
   Config>set data-link frame relay
   Interface Number [0]? 2
   ```

2. フレーム・リレー構成プロセスに入る。

   ```
   Config>network
   What is the network number [0]?2
   Frame Relay user configuration
   FR Config>
   ```

   注: 1 次フレーム・リレー・インターフェースを構成するために、残りの 2 つのステップのうちの *1* つ だけを実行します。

3. **add permanent-virtual-circuit** コマンドを使用して、PVC を追加する。

   PVC を必須として構成するには、次のようにします。

   『Is circuit required for interface operation ?』 という問いに対して **y** と入力する。

   PVC を必須 PVC グループのメンバーとして構成するには、次のようにします。

   a. 『Does circuit belong to a Required PVC group ?』 という問いに対して **y** を入力する。

   b. 『What is the group name ?』 の問いに応答して、グループ名を入力する。

   すでに PVC が追加されている場合は、 **change permanent-virtual-circuit** コマンドを使用して、PVC を必須として構成し、該当する場合は、それを必須 PVC グループに割り当てます。詳細については、409ページの『第31章 フレーム・リレー・インターフェースの使用』 を参照してください。

   ```
   FR Config>add permanent-virtual-circuit
   Circuit number [16]?
   Committed Information Rate (CIR) in bps [64000]?
   Committed Burst Size (Bc) in bits [64000]?
   Excess Burst Size (Be) in bits [0]?
   ```

```
Assign circuit name []?
Is circuit required for interface operation [N]?y
Does the circuit belong to a required PVC group [N]? y
What is the group name []?group1
```

4. 必要な場合は、No-PVC 機能を使用可能にする。

   注: このステップは、直前のステップを飛ばした場合にのみ 実行してください。

   ```
   FR Config>enable no-pvc
   ```

この他にも、フレーム・リレーに対して設定できるパラメーターがあります。詳細については、409ページの『第31章 フレーム・リレー・インターフェースの使用』 を参照してください。

ISDN インターフェースとダイヤル回線の構成

ルーター A とルーター D 間の ISDN インターフェースとダイヤル回線を構成します。ISDN インターフェースおよびダイヤル回線の構成方法についての詳しい説明は、619ページの『第45章 ISDN インターフェースの使用』 を参照してください。

WAN 復元とは異なり、代替リンクとして使用されるダイヤル回線には、ルーティング・プロトコルを構成する必要があります。このルート可能プロトコルは、保守パケットを送信するのを防止できないので、代替リンクは再ルートの必要がなくてもコネクションを確立します。この場合、代替リンクを再ルートにのみ使用したいときは、ダイヤル回線を使用不可に設定します。ダイヤル回線を使用不可にするには、`Config>` プロンプトで **disable interface** コマンドを入力します。

ISDN インターフェースに複数のダイヤル回線を割り当てた場合、ダイヤル回線に優先順位を設定することができます。すべての B チャネルが、物理インターフェース上にアクティブのダイヤル回線を持っており、高い優先順位の回線がパケットを受信する場合、最低優先順位のコネクションは終了され、高い優先順位の回線がコネクションを確立します。

優先順位は 0 〜 15 に設定できます。15 が最高優先順位の回線で、0 が最低優先順位の回線です。新規ダイヤル回線のデフォルト優先順位は 8 です。優先順位を変更する場合は、`Circuit Config>` プロンプトで **set priority** と入力します。

代替リンクの割り当てと構成

WAN 再ルート構成プロセスに入って、ダイヤル回線を LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ ダイヤル回線の代替リンクとして割り当て、必要な場合には、安定化期間 (stabilization periods) または復帰時刻 (time-of-day revert-back) ウィンドウ (もしくは、その両方) を指定します。

安定化期間には、次の 2 種類があります。

- *最初の安定化期間 (First stabilization period)* は、ルーターが最初に 1 次インターフェースの起動を試みたときに、1 次インターフェースがアクティブになるのを待つ時間の長さです。最初の安定化期間が経過しても 1 次がアップにならない場合、WAN 再ルートは代替リンクを起動します。
- *安定化期間 (Stabilization period)* は、ルーターが代替リンクから 1 次リンクに戻す前に、1 次リンクの信頼性を確認するために待つ時間の長さです。

復帰時刻 (time-of-day revert-back) ウィンドウは、1 次がアップになり、構成された安定化期間が経過した後で 1 次に戻す具体的な時刻です。

ユーザーは 24 時間クロックを使用して、復帰ウィンドウの開始時刻と停止時刻を指定します。開始時刻に達するまで、2 次はアップのまま維持され、ダウンにされません。 1 次がアップになる時刻が、開始時刻と停止時刻 (ウィンドウ内の) の間にある場合、安定化期間が経過した後、ただちに 1 次リンクに切り替わります。

代替リンクの割り当てと構成は、以下の手順で行います。

1. WAN 復元構成プロセスに入る。

```
Config>feature wrs
WAN Restoral user configuration
```

2. ダイヤル回線を、1 次フレーム・リレー・インターフェースの代替リンクとして割り当てる。

```
WRS Config>add alternate-circuit
Alternate interface number  [0]? 4
Primary interface number  [0]? 1
```

3. 代替回線を使用可能にする。

```
WRS Config>enable alternate-circuit
Alternate interface number  [0]? 4
```

4. オプションで、最初の安定化期間を指定する。

   特定の 1 次インターフェースに対する最初の安定化期間を設定するには、**set first-stabilization-period** コマンドを使用します。特定の期間が設定されていないすべてのインターフェースに対するデフォルトの最初の安定化期間を設定するには、**set default first-stabilization-period** コマンドを使用します。

```
WRS Config>set first-stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?

WRS Config>set default first-stabilization-period
Default first primary stabilization time (0 - 3600 seconds) [0]?
```

5. オプションで、安定化期間を設定する。特定のインターフェースに対する安定化期間を設定するには、**set stabilization-period** コマンドを使用します。特定の期間が設定されていないすべてのインターフェースに対するデフォルトの安定化期間を設定するには、**set default stabilization-period** コマンドを使用します。

```
WRS Config>set stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?
WRS Config>set default stabilization-period
Default first primary stabilization time (0 - 3600 seconds) [0]?
```

6. オプションで、復帰時刻ウィンドウを指定する。

   特定のインターフェース・ウィンドウの開始時刻と停止時刻を設定するには、start-time-of-day-revert-back コマンドと stop-time-of-day-revert-back コマンドを使用します。デフォルト値のゼロは、ウィンドウが構成されないことを意味します。24 時間クロックは、午前 1 時に開始して、夜中の 24 時に終了します。開始時刻と停止時刻が同じ (ただし、ゼロでない) 場合、復帰は正確にその時刻に起こります。

   以下は、復帰ウィンドウの設定を示す 2 つの例です。

   a. 開始時刻が 23 で、停止時刻が 3 のとき、午後 11 時から午前 3 時までの復帰ウィンドウを生成します。

b. 開始時刻が 1 で、停止時刻が 5 のとき、午前 1 時から午前 5 時までの復帰ウィンドウを生成します。

```
WRS Config> set start-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]?
WRS Config> set stop-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured) [0]?
```

第60章 ネットワーク・ディスパッチャー機能の使用

この章では、ネットワーク・ディスパッチャー機能の使用法について説明します。本章には、以下の節が含まれています。

- 『ネットワーク・ディスパッチャーの概説』
- 796ページの『ネットワーク・ディスパッチャーによる TCP/IP の平衡化』
- 797ページの『ネットワーク・ディスパッチャーの高可用性』
- 799ページの『ネットワーク・ディスパッチャーの構成』

ネットワーク・ディスパッチャーについての追加情報は、 *Interactive Network Dispatcher User's Guide, GC31-8496* を参照してください。

ネットワーク・ディスパッチャーの概説

ネットワーク・ディスパッチャーとは、TCP/IP セッション要求をサーバー・グループ内の種々のサーバーに転送し、すべてのサーバー間で要求の負荷平衡を図ることによって、サーバーの性能を高める機能です。この転送は、ユーザーおよび他のアプリケーションには透過的です。ネットワーク・ディスパッチャーは、E メール、サーバー、ワールド・ワイド・ウェブ (WWW) サーバー、分散並列データベース照会、およびその他の TCP/IP アプリケーションに役立ちます。

ネットワーク・ディスパッチャーは、ピーク需要時の問題に対処するための、強力で、柔軟で、スケーラブルなソリューションを提供することにより、ユーザー・サイトの潜在的能力を最大限に発揮させるのに役立ちます。ピーク需要時にネットワーク・ディスパッチャーは、着信要求を処理するための最適なサーバーを自動的に見つけます。

ネットワーク・ディスパッチャー機能は、負荷平衡を取るためにドメイン・ネーム・サーバーを使用しません。負荷平衡と管理を固有に組み合わせたソフトウェアを使用して、サーバー間のトラフィックの平衡を取ります。また、ネットワーク・ディスパッチャーは、障害のあるサーバーを検出し、他の利用可能なサーバーにトラフィックを転送することもできます。

ネットワーク・ディスパッチャー・マシンに送られるすべてのクライアント要求は、動的に設定される重みに基づいて、ネットワーク・ディスパッチャーが最適サーバーとして選択したサーバーに転送されます。これらの重みは、デフォルト値を使用することも、構成プロセスで値を変更することもできます。

サーバーからクライアントへの応答には、ネットワーク・ディスパッチャーは介入しません。ネットワーク・ディスパッチャーと通信するために、サーバー上にソフトウェアを追加する必要はありません。

ネットワーク・ディスパッチャー機能は、大規模でスケーラブルなサーバー網を、安定した状態で効率的に管理するためのかぎになります。ネットワーク・ディスパッチャーを使用すると、多数の個別のサーバーをリンクして、単一のバーチャル・サーバーのように見せることができます。世界には、ユーザーのサイトは単一の IP ア

ドレスのように見えます。ネットワーク・ディスパッチャーは、ドメイン・ネーム・サーバーから独立して機能します。要求はすべてネットワーク・ディスパッチャー・マシンの IP アドレスに送られます。

ネットワーク・ディスパッチャーは、クラスター化されたサーバーへのトラフィックの負荷平衡に大きく貢献し、サイトの安定した、効率的な管理を実現します。

ネットワーク・ディスパッチャーによる TCP/IP の平衡化

負荷平衡には、さまざまなアプローチがあります。ある方法では、最初のサーバーが遅かったり応答しない場合、ユーザーが任意に異なるサーバーを選択することができます。また、ある方法はラウンドロビン方式で、ドメイン・ネーム・サーバーが、要求を処理するサーバーを選択します。この方法は比較的すぐれていますが、ターゲット・サーバー上の現在の負荷は考慮に入れられず、ターゲット・サーバーが利用可能であるかどうかさえ考慮されません。

ネットワーク・ディスパッチャーは、要求のタイプ、サーバー上の負荷の分析、またはユーザーが割り当てる 1 組の構成可能な重みに基づいて、種々のサーバーへの要求の負荷平衡を取ることができます。異なるタイプの平衡化を個別に管理するために、ネットワーク・ディスパッチャーは、以下のコンポーネントを備えています。

実行プログラム

受信した要求のタイプに基づいて、コネクションの負荷平衡を取ります。標準的な要求タイプとしては HTTP、FTP、および SSL があります。このコンポーネントは、常に実行されます。

アドバイザー

サーバーに照会し、各サーバーのプロトコルによって結果を分析します。アドバイザーは、適切な重みを設定するために、この情報を**マネージャー** に渡します。アドバイザーは、任意選択のコンポーネントです。

ネットワーク・ディスパッチャーは、FTP および HTTP のアドバイザー、ならびに MVS システム上の Workload Manager (WLM) を用いて動作する MVS アドバイザーをサポートします。 WLM は、個々の MVS ID 上の作業負荷の量を管理します。ネットワーク・ディスパッチャーは、MVS サーバーへの要求の負荷平衡を取るために、WLM を活用することができます。

マネージャー

以下に基づいて、サーバーの重みを設定します。

- 実行プログラムの内部カウンター
- アドバイザーによって提供されたサーバーからのフィードバック
- システム監視プログラムからのフィードバック

マネージャーは、任意選択のコンポーネントです。ただし、マネージャーを使用しない場合には、ネットワーク・ディスパッチャーは、現行のサーバーの重みに基づき、ラウンドロビン・スケジューリング方式を使用して負荷の平衡を図ります。

ネットワーク・ディスパッチャーの高可用性

ネットワーク・ディスパッチャーの基本機能には以下のような特性があり、いろいろな観点から、これが単一障害点になることを示しています。

- 入ってくるすべてのトラフィックを調べます。既存のコネクションへの一部のパケットが、異なるネットワーク・ディスパッチャーを経由する異なるパスを使用してサーバーに達する場合、サーバーは即時にそのコネクションをリセットします。
- 確立されたすべてのコネクションを追跡し、それを終了することはありませんが、ネットワーク・ディスパッチャーのコネクション・テーブルからエントリーが失われると、コネクションはリセットされます。
- それより前のホップ・ルーターからは、それが最終ホップであり、コネクションの終端であるように見えます。

これらの特性により、次のような障害が発生した場合、クラスター全体にとって重大なものになります。

- 何らかの理由でネットワーク・ディスパッチャーに障害が生じた場合、すべてのコネクション・テーブルが失われます。したがって、クライアントからサーバーへの既存のコネクションもすべて失われます。クライアントをサーバーに誘導できる第 2 のネットワーク・ディスパッチャーが存在すると仮定しても、通常のルーティング・プロトコル遅延 (数分かかることもある) の後でしか、新しいコネクションを確立することができません。
- 直前の IP ルーターへの構成済みネットワーク・ディスパッチャー・インターフェースに障害が生じた場合、同じネットワーク・ディスパッチャーに到達できる別のインターフェースが存在する必要があります。その場合は IP ルーターによって回復されますが (ARP エージング機構を使用して、数分の遅れで)、そうでない場合は、すべてのコネクションが失われます。
- サーバーにインターフェースするネットワーク・ディスパッチャーに障害が生じた場合、直前のホップ・ルーターはそのネットワーク・ディスパッチャーが最終ホップであるものと想定するので、新しいコネクションを再ルートしません。既存のコネクションは失われ、新しいコネクションは確立されないことになります。

いずれの障害の場合も (これらは、ネットワーク・ディスパッチャーの障害のみならず、ネットワーク・ディスパッチャーの近隣の障害でもあります)、すべての既存のコネクションは失われます。たとえ、バックアップのネットワーク・ディスパッチャーが標準 IP 回復機構を稼働していても、最善の場合でも回復に時間がかかる上に、新規のコネクションにしか適用されません。最悪の場合には、コネクションは回復しません。

ネットワーク・ディスパッチャーの可用性を高めるために、ネットワーク・ディスパッチャー高可用性機能は、以下の機構を使用しています。

- 同じクライアントおよび同じクラスター・サーバーへの接続性、およびネットワーク・ディスパッチャー相互間の接続性を備えている 2 つのネットワーク・ディスパッチャー
- ネットワーク・ディスパッチャーの障害を検出するための、2 つのネットワーク・ディスパッチャー間の 『ハートビート』 機構

ネットワーク・ディスパッチャーの使用

- 各ネットワーク・ディスパッチャーから到達できる IP ホストと到達できないホストを識別するための、到達可能性基準
- ネットワーク・ディスパッチャー・データベース (つまり、コネクション・テーブル、到達可能性テーブル、およびその他のテーブル) の同期化
- アクティブ・ネットワーク・ディスパッチャー (特定のクラスター・サーバーを担当する) とスタンドバイ・ネットワーク・ディスパッチャー (そのクラスター・サーバーに継続的に同期化される) を選ぶ論理
- 論理またはオペレーターがアクティブとスタンドバイを切り替えることに決定した場合、高速で IP の引き継ぎを実行する機構

障害の検出

障害検出の基本的基準 (ハートビート・メッセージによって検出される、アクティブ・ネットワーク・ディスパッチャーとスタンドバイ・ネットワーク・ディスパッチャー間の接続性の損失) の他に、『到達可能性基準』 と呼ばれるもう 1 つの障害検出機構があります。ネットワーク・ディスパッチャーの構成時に、各ネットワーク・ディスパッチャーが正しく動作するために到達可能でなければならないホストのリストを指定します。ホストは、ルーター、IP サーバー、あるいはその他のタイプのホストが可能です。ホスト到達可能性は、そのホストに PING することによって入手します。

ハートビート・メッセージを送れない場合、あるいはアクティブ・ネットワーク・ディスパッチャーが到達可能性基準を満たさなくなり、スタンドバイ・ネットワーク・ディスパッチャーが到達可能である場合、切り替えが行われます。利用可能なあらゆる情報に基づいて決定を下せるように、アクティブ・ネットワーク・ディスパッチャーは、その到達可能性の能力をスタンドバイ・ネットワーク・ディスパッチャーに定期的に送信します。スタンドバイ・ネットワーク・ディスパッチャーは、その能力を自身の能力と比較して、切り替えるかどうかを決定します。

キャッシュ同期

ネットワーク・ディスパッチャーによって同期化される主なデータは、テーブル・エントリーです。ネットワーク・ディスパッチャー高可用性機能は、キャッシュ同期プロトコルを使用して、必ず両方のネットワーク・ディスパッチャーに同じエントリーが含まれているようにします。この同期は、転送遅延に設定された誤りマージンを考慮します。プロトコルは、同位のデータベースを初期に同期化し、その後も定期的に更新してデータベースを維持します。

回復方法

ネットワーク・ディスパッチャーに障害が生じた場合、IP 引き継ぎ機構が、速やかにすべてのトラフィックをスタンドバイ・ネットワーク・ディスパッチャーに転送します。データベース同期機構によって、スタンドバイはアクティブ・ネットワーク・ディスパッチャーと同じエントリーを持つことが保証されています。ネットワーク (クライアントとバック・エンド・サーバー間の中間部分のハードウェアまたはソフトウェア) に障害が発生した場合、動作しているスタンドバイ・ネットワーク・ディスパッチャーを通る代替パスが存在するときは、その代替パスを経由するように切り替えられます。

IP 引き継ぎ

注: クラスター IP アドレスは、直前のホップ・ルーター (IP ルーター) と同じ論理サブネット上に存在するものと想定しています。

IP ルーターは、ARP プロトコルを用いてクラスター・アドレスを解決します。 IP 引き継ぎを行うために、ネットワーク・ディスパッチャー (アクティブになるスタンドバイ) は、自分自身に対して ARP 要求を出します。これは、そのクラスターの論理サブネットに属するすべての直接接続ネットワークに同報通信されます。それより前のホップの IP ルーターは、それぞれの ARP テーブルを更新して (RFC826 に従って)、そのクラスターへのすべてのトラフィックを、新たにアクティブになった (前はスタンドバイだった) ネットワーク・ディスパッチャーに送るようにします。

ネットワーク・ディスパッチャーの構成

ユーザー・サイトをサポートするネットワーク・ディスパッチャーを構成するには、いろいろな方法があります。ユーザー・サイトに、すべてのカスタマーが接続するホスト名が 1 つしかない場合は、1 つのクラスターと任意の数のポート (接続を受信する) を定義することができます。この構成を 図40 に示します。

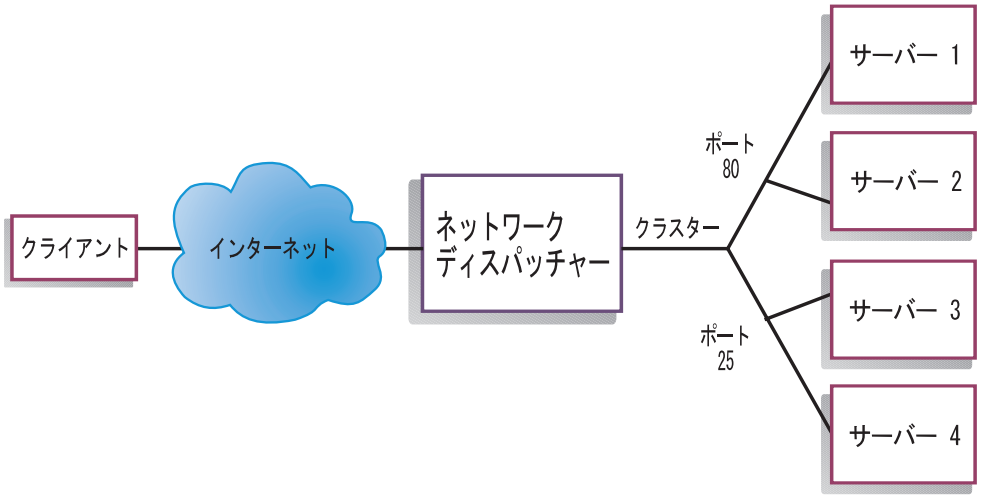


図 40. 1 つのクラスターと 2 つのポートを持つように構成されたネットワーク・ディスパッチャーの例

ユーザーのサイトで、複数の会社または部門がそれぞれ異なる URL を使用してサイトにアクセスするコンテンツ・ホスティングを行っている場合には、ネットワーク・ディスパッチャーを別の方法で構成することが必要になります。この場合は、800ページの図41 に示すように、各会社または部門ごとに 1 つのクラスターを定義し、その URL で接続を受け取る任意の数のポートを構成することができます。

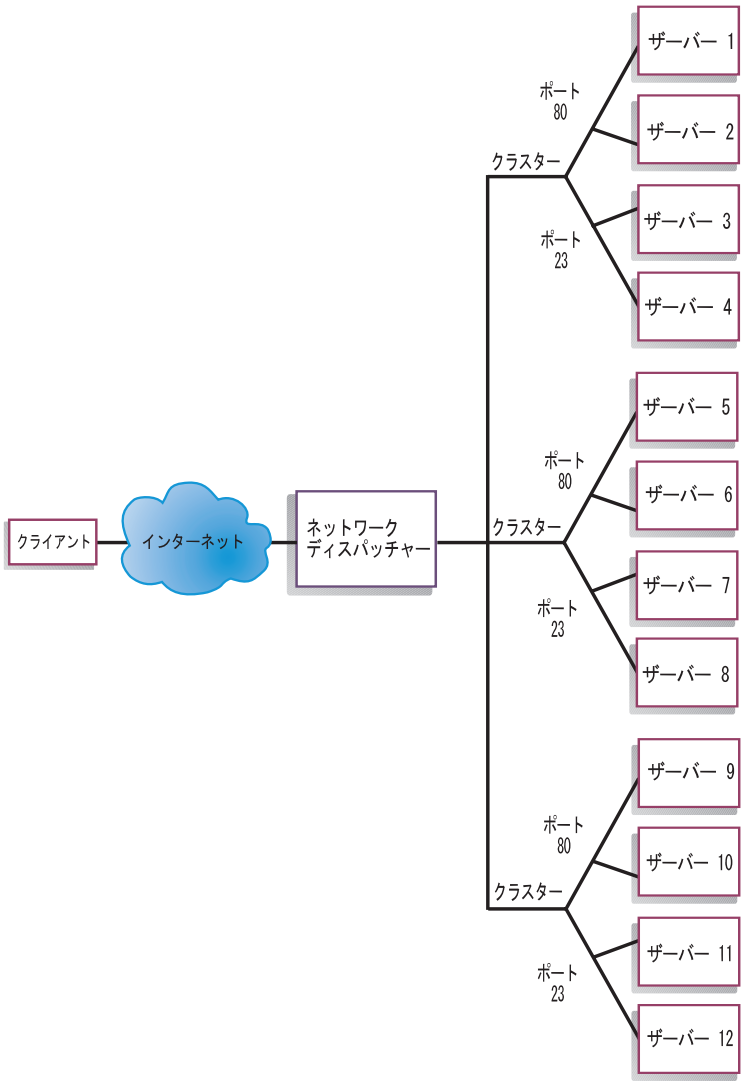


図 41. 3 つのクラスターと 3 つの URL を持つように構成されたネットワーク・ディスパッチャーの例

ネットワーク・ディスパッチャーの第 3 の構成方法は、サポートされる各プロトコル専用の多数のサーバーがある、非常に大規模なサイトに適しています。たとえば、大きなダウンロード可能ファイル用の直接 T3 回線を持つ個別 FTP サーバーを構成することができます。この場合は、801ページの図42 に示すように、各プロトコルに対して、ポートは 1 つであるが多数のサーバーを持つクラスターを定義できます。

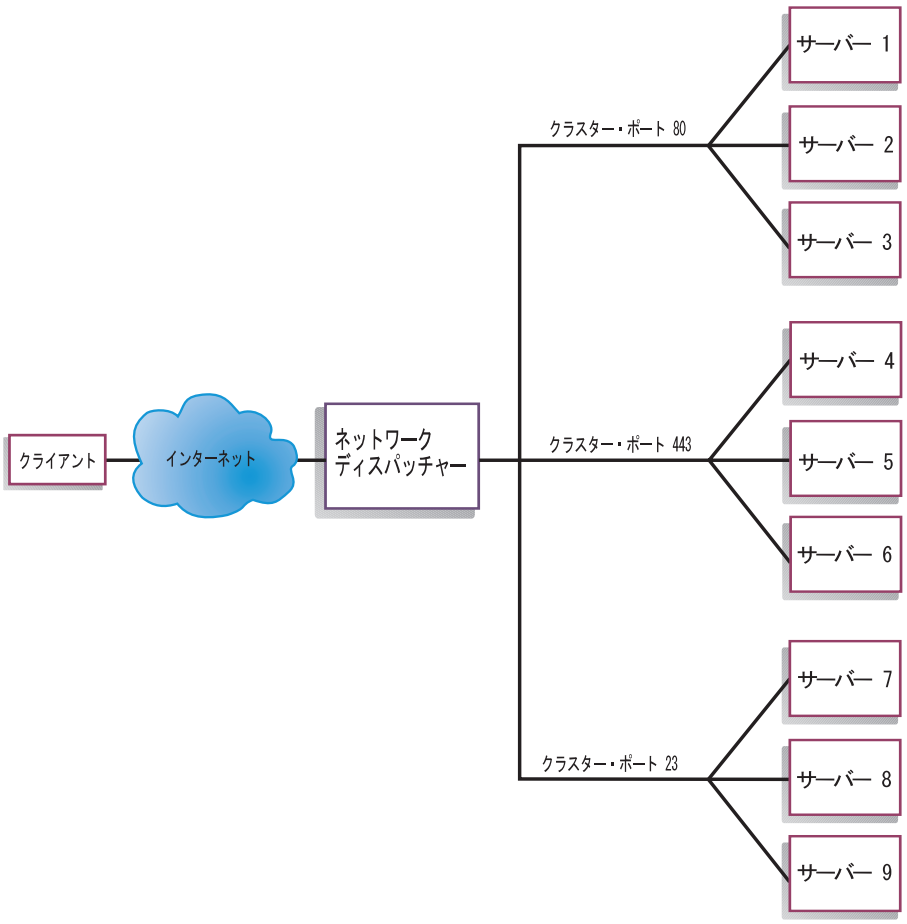


図 42. 3 つのクラスターと 3 つのポートを持つように構成されたネットワーク・ディスパッチャーの例

構成ステップ

ネットワーク・ディスパッチャーを構成する前に、次のことを行います。

1. ネットワーク・ディスパッチャーがサーバーへの直接インターフェースを持っていることを確認する。サーバーはエンタープライズ・ルーターまたはインターネットへの独立したコネクションを持ち、サーバーからクライアントへの発信トラフィックがネットワーク・ディスパッチャーをバイパスするようにすることができます。ただし、この独立したコネクションは構成する必要はありません。

   ユーザーのネットワークにとって高可用性が重要である場合、標準的な高可用性構成を 802ページの図43 に示してあります。

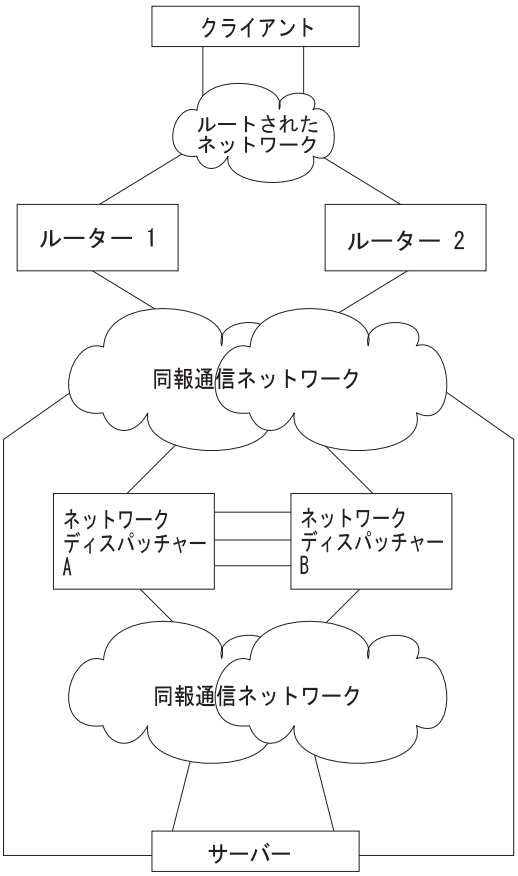


図 43. 高可用性ネットワーク・ディスパッチャー構成

2. 装置のインターフェースを構成する。これには、すべてのインターフェース、すべてのインターフェース上の IP アドレス、およびすべての該当するプロトコルの構成が含まれます。また、**set internal-ip-address** コマンドを使用して、内部 IP アドレスを構成することも必要です。マネージャーおよびアドバイザー・コンポーネントを使用する計画の場合は、これは必須です。 **set internal-ip-address** コマンドの詳細については、 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻 バージョン 3.1* を参照してください。
3. 装置をリブートまたはリスタートする。

IBM 2210 上のネットワーク・ディスパッチャーの構成

IBM 2210 上のネットワーク・ディスパッチャーを構成するには、次のようにします。

1. **feature ndr** コマンドを使用して、ネットワーク・ディスパッチャー機能にアクセスする。
2. **enable executor** および **enable manager** コマンドを使用して、実行プログラムとマネージャーを使用可能にする。
3. **add cluster** コマンドを使用して、クラスターを構成する。
4. 対応するプロトコルにサービスする各クラスター・サーバーごとに、**add port** を使用して TCP 着信ポートを構成する。ポートの例は、HTTP の場合は 80、FTP の場合は 20 または 21、および Telnet の場合は 23 です。

5. **add server** コマンドを使用して、サーバーを構成する。サーバーは、常にポートとクラスターに対応しています。 1 つのサーバーは複数のポートにサービスすることが可能であり、1 つのポートは複数のサーバーからサービスを受けることが可能であり、またサーバーのオペレーティング・システムが複数の別名をサポートする場合には、1 つのサーバーが複数のクラスターに属することも可能です。
6. **add advisor** コマンドを使用して、アドバイザーを構成する。

   注: MVS アドバイザーの場合、どのクラスターにもポート 10007 を定義してはなりません。アドバイザーは、構成されたすべてのサーバーのリストを探索して、該当するサーバーを見つけます。
7. **enable advisor** コマンドを使用して、構成したアドバイザーを使用可能にする。

高可用性のネットワーク・ディスパッチャーを構成している場合は、以下のステップを続けてください。そうでない場合は、これで構成は完了です。

注: 以下のステップは、1 次ネットワーク・ディスパッチャーで実行した後、バックアップでも実行してください。

8. **add backup** コマンドを使用して、このネットワーク・ディスパッチャーが 1 次であるかバックアップであるか、また切り替えが手動であるか自動であるかを構成する。
9. **add heartbeat** コマンドを使用して、1 次のバックアップのネットワーク・ディスパッチャー間でハートビートを行うすべてのパスを構成する (2 つ以上構成することが推奨されます)。パスは、発信元および宛先 IP アドレスで指定します。
10. **add reach** コマンドを使用して、ネットワーク・ディスパッチャーが完全なサービスを行うために到達可能であることが必要なホスト IP アドレスのリストを構成する。通常は、これはサーバー、エンタープライズ・ルーター、または管理ステーションのサブセットです。

set、**remove**、および **disable** コマンドを使用して、構成を変更することができます。

ネットワーク・ディスパッチャー用のサーバーの構成

サーバー上のネットワーク・ディスパッチャーを構成するには、次のようにします。

1. ループバック装置に別名を付ける。

   TCP サーバーが機能するためには、クラスター・アドレスに対してループバック装置 (通常は ***lo0*** と呼ばれる) を設定する (できれば、別名を付ける) ことが必要です。ネットワーク・ディスパッチャーは、パケットを TCP サーバー・マシンに転送する前に、TCP/IP パケット内の 宛先 IP アドレスを変更しません。ループバック装置をクラスター・アドレスに設定または別名指定した場合、TCP サーバー・マシンは、別のマシンあてのパケットを受け入れます。

   ネットワーク・インターフェースの別名指定をサポートするオペレーティング・システム (AIX、Solaris、または Windows NT など) を使用している場合には、別名 ***lo0*** をクラスター・アドレスに割り当てます。別名をサポートするオペレーティング・システムを使用する利点は、TCP サーバー・マシンが複数のクラスター・アドレスにサービスするように構成できることです。

別名をサポートしないオペレーティング・システム (HP-UX および OS/2 など) を使用している場合は、***lo0*** をクラスター・アドレスに設定する必要があります。

サーバーが、TCP/IP V3R2 を実行する MVS システムの場合、VIPA アドレスをクラスター・アドレスに設定する必要があります。これはループバック・アドレスとして機能します。 VIPA アドレスは、MVS ノードに直接接続されたサブネットに属していてはなりません。 MVS システムが TCP/IP V3R3 を実行している場合は、ループバック装置をクラスター・アドレスに設定する必要があります。

2. 余分なルートがないかチェックする。

   ループバック装置のネットワーク・マスクは通常 255.0.0.0 なので、おそらくデフォルト・ルートが作成されます。このルートは除去することが必要です。

   Windows NT での余分なルートのチェックは、**route print** コマンドを使用して行います。

   すべての UNIX システムおよび OS/2 での余分なルートのチェックは、**netstat -nr** コマンドを使用して行います。

3. 余分なルートを削除する。

   余分なルートを削除するには、表94 から、該当するオペレーティング・システムのコマンドを使用します。

表 94. 各種オペレーティング・システムのルート削除コマンド

オペレーティング・システム	**コマンド**
AIX	**route delete -net** *network_address cluster_address*
HP-Unix	**route delete net** *cluster_address*
Solaris	ルートを削除する必要はありません。
OS/2	ルートを削除する必要はありません。
Windows NT	**route delete** *network_address cluster_address* **注:** このコマンドは MS-DOS プロンプトで入力する必要があります。

第61章 ネットワーク・ディスパッチャー機能の構成および監視

この章では、ネットワーク・ディスパッチャー機能の構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

ネットワーク・ディスパッチャー構成コマンドへのアクセス

ネットワーク・ディスパッチャー構成環境にアクセスするには、次のようにします。

1. OPCON プロンプト (*) で **talk 6** と入力する。
2. `Config >` プロンプトで **feature ndr** コマンドを入力する。

ネットワーク・ディスパッチャー構成コマンド

表95 は、ネットワーク・ディスパッチャー構成コマンドの要約を示しており、表の後に個々のコマンドの説明があります。これらのコマンドは `NDR Config >` プロンプトで入力します。

表 95. ネットワーク・ディスパッチャー構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	ネットワーク・ディスパッチャーの各種のコンポーネント (アドバイザー、クラスター、ポート、およびサーバーを含む) を構成します。
Clear	ネットワーク・ディスパッチャー構成全体を消去します。
Disable	ネットワーク・ディスパッチャーのバックアップ、実行プログラム、およびマネージャー・コンポーネントを使用不可にします。特定のアドバイザーも使用不可にします。
Enable	ネットワーク・ディスパッチャーのバックアップ、実行プログラム、およびマネージャー・コンポーネントを使用可能にします。特定のアドバイザーも使用可能にします。
List	ネットワーク・ディスパッチャー構成全体または構成の特定部分を表示します。
Remove	ネットワーク・ディスパッチャー構成の特定部分を除去します。
Set	アドバイザー、クラスター、ポート、サーバー、またはネットワーク・ディスパッチャー・マネージャーの構成パラメーターを変更します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、アドバイザー、クラスター、ポート、およびサーバーを構成し、ネットワーク・ディスパッチャーを介して到達可能なホストまたはサブネットを指定

するのに使用します。高可用性の場合には、このネットワーク・ディスパッチャーが 1 次かバックアップか、ならびにハートビートおよびキャッシュ同期に使用する IP アドレスも構成することができます。

構文:

add advisor . . .
backup . . .
cluster . . .
heartbeat . . .
port . . .
reach . . .
server . . .

Advisor *name port interval timeout*

アドバイザーの名前とポートを指定します。このパラメーターは、アドバイザーが特定のプロトコルに関する情報を収集する頻度、およびアドバイザーがプロトコルを利用不能と見なすまでに必要な時間数も指定します。

name アドバイザーのタイプを指定します。

有効値: 0、1、2

0 = FTP

1 = HTTP

2 = MVS

デフォルト値: 1

port このアドバイザーのポート番号を指定します。

有効値: 0 ～ 65535

デフォルト値:

アドバイザー番号	デフォルト値
0	21
1	80
2	10007

interval

アドバイザーが各サーバーのプロトコルを照会する頻度 (秒数) を指定します。この値の半分の時間、サーバーから応答がないと、アドバイザーはそのプロトコルを利用不能と見なします。

有効値: 0 ～ 65535

デフォルト値: 5

timeout

アドバイザーがプロトコルを利用不能と見なすまでに必要な時間間隔 (秒数) を指定します。

マネージャーは、負荷平衡を決めるのに古い情報が使用されるのを防止するために、タイム・スタンプがこのパラメーターで設定された時刻より古いアドバイザーからの情報は使用しません。アドバイザー・タイムアウトは、アドバイザー・ポーリング間隔より大きい値でなければなりません。タイムアウトの方が小さいと、マネージャーは使用する必要がある報告を無視してしまいます。デフォルトでは、アドバイザーの報告はタイムアウトになりません。

このタイムアウト値は通常、アドバイザーを使用不可にした場合に適用されます。このパラメーターを、前に説明した interval/2 タイムアウト (これは、サーバーの応答がない時間に関するものです) と混同しないでください。

有効値: 0 ～ 65535

デフォルト値: 0、これは、プロトコルは常に利用可能と見なされることを意味しています。

例:

```
add advisor
Advisor name (0=ftp, 1=http, 2=mvs) [1]? 1
Port number [80]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
```

backup *role strategy*

このネットワーク・ディスパッチャーがバックアップであるか、1 次であるかを指定します。

role

これが 1 次ネットワーク・ディスパッチャーであるか、バックアップ・ネットワーク・ディスパッチャーであるかを定義します。このコマンドは、冗長構成を使用し、高可用性機能を実行したい場合にのみ使用します。この場合には、ハートビート (**add heartbeat**) および到達可能性 (**add reach**) も構成する必要があります。

有効値: 0 または 1

0 = 1 次

1 = バックアップ

デフォルト値: 0

strategy

ネットワーク・ディスパッチャーは、自動的に 1 次モードに戻るのか、手動で戻すのかを指定します。 1 次ネットワーク・ディスパッチャーに障害が起きてスタンドバイになり (バックアップが IP 引き継ぎ機能を実行したことを意味します)、その後で再び利用可能になったとき、strategy が *automatic* に設定されている場合は常に、キャッシュが同期化されるとただちに自動的にアクティブ・ネットワーク・ディスパッチャーになります。 strategy が *manual* に設定されている場合、元の 1 次はスタンドバイ・モードになり、オペレーターが **switchover** コマンドを使用しないと、再びそれをアクティブにすることはできません。 829ページの『Switchover』を参照してください。

有効値: 0 または 1

0 = 自動

1 = 手動

デフォルト値: 0

例:

```
add backup
Role (0=Primary, 1=Backup) [0]?
Switch back strategy (0=Auto, 1=Manual) [0]?
```

cluster *address FIN-count FIN-timeout FIN-stale-timer*

クラスターの IP アドレス、および実行プログラムがネットワーク・ディスパッチャー・データベースから不要情報収集を行う頻度を指定します。

address

クラスターの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

FIN-count

実行プログラムが *FIN-timeout* の経過後にネットワーク・ディスパッチャー・データベースから未使用コネクション情報の除去を試みる前に、FIN 状態にあることが必要なコネクションの数を指定します。

有効値: 0 ～ 65535

デフォルト値: 4000

FIN-timeout

コネクションが FIN 状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから未使用コネクション情報の除去を試みます。

有効値: 0 ～ 65535

デフォルト値: 30

FIN-stale-timer

コネクションが非アクティブ状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースからコネクションの情報の除去を試みます。

有効値: 0 ～ 65535

デフォルト値: 1500

例:

```
add cluster
Cluster address [0.0.0.0]? 131.2.24.91
FIN count [4000]?
FIN timeout [30]?
FIN stale timer [1500]?
```

heartbeat *address1 address2*

ハートビート・メッセージ用の 1 つのパスを指定します。高信頼性の動作を行うためには、複数のエントリーを構成することが推奨されます。ハートビート・メッセージは、*address1* (このネットワーク・ディスパッチャーに属する) から *address2* (相手のネットワーク・ディスパッチャーに属する) へ流れます。

address1

ハートビート・メッセージの発信元のこのネットワーク・ディスパッチャーのインターフェースの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

address2

ハートビート・メッセージの着信先の同位ネットワーク・ディスパッチャーのインターフェースの IP アドレスを指定します。このアドレスは、*address1* に指定されたインターフェースから到達可能でなければなりません。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

例:

```
add heartbeat
Source Heartbeat address [0.0.0.0]? 131.2.25.90
Target Heartbeat Address [0.0.0.0]? 131.2.25.92
```

port *cluster-address port# max-weight port-mode*

ポートとポートの属性を指定します。

cluster-address

クラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値: 0 〜 65535

デフォルト値: 80

port-mode

ポートが、1 つのクライアントからのすべての要求を 1 つのサーバーに送る (sticky と呼ばれる) か、パッシブ ftp を使用する (pftp) か、またはこのクラスターでは特定のプロトコルを使用しない (none) かを指定します。

有効値: sticky、pftp、または none

デフォルト値: none

max-weight

このポート上のサーバーの最大重みを指定します。これは、実行プログラムが各サーバーに与える要求数の相違に影響します。

有効値: 0 〜 100

デフォルト値: 20

例:

```
add port
Cluster address [0.0.0.0]? 131.2.25.91
Port number [80]? 80
Max weight (0-100) [20]? 35
Port mode (none=0, sticky=1, pftp=2) [0]?
```

reach *address*

ネットワーク・ディスパッチャーが正しく動作するために到達可能であることが必要なホスト・アドレスを指定します。これは、サーバー・アドレス、ルーター・アドレス、管理ステーション・アドレス、あるいはその他の IP ホストのいずれでも構いません。

address

ターゲット IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

例:

```
add reach
Address to reach [0.0.0.0]?
```

server *cluster-address port# server-address server-weight server-state*

クラスター内のサーバーの属性を指定します。

cluster-address

このサーバーが属するクラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

port# このサーバーへのコネクションを介して実行されるプロトコルを指定します。

有効値: 0 〜 65535

デフォルト値: 80

server-address

サーバーの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

server-weight

実行プログラムのために、サーバーの重みを指定します。これは、ネットワーク・ディスパッチャーがこの特定サーバーに要求を送信する頻度に影響を与えます。

有効値: 0 〜 add port コマンドで指定した *max-weight* の値

デフォルト値: port コマンドの max-weight

server-state

実行プログラムが処理を開始するときに、サーバーを利用可能と見なすか、利用不能と見なすかを指定します。

有効値: 0 (ダウン) または 1 (アップ)

デフォルト値: 1

例:

```
add server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [80]? 80
Server address [0.0.0.0]? 131.2.25.94
Server weight [35]?
Server state (down=0 up=1) [1]?
```

パラメーター構成の制限

表96 は、ネットワーク・ディスパッチャーに構成できる種々の項目の制限をリストしています。

表 96. パラメーター構成の制限

パラメーター	制限
アドバイザー	各 2210 につき 8
クラスター	各 2210 につき 32
ハートビート	各 2210 につき 8
ポート	各クラスターにつき 8
リーチ	各 2210 につき 8
サーバー	各ポートにつき 32

Clear

clear コマンドは、ネットワーク・ディスパッチャー構成全体を消去するのに使用します。

構文:

clear

Disable

disable コマンドは、ネットワーク・ディスパッチャーのコンポーネントを使用不可にするのに使用します。

構文:

disable advisor . . .
backup
executor
manager

advisor *name port*
ネットワーク・ディスパッチャーからアドバイザーを使用不可にします。

name アドバイザーのタイプを指定します。

有効値: 0、1、2

0 = FTP
1 = HTTP
2 = MVS

デフォルト値: 0

port このアドバイザーのポート番号を指定します。

有効値: 0 ～ 65535

デフォルト値: 0

例:

```
 disable advisor
Advisor name (0=ftp, 1=http, 2=mvs) [1]? 1
Port number [0]? 80
```

backup

ネットワーク・ディスパッチャーのバックアップ機能を使用不可にします。

例:

```
 disable backup
Backup is now disabled.
```

executor

ネットワーク・ディスパッチャーの実行プログラムを使用不可にします。実行プログラムを使用不可にすると、ネットワーク・ディスパッチャー機能は使用不可になります。

例:

```
 disable executor
Network dispatcher executor is disabled.
```

注: 実行プログラムを使用不可にすると、マネージャー、アドバイザー、および高可用性機能は停止します (現在実行されている場合)。

manager

ネットワーク・ディスパッチャーのマネージャーを使用不可にします。マネージャーは、オプション・コンポーネントです。ただし、マネージャーを使用しない場合には、ネットワーク・ディスパッチャーは、現行のサーバーの重みに基づき、ラウンドロビン・スケジューリング方式を使用して負荷の平衡を図ります。

例:

```
 disable manager
Network dispatcher manager is disabled.
```

注: マネージャーはアドバイザーの前提条件なので、マネージャーを使用不可にすると、すべてのアドバイザーは実行を停止します。

Enable

enable コマンドは、ネットワーク・ディスパッチャーのコンポーネントを使用可能にするのに使用します。

構文:

enable advisor . . .
backup
executor
manager

advisor *name port*

アドバイザーをネットワーク・ディスパッチャーに使用可能にします。

name アドバイザーのタイプを指定します。

有効値: 0、1、2

0 = FTP

1 = HTTP

2 = MVS

port このアドバイザーのポート番号を指定します。

有効値: 0 ～ 65535

デフォルト値: 0

例:

```
 enable advisor
Advisor name (0=ftp, 1=http, 2=mvs) [1]? 1
Port number [0]? 80
```

注: マネージャー・コンポーネントはアドバイザーの前提条件なので、アドバイザーを使用可能にする前に、マネージャーを使用可能にしておく必要があります。また、アドバイザーを正しく稼働するためには、**set internal-ip-address** コマンドを使用して、内部 IP アドレスを設定しておくことも必要です。 **set internal-ip-address** コマンドの詳細については、 *Nways マルチプロトコル・ルーティング・サービス プロトコルの構成と監視 解説書 第 1 巻 バージョン 3.1* を参照してください。

backup

ネットワーク・ディスパッチャーのバックアップ機能を使用可能にします。

例: enable backup

注: バックアップを使用可能にする前に、少なくとも 1 つのハートビートを追加する必要があります。

executor

ネットワーク・ディスパッチャーの実行プログラムを使用可能にします。

例:

```
enable executor
Network dispatcher executor is enabled.
```

manager

ネットワーク・ディスパッチャーのマネージャーを使用可能にします。

例:

```
enable manager
Network dispatcher manager is enabled.
```

初めてマネージャーを使用可能にすると、以下のデフォルト値を使用して、マネージャー・レコードが作成されます。

Interval:

2 秒

Refresh-Cycle:

2

Sensitivity:

5 %

Smoothing:
1.5

Proportions:

Active:
50%

New: 50%

Advisor:
0

System:
0

上記のパラメーターについての説明は、818ページの『Set』 を参照してください。

List

list コマンドは、ネットワーク・ディスパッチャーに関する情報を表示するのに使用します。

構文:

list all
advisors
backup
cluster
manager
ports
servers

all すべてのネットワーク・ディスパッチャー構成情報を表示します。これには、アドバイザー、バックアップ、クラスター、マネージャー、ポート、およびサーバーに対して表示される情報と同じものが含まれています。

例:

```
NDR Config>
list all

Executor: Enabled

Manager: Enabled

        Interval        Refresh-Cycle   Sensitivity     Smoothing
        2               2               5 %             1.50
        Proportions:    Active  New     Advisor         System
                        50 %    50 %    0 %             0 %

Advisor:
        Name    Port    Interval        TimeOut         State
        http    80      5               0               Enabled
        MVS     10007   15              0               Enabled

Backup: Enabled
        Role            Strategy
        PRIMARY         AUTOMATIC

        Reachability:   Address         Mask            Type
```

```
                              131.2.25.93     255.255.255.255 HOST
                              131.2.25.94     255.255.255.255 HOST

              HeartBeat Configuration:
                 Source Address:  131.2.25.90 Target Address:   131.2.25.92
                 Source Address:  132.2.25.90 Target Address:   132.2.25.92

       Clusters:
              Cluster-Addr    FIN-count       FIN-timeout     Stale-timer
              131.2.25.91     4000            30              1500

       Ports:
              Cluster-Addr    Port#   Weight  Port-Mode
              131.2.25.91     23      20 %    none
              131.2.25.91     80      20 %    none

       Servers:
              Cluster-Addr    Port#   Server-Addr     Weight  State
              131.2.25.91     23      131.2.25.93     20 %    up
              131.2.25.91     23      131.2.25.94     20 %    up
              131.2.25.91     80      131.2.25.93     20 %    up
              131.2.25.91     80      131.2.25.94     20 %    up
```

advisors
ネットワーク・ディスパッチャーのアドバイザーの構成を表示します。

backup
ネットワーク・ディスパッチャーのバックアップ構成を表示します。

cluster
ネットワーク・ディスパッチャーのクラスターの構成を表示します。

manager
ネットワーク・ディスパッチャーのマネージャーの構成を表示します。

ports ネットワーク・ディスパッチャーのポートの構成を表示します。

servers
ネットワーク・ディスパッチャーのクラスターに対応するサーバーの構成を表示します。

Remove

remove コマンドは、ネットワーク・ディスパッチャー構成の一部を削除するのに使用します。

構文:

remove advisor . . .
backup
cluster . . .
heartbeat . . .
port . . .
reach . . .
server . . .

advisor *name port*
ネットワーク・ディスパッチャー構成から特定のアドバイザーを除去します。

name アドバイザーのタイプを指定します。

有効値: 0、1、2

0 = FTP

1 = HTTP

2 = MVS

port このアドバイザーのポート番号を指定します。

有効値: 0 ～ 65535

デフォルト値: 0

例:

```
remove advisor
Advisor name (0=ftp, 1=http, 2=mvs) [1]?
Advisor port [0]? 80
```

backup

高可用性機能を除去します。

注: バックアップは、ハートビートおよびリーチ機能の前提条件なので、バックアップを除去すると、ハートビートおよびリーチは実行を停止します。

例: `remove backup`

cluster *address*

ネットワーク・ディスパッチャー構成からクラスターを除去します。

address

クラスターの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

注: クラスターを除去すると、そのクラスターに関連したすべてのポートおよびサーバーも除去されます。

例:

```
remove cluster
WARNING: Deleting a cluster will make any port or server
         associated with it to also be deleted.
Cluster address [0.0.0.0]? 131.2.25.91
```

heartbeat *address*

ネットワーク・ディスパッチャー構成からハートビート・アドレスを除去します。

address

クラスターの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

例:

```
remove heartbeat
Target address [0.0.0.0]? 131.2.25.92
```

port *cluster-address port#*

ネットワーク・ディスパッチャー構成内の特定クラスターからポートを除去します。

cluster-address

クラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値: 0 〜 65535

デフォルト値: 0

注: ポートを除去すると、そのポートに関連したすべてのサーバーも除去されます。

例:

```
remove port
WARNING: Deleting a port will also delete any servers associated with it.
Cluster address [0.0.0.0]? 7.82.142.15
Port number [0]? 80
```

reach *address*

ネットワーク・ディスパッチャーが到達可能であることが必要なホストのリストからサーバーを除去します。

address

クラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

例:

```
remove reach
Target address [0.0.0.0]? 9.82.142.15
```

server *cluster-address port# server-address*

ネットワーク・ディスパッチャー構成内のクラスターとポートからサーバーを除去します。

cluster-address

クラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値: 0 〜 65535

デフォルト値: 80

server-address

クラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

例:

```
remove server
Cluster address [0.0.0.0]? 7.82.142.15
Port number [0]? 80
Server address [0.0.0.0]? 20.21.22.15
```

Set

set コマンドは、既存のアドバイザー、クラスター、ポート、またはサーバーの属性を変更するのに使用します。ネットワーク・ディスパッチャーのマネージャーの属性を定義することもできます。

構文:

set advisor . . .
cluster . . .
manager . . .
port . . .
server . . .

advisor *name port# interval timeout*

アドバイザーのポート番号、インターバル、およびタイムアウトを変更します。

name アドバイザーのタイプを指定します。

0 = FTP
1 = HTTP
2 = MVS

有効値: 0、1、2

デフォルト値: 1

port このアドバイザーのポート番号を指定します。

有効値: 0 ～ 65535

デフォルト値: 0

interval

アドバイザーが各サーバーのプロトコルを照会する頻度を指定します。この値の半分の時間が、サーバーから応答がないまま満了すると、アドバイザーはそのプロトコルを利用不能と見なします。

有効値: 0 ～ 65535

デフォルト値: 5

timeout

アドバイザーがプロトコルを利用不能と見なすまでに必要な時間間隔 (秒数) を指定します。

マネージャーは、負荷平衡を決めるのに古い情報が使用されるのを防止するために、タイム・スタンプがこのパラメーターで設定され

た時刻より古いアドバイザーからの情報は使用しません。アドバイザー・タイムアウトは、アドバイザー・ポーリング間隔より大きい値でなければなりません。タイムアウトの方が小さいと、マネージャーは使用する必要がある報告を無視してしまいます。デフォルトでは、アドバイザーの報告はタイムアウトになりません。

このタイムアウト値は通常、アドバイザーを使用不可にした場合に適用されます。このパラメーターを、前に説明した interval/2 タイムアウト (これは、サーバーの応答がない時間に関するものです) と混同しないでください。

有効値: 0 〜 65535

デフォルト値: 0、これは、プロトコルは常に利用可能と見なされることを意味しています。

例:

```
set advisor
Advisor name (0=ftp, 1=http, 2=mvs) [0]?
Port number [0]? 21
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 20
```

cluster *address FIN-count FIN-timeout FIN-stale-timer*

ネットワーク・ディスパッチャー構成内のクラスターの FIN-count、FIN-timeout、および FIN-stale-timer を変更します。

address

クラスターの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

FIN-count

実行プログラムが *FIN-timeout* の経過後にネットワーク・ディスパッチャー・データベースから未使用コネクション情報の除去を試みる前に、FIN 状態にあることが必要なコネクションの数を指定します。

有効値: 0 〜 65535

デフォルト値: 4000

FIN-timeout

実行プログラムがネットワーク・ディスパッチャー・データベースから未使用コネクション情報の除去を試みる前に経過する必要がある秒数を指定します。

有効値: 0 〜 65535

デフォルト値: 30

FIN-stale-timer

コネクションが非アクティブ状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースからコネクション情報の除去を試みます。

有効値: 0 〜 65535

デフォルト値: 1500

例:

```
set cluster
Cluster address [0.0.0.0]? 131.2.25.91
FIN count [4000]? 4500
FIN timeout [30]? 40
FIN stale timer [1500]? 2000
```

manager *interval proportion refresh sensitivity smoothing*

マネージャーが要求を満たす最善サーバーを判別するのに使用する値を設定します。

interval

実行プログラムがコネクションの負荷平衡に使用するサーバーの重みを、マネージャーが更新する前に経過する時間 (秒数) を指定します。

有効値: 0 ～ 65535

デフォルト値: 2

proportion

マネージャーが重み付けを決定する際の外部ファクターの相対的な重要度を指定します。比率の合計は 100% に等しくならなければなりません。ファクターには、次のものがありあす。

アクティブ (active)

実行プログラムによって追跡される各 TCP/IP サーバー上のアクティブ・コネクションの数

有効値: 0 ～ 100

デフォルト値: 50

new 実行プログラムによって追跡される各 TCP/IP サーバー上の新規コネクションの数

有効値: 0 ～ 100

デフォルト値: 50

advisor

ネットワーク・ディスパッチャーに定義されたアドバイザーからの入力

有効値: 0 ～ 100

デフォルト値: 0

システム (system)

MVS システム監視ツール WLM からの入力

有効値: 0 ～ 100

デフォルト値: 0

refresh

マネージャーが実行プログラムから状態を要求する頻度を指定します。このパラメーターは、*intervals* の回数として指定します。

有効値: 0 ～ 100

デフォルト値: 2

sensitivity

ポート上のすべてのサーバーの重み比率の変動を指定します。この後、マネージャーは、実行プログラムがコネクションの負荷平衡に使用する重みを更新します。

有効値: 0 ～ 100

デフォルト値: 5

smoothing

サーバーの重みが変動できる量の限界を指定します。平滑化 (smoothing) は、要求の配分が変動する頻度を最小化します。平滑化インデックスが高くなると、重みの変動は少なくなります。平滑化インデックスが低くなると、重みの変動は大きくなります。

有効値: 1.0 ～ 42 949 673.00 間の 10 進値

デフォルト値: 1.5

注: 小数点以下 2 桁までしか指定できません。

例:

```
set manager
Interval (in seconds) [2]? 3
Active proportion [50]? 40
New proportion [50]? 38
Advisor proportion [0]? 20
System proportion [0]? 2
Refresh cycle [2]? 4
Sensitivity threshold [5]? 10
Smoothing index (>1.00) [1.50]? 200
```

port *cluster-address port# weight*

特定のクラスターのポート番号と重みを変更します。

cluster-address

クラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値: 0 ～ 65535

デフォルト値: 80

weight

このポート上のサーバーの重みを指定します。これは、実行プログラムが各サーバーに与える要求数の相違に影響します。

有効値: 0 ～ 100

デフォルト値: 20

例:

```
set port
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]? 23
Max. weight (0-100) [20]? 30
```

server *cluster-address port# server-address weight state*

クラスター内の特定のサーバーのポート番号、サーバー・アドレス、サーバー状態、およびサーバーの重みを変更します。

cluster-address

このサーバーが属するクラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

port# このサーバーへのコネクションを介して実行されるプロトコルを指定します。

有効値: 0 ～ 65535

デフォルト値: 80

server-address

サーバーの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値: 0.0.0.0

state 実行プログラムが処理を開始するときに、サーバーを利用可能と見なすか、利用不能と見なすかを指定します。

有効値: 0 (ダウン) または 1 (アップ)

デフォルト値: 1

weight

実行プログラムのために、サーバーの重みを指定します。これは、ネットワーク・ディスパッチャーがこの特定サーバーに要求を送信する頻度に影響を与えます。

有効値: 0 ～ add port コマンドで指定した *max-weight* の値

デフォルト値: port コマンドの max-weight

例:

```
set server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]? 80
Server address [0.0.0.0]? 131.2.25.94
Server weight [20]? 25
Server state (down=0, up=1) [1]? 1
```

ネットワーク・ディスパッチャー監視コマンドへのアクセス

ネットワーク・ディスパッチャー監視環境にアクセスするには、次のようにします。

1. OPCON プロンプト (*) で **talk 5** と入力する。
2. GWCON プロンプト (+) で **feature ndr** と入力する。

ネットワーク・ディスパッチャー監視コマンド

表97 は、ネットワーク・ディスパッチャー監視コマンドの要約を示しており、表の後に個々のコマンドの説明があります。これらのコマンドは NDR > プロンプトで入力します。

表 97. ネットワーク・ディスパッチャー監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	現在構成されているアドバイザー、クラスター、ポート、またはサーバーの属性を表示します。
Quiesce	これ以上の接続要求をサーバーに送信してはならないことを指定します。ハートビートおよびリーチ機能も一時的に停止します。
Report	アドバイザーおよびマネージャーに関する情報の報告を表示します。
Status	カウンター、クラスター、ポート、サーバー、アドバイザー、マネージャー、およびバックアップの現在の状態を表示します。
Switchover	スタンバイ・モードで動作しているネットワーク・ディスパッチャーを、強制的にアクティブ・ネットワーク・ディスパッチャーにします。このコマンドは、切り替えモードとして「手動」を指定した場合に使う必要があります。
Unquiesce	サーバーが構成されている各ポート上の以前に静止されたサーバーに対して、ネットワーク・ディスパッチャーのマネージャーが 0 より大きい重みを割り当てることを許可します。このアクションにより、選択されたサーバーに対して新規の接続要求を送ることができるようになります。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、ネットワーク・ディスパッチャーに関する情報を表示するのに使用します。

構文:

list advisor
cluster
port
server

advisor

ネットワーク・ディスパッチャーのアドバイザーの構成を表示します。

例:

```
list advisor
Advisor list requested.

-----------------------------------------
| ADVISOR |  PORT  |  TIMEOUT  |  STATUS  |
-----------------------------------------
|  ftp    |    23  |         5 |   ACTIVE |
|  Http   |    80  | unlimited |   ACTIVE |
|  MVS    | 10007  | unlimited |   ACTIVE |
-----------------------------------------
```

ネットワーク・ディスパッチャーの構成

cluster

ネットワーク・ディスパッチャーのクラスターの構成を表示します。

例:

```
list cluster
EXECUTOR INFORMATION:
 --------------------
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996
Number of defined clusters: 2

CLUSTER LIST:
-------------
  131.2.25.91
  10.11.12.2
```

port ネットワーク・ディスパッチャーのポートの構成を表示します。

例:

```
list port
Cluster Address [0.0.0.0]? 131.2.25.91

-----------------------------------------------
| CLUSTER:       131.2.25.91                  |
|---------------------------------------------|
|   PORT   |    MAXWEIGHT   |  STICKY/PFTP    |
|---------------------------------------------|
|     23   |         30     |    neither      |
|     80   |         20     |    neither      |
-----------------------------------------------
```

server ネットワーク・ディスパッチャーのクラスターに対応するサーバーの構成を表示します。

例:

```
list server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port is sticky.................. FALSE
Port is for passive ftp......... FALSE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port is sticky.................. FALSE
Port is for passive ftp......... FALSE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
```

Quiesce

quiesce コマンドは、ハートビートまたはリーチ機能を一時的に停止するか、またはこれ以上の接続要求をサーバーに送信しないように指定するのに使用します。

構文:

quiesce heartbeat

manager

reach

heartbeat *address*

ハートビート機能用に選択されたパスを停止します。 *address* は、このネットワーク・ディスパッチャーのハートビート・メッセージの送信先のリモート・ネットワーク・ディスパッチャーの IP アドレスです。

例:

```
quiesce heartbeat
Remote Address [0.0.0.0]? 131.2.25.94
```

manager *address*

指定されたサーバーには、これ以上の接続要求をしてはならないことを指定します。 *Address* は、そのサーバーの IP アドレスです。

例:

```
quiesce manager
Server Address [0.0.0.0]? 131.2.25.93
```

reach *address*

到達可能かどうかを判別するための、ネットワーク・ディスパッチャーによる指定のアドレスへのポーリングを停止します。ただし、*address* は、到達可能性基準に含まれている IP アドレスです。

例:

```
quiesce reach
Reach Address [0.0.0.0]? 131.2.25.92
```

Report

report コマンドは、アドバイザーまたはマネージャーの報告を表示するのに使用します。

構文:

report advisor

manager

advisor *type port#*

特定のアドバイザーに関する情報の報告を表示します。

type アドバイザーのタイプです。 0 = ftp、1 = http、2 = MVS。

port# ポート番号です。

例:

```
report advisor
0=ftp, 1=http, 2=MVS
Advisor name [0]? 1
Port number [0]? 80

-------------------------------
|      ADVISOR:     http      |
|      PORT:          80      |
-------------------------------
| 131.2.25.93      |       0  |
| 131.2.25.94      |      16  |
-------------------------------
```

manager

現行のマネージャー情報の報告書を表示します。

例:

```
report manager

-----------------------------------
|  HOST TABLE LIST  |   STATUS    |
-----------------------------------
|  131.2.25.93      |    ACTIVE   |
|  131.2.25.94      |    ACTIVE   |
-----------------------------------

-------------------------------------------------------------------------------
|131.2.25.91    |WEIGHT | ACTIVE % 50  |  NEW % 50    | PORT %  0 |SYSTEM %  0|
|               ---------------------------------------------------------------
|PORT:   23     |NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
-------------------------------------------------------------------------------
|131.2.25.93    | 10| 10|  10|        0|  10|        0|   0|     0|-999|    -1|
|131.2.25.94    | 10| 10|  10|        0|  10|        0|   0|     0|-999|    -1|
-------------------------------------------------------------------------------
|PORT TOTALS:   | 20| 20|    |        0|    |        0|    |     0|    |    -2|
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
|131.2.25.91    |WEIGHT | ACTIVE % 50  |  NEW % 50    | PORT %  0 |SYSTEM %  0|
|               ---------------------------------------------------------------
|PORT:   80     |NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
-------------------------------------------------------------------------------
|131.2.25.93    | 10| 10|  10|        0|  10|        1|  16|     0|-999|    -1|
|131.2.25.94    | 10| 10|  10|        0|  10|        1|   3|    16|-999|    -1|
-------------------------------------------------------------------------------
|PORT TOTALS:   | 20| 20|    |        0|    |        0|    |    16|    |    -2|
-------------------------------------------------------------------------------


-----------------------------------------
| ADVISOR |  PORT  |  TIMEOUT  |  STATUS  |
-----------------------------------------
|  http   |    80  | unlimited |   ACTIVE |
|  MVS    | 10007  | unlimited |   ACTIVE |
-----------------------------------------
Manager report requested.
```

Status

status コマンドは、アドバイザー、バックアップ、カウンター、クラスター、マネージャー、ポート、およびサーバーの状態を入手するのに使用します。

構文:

status advisor
backup
cluster
counter
manager
port
server

advisor *type port#*

特定のアドバイザーの状態を入手します。

type アドバイザーのタイプです。 0 = ftp、1 = http、2 = MVS。

port# ポート番号です。

例:

```
status advisor
0=ftp, 1=http, 2=MVS
Advisor name [0]?
```

```
Port number [0]? 21

Advisor ftp on port 21 status:
==============================
Logging level..... 0
Interval.......... 10
```

backup

バックアップ機能の状態を入手します。

例:

```
status backup
 Dumping status ...
 Role : PRIMARY   Strategy : AUTOMATIC  State : ND_ACTIVE Sub-State : ND_SYNCHRONIZED
 <<Preferred Target : 132.2.25.92>>

 Dumping HeartBeat Status ...
 .....Heartbeat target : 131.2.25.92 Status : UNREACHABLE
 .....Heartbeat target : 132.2.25.92 Status : REACHABLE

 Dumping Reachability Status ...
 .....Host:131.2.25.93   Local:REACHABLE
 .....Host:131.2.25.94   Local:REACHABLE
```

cluster *address*

指定されたクラスターの状態を入手します。ただし、*address* は、クラスターの IP アドレスです。

例:

```
status cluster
Cluster Address [0.0.0.0]? 131.2.25.91

EXECUTOR INFORMATION:
 ---------------------
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996

CLUSTER INFORMATION:
 --------------------
Address......................... 131.2.25.91
Number of target ports.......... 2
FIN clean up count.............. 4000
Connection FIN timeout.......... 30
Active connection stale timer... 1500

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port is sticky.................. FALSE
Port is for passive ftp......... FALSE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port is sticky.................. FALSE
Port is for passive ftp......... FALSE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 Active: 0 FIN 0 Status: up Saved Weight: -1
```

counter

すべてのカウンターの状態を入手します。

例:

```
status counter
Internal counters from executor:
--------------------------------
Total number of packets into executor...... 2684
Discarded because headers too short........ 0
Packets to non forwarding address.......... 0
Total packets for cluster processing (C)... 2684
```

```
Packets not addressed to a cluster(port)... 0

Cluster processing results:
---------------------------
Errors..................................... 0
Discarded.................................. 0
Own address................................ 0
Forward requested.......................... 2684
Forward discarded with error............... 0

Other processing problems:
--------------------------
Total packets dropped (C).................. 0
```

manager

マネージャーの状態を入手します。

例:

```
status manager
Number of defined hosts... 2
Sensitivity............... 0%
Smoothing factor.......... 2
Interval.................. 3
Weights refresh cycle..... 4

Active connections gauge proportion......... 40%
New connections counter(delta) proportion... 38%
Advisor gauge proportion.................... 20%
System Metric proportion....................  2%

Manager status requested.
```

port *clusteraddress port#*

特定のポートの状態を入手します。ただし、

clusteraddress
クラスターの IP アドレスです。

port# クラスターのポート番号です。

例:

```
status port
Cluster Address [0.0.0.0]? 131.2.25.91
Port number [0]? 80

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port is sticky.................. FALSE
Port is for passive ftp......... FALSE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 Active: 3431 FIN 3780 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890  Active: 2980 FIN 2390 Status: up Saved Weight: -1
```

server *address*

特定のサーバーの状態を入手します。ただし、*address* は、サーバーが属するクラスターの IP アドレスです。

例:

```
status server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port is sticky.................. FALSE
Port is for passive ftp......... FALSE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 140 Active: 50 FIN 45 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 250 Active: 60 FIN 54 Status: up Saved Weight: -1
```

```
PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port is sticky.................. FALSE
Port is for passive ftp......... FALSE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 Active: 3431 FIN 3780 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890  Active: 2980 FIN 2390 Status: up Saved Weight: -1
```

Switchover

switchover コマンドは、切り替え方式が「手動」の場合、スタンバイ・モードで動作しているネットワーク・ディスパッチャーを、強制的にアクティブ・ネットワーク・ディスパッチャーにするのに使用します。このコマンドは、スタンドバイ・モードのネットワーク・ディスパッチャーが稼働しているホストで入力する必要があります。

構文:

switchover

Unquiesce

unquiesce コマンドは、以前に **quiesce** コマンドを使用して停止したハートビート、マネージャー、またはリーチ機能をリスタートするのに使用します。

構文:

unquiesce heartbeat
manager
reach

heartbeat *address*

ハートビート・メッセージ用のパスをリスタートします。ただし、*address* は、このネットワーク・ディスパッチャーのキープアライブ・メッセージの送信先のリモート・ネットワーク・ディスパッチャーの IP アドレスです。

例:

```
unquiesce heartbeat
Remote Address [0.0.0.0]? 9.10.11.1
```

manager *address*

指定のサーバーへの接続要求の送信をリスタートします。 *Address* は、そのサーバーの IP アドレスです。

例:

```
unquiesce manager
Server Address [0.0.0.0]? 20.21.22.15
```

reach *address*

到達可能かどうかを判別するための、ネットワーク・ディスパッチャーによる指定のアドレスへのポーリングをリスタートします。ただし、*address* は到達可能性基準に含まれている IP アドレスです。

例:

```
unquiesce reach
Reach address [0.0.0.0]? 20.3.4.5
```

第62章 データ圧縮サブシステムの使用

この章では、フレーム・リレーおよび PPP インターフェースを介した 2210 上のデータ圧縮について説明します。本章には、以下の節が含まれています。

- 『データ圧縮の概説』
- 『データ圧縮の概念』

データ圧縮は、フレーム・リレーおよび PPP インターフェースでサポートされます。

データ圧縮の概説

データ圧縮は、装置上のネットワーク・インターフェースの有効帯域幅を増やす手段を提供します。主として低速の WAN リンクでの使用を目的としています。

装置上のデータ圧縮は、PPP およびフレーム・リレー・インターフェースでサポートされます。

- PPP インターフェースの場合、圧縮は、インターネット技術作業部会の RFC 1962 に定義されている圧縮制御プロトコル (CCP) に準拠して実現されています。 CCP は、圧縮の使用を交渉する基礎になる機構、および複数の可能な圧縮アルゴリズムまたはプロトコルの中から選択する手段を提供します。

  この装置は、2 種類の圧縮プロトコルを提供します。すなわち、RFC 1974 に定義されている Stac-LZS と、RFC 2118 に記述されている Microsoft ポイント・ポイント圧縮プロトコル (MPPC) です。これらは両方とも Stac Electronics によって提供された圧縮アルゴリズムに基づいています。
- フレーム・リレー・インターフェースの場合、圧縮は、フレーム・リレー・フォーラム技術委員会によって作成された FRF.9、 *Data Compression over Frame Relay Implementation Agreement* に準拠して実現されています。 FRF.9 は、データ圧縮プロトコル (DCP) を記述し (PPP の CCP をモデルにした)、同様に、各種の圧縮アルゴリズムおよびオプションを交渉する手段を提供しています。装置は DCP 『モード 1』 ネゴシエーションをサポートします。 FRF.9 には、より汎用化された 『モード 2』 も記述されていますが、これはサポートされません。圧縮そのものは、PPP Stac-LZS プロトコルで使用されるのと同じ圧縮エンジンを使用して行われます。

データ圧縮の概念

装置上のデータ圧縮は、リンク上の利用可能な帯域幅をより効率的に使用して、ネットワーク・リンクのスループットを高める手段を提供します。その基本原理は簡単です。つまり、リンクを流れるデータをできるだけコンパクトな形にすることにより、一定の速度のリンクで転送にかかる時間をできるだけ少なくすることです。

データ圧縮は、ネットワーク・モデルのさまざまなレイヤーで実行できます。たとえば、あるアプリケーションがネットワーク上の別の場所にある同位アプリケーションにデータを転送する前に圧縮したり、あるいは単に 2 つのノード間でビット列の受け渡しを行っているデータ・リンク・レイヤーで装置が圧縮を行うといったこと

が可能です。この圧縮の方法とその効率は、さまざまなファクターによって決まります。このファクターとしては、圧縮を実行するネットワーク・レイヤー、圧縮機能と解凍機能が持っている圧縮されるデータに対する知識、選択された圧縮アルゴリズム、および圧縮される実際のデータなどがあります。通常は、最良の圧縮を達成できるのは、アプリケーション・レイヤーです。たとえば、ファイル転送アプリケーションは、圧縮する前にデータ・ファイル全体を入手できるので、ファイルに対して各種の圧縮アルゴリズムを試し、その特定ファイルのデータに最適なアルゴリズムを見つけることができます。しかし、これはその 1 つタイプのアプリケーションの圧縮としてはすぐれているかもしれませんが、ネットワーク上を流れる大量のトラフィックの圧縮の一般的問題の解決にはあまり役に立ちません。現在、ほとんどのネットワーク・アプリケーションは、データを生成する時点で圧縮していないからです。

装置での圧縮は、これよりはるかに低いネットワーク・レイヤー、つまりデータ・リンク・レイヤーで行われます。装置内で、リンクを介して転送される個々のパケットが圧縮されます。圧縮はパケットが装置を通過するときにリアルタイムで行われます。送信側は転送する直前にパケットを圧縮し、受信側は受信すると同時にパケットを解凍します。この動作は、高位レイヤーのネットワーク・プロトコルには透過的です。

データ圧縮の基本

データ圧縮機能は、データ内の 『冗長』 情報を認識し、できるだけ冗長度の少ない別のデータ・セットを生成します。『冗長』 情報というのは、現在利用可能なデータに基づいて導出し、再作成することが可能な情報を言います。たとえば、圧縮機能は、データ・ストリーム内の反復文字パターンを認識し、これらの反復パターンを、そのパターンを表す短い符号列で置き換えます。圧縮機能と解凍機能でこれらの符号列に関する認識が一致している限り、必ず解凍機能は圧縮されたデータから元のデータを再作成することができます。

元のデータ内のシーケンスを、圧縮された出力の対応するシーケンスにマッピングしたものを、一般に***データ・ディクショナリー*** と呼んでいます。これらのディクショナリーは、静的に定義すること (圧縮機能と解凍機能が利用できる経験に基づく情報) も、動的に生成すること (通常は、圧縮している情報に基づく) もできます。静的ディクショナリーは、処理されるデータが限定された既知の性質を持っており、汎用圧縮機能を使用してもあまり効率的ではない環境に最適です。ほとんどの圧縮システム (装置上の圧縮機能も含む) は、動的ディクショナリーを使用しています。 2210 上のデータ・ディクショナリーは、現在処理中のパケットと以前に処理されたパケットについての知識に基づいていますが、他のレイヤーで圧縮が行われるときに存在する可能性があるデータ・ストリームを 『見通す』 能力は備えていません。データ・ディクショナリーが動的に生成され、以前に処理されたデータにのみ基づくシステムは、***ヒストリー*** とも呼ばれます。 この章の残りの部分ではヒストリーとデータ・ディクショナリーという用語を同義の用語として使用しますが、他の環境では、ヒストリーは特定の形のデータ・ディクショナリーを表すことを理解しておくことが必要です。

装置は動的ディクショナリーを使用し、圧縮機能と解凍機能はそれぞれのディクショナリーを同期に保つ必要があるということは、データ圧縮は 2 つのエンドポイント間で受け渡されるデータ・ストリームに適用されることを意味しています。つま

り、ルーター上の圧縮はコネクション指向のプロセスであり、コネクションのエンドポイントは、圧縮機能と解凍機能そのものです。ストリーム上で圧縮が開始されると、両端はそれぞれのデータ・ディクショナリーを事前設定された開始状態にリセットし、データを受信するとその状態を更新します。

各パケットごとに個別に圧縮を実行し、各パケットを処理する前にヒストリーをリセットすることも可能です。しかし通常は、パケットとパケットの間ではデータ・ディクショナリーはリセットされません。これは、ヒストリーは現行パケットの内容だけでなく、以前に処理されたパケットの内容にも基づくことを意味しています。これにより、圧縮機能が冗長度を除去するために探索するデータの量が増えるので、全体的な圧縮効率が上がるのが一般的です。一例として、あるホストが IP を使用して別のホストに 『PING』 している場合を考えてみます。一連のパケットが送信されますが、各パケットは通常、直前に送信されたパケットとほぼ同じです。圧縮機能は、最初のパケットの圧縮ではあまり効率を上げることができないかもしれませんが、後続のパケットがそれぞれ直前に送信されたものに非常によく似ていることを認識し、それらのパケットでは非常に圧縮されたバージョンを生成できるようになります。

圧縮機能と解凍機能のヒストリーは、各パケットを受信するたびに変更されるので、圧縮機構はパケットの損失、破壊、または再配列を検知できます。装置で採用されている圧縮プロトコルには、シグナル機構が組み込まれており、これにより圧縮機能と解凍機能が同期の喪失を検出し、相互に再同期できるようになっています (たとえば、伝送誤りのためにパケットが損失した場合などに必要になります)。これは通常、各パケットにシーケンス番号を含め、解凍機能がこの番号をチェックして、すべてのパケットを順序通りに受信していることを確認する方法で行われます。誤りを検出すると、自身を事前設定された開始状態にリセットし、圧縮機能にも同様にリセットするようにシグナルし、圧縮機能自体もリセットしたことを知らせる確認応答を待ちます (着信した圧縮パケットを廃棄して)。

リンクでの圧縮は一般的に、リンク上の両方向のデータに対して実行されます。通常は、834ページの図44 に示すように、コネクションの各端に圧縮機能と解凍機能の両方があり、コネクションの他端の相手と通信します。出力 (圧縮) 側は、入力 (解凍) 側から独立して動作します。リンクの各方向でまったく異なる圧縮アルゴリズムを使用することも可能です。リンク・コネクションが確立されると、そのリンクの圧縮制御プロトコルが相手側と交渉し、そのコネクションで使用する圧縮アルゴリズム (1 つまたは複数) を決めます。 2 つの端が使用する圧縮プロトコルについて合意できない場合には、圧縮は行われず、リンクは通常どおりに動作します (つまり、パケットは圧縮されない形で送信されます)。

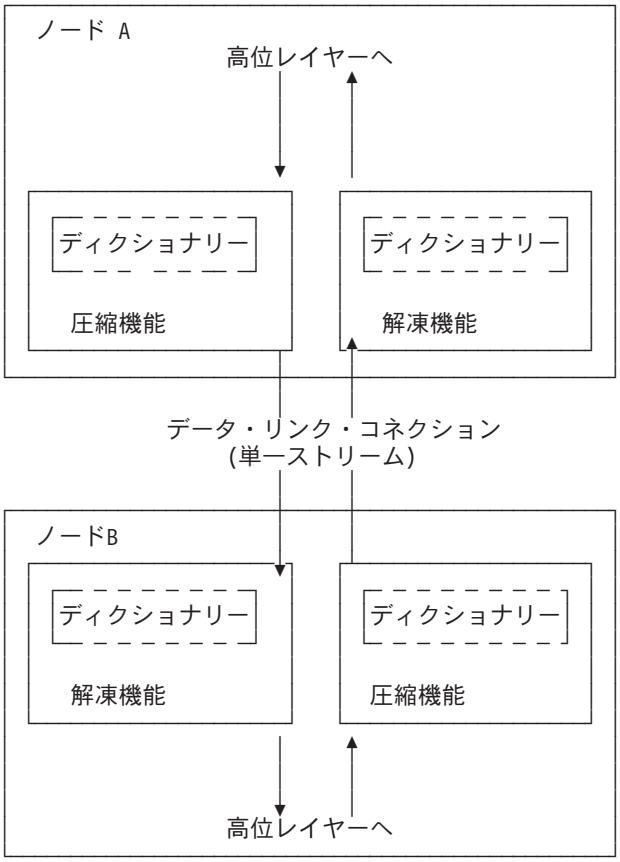


図 44. データ・ディクショナリーを使用した双方向データ圧縮の例

ストリームというのは、実際には、リンクの一端の特定の圧縮プロセスとリンクの他端の対応する解凍プロセス間のコネクションを表しているので、単なる 2 つのノード間の 『コネクション』 ではなく、より特定的な意味をもっています。精巧な圧縮プロトコルは、2 つのホスト間のデータ・フローを複数のストリームに分割し、個々のストリームを独立して圧縮することも可能です。たとえば、PPP の CCP は、単一の PPP リンク上で複数のヒストリーを使用することを交渉できます。ただし、ルーターはこれをサポートしません。

考慮事項

データ圧縮を使用するか、しないかの選択は、必ずしも容易ではありません。コネクション上の圧縮を使用可能にする前に、いくつかの要因を考慮する必要があります。

CPU 負荷

データ圧縮は、演算に負担のかかる手順です。圧縮するデータの量が増えるほど (単位時間当り)、装置のプロセッサーにかかる負荷が大きくなります。負荷が大きくなり過ぎると、圧縮が行われる装置だけでなく、すべてのネットワーク・インターフェース上の装置の性能が低下します。

実際上は、装置には複数のプロセッサーが搭載されており、非対称マルチプロセッシングを使用しているので (たとえば、メイン・プロセッサーと直列式で動作するリンク入出力処理装置)、プロセッサーの負荷への影響は、必ずしも簡単に測定できるわけではありません。圧縮動作はパケットの転送とオーバーラップしている部分があるので、この負荷は事実上まったく透過的であり、問題がない場合もあります。しかし、装置のプロセッサーに過剰な負担をかけ、性能を低下させる可能性もあります。

おおまかな原則として、圧縮を使用可能にするのは、低速の WAN リンク、つまり速度が約 64 KB (標準的な ISDN ダイヤル・リンクの速度) までのリンクにのみ限るべきです。すべてのリンク上の圧縮されるデータの総帯域幅は、1 秒につき数百 KB に限定する必要があるものと思われます。 ISDN 1 次群速度アダプターのすべてのチャネルで圧縮を実行するのは賢明でありません。

装置構成パラメーターの中には、同時に圧縮を実行できるコネクションの数を制限することができるものがあります。その場合、実際に圧縮を実行している台数より多くのインターフェースに対して、圧縮を使用可能に設定することも可能です。アクティブ圧縮コネクション数の限界に達すると、少なくとも既存の圧縮リンクが切断されるまでは、追加のコネクションは圧縮の使用を交渉しなくなるだけです。

メモリーの使用量

圧縮を構成するときに考慮する必要がある 1 つの問題は、メモリー所要量です。圧縮および解凍ヒストリーは、装置の限られた資源であるメモリーをかなり使用します。たとえば、Stac-LZS アルゴリズムでは、圧縮ヒストリーに約 16 KB、解凍ヒストリーに約 8 KB 必要です。これらのヒストリーは、確立される各コネクションごとに存在しなければならない (圧縮ヒストリーは、相手側ルーター内の対応する解凍ヒストリーと同期される) ので、この問題は一層大きくなります。 PPP リンクの場合、これは 1 つの圧縮ヒストリーと 1 つの解凍ヒストリーを意味しています (リンク上のデータ圧縮が双方向で実行されているものと想定した場合)。フレーム・リレー・リンクの場合は、このようなヒストリーが多数必要になる可能性があります (確立される各バーチャル・コネクション (DLCI) ごとに 1 組み)。

装置は、ブート時に、一定数の圧縮ヒストリーと解凍ヒストリーを割り振ります。これらは常に組みにして、***圧縮コンテキスト*** として (コンテキストは、1 つの圧縮ヒストリーと 1 つの解凍ヒストリーを単に結合したもの) 割り振られます。技術的には、圧縮と解凍は独立した機能であり、圧縮ヒストリーと解凍ヒストリーの割り当ては独立して行うことが可能ですが、実際上は、圧縮はいつも双方向で実行されるのが一般的なので、運用を簡単にするために、メモリーの管理と構成は、個々のヒストリーではなく、コンテキストを対象にして行われます。各コンテキストには 24 KB が割り振られ、これには圧縮および解凍ヒストリーに必要なメモリーが含まれています。

装置がリンク上で圧縮コネクションの確立を試みる際には、必ず割り振られたコンテキストのプールから 1 つのコンテキストを確保することから始めます。利用可能なコンテキストがない場合には、そのコネクションでは圧縮は行われません。ルーターは、後でコンテキストが利用可能になった時点で、そのコネクションでの圧縮の開始を試みることもできます。

割り振られる圧縮コンテキストの数は、構成可能なパラメーターです。 割り振られるコンテキスト数の設定値は、使用されるメモリーの量と、圧縮を使用して同時に動作できるコネクションの最大数の両方を制限します。同時に動作する圧縮コネクションの数を制限することは、CPU の負荷問題を制御するのに役立つ 1 つの手段となります。

データの内容

あるコネクションの圧縮を使用可能にする前に、そのコネクションで転送されるデータの実際の性質を考慮することが必要です。圧縮は、データのタイプによって効果がさまざまです。ほぼ同一の情報が多数含まれているパケット (たとえば、IP『PING』 によって生成される 1 組のパケット) は、一般的に非常によく圧縮されます。リンクを通る標準的なランダム・テキストおよび 2 進データの圧縮比率は 1.5:1 ～ 3:1 程度です。まったく圧縮されないデータもあります。特に、すでに圧縮されているデータは、さらに圧縮されることはめったにありません。事実、以前に圧縮されたデータが圧縮エンジンを通過するときに、実際上拡張されることもあります。

あるコネクションを通るデータのほとんどが圧縮データから成ることが前もって分かっている場合には、そのコネクションでは圧縮を使用可能にしないことをお勧めします。これに該当する例として、主に FTP ファイル・アーカイブ・サイト用として設定されたホストへのコネクションがあります。この場合、転送に使用されるファイルはすべて、圧縮した形でホストに保管されています。

リンク・レイヤーの圧縮

考慮する必要がある要因の最後のものは、2 つのホスト間のネットワーク・リンクの性質です。圧縮は、装置のハードウェア・インターフェースよりも下位レイヤーで実行される可能性があります。特に、多くの最新モデムには、そのハードウェアとファームウェアにデータ圧縮機構が組み込まれています。下位レイヤー (装置の外部) のリンクで圧縮が行われる場合には、そのインターフェースの装置上のデータ圧縮を使用可能にしないのが最善です。前にも述べたように、すでに圧縮されたデータ・ストリームを圧縮しても、通常は無効であり、実際に性能がいくぶん低下することもあります。ルーターの方がリンク・ハードウェアよりはるかに圧縮効率が高いと確信できる特別な理由がない限り、圧縮はリンク・ハードウェアに任せるのが最良です。

PPP リンク上でのデータ圧縮の使用

2210 は、PPP 圧縮制御プロトコル (CCP) を使用して、リンク上での圧縮の使用を交渉します。 CCP は、特定の圧縮プロトコル (リンクの各方向に異なるプロトコルを使用することも可能です) および各種のプロトコル特有のオプションの使用を交渉するための汎用機構を提供します。このソフトウェアは Stac-LZS および MPPC プロトコルをサポートするので、2 つのノード間でデータ圧縮の交渉を正常に行うためには、相手側も少なくともこれらのアルゴリズムの 1 つがサポートされることが必要です。また、圧縮が機能するためには、2 つのノード間でアルゴリズム特有のオプションについても合意する必要があります。

PPP リンク上のデータ圧縮の構成

PPP リンク上のデータ圧縮を構成するには、次のようにします。

1. **enable ccp** コマンドを使用して、リンク上の CCP プロトコルを使用可能にする。これにより、リンクは他のノードと圧縮を交渉できるようになります。交渉には、使用する圧縮プロトコルとプロトコル特有のオプションが含まれます。
2. **set ccp protocols** コマンドを使用して、交渉できる圧縮プロトコルを選択する。
3. **set ccp options** コマンドを使用して、各圧縮プロトコルの交渉可能パラメーターを設定する。

list ccp コマンドを使用すると、現行の圧縮構成を表示することができます。

表98 は、利用可能なコマンドをリストし、図45 は、PPP リンク上の圧縮の構成例を示しています。これらのコマンドについての詳しい説明は、484ページの『ポイント・ポイント構成コマンド』 を参照してください。

表 98. PPP データ圧縮構成コマンド

データ圧縮コマンド	アクション
disable ccp	データ圧縮を使用不可にします。
enable ccp	データ圧縮を使用可能にします。
set ccp options	圧縮アルゴリズムのオプションを設定します。
set ccp algorithms	圧縮プロトコルの優先順位付けされたリストを指定します。
list ccp	圧縮構成を表示します。

```
Config> network 1 1

Point-to-Point user configuration
PPP Config> enable ccp
PPP Config> set ccp options 2
STAC: # histories [1]? 1
STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext) [3]? 3
PPP Config> list ccp
CCP Options
-----------

Data Compression enabled
Algorithm list: STAC-LZS
Stac: histories 1
Stac: check_mode SEQ
```

図 45. PPP リンク上の圧縮の構成例

注:

1. network コマンドは、PPP リンクのネットワーク・インターフェースを選択します。リンクが PPP ダイヤル回線の場合は、**encapsulator** コマンドを使用して、PPP 構成メニューにアクセスすることが必要です。
2. CCP を使用可能にしたが、リンクのプロトコルを設定しなかった場合、ソフトウェアは自動的にリンクがプロトコル STAC および MPPC を使用するように設定します (これは、コマンド **set ccp protocols stac mppc** を入力した場合と同じです)。

   複数のプロトコルを設定する場合、プロトコルの設定順序によって、そのリンクの交渉の優先順位が決まります。

ルーターが 1 つのリンク上で複数の圧縮プロトコルをサポートしている場合、ある種のダイヤルイン・クライアントを接続できない場合があります。このような状態になった場合は、ccp プロトコルを STAC または MPPC に設定してください。

3. **set ccp protocols none** を入力すると、ソフトウェアは自動的にリンク上の圧縮を使用不可にします。

PPP リンク上の圧縮の監視

圧縮の監視は、他の PPP コンポーネントの監視と同様です。 501ページの『インターフェース監視プロセスへのアクセス』 で、PPP コンソール環境へのアクセス方法とコマンドの詳細について説明しています。 表99 は、圧縮関連のコマンドをリストしています。 図46 は、PPP インターフェース上の圧縮のリスト例です。

表 99. PPP データ圧縮監視コマンド

コマンド	機能
list control ccp	CCP 状態と交渉済みのオプションをリストします。
list ccp	CCP パケット統計をリストします。
list cdp または **list compression**	圧縮データグラム統計をリストします。

```
+ network 1
PPP > list control ccp

CCP State:                Open
Previous State:           Ack Sent
Time Since Change:        2 minutes and 52 seconds

Compressor:   STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ

PPP > list ccp

CCP Statistic             In                        Out
-------------             --                        ---

Packets:                  2                         3
Octets:                   18                        27
Reset Reqs:               0                         0
Reset Acks:               0                         0
Prot Rejects:             1                         -

PPP > list cdp

Compression Statistic     In                        Out
---------------------     --                        ---

Packets:                  19541                     19542
Octets:                   2550673                   2740593
Compressed Octets:        821671                    899446
Incompressible Packets:   0                         0
Discarded Packets:        0                         -
Prot Rejects:             0                         -
Compression Ratios:       3.11                      3.24
```

図 46. PPP インターフェース上の圧縮の監視

フレーム・リレー・リンク上でのデータ圧縮の使用

グローバル圧縮パラメーターを構成し、インターフェース上の圧縮を使用可能にした後で、フレーム・リレー・インターフェース上の個々の回線 (PVC) のパラメーターを設定する必要があります。インターフェースに定義されている各回線上の圧縮を使用可能にすることができ、交渉が正常に行われた各回線は、グローバル・プールから 1 つの圧縮コンテキストを使用します。また、インターフェース上の圧縮を使用不可にすることもできます。これは、そのインターフェース上のどの回線も、圧縮されたデータ・トラフィックを伝送できなくなることを意味しています。

フレーム・リレー・リンク上のデータ圧縮の構成

FR リンク上のデータ圧縮を構成するには、次のようにします。

1. **enable compression** コマンドを使用して、インターフェース上の圧縮を使用可能にする。これにより、リンクは他のノードと圧縮を交渉できるようになります。
2. **add permanent-virtual-circuit** コマンドを使用して、圧縮データを伝送する各新規 PVC 上の圧縮を使用可能にする。 **change permanent-virtual-circuit** コマンドを使用すると、既存の PVC を変更できます。

現行の圧縮構成を表示したい場合は、**list lmi** または **list permanent-virtual-circuit** コマンドを使用します。

840ページの表100 は、フレーム・リレー・リンク上の圧縮を構成するのに利用可能なコマンドをリストしています。また、840ページの図47 は、フレーム・リレー・リンクの構成例を示しています。フレーム・リレー構成コマンドについての詳細は、429ページの『フレーム・リレー構成コマンド』 を参照してください。

```
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Maximum number of run-time compression PVCs (zero means no limit) [0]? 0
Do you want orphan PVCs to perform compression [Y]? n
The number of currently defined non-compression PVCs is 4
Would you like to change them all to compression PVCs [N]? y

FR Config> add perm

Circuit number [16]? 22
Committed Information Rate (CIR) in bps [65536]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []? cir22
Is circuit required for interface operation [N]?
Do you want to have data compression performed [Y]?

FR Config>list lmi

                        Frame Relay Configuration


  LMI enabled            =      No  LMI DLCI                       =       0
  LMI type               =    ANSI  LMI Orphans OK                 =     Yes
  CLLM enabled           =      No  Timer Ty seconds               =      11

  Protocol broadcast     =     Yes  Congestion monitoring          =     Yes
  Emulate multicast      =     Yes  CIR monitoring                 =      No
  Notify FECN source     =      No  Throttle transmit on FECN      =      No

  Data compression       =     Yes  Orphan compression             =      No
  Compression PVC limit  =    None  Number of compression PVCs     =       2

  PVCs P1 allowed        =      64  Interface down if no PVCs      =      No
  Timer T1 seconds       =      10  Counter N1 increments          =       6
  LMI N2 error threshold =       3  LMI N3 error threshold window =       4
  MIR % of CIR           =      25  IR % Increment                 =      12
  IR % Decrement         =      25  DECnet length field           =      No
  Default CIR            =   65536  Default Burst Size            =   64000
  Default Excess Burst   =       0

FR Config>list perm

  Maximum PVCs allowable =      64
  Total PVCs configured  =       2

             Circuit                Circuit   Circuit     CIR    Burst  Excess
              Name                  Number     Type      in bps  Size   Burst
---------------------------------- ------- ----------- ------- ------- -----
 circ16                              16    @ Permanent   65536   64000       0
 cir22                               22    @ Permanent   65536   64000       0

* = circuit is required
# = circuit is required and belongs to a required PVC group
@ = circuit is data compression capable
```

図 47. フレーム・リレー・リンク上の圧縮の構成例

表 100. データ圧縮構成コマンド

コマンド	アクション
add permanent-virtual-circuit #	インターフェース上に定義された特定の PVC 上のデータ圧縮を使用可能にするのに使用します。
change permanent-virtual-circuit #	特定の PVC がデータを圧縮するかどうかを変更するのに使用します。
disable compression	データ圧縮を使用不可にします。
enable compression	データ圧縮を使用可能にします。
list lmi	インターフェースの現行構成を表示します。

表 100. データ圧縮構成コマンド (続き)

コマンド	アクション
list permanent	回線に関する要約情報をリストします。

注: オーファン回線上の圧縮を使用可能にすると、装置上のネイティブ PVC が利用可能な圧縮コンテキストの数が減ります。

すでに圧縮が使用可能になっているフレーム・リレー・インターフェース上の圧縮を使用可能にすると、ソフトウェアは、841ページに示すように、圧縮パラメーターを変更したいかどうかを尋ねます。圧縮を使用不可にせずに、インターフェース上の圧縮を変更できます。

```
Example of changing compression on Frame Relay Interfaces
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Data compression already enabled.
Do you wish to continue and change an interface parameter [Y]
Maximum number of run-time compression PVCs (zero means no limit) [0]? 32
Do you want orphan circuits to perform compression []?
Do you want to change the compression capability of all of your existing PVCs [N]?
```

フレーム・リレー・リンク上のデータ圧縮の監視

圧縮の監視は、他のフレーム・リレー・コンポーネントの監視と同様です。 453ページの『フレーム・リレー監視コマンド』 で、フレーム・リレー・コンソール環境へのアクセス方法とコマンドの詳細について説明しています。 表101 は、圧縮関連のコマンドをリストしています。 『フレーム・リレー・インターフェースまたは回線上の圧縮の監視の例』 は、フレーム・リレー・インターフェース上の圧縮のリスト例です。

表 101. フレーム・リレー・データ圧縮監視コマンド

コマンド	表示
list lmi	インターフェースの現在の状態をリストします。
list permanent	回線に関する要約情報をリストします。
list circuit	回線の現在の状態をリストします。

フレーム・リレー・インターフェースまたは回線上の圧縮の監視の例

```
+ network 2
FR 2 > list lmi

Management Status:
  ------------------

    LMI enabled          =      No  LMI DLCI                  =       0
    LMI type             =    ANSI  LMI Orphans OK            =     Yes
    CLLM enabled         =      No

    Protocol broadcast   =     Yes  Congestion monitoring     =     Yes
    Emulate multicast    =     Yes  CIR monitoring            =      No
    Notify FECN source   =      No  Throttle transmit on FECN =      No
    PVCs P1 allowed      =      64  Interface down if no PVCs =      No
    Line speed (bps)     =   64000  Maximum frame size        =    2048
    Timer T1 seconds     =      10  Counter N1 increments     =       6
    LMI N2 threshold     =       3  LMI N3 threshold window   =       4
    MIR % of CIR         =      25  IR % Increment            =      12
    IR % Decrement       =      25  DECnet length field       =      No
    Default CIR          =   65536  Default Burst Size        =   64000
    Default Excess Burst =       0
```

```
   Current receive sequence  =  0
   Current transmit sequence =  0
   Total status enquiries    =       0  Total status responses   =       0
   Total sequence requests   =       0  Total responses          =       0

   Data compression enabled  =     Yes  Orphan Compression       =      No

   Compression PVC limit     =    None  Active compression PVCs  =       1

  PVC Status:
  -----------

   Total allowed  =      64  Total configured  =       1
   Total active   =       1  Total congested   =       0
   Total left net =       0  Total join net    =       0

FR 2 > list permanent

 Circuit                                  Orphan  Type/   Frames      Frames
 Number            Circuit Name           Circuit State Transmitted  Received
 ------- -------------------------------- ------- ----- ----------- --------

     16  circ16                             No   @ P/A        58364      58355
     22  circ22                             No   & P/A        58364      58355

    A - Active   I - Inactive   R - Removed   P - Permanent   C - Congested
    * - Required               # - Required and belongs to a PVC group
    @ - Data compression capable but not operational
    & - Data compression capable and operational
FR 2 > list circuit 22

 Circuit name = circ22

     Circuit state        =    Active  Circuit is orphan   =           No
     Frames transmitted   =     58391  Bytes transmitted   =      2676894
     Frames received      =     58383  Bytes received      =      2671009
     Total FECNs          =         0  Total BECNs         =            0
     Times congested      =         0  Times Inactive      =            0
     CIR in bits/second   =     65536  Potential Info Rate =        64000
     Committed Burst (Bc) =     64000  Excess Burst (Be)   =            0
     Minimum Info Rate    =     16000  Maximum Info Rate   =        64000
     Required             =        No  PVC group name      =   Unassigned

     Compression capable  =       Yes  Operational         =          Yes
     R-R's received       =         0  R-R's transmitted   =            0
     R-A's received       =         0  R-A's transmitted   =            0
     R-R mode discards    =         0  Enlarged frames     =            0
     Decompress discards  =         0  Compression errors  =            0
     Rcv error discards   =         0

     Compression ratio    =  1.00 to 1  Decompression ratio =    1.00 to 1

     Current number of xmit frames queued                  =            0
     Xmit frames dropped due to queue overflow             =            0
```

第63章 データ圧縮の構成と監視

2210 上のデータ圧縮の構成は、2 段階のプロセスです。中心となる圧縮システムは、ソフトウェアの 『機能』 です。構成および監視タスク (ルーター内の GWCON および CONFIG プロセス) で CMPRS 機能を選択することにより、グローバル・パラメーターを設定したり、監視したりすることができます。グローバル・パラメーターの構成に加えて、圧縮データ・トラフィックを転送する各ネットワーク・インターフェース (PPP またはフレーム・リレー) の圧縮も構成する必要があります。

この節では、最初に圧縮機能の構成と監視について説明し、その後で PPP およびフレーム・リレー・インターフェース上の圧縮の構成と監視について説明します。

構成機能の構成

圧縮機能の唯一の構成可能パラメーターは、装置のブート時に割り振られる圧縮コンテキストの数です。使用可能なコンテキストの数によって、同時にアクティブにできるコネクションの数が制限されるとともに、圧縮ヒストリー用に確保しておくメモリーの量が決まります。コンテキストの数をゼロに設定すると、すべてのインターフェース上の圧縮が使用不可にされます。

構成プロセスで、圧縮構成コマンドにアクセスするために、`Config >` プロンプトで **feature cmprs** コマンドを入力します。割り振られるコンテキストの数を変更する場合は、**SET MAXCONTEXTS *n*** コマンドを使用します。ただし、***n*** はコンテキストの数です。現行の構成を見たい場合は、**list** コマンドを使用します。構成コマンド・セット全体の要約を 表102 に示し、構成例を 図48 に示します。

```
Config> feature cmprs

Data Compression Global Configuration
CMPRS Config> ?
LIST
SET
EXIT

CMPRS Config> set ?
MAXCONTEXTS

CMPRS Config> set maxcontexts
Number of compression contexts to allocate? (0 - 1000) [0]? 10

CMPRS Config> list
Number of compression contexts to allocate: 10
```

図 48. 圧縮機能の構成

表 102. 圧縮構成コマンド

コマンド	アクション
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	maxcontexts の現行の設定値を表示します。

表 102. 圧縮構成コマンド (続き)

コマンド	アクション
Set	すべてのインターフェースで利用可能な圧縮コンテキストの最大数を設定します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、*maxcontexts* の現行の設定値を表示するのに使用します。

構文:

list

Set

set コマンドは、データ圧縮を同時に使用できるインターフェースの最大数を設定するのに使用します。

構文:

set maxcontexts *n*

maxcontexts *n*

インターフェースで利用可能な圧縮コンテキストの最大数を設定します。このパラメーターにより、装置は圧縮コンテキスト用のメモリー・プールを割り振ります。 maxcontexts を 0 に設定すると、たとえインターフェース上の圧縮を使用可能にしても、どのインターフェースでもデータの圧縮は行われません。

注: この値を高く設定し過ぎると、過剰なメモリーが使用され、装置のスループットを低下させる可能性があります。

デフォルト値: 0

有効値: 0 ～ 1000

例: `set maxcontexts`

```
Number of compression contexts to allocate? (0-1000)? [0]? 10
```

圧縮機能の監視

監視プロセスで、圧縮監視コマンドにアクセスするために、+ プロンプトで **feature cmprs** コマンドを入力します。 表103 は、利用可能なコマンドをリストしています。

表 103. 圧縮監視コマンド

コマンド	アクション
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。

表 103. 圧縮監視コマンド (続き)

コマンド	アクション
List	使用しているメモリーまたはコンテキストをリストします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』を参照してください。

List

list コマンドは、現在使用されているメモリーまたはコンテキストのいずれかをリストするのに使用します。

構文:

list all

contexts usage

memory usage

all 使用されているコンテキスト、そのコンテキストを使用しているインターフェース、およびメモリー使用量の統計を表示します。この出力は、list contexts usage と list memory usage の表示を組み合わせたものです。

例: `list all`

context usage
インターフェースによって現在割り振られているすべての圧縮コンテキストを表示します。この画面によって、どのインターフェースが現在データ・トラフィックを圧縮しているかが分かります。

例: `list context usage`

```
Compression System Context (Data Dictionary) Usage
--------------------------------------------------

   CTX  Net Interface   Channel   Status
   ---  --- ----------  --------- --------------------
     0    2  FR/0             16 In use
     1    1  PPP/0             1 In use

Total: 10     Free: 8     In Use/Reserved: 2
```

CTX これは、コンテキストのタグを識別するコンテキスト番号です。装置は、ブート時にコンテキストのプールを作成し、プール内の各コンテキストに番号を割り当てます。コンテキスト番号は、一部の圧縮関連の ELS メッセージにも表示されます。

Net これは、特定のコンテキストが割り振られたネットワーク・インターフェースの番号です。

Interface
これはネットワーク・インターフェースの名前です。

Channel
チャネルは、同じネットワーク・インターフェースに割り振られた複数のコンテキストを区別するのに使用される識別子です。ネットワーク番号とチャネル番号の組み合わせによって、1 つの圧縮ストリームを固有に識別します。 PPP リンクの場合、リンク上には 1 つの圧縮データ・ストリームしか流れないので、この番号は常に 1 です。

フレーム・リレー・リンクの場合、この番号は圧縮トラフィックを伝送している特定の回線のバーチャル・サーキット番号 (DLCI) です。

Status

このフィールドはコンテキストの現在の状態を示しており、ほぼ常に 『In use』 です。ときには 『Defunct』 が表示されることがありますが、これはリンク上の圧縮は切断されたが、コンテキストがまだプールに解放されて再使用できるようになっていないことを示しています。

memory usage

圧縮機能の現在の状態に関する基本的な統計を表示します。出力に表示されるのは、割り振られた圧縮コンテキストの数、現在使用されているコンテキストの数、コンテキストに必要なメモリーの量、および圧縮コンテキスト用に予約されているメモリーの合計量です。

例:

```
list memory usage

Compression System Memory Usage Statistics
-------------------------------------------

Number of contexts allocated:            0 *        in use: 0
Size of compression context:             24624
   = Max compression history size:       16396
   + Max decompression history size:     8200
   + Overhead:                           28
Total memory allocated for contexts:     0

* Compression is disabled due to inability to allocate
  the requested number of contexts (500).
```

第64章 ローカルまたはリモート認証の使用

認証とは、ユーザー (または、エンティティー) が誰であるかを判別するアクションです。 2210 上の PPP プロトコルに対するユーザー・アクセスを認証することは、PPP 認証プロトコルの PAP 、CHAP、 および SPAP に関連しているので、ユーザー・プロファイル管理の柔軟性が拡張されます。 PAP 、CHAP、および SPAP の構成についての追加情報は、474ページの『PPP 認証プロトコル』 を参照してください。

認証は、ローカルで構成することも、ユーザー構成を統合して構成する (ネットワーク上の認証サーバーを使用して、ネットワーク全体の認証要求に応じる) こともできます。 IBM 2210 は、ローカルで維持される認証、および以下の認証サーバー・プロトコルを実装しています。

- Radius
- TACACS
- TACACS+

認証、許可、および会計 (AAA) セキュリティー

認証、許可、および会計 (AAA) セキュリティーは、サービスへのアクセスを制御できる構成可能なプロトコルです。 AAA は、ローカルまたはリモートで実行するように構成できます。

セキュリティー・プロトコルは、3 つのタイプの機能に対して構成することができます。

- PPP リンク
- ログイン・ユーザー (Telnet/コンソール・ログイン)
- トンネル

構成は 1 次サーバーと 2 次サーバーを設定することによって行います。サーバー情報は、AAA 構成とは別に構成され、別に保管されます。サーバー・プロファイルは、構成時に提供された名前によって参照されます。

どの環境下でも、会計はローカルに行うことはできず、Radius または TACACS+ でなければなりません。

許可は、ローカルで行うか、あるいは Radius または TACACS+ を使用してリモート認証を介して行うことしかできません。

AAA セキュリティーとは

AAA セキュリティーというのは、この装置のセキュリティー・システムの名前です。これには、以下のものが含まれています。

認証 ユーザーを識別するアクション。認証は、アクセス用の名前とパスワードを利用します。

許可 ユーザーのアクセスを許可するかどうかを決めるアクション。許可要求は、

そのユーザーは認証されていないことを示している可能性があります。その場合、許可エージェントは、未認証ユーザーが問題のサービスへのアクセスを許されるかどうかを判別します。

会計 ユーザーがセッションを開始または停止したときに記録するアクション。サポートされる会計レコードには 2 つのタイプがあります。

開始レコード
サービスが開始されようとしていることを示します。

停止レコード
サービスが終了したことを示します。

PPP の使用

ポイント・ポイント・プロトコル (PPP) の場合、以下の機能を構成できます。

- 認証
- 許可
- 会計

各機能は独自のセキュリティー・プロトコルを持っており、それぞれ独立して構成することができます。

- 認証プロトコルの設定値は、許可または会計には無効です。
- 許可プロトコルの設定値は、認証または会計には無効です。
- 会計プロトコルの設定は、認証または許可には影響を与えません。
- AAA をリモートに設定すると、認証はリモートに設定され、許可もリモートに設定され、会計もリモートに設定されます。
- AAA をローカルに設定すると、認証はローカルに設定され、許可もローカルに設定され、会計は無視に設定されます。認証または許可を使用不可にすることはできません。

この環境で使用する PPP 構成コマンドについての詳細は、484ページの『ポイント・ポイント構成コマンド』を参照してください。

有効な PPP セキュリティー・プロトコル

有効な PPP セキュリティー・プロトコルは、次のとおりです。

認証方式
Local、RADIUS、TACACS Plus、TACACS

許可方式
Local、RADIUS、TACACS Plus

会計方式
RADIUS、TACACS Plus

表 104. PPP セキュリティー・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	無視
AAA をリモートに設定	リモート	リモート	リモート

表 104. PPP セキュリティー・プロトコルの設定 (続き)

アクション	認証	許可	会計
AUTHENT をローカルに設定	ローカル	無視	無視
Author をローカルに設定	無視	ローカル	無視
AUTHENT をリモートに設定	リモート	無視	無視
AUTHOR をリモートに設定	無視	リモート	無視
ACCOUNTING をリモートに設定	無視	無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可
AUTHENT 使用不可	n/a	n/a	n/a
AUTHOR 使用不可	n/a	n/a	n/a

ログインの使用

ログイン AAA 構成の場合、リモートまたはローカルを選択することができます。ローカル認証が必要な場合は、ローカル許可も使用する必要があります。リモート認証が選択されている場合には、リモート許可も使用する必要があります。会計はローカルではサポートされないので、認証と許可をローカルで行う場合は、会計を使用不可にする必要があります。

重要: コンソール・ログインを使用可能にする前に、コンソール・ログインを使用不可にして、構成を保管してください。ログイン認証が Radius または TACACS+ を使用するリモート・サーバーに設定されており、ルーターが認証サーバーに到達できない場合には、ルーターへのアクセスは拒否されます。コンソール・ログインを使用不可にすることによって、ロックアウト状態を防止できます。

リモート認証が構成されている場合、許可は別のリモート許可プロトコル (Radius または TACACS+) に設定することができ、会計は Radius または TACACS+ を使用するように設定できます。

- AAA をローカルに設定すると、認証はローカルに設定され、許可もローカルに設定され、会計は使用不可に設定されます。
- AAA をリモートに設定すると、認証はリモートに設定され、許可は認証と同じに設定され、会計も同じに設定されます。
- 認証プロトコルをローカルに設定すると、自動的に許可プロトコルを同じに設定し、会計を使用不可にします。
- 認証プロトコルをリモートに設定すると、自動的に許可プロトコルを同じに設定し (許可プロトコルがローカルに設定されている場合)、会計プロトコルを無視します。
- 許可プロトコルをリモートに設定すると、自動的に認証プロトコルを同じに設定し (認証プロトコルがローカルに設定されている場合)、会計プロトコルを無視します。
- 会計プロトコルをリモートに設定すると、自動的に認証プロトコルを同じに設定し (認証プロトコルがローカルに設定されている場合)、許可プロトコルも同じに設定します (許可がローカルに設定されている場合)。
- 会計プロトコルを使用不可に設定しても、認証または許可プロトコルには影響を与えません。

ローカルまたはリモート認証の使用

- 認証または許可を使用不可にすることはできません。

有効なログイン/管理セキュリティー・プロトコル

有効なログイン/管理セキュリティー・プロトコルは、次のとおりです。

認証/許可方式

Local、RADIUS、TACACS Plus

会計方式

RADIUS、TACACS Plus

表 105. ログイン・セキュリティー・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	使用不可
AAA をリモートに設定	リモート	リモート	リモート
AUTHENT をローカルに設定	ローカル	ローカル	使用不可
AUTHOR をローカルに設定	ローカル	ローカル	使用不可
AUTHENT をリモートに設定	リモート	リモート、ローカルの場合は他を無視	無視
AUTHOR をリモートに設定	リモート、ローカルの場合は他を無視	リモート	無視
ACCOUNTING をリモートに設定	リモート、ローカルの場合は他を無視	リモート、ローカルの場合は他を無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可
AUTHEN 使用不可	n/a	n/a	n/a
AUTHOR 使用不可	n/a	n/a	n/a

トンネルの使用

トンネル認証は、トンネル許可と同じに設定する必要があります。トンネル認証がローカルまたはリモートに設定されている場合は、会計を使用可能にすることができます。トンネル認証サーバーと許可サーバーは同じでなければなりません。

有効なトンネル・セキュリティー・プロトコル

有効なトンネル・セキュリティー・プロトコルは、次のとおりです。

認証/許可

Local、RADIUS

許可 Local、RADIUS

会計方式

RADIUS、TACACS Plus

表 106. トンネル・セキュリティー・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	無視
AAA をリモートに設定	リモート	リモート	リモート
AUTHENT をローカルに設定	ローカル	ローカル	無視
Author をローカルに設定	ローカル	ローカル	無視
AUTHENT をリモートに設定	リモート	リモート	無視
AUTHOR をリモートに設定	リモート	リモート	無視
ACCOUNTING をリモートに設定	無視	無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可
AUTHENT 使用不可	n/a	n/a	n/a
AUTHOR 使用不可	n/a	n/a	n/a

パスワード規則

ローカル認証では、パスワードを使用してログイン・アクセスを制御することができます。以下の規則のいずれか、またはすべてに照らして、パスワードが検査されます。

- 少なくとも ? 文字の長さ
- 少なくとも 1 字の英字が含まれている
- 少なくとも 1 字の非英字が含まれている
- 最初の位置に非数字がある
- 最後の位置に非数字がある
- 前のパスワードで使用されたのと同じ連続文字が 3 字しか含まれていない
- 2 連続文字しか含まれていない
- ユーザー ID がパスワードの一部として含まれていない
- 直前の 3 つのパスワードのいずれとも同じでない
- ? 日ごとに変更される
- ? 回のログイン失敗後にロックアウトされる

認証サーバーとは

認証サーバー とは、ネットワークのユーザー ID とパスワードの妥当性を検査するネットワーク内のサーバーです。装置が認証サーバーを通して認証するように構成されている場合、装置は認証プロトコルからパケットを受信すると、ユーザー ID とパスワードをサーバーに渡して認証を依頼します。ユーザー ID とパスワードが正しい場合、サーバーは肯定応答します。その場合、装置は要求の発信元と通信することができます。装置から受け取ったユーザー ID とパスワードが見つからない場合、サーバーは装置に否定応答します。その場合、装置は認証要求を受け取ったセッションをリジェクトします。

第65章 認証の構成

この章では、認証の構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

- 『認証構成プロンプトへのアクセス』
- 『認証構成コマンド』

認証構成プロンプトへのアクセス

`Authent config >` プロンプトにアクセスするには、次のようにします。

1. `*` プロンプトで **talk 6** と入力する。
2. `Config >` プロンプトで **feature auth** と入力する。

認証構成コマンド

表107 は、`Authent config >` プロンプトで利用可能なコマンドをリストしています。

表 107. 認証構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Disable	AAA の会計を使用不可にします。
List	AAA 構成パラメーターを表示します。
Login	ログイン用の AAA を構成します。
Nets-info	ローカル PPP 認証に関する情報を表示します。
Password-rules	パスワード規則を構成します (使用可能または使用不可)。
PPP	PPP 用の AAA を構成します。
Quickset	認証方式を迅速に構成します。
Servers	個々のリモート AAA サーバーを構成します。
Set	タイプに関係なく、認証パラメーターを構成します。
Tunnel	L2TP トンネル用の AAA を構成します。
User-profile	ローカル PPP ユーザーを構成します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Disable

disable コマンドは、会計を使用不可にするのに使用します。

構文:

disable accounting

List

list コマンドは、AAA パラメーターを表示するのに使用します。

構文:

list accounting
authentication
authorization
all
config

```
AAA Config> list all
ppp AAA configuration...
 ppp authentication        : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 ppp authorization         : locallist
 ppp accounting            : Disabled
tunnel AAA configuration...
 tunnel authentication     : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 tunnel authorization      : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 tunnel accounting         : Disabled
login AAA configuration...
 login authentication      : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 login authorization       : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 login accounting          : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
```

```
AAA Config> list accounting all
accounting AAA configuration...
 accounting ppp            : Disabled
 accounting tunnel         : Disabled
 accounting login          : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
AAA Config> list accounting config
accounting ppp            : Disabled
accounting login          : Radius        serv01
accounting tunnel         : Disabled
AAA Config> list authentication all
authentication AAA configuration...
 authentication ppp        : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 authentication tunnel     : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
```

Login

login コマンドは、ログイン用の AAA を構成するのに使用します。

表108 は、**login** コマンドと共に使用できるサブコマンドをリストしています。

表 108. ログイン・サブコマンド

コマンド	機能
Disable	ログインの会計を使用不可にします。
List	ログイン用の AAA 構成パラメーターを表示します。
Set	ログイン用の AAA 構成パラメーターを設定します。

Disable

login disable コマンドは、会計を使用不可にするのに使用します。

構文:

login disable accounting

List

login list は、AAA 構成パラメーターを表示するのに使用します。

構文:

login list all

accounting

authentication

authorization

config

Set

login set コマンドは、認証パラメーターを構成するのに使用します。

構文:

login set aaa

accounting

authentication

authorization

aaa *authtype*
認証、許可、および会計タイプを設定します。 *Authtype* は、以下のいずれかです。

local 認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

accounting *authtype*
会計タイプを設定します。 *Authtype* は、以下のいずれかです。

remote
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authentication *authtype*
認証タイプを設定します。 *Authtype* は、以下のいずれかです。

local 認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authorization *authtype*
許可タイプを設定します。 *Authtype* は、以下のいずれかです。

local 許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

Nets-info

nets-info コマンドは、各 PPP インターフェースに現在構成されている PPP 認証プロトコルを表示します。

構文:

nets-info

Password-rules

password-rules コマンドは、パスワードを構成する (使用可能または使用不可) のに使用します。

表109 は、**password-rules** コマンドと共に使用できるサブコマンドをリストしています。

表 109. ログイン・サブコマンド

コマンド	機能
Disable	パスワード規則を使用不可にします。
Enable	パスワード規則を使用可能にします。
List	パスワード規則の現在の状態 (使用可能または使用不可) を表示します。

Disable

password-rules disable コマンドは、任意のまたはすべてのパスワード規則を使用不可にするのに使用します。

構文:

password-rules disable all
compare-ident-prev
change-days
first-non-numeric
force-change
ident-chars
last-non-numeric
lockout
minimum-length

one-alpha

one-nonalpha

prev-three

userid-contained

compare-ident-prev
前のユーザー識別とパスワード変更を要求しているユーザーとを比較します。

change-days
パスワード変更が必要になる前の最大日数

有効値: 0 ～ 360

デフォルト値: 180

first_non-numeric
パスワードの先頭文字で、数字は使えません。

有効値: 任意の非数字

デフォルト値: なし

force-change
最大変更日数が満了した後で、パスワード変更を強制します。旧パスワード、新規パスワード、および新規パスワードの検証を求めるプロンプトが出ます。

有効値: 0 ～ 360

デフォルト値: 180

ident-chars
前のパスワードの同じ位置に使用された文字が 3 字より多く含まれていてはなりません。

last-non-numeric
パスワードの最後の文字は数字であってはなりません。

有効値: 任意の非数字

デフォルト値: なし

lockout
ロックアウトされる前のパスワードの試行回数

有効値: 0 ～ 360

デフォルト値: 3

minimum-length
有効なパスワードに必要な最小文字数

有効値: 1 ～ 31

デフォルト値: 8

maximum-length
パスワードに含めることができる最大文字数

有効値: 1 ～ 31

デフォルト値: 8

one-alpha
パスワードの少なくとも 1 文字は英字でなければなりません。

one-nonalpha
パスワードの少なくとも 1 文字は数字でなければなりません。

prev-three
パスワードは、最後の 3 つのパスワードのいずれとも同じであってはなりません。

userid-contained
ユーザー ID をパスワードの一部として含めることはできません。

Enable

password-rules enable コマンドは、任意のまたはすべてのパスワード規則を使用可能にするのに使用します。パスワード規則についての説明は、**disable** コマンドを参照してください。

構文:

password-rules enable all
compare-ident-prev
change-days
first-non-numeric
force-change
ident-chars
last-non-numeric
lockout
minimum-length
one-alpha
one-nonalpha
prev-three
userid-contained

List

password-rules list コマンドは、パスワード規則の現在の状態 (使用不可または使用可能) を表示するのに使用します。

構文:

password-rules list

PPP

ppp コマンドは、PPP 用の AAA を構成するのに使用します。

表110 は、**ppp** コマンドと共に使用できるサブコマンドをリストしています。

表 110. PPP サブコマンド

コマンド	機能
Disable	PPP の会計を使用不可にします。
List	PPP 用の AAA 構成パラメーターを表示します。
Set	PPP 用の AAA 構成パラメーターを設定します。

Disable

ppp disable コマンドは、PPP の会計を使用不可にするのに使用します。

構文:

ppp disable accounting

List

ppp list コマンドは、PPP 用の AAA 構成パラメーターを表示するのに使用します。

構文:

ppp list all
accounting
authentication
authorization
config

Set

ppp set コマンドは、PPP 用の AAA 構成パラメーターを表示するのに使用します。

構文:

ppp set aaa
accounting
authentication
authorization

aaa *authtype*
認証、許可、および会計タイプを設定します。 *Authtype* は、以下のいずれかです。

local 認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

accounting *authtype*
会計タイプを設定します。 *Authtype* は、以下のいずれかです。

remote
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authentication *authtype*
認証タイプを設定します。 *Authtype* は、以下のいずれかです。

local 認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authorization *authtype*
許可タイプを設定します。 *Authtype* は、以下のいずれかです。

local 許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

Servers

servers コマンドは、個々のリモート AAA サーバーを構成するのに使用します。

表111 は、**servers** コマンドと共に使用できるサブコマンドをリストしています。

表 111. サーバー・サブコマンド

コマンド	機能
Add	リモート AAA サーバー・プロファイルを追加します。
Change	リモート・サーバー・プロファイルを変更します。
Delete	リモート・サーバー・プロファイルを削除します。
Lists	AAA サーバー・プロファイル情報を表示します。

Add

servers add コマンドは、リモート・サーバー・プロファイルを追加するのに使用します。

構文:

servers add name

radius 認証タイプを、Radius 認証サーバー・プロトコルを使用するように設定します。

以下のパラメーターの値を設定できます。

key-for-encryption:
暗号化キーを指定します。

有効値: 最大 32 字の長さの任意の英数字列

デフォルト値: なし

primary-server-address:
1 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

retries

有効値: 1 ～ 100

デフォルト値: 3

retry-interval

有効値: 1 ～ 60

デフォルト値: 3

secondary-server-address:
2 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Author-Authent
認証時に許可属性が転送されるかどうかを指定します。

有効値: yes、no

デフォルト値: yes

tacacs
認証タイプを、TACACS 認証サーバー・プロトコルを使用するように設定します。

以下のパラメーターの値を設定できます。

primary-server-address:
1 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

retries

有効値: 1 ～ 100

デフォルト値: 3

retry-interval

有効値: 1 〜 60

デフォルト値: 3

secondary-server-address:
2 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

tacacsplus
認証タイプを、TACACS+ 認証サーバー・プロトコルを使用するように設定します。

以下のパラメーターの値を設定できます。

encryption:
暗号化を使用するかどうかを指定します。

有効値: yes、no

デフォルト値:

key-for-encryption:
使用する暗号化キーを指定します。

有効値: 任意の 16 の 16 進数値

デフォルト値:

primary-server-address:
1 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

privilege-level

有効値: 0 〜 15

デフォルト値: 0

restarts
リスタートの回数を設定します。このパラメーターには、タイムアウトによるリスタートは含まれず、サーバーによって要求されたリスタートのみを対象にしています。

有効値: 0 〜 3200

デフォルト値: 0

time-to-connect
サーバーから認証を得るために許容される時間数。

有効値: 1 〜 60

デフォルト値: 9

secondary-server-address:
2 次認証サーバーのアドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Change

servers change コマンドは、リモート・サーバー・プロファイルを変更するのに使用します。リモート・サーバー・プロファイルの説明は、**add** コマンドの項を参照してください。

構文:

servers change	radius
	tacacs
	tacacsplus

リモート・サーバー・プロファイルの説明は、**servers add** コマンドの項を参照してください。

Delete

servers delete コマンドは、リモート・サーバー・プロファイルを削除するのに使用します。リモート・サーバー・プロファイルの説明は、**add** コマンドの項を参照してください。

構文:

servers delete	radius
	tacacs
	tacacsplus

リモート・サーバー・プロファイルの説明は、**servers add** コマンドの項を参照してください。

List

servers list コマンドは、AAA サーバー・プロファイル情報を表示するのに使用します。

構文:

servers list	all
	names
	profile

Set

set コマンドは、ログイン、 PPP、および L2TP トンネルのパラメーターを設定するのに使用します。

構文:

set	aaa

accounting

authentication

authorization

aaa *authtype*
認証、許可、および会計タイプを設定します。 *Authtype* は、以下のいずれかです。

local 認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

accounting *authtype*
ログイン、PPP、およびトンネルの会計タイプを設定します。 *Authtype* は、以下のいずれかです。

remote
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authentication *authtype*
ログイン、PPP、およびトンネルの認証タイプを設定します。 *Authtype* は、以下のいずれかです。

local 認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authorization *authtype*
ログイン、PPP、およびトンネルの許可タイプを設定します。 *Authtype* は、以下のいずれかです。

local 許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

Tunnel

tunnel コマンドは、L2TP トンネル用の AAA を構成するのに使用します。

表112 は、**tunnel** コマンドと共に使用できるサブコマンドをリストしています。

表 112. トンネル・サブコマンド

コマンド	機能
Disable	L2TP トンネルの会計を使用不可にします。
List	L2TP トンネル用の AAA 構成パラメーターを表示します。
Set	L2TP トンネル用の AAA 構成パラメーターを設定します。

Disable

tunnel disable コマンドは、L2TP トンネルの会計を使用不可にするのに使用します。

構文:

tunnel disable accounting

List

tunnel list コマンドは、L2TP トンネル用の AAA を表示するのに使用します。

構文:

tunnel list all
accounting
authentication
authorization
config

Set

tunnel set コマンドは、L2TP トンネル用の AAA 構成パラメーターを設定するのに使用します。

構文:

tunnel set aaa
accounting
authentication
authorization

aaa *authtype*

認証、許可、および会計タイプを設定します。 *Authtype* は、以下のいずれかです。

local 認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

accounting *authtype*
会計タイプを設定します。 *Authtype* は、以下のいずれかです。

remote
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authentication *authtype*
認証タイプを設定します。 *Authtype* は、以下のいずれかです。

local 認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authorization *authtype*
許可タイプを設定します。 *Authtype* は、以下のいずれかです。

local 許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

remote
許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

User-profiles

user-profiles コマンドは、`User profile config>` コマンド・プロンプトにアクセスするのに使用します。このプロンプトから、以下のコマンドにアクセスできます。

表 113. ユーザー・プロファイル構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add	PPP ユーザー・プロファイルを追加します。
Change	PPP ユーザー・プロファイルを変更します。
Delete	PPP ユーザー・プロファイルを削除します。
Disable	PPP ユーザー・プロファイルを使用不可にします。

表 113. ユーザー・プロファイル構成コマンド (続き)

コマンド	機能
Enable	PPP ユーザー・プロファイルを使用可能にします。
List	PPP ユーザー・プロファイル情報をリストします。
Report	PPP ユーザー・プロファイル・レポートを生成します。
Reset-user	PPP ユーザー・プロファイルをリセットします。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、ユーザー・プロファイルを追加するのに使用します。

構文:

add ppp-user

tunnel

```
User profile config> add ppp-user
Enter name:  []? ppp01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Number of days before password expiry[0-1000] [0]?
IP address: [0.0.0.0]?
Enable encryption for this user/port (y/n) [No]:
Disable user ? (Yes, No): [No]
     PPP user name: ppp01
            Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
User 'ppp01' has been added
```

Name PPP ユーザーのユーザー ID を入力します。

Password
PPP ユーザーのパスワードを入力します。

Verify password
検証のために、パスワードを前と正確に同じに再度入力します。

Allow inbound access
このユーザー・プロファイルへの着信アクセスを許可します。

有効値: yes、no

デフォルト値: no

Will user be tunneled?
ユーザーをトンネル伝送するかどうかを指定します。

有効値: yes、no

デフォルト値: no

Number of days
パスワードが失効する前の日数

有効値: 0 ～ 360

デフォルト値: 180

IP address

IP アドレス

有効値: 任意の有効な IP アドレス

デフォルト値: なし

Enable encryption

このユーザー/ポートの暗号化を使用可能にするかどうかを指定します。

有効値: yes、no

デフォルト値: no

Disable user

ユーザー・プロファイルを使用不可にします。

有効値: yes、no

デフォルト値: no

```
User profile config> add tunnel
Enter name:  []? tunnel01
Enter hostname to use when connecting to this peer: []? host01
set shared secret? (Yes, No): [No]
Tunnel-Server endpoint address: [0.0.0.0]?
       Tunnel name: tunnel01
          Endpoint: not configured
          Hostname: host01
User 'tunnel01' has been added
```

Change

change コマンドは、ユーザー・プロファイルを変更するのに使用します。

構文:

change	ppp-user
	tunnel

Delete

delete コマンドは、ユーザー・プロファイルを削除するのに使用します。

構文:

delete	ppp-user
	tunnel

Disable

disable コマンドは、ユーザー・プロファイルを使用不可にするのに使用します。

構文:

disable	*name*

Enable

enable コマンドは、ユーザー・プロファイルを使用可能にするのに使用します。

構文:

enable *name*

List

list コマンドは、ユーザー・プロファイル情報をリストするのに使用します。

構文:

list ppp-user

tunnel

```
User profile config> list ppp-user
List  (Name, Verb, User, Addr, Encr, zdump): [Verb]
     PPP user name: ppp01
            Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
1 record displayed.
```

List リスト情報にアクセスする方法を指定します。

有効値: name, verb, user, addr, encr, zdump

デフォルト値: verb

PPP user name
ユーザー名をリストします。

Expiry
有効期限をリストします。

User IP address
ユーザー IP アドレスをリストします。

Encryption
暗号化が使用可能か使用不可かをリストします。

Status
状態が使用可能か使用不可かをリストします。

Login attempts
ユーザーがログインを試行した回数をリストします。

Login failures
ログインに失敗した試行回数をリストします。

Lockout attempts
ロックアウトの試行回数をリストします。

Report

report コマンドは、PPP ユーザー・プロファイル・レポートを生成するのに使用します。

構文:

report

- addresses
- all
- callback
- dialout
- dump
- encrypt
- name
- password
- time
- user

```
User profile config> report addresses
PPP user name      User IP address
-----------------  ------------------
ppp01              Interface Default
1 record displayed.
User profile config> report all
     PPP user name: ppp01
            Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
1 record displayed.
User profile config> report callback
PPP user name      Callback type        Phone Number
-----------------  -------------------  --------------------
ppp01
1 record displayed.
User profile config> report dialout
PPP user name      Dial-out
-----------------  ---------------
ppp01
1 record displayed.
User profile config> report dump
Enter user name:  []? user01
User profile config> report encrypt
PPP user name      Encryption
-----------------  ---------------
ppp01              Not Enabled
1 record displayed.
User profile config> report name
PPP user name
-----------------
ppp01
1 record displayed.
```

```
User profile config> report password
PPP user name      Expiry        Grace
-----------------  ------------  ------
ppp01              <unlimited>
1 record displayed.
User profile config> report time
PPP user name      Time alotted
-----------------  ------------------
ppp01
1 record displayed.
User profile config> report user
Enter user name:  []? login01
     PPP user name: login01
        Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
```

Reset-user

reset-user コマンドは、ユーザー・プロファイルをリセットするのに使用します。

構文:

reset-user *name*

第66章 暗号化の概説

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

暗号化の目的は、プライバシーを保証するために、データを読み取り不能な形にして転送することです。***暗号化された*** データは、元のデータを入手するためには、暗号化解除する必要があります。

Nways 装置は、データ暗号化規格 (DES) 暗号化ブロック・チェーン (CBC) モードをサポートします。 DES は対称形暗号化規格で、PPP の暗号化と暗号化解除には 56 ビット・キーを使用し、フレーム・リレーの暗号化と暗号化解除には 40 ビット・キーを使用します。

PPP またはフレーム・リレー・リンク上で転送されるデータを暗号化することができます。 PPP の暗号化については、RFC 1968 および 1969 に記述されています。フレーム・リレー暗号化サポートは、専有のものです。

PPP 暗号化

暗号化制御プロトコルは、PPP プロトコルを使用したポイント・ポイント・リンク通信で、ルーターが暗号化の使用を交渉するのに使用します。暗号化制御プロトコルは、PPP リンクを介して使用する暗号化および暗号化解除アルゴリズムを交渉するための汎用機構を提供します。 PPP リンクの各方向でそれぞれ異なる暗号化アルゴリズムを交渉することも可能です。

暗号化と暗号化解除の方式を***暗号化アルゴリズム*** と言います。暗号化アルゴリズムは、キーを使用して、暗号化と暗号化解除を制御します。圧縮とは異なり、ルーターはリンクの両方向で暗号化を行います。一方向のみの暗号化はセキュリティー上の危険があるからです。 ECP が両方向の暗号化アルゴリズムを交渉できない場合、リンクは終了します。

PPP の暗号化の構成

データ・リンク・レイヤーで暗号化を使用するように装置を構成するには、以下の手順で行います。

1. リモート装置およびローカル PPP インターフェースの暗号化キーを設定する。

   リモート装置の暗号化キーは、`Config >` プロンプトで **add ppp-user** コマンドを使用して設定します (56ページの『Add』 を参照してください)。

   ローカル PPP インターフェースの暗号化キーは、**set name** コマンドを使用して設定します (491ページの『Set』 を参照してください)。

2. `PPP Config>` プロンプトで **enable ecp** コマンドを使用して、個々の PPP リンクが暗号化制御プロトコル (ECP) を使用するように構成する (486ページの『Enable』 を参照してください)。

3. PAP、CHAP、または SPAP を使用可能にする。

また、暗号化を使用不可にする、ユーザーの暗号化キーを変更する、暗号化の状態をリストする、あるいは暗号化を要求するときに装置が使用する名前と暗号化キーを設定するといったことも可能です。詳細については、以下の個所を参照してください。

- 暗号化を使用不可にするには、484ページの『Disable』 の **disable ecp** コマンドの高を参照してください。
- ユーザーの暗号化キーの変更については、63ページの『Change』 の **change ppp-user** コマンドの項を参照してください。
- 暗号化の状態をリストするには、487ページの『List』 の **list ecp** コマンドの項を参照してください。
- 装置の名前と暗号化キーの設定については、491ページの『Set』 の **set name** コマンドの項を参照してください。

PPP の暗号化の監視

インターフェース上の各種の暗号化設定を監視するには、次のようにします。

1. **talk 5** コマンドを使用して、監視プロンプトにアクセスする。
2. **network x** コマンドを使用して、監視するインターフェースを選択する。このコマンドは `PPP x>` プロンプトで入力します。

このプロンプトから、次のことが行えます。

- 暗号化の現行状態、最新の暗号化ネゴシエーション、暗号化状態変更以降の経過時間、および暗号化機能によって使用されているアルゴリズムをリストする。 (504ページの **list control ecp** コマンドを参照してください。)
- インターフェースで送受信された暗号化制御パケットをリストする。 (517ページの **list ecp** コマンドを参照してください。)
- インターフェースで送信または受信された、暗号化されたデータ・パケットをリストする。 (518ページの list edp コマンドを参照してください。)

フレーム・リレー・インターフェース上の暗号化の構成

注: フレーム・リレーは、専有の暗号化方式を使用します。

データ暗号化は、暗号化を使用可能にしたすべてのインターフェースでサポートされます。暗号化が使用可能にされているインターフェース上の個々の回線を、必要に応じて、暗号化を実行する、または実行しないとして個別に構成することができます。

フレーム・リレー・リンク上で暗号化を使用するように装置を構成するには、以下の手順で行います。

1. **talk 6** コマンドを使用して、フレーム・リレー構成プロンプトにアクセスする。
2. **net** # コマンドを使用して、暗号化を可能にしたいフレーム・リレー・インターフェースを選択する。

3. **enable encryption** コマンドを使用して、フレーム・リレー・インターフェース上の暗号化を使用可能にする。 437ページの『Enable』を参照してください。
4. **add permanent-virtual-circuit** コマンドを使用して、暗号化が可能なパーマネント・バーチャル・サーキットを追加し、各 PVC ごとに暗号化キーを定義する。 430ページの『Add』を参照してください。
5. 構成する各暗号化可能インターフェースごとに、ステップ 1 ～ 4 を繰り返す。

注: FR パーマネント・バーチャル・サーキットの暗号化が使用可能にされている場合、バーチャル・サーキットの反対側の装置との暗号化の交渉が正常に行われない限り、データは回線上に流れません。暗号化はオーファン回線に対してはサポートされません。暗号化キーを入力するために PVC を構成する必要があるからです。

インターフェースの暗号化を使用不可にする、PVC の暗号化の設定値を変更する、あるいは暗号化の状態をリストすることもできます。詳細については、以下の個所を参照してください。

- インターフェース上の暗号化を使用不可にする場合は、435ページの『Disable』 の **disable encryption** を参照してください。
- PVC の暗号化の設定値を変更する場合は、433ページの『Change』の **change permanent-virtual-circuit** コマンドを参照してください。
- 暗号化の状態をリストする場合は、441ページの『List』の **list all**、**list lmi**、および **list permanent-virtual-circuit** コマンドを参照してください。

フレーム・リレー・インターフェース上の暗号化の監視

インターフェース上の各種の暗号化設定を監視するには、次のようにします。

1. **talk 5** コマンドを使用して、監視プロンプトにアクセスする。
2. **network** # コマンドを使用して、監視したいインターフェースを選択する。このコマンドを使用すると、FR *x*> プロンプトが表示されます。

このプロンプトから、インターフェース、PVC、または回線の暗号化の現行状態をリストすることができます。 454ページの『List』を参照してください。

第67章 サービス品質 (QoS) の使用

この章では、装置のサービス品質 (QoS) 機能の使用法について説明します。

サービス品質 (QoS) の概要

この QoS 機能は、LAN エミュレーションのデータ・ダイレクト VCC の ATM QoS 機能の利点を活用したものです。このサポートは 『LAN エミュレーションの構成可能 QoS』 と呼ばれています。この機能の主要な属性と利点は、次のとおりです。

- LE クライアントは、そのデータ・ダイレクト VCC 用に構成された QoS パラメーターを使用します。
- QoS パラメーターは、以下に対して構成することができます。
  - LE クライアント
  - ATM インターフェース
- 構成された QoS パラメーター・セットは、ATM フォーラム UNI 3.0/3.1 信号に使用されます。これらのパラメーターには、ピーク・セル速度、持続セル速度、QoS クラス、および最大バースト・サイズが含まれます。
- LE クライアントが、サポートできないトラフィック・パラメーターをもつ VCC を受け入れる/確立するのを防止するために、VCC 当りの最大予約帯域幅を構成することができます。
- QoS ネゴシエーション・メカニズムにより、参加している LE クライアントは相互の QoS パラメーターを知ることができます。データ・ダイレクト VCC は、交渉されたパラメーターを使用して設定されます。

QoS の利点

- LE クライアント、ATM インターフェース、またはエミュレートされた LAN に対して QoS を使用すると、LANE データ・ダイレクト VCC は、以下のような利点が得られます。
  - ある LE クライアントに必要な QoS が、ELAN 上の他のクライアントに必要な QoS と異なっている場合、その LE クライアントに QoS を構成することができます。たとえば、LE クライアントがファイル・サーバーとして動作している場合、ファイル・サーバーとの間でやり取りされるすべてのトラフィックに対して適切な QoS パラメーターを構成したい場合があります。
  - ある ATM インターフェース上のすべての LE クライアントが同一の 1 組のパラメーターを使用するようにしたい場合、その ATM インターフェースに QoS を構成することができます。たとえば、ある ATM インターフェースが 25 Mbps で接続されている場合、155-Mbps インターフェースとは異なる適切なパラメーターを構成できます。

第68章 サービス品質 (QoS) の構成および監視

この章では、ルーター内の LAN および ELAN インターフェースのサービス品質 (QoS) の構成コマンドおよび動作コマンドについて説明します。本章には、以下の節が含まれています。

QoS 構成パラメーター

この節では、QoS の構成に使用される 9 つのパラメーターについて説明します。次の 6 つのパラメーターは、LE クライアント、ATM インターフェース、およびエミュレートされた LAN に対して構成することができます。

1. max-reserved-bandwidth
2. traffic-type
3. peak-cell-rate
4. sustained-cell-rate
5. max-burst-size
6. qos-class

次の 2 つのパラメーターは、エミュレートされた LAN および LE クライアントに対して構成することができます。

1. *validate-pcr-of-best-effort-vccs*
2. *negotiate-qos*

accept-qos-parms-from-lecs パラメーターは、LE クライアントに対してのみ構成できます。

最初の 6 つのパラメーターは、LE クライアントによって確立されるデータ・ダイレクト VCC のトラフィック特性を制御します。最初のパラメーターは LE クライアントが受信した呼にも適用されます。次の特性は、LE クライアントによって確立されるすべてのデータ・ダイレクト VCC に関連するものです。

- ベストエフォート・トラフィック用の帯域幅は予約されません。
- トラフィック・パラメーターは順方向と逆方向の両方に適用されます。

- 予約帯域幅接続がトラフィック・パラメーターまたは QoS クラスが原因でリジェクトされた場合、その呼は、構成されたピーク・セル速度を使用して、ベストエフォート接続として再試行されます (VCC が解放された理由は、解放時の原因符号または復旧完了メッセージを使用して判別します)。
- ベストエフォート接続がピーク・セル速度が原因でリジェクトされた場合、その呼は、より低い PCR を使用して自動的に再試行されることがあります。再試行は、以下の条件下で行われます。
  1. リジェクトされた PCR が 100 Mbps を超えている場合、呼は 100 Mbps のPCR で再試行されます。
  2. そうでない場合、リジェクトされた PCR が 25 Mbps を超えている場合には、呼は 25 Mbps の PCR で再試行されます。

最大予約帯域幅 (max-reserved-bandwidth)

データ・ダイレクト VCC に対して許容される最大予約帯域幅。このパラメーターは、LE クライアントが受信するデータ・ダイレクト VCC の呼と、LE クライアントが発信するデータ・ダイレクト VCC の呼の両方に適用されます。着呼の場合、このパラメーターはデータ・ダイレクト VCC の最大許容 SCR を定義します。着呼に SCR が指定されていない場合には、このパラメーターは予約帯域幅をもつデータ・ダイレクト VCC の最大許容 PCR を定義します。

受信した呼のトラフィック・パラメーターがこれより高い速度に指定されている場合、その呼は解放されます。着呼に SCR が指定されている場合、その呼は PCR または最大バースト・サイズが原因でリジェクトされることはありません。このパラメーターによる制約は BEST_EFFORT 接続には適用されません。発呼の場合、このパラメーターは、データ・ダイレクト VCC 用に要求できる予約帯域幅の上限を設定します。したがって、トラフィック・タイプ (traffic-type) および持続セル速度 (sustained-cell-rate) パラメーターは、このパラメーターに依存します。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

0

トラフィック・タイプ (traffic-type)

データ・ダイレクト VCC のトラフィック・タイプ。 QoS パラメーターが交渉されない場合、このパラメーターは LE クライアントからの発呼のタイプを指定します。QoS パラメーターが交渉される場合には、このパラメーターは、データ・ダイレクト VCC のトラフィック特性を指定します。 QoS パラメーターが交渉されるときには、発信元またはターゲット LEC のどちらかの LEC が予約帯域幅接続を望み、両方の LEC が予約帯域幅接続をサポートしている場合 (つまり、max-reserved-bandwidth > 0) には、2 つの LEC 間で予約帯域幅データ・ダイレクト VCC の確立が試みられます。そうでない場合は、データ・ダイレクト VCC はベストエフォート接続になります。
依存関係: 最大予約帯域幅 (max-reserved-bandwidth)

有効値:

best_effort または reserved_bandwidth

デフォルト値:
best_effort

ピーク・セル速度 (peak-cell-rate)

データ・ダイレクト VCC のピーク・セル速度。 QoS パラメーターが交渉されない場合、このパラメーターは LE クライアントが発信するデータ・ダイレクト VCC の呼の PCR トラフィック・パラメーターを指定します。 QoS パラメーターが交渉される場合には、このパラメーターは、データ・ダイレクト VCC の PCR トラフィック・パラメーターを指定します。交渉されたベストエフォート VCC では、2 つの LEC の PCR の最小値が使用されます。

予約帯域幅が交渉され、一方の LE クライアントのみが予約帯域幅接続を要求している場合、その LEC の PCR がデータ・ダイレクト VCC に使用され、ローカル ATM 装置の回線速度による上限が適用されます。両方の LE クライアントのみが予約帯域幅接続を要求している場合には、LE クライアント の PCR の最大値がデータ・ダイレクト VCC に使用され、ローカル ATM 装置の回線速度による上限が適用されます。

有効値:
0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:
LEC ATM 装置の回線速度 (Kbps)

持続セル速度 (sustained-cell-rate)

データ・ダイレクト VCC の持続セル速度。 QoS パラメーターが交渉されない場合、このパラメーターは LE クライアントが発信するデータ・ダイレクト VCC の呼の SCR トラフィック・パラメーターを指定します。 QoS パラメーターが交渉される場合は、このパラメーターは、データ・ダイレクト VCC の SCR トラフィック・パラメーターを指定します。

予約帯域幅が交渉され、一方の LE クライアントのみが予約帯域幅接続を要求している場合、その LEC の SCR がデータ・ダイレクト VCC に使用されます (他方の LEC の max-reserved-bandwidth パラメーターによる上限が適用されます)。両方の LE クライアントが予約帯域幅接続を要求している場合には、LE クライアントの SCR の最大値がデータ・ダイレクト VCC に使用されます (両方の LEC の max-reserved-bandwidth パラメーターによる上限が適用されます)。いずれの場合も (交渉または非交渉)、シグナルされる SCR がシグナルされる PCR に等しい場合には、呼は PCR のみを用いてシグナルされます。

依存関係: 最大予約帯域幅 (max-reserved-bandwidth)、トラフィック・タイプ (traffic-type)、およびピーク・セル速度 (peak-cell-rate)。このパラメーターは、トラフィック・タイプが RESERVED_BANDWIDTH の場合にのみ適用されます。

有効値:
0 から最大予約帯域幅とピーク・セル速度の最小値までの範囲内の整数値 (Kbps)

デフォルト値
なし

最大バースト・サイズ (max-burst-size)

データ・ダイレクト VCC の最大バースト・サイズ。 QoS パラメーターが交渉されない場合、このパラメーターは LE クライアントが発信するデータ・ダイレクト VCC の呼の「最大バースト・サイズ」トラフィック・パラメーターを指定します。 QoS パラメーターが交渉される場合には、このパラメーターは、データ・ダイレクト VCC の「最大バースト・サイズ」トラフィック・パラメーターを指定します。

予約帯域幅が交渉され、一方の LE クライアントのみが予約帯域幅接続を要求している場合、その LEC の「最大バースト・サイズ」がデータ・ダイレクト VCC に使用されます。両方の LE クライアントが予約帯域幅接続を要求している場合には、LE クライアントの「最大バースト・サイズ」の最大値が、データ・ダイレクト VCC に使用されます。

いずれの場合も (交渉または非交渉)、SCR がシグナルされる場合にのみ、最大バースト・サイズがシグナルされます。このパラメーターはセル単位で表し、最大データ・フレーム・サイズ (LEC の C3 パラメーターで指定) の整数倍として構成しますが、1 が下限です。

依存関係: このパラメーターは、トラフィック・タイプが RESERVED_BANDWIDTH の場合にのみ適用されます。

有効値:
整数のフレーム数。0 より大きいことが必要です。

デフォルト値:
1 フレーム

QoS クラス (qos-class)

予約帯域幅の呼の QoS クラス。 QoS パラメーターが交渉されない場合、このパラメーターは LE クライアントが発信する予約帯域幅データ・ダイレクト VCC の呼に使用される QoS クラスを指定します。 QoS パラメーターが交渉される場合には、このパラメーターは、データ・ダイレクト VCC の QoS クラスを指定します。 QoS クラスが未指定の場合は、常にベストエフォート呼が使用されます。 指定された QoS クラスは、セル損失比率やセル転送遅延など、ATM 性能パラメーターの目標値を定義します。

UNI 仕様には、以下のように記述されています。

指定 QoS クラス 1
現行のディジタル専用回線の効率に匹敵する効率を生成する必要がある。

指定 QoS クラス 2
電話会議およびマルチメディア・アプリケーションにおけるパケット化ビデオおよびオーディオ用

指定 QoS クラス 3
コネクション型プロトコル (フレーム・リレーなど) の相互運用性が目的

指定 QoS クラス 4
コネクションレス型プロトコル(IP または SMDS など) の相互運用性が目的

LEC は、上記のすべての QoS クラスの呼を受け入れることができる必要があります。 QoS パラメーターが交渉される場合、2 つの LEC に構成されている QoS クラスが比較され、要件が厳しい方の QoS クラスが適用されます。

有効値:

0: 未指定 QoS クラスの場合

1: 指定 QoS クラス 1 の場合

2: 指定 QoS クラス 2 の場合

3: 指定 QoS クラス 3 の場合

4: 指定 QoS クラス 4 の場合

デフォルト値:

0 (未指定 QoS クラス)

ベストエフォート VCC の PCR の検証 (validate-pcr-of-best-effort-vccs)

ベストエフォート VCC のピーク・セル速度を検証するのに使用します。 FALSE の場合、シグナルされた順方向 PCR に関係なく、ベストエフォート VCC は受け入れられます。 TRUE の場合、シグナルされた順方向 PCR が、LE クライアント ATM 装置の回線速度を超えている場合、ベストエフォート VCC はリジェクトされます。逆方向 PCR が原因で呼がリジェクトされることはありません。シグナルされた逆方向 PCR は、回線速度を超えていない場合は、受け入れられます。そうでない場合は、発呼側への伝送は回線速度で行われます。

注:

1. 順方向 PCR が回線速度を超えているベストエフォート VCC を受け入れると、過度の再送のために性能が低下する可能性があります。しかし、このような VCC をリジェクトすると、相互運用性に問題が生じる可能性があります。
2. 利用不能な回線速度が原因で呼がリジェクトされたときに、発呼側がより低速の PCR を用いて再試行する場合は、YES に設定しておくと便利です。

有効値:

yes, no

デフォルト値:

no

QoS ネゴシエーション (negotiate-qos)

データ・ダイレクト VCC の QoS パラメーターのネゴシエーションを使用可能にします。このパラメーターを使用可能にするのは、IBM MSS LES に接続する場合に限ります。このパラメーターを YES に設定すると、LE クライアントは、IBM トラフィック・パラメーター TLV を、LES に送信する LE_JOIN_REQUEST および LE_ARP_RESPONSE フレームに組み込みます。この TLV には、最大予約帯域幅、トラフィック・タイプ、ピーク・セル速度、持続セル速度、最大バースト・サイズ、および QoS クラスの値が含まれます。 IBM トラフィック・パラメーター TLV は、LES が LE クライアントに戻す LE_ARP_RESPONSE にも組み込まれることがあります。

LE クライアントが受信した LE_ARP_RESPONSE に TLV が含まれていない場合は、ローカル構成パラメーターを使用してデータ・ダイレクト VCC を設定する必要があります。 LE_ARP_RESPONSE に TLV が含まれている場合、LE クライアントは、データ・ダイレクト VCC をシグナルする前に、TLV の内容を対応するローカル値と比較して、両方のパーティーに受け入れられる『ネゴシエーションされた』 または『最善』 パラメーター・セットを判別することが必要です。

有効値:

yes, no

デフォルト値:

no

LECS からの QoS パラメーター受け入れ (accept-qos-parms-from-lecs)

このパラメーターは、LE クライアントが LECS からの QoS パラメーターを受け入れ/リジェクトするように構成することができます。このパラメーターが YES の場合、LE クライアントは、LE_CONFIGURE_RESPONSE フレーム内の LE クライアントから入手した QoS パラメーターを使用することが必要です。つまり、LE クライアントからの QoS パラメーターが、ローカル構成 QoS パラメーターを上書きします。このパラメーターが NO の場合、LE クライアントは、LE クライアントからの LE_CONFIGURE_RESPONSE フレームで受信した QoS パラメーターを無視します。

有効値:

yes, no

デフォルト値:

no

QoS 構成プロンプトへのアクセス

サービス品質 (QoS) 構成コマンドにアクセスするには、CONFIG プロセスから **feature** コマンドを入力します。 **feature** と入力し、その後に機能番号 (6) または短縮名 (QOS) を入力します。たとえば、次のように入力します。

```
Config> feature qos
Quality of Service - Configuration
QoS Config>
```

QoS Config> プロンプトにアクセスすると、LE クライアント、または ATM インターフェースのサービス品質 (QoS) を構成することができます。 QoS Config> プロンプトで **exit** コマンドを入力すれば、いつでも Config> プロンプトに戻ることができます。

あるいは、以下のようにエンティティーにアクセスすることにより、LE クライアント、または ATM インターフェースの QoS パラメーターを構成することもできます。

- LE クライアント
  1. Config> プロンプトで、**network** コマンドと LE クライアント・インターフェース番号を入力する。
  2. LE Client configuration> プロンプトで、**qos-configuration** と入力する。

     例:

```
config> network 3
Token Ring Forum Compliant LEC Config> qos-configuration
LEC QoS Config>
```

- ATM インターフェース
  1. Config> プロンプトで、**network** コマンドと ATM インターフェース番号を入力して、ATM Config> プロンプトを表示する。
  2. **interface** パラメーターを入力して、ATM Interface Config> プロンプトを表示する。
  3. ATM InterfaceConfig> プロンプトで、**qos-configuration** と入力する。

     例:

```
config> network 0
ATM Config> interface
ATM Interface Config> qos-configuration
ATM-I/F 0 QoS>
```

サービス品質 (QoS) コマンド

この節では、QoS 構成コマンドの要約を示します。以下のコマンドを使用して、サービス品質 (QoS) を構成します。コマンドは QoS Config> プロンプトから入力します。

表 114. サービス品質 (QoS) 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
le-client	選択された LE クライアントの LE Client QoS configuration > プロンプトを表示します。
atm-interface	選択された ATM インターフェースの ATM Interface QoS configuration> プロンプトを表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

LE クライアント QoS 構成コマンド

この節では、特定の LE クライアントの QoS を構成するためのコマンドの要約を示し、個々のコマンドについて説明します。

以下のコマンドは LEC QoS config> プロンプトで使用します。

表 115. LE クライアントのサービス品質 (QoS) 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	LE クライアントの現行 QoS 構成をリストします。
Set	LE クライアントの QoS パラメーターを設定します。
Remove	LE クライアントの QoS 構成を除去します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、この LE クライアントの QoS 構成をリストするのに使用します。QoS パラメーターは、少なくとも 1 つのパラメーターが特別に構成されている場合にのみリストされます (例 1 を参照)。そうでない場合には、パラメーターはリストされません (例 2 を参照)。

構文:

list

例 1:

```
LEC QoS Config>
list

           LE Client QoS Configuration for Data Direct VCCs
           ========================================
     (ATM interface number = 0,  LEC interface number = 3)

  Maximum Reserved Bandwidth for a Data-Direct VCC = 10000 Kbps
  Data-Direct VCC Type ........................... = Best-Effort
  Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
  Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
  Desired QoS Class of Reserved Connections ...... = 0
  Max Burst Size of Reserved Connections    ...... = 0 frames

  Validate Peak Rate of Best-Effort connections .. = No
  Enable QoS Parameter Negotiation ............... = Yes
  Accept QoS Parameters from LECS ................ = Yes

LEC QoS Config>
```

例 2:

```
LEC QoS Config> list

   QoS has not been configured for this LEC.
   Please use the SET option to configure QoS.

LEC QoS Config>
```

Set

set コマンドは、LE クライアントの QoS パラメーターを指定するのに使用します。

構文:

set

- accept-qos-parms-from-lecs
- all-default-values
- max-burst-size
- max-reserved-bandwidth
- negotiate-qos
- peak-cell-rate
- qos-class
- sustained-cell-rate
- traffic-type
- validate-pcr-of-best-effort-vccs

accept-qos-parms-from-lecs

このオプションは、LE クライアントが LECS から TLV として受信した QoS パラメーターの受け入れ/リジェクトを使用可能/使用不可にするのに使用します。このパラメーターの詳しい説明は、884ページの『LECS からの QoS パラメーター受け入れ (accept-qos-parms-from-lecs)』 を参照してください。

有効値:

YES, NO

デフォルト値:

YES

例:

```
LEC QoS Config> se acc y
LEC QoS Config>
```

all-default-values

このオプションは、QoS パラメーターをデフォルト値に設定するのに使用します。下記の例には、デフォルト値もリストされています。

例:

```
LEC QoS Config> set all-default-values
   Failed to locate existing QoS configuration record!
   Using a new set of default values ...
   Initializing all parameters to default values
   LEC QoS Config>  list

              LE Client QoS Configuration for Data Direct VCCs
              ========================================
         (ATM interface number = 0,  LEC interface number = 3)

     Maximum Reserved Bandwidth for a Data-Direct VCC = 0 Kbps
     Data-Direct VCC Type ........................... = Best-Effort
     Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
     Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
     Desired QoS Class of Reserved Connections ...... = 0
     Max Burst Size of Reserved Connections    ...... = 0 frames

     Validate Peak Rate of Best-Effort connections .. = No
     Enable QoS Parameter Negotiation ............... = No
     Accept QoS Parameters from LECS ................ = Yes

  LEC QoS Config>
```

max-burst-size

フレームの最大バースト・サイズを設定します。このパラメーターの詳しい説明は、882ページの『最大バースト・サイズ (max-burst-size)』 を参照してください。

有効値:

整数のフレーム数。0 より大きいことが必要です。

デフォルト値:

1 フレーム

例:

```
LEC QoS Config> se ma
   Maximum Burst Size in Kbps [1]? 10000
   LEC QoS Config>
```

max-reserved-bandwidth

このオプションは、各データ・ダイレクト VCC に許容される最大予約帯域幅を設定するのに使用します。このパラメーターの詳しい説明は、880ページの『最大予約帯域幅 (max-reserved-bandwidth)』 を参照してください。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

0

例:

```
LEC QoS Config> set max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]? 20000
LEC QoS Config>
```

negotiate-qos

このオプションは、QoS ネゴシエーションへの LE クライアントの参加を使用可能/使用不可にするのに使用します。このパラメーターの詳しい説明は、883ページの『QoS ネゴシエーション (negotiate-qos)』 を参照してください。

有効値:

YES, NO

デフォルト値:

NO

例:

```
LEC QoS Config> se neg y
LEC QoS Config>
```

peak-cell-rate

データ・ダイレクトのピーク・セル速度を設定します。このパラメーターの詳しい説明は、881ページの『ピーク・セル速度 (peak-cell-rate)』 を参照してください。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

LEC ATM 装置の回線速度 (Kbps)

例:

```
LEC QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
LEC QoS Config>
```

qos-class

データ・ダイレクト VCC の QoS クラスを設定します。このパラメーターの詳しい説明は、882ページの『QoS クラス (qos-class)』 を参照してください。

有効値:

0: 未指定 QoS クラスの場合

1: 指定 QoS クラス 1 の場合

2: 指定 QoS クラス 2 の場合

3: 指定 QoS クラス 3 の場合

4: 指定 QoS クラス 4 の場合

デフォルト値:

0 (未指定 QoS クラス)

例:

```
LEC QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
LEC QoS Config>
```

sustained-cell-rate

データ・ダイレクト VCC の持続セル速度を設定します。このパラメーターの詳しい説明は、881ページの『持続セル速度 (sustained-cell-rate)』 を参照してください。

有効値:

0 から最大予約帯域幅とピーク・セル速度の最小値までの範囲内の整数値 (Kbps)

デフォルト値

なし

例:

```
LEC QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
LEC QoS Config>
```

traffic-type

データ・ダイレクト VCC のトラフィックを設定します。このパラメーターの詳しい説明は、880ページの『トラフィック・タイプ (traffic-type)』 を参照してください。

有効値:

BEST_EFFORT または RESERVED_BANDWIDTH

デフォルト値:

BEST EFFORT

例:

```
LEC QoS Config>set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved-Bandwidth
Data Direct VCC Type [0]? 1
NOTE: Peak Cell Rate has been reset to 1
      Sustained Cell Rate has been reset to 1
      Max Reserved Bandwidth has been reset to 1
      Please configure appropriate values.
LEC QoS Config>
```

validate-pcr-of-best-effort-vccs

このオプションは、この LE クライアントが受信したデータ・ダイレクト VCC の呼の「ピーク・セル速度」トラフィック・パラメーターを使用可能/使用不可にするのに使用します。このパラメーターの詳しい説明は、883ページの『ベストエフォート VCC の PCR の検証 (validate-pcr-of-best-effort-vccs)』を参照してください。

有効値:

YES, NO

デフォルト値:

NO

例:

```
LEC QoS Config> se val y
LEC QoS Config>
```

Remove

remove コマンドは、この LE クライアントの QoS 構成を除去するのに使用します。

構文:

remove

例:

```
LEC QoS Config> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the LEC QoS configuration be deleted? [No]: yes
Deleted QoS configuration successfully
LEC QoS Config>
```

ATM インターフェース QoS 構成コマンド

表 116. LE クライアントのサービス品質 (QoS) 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	現行の ATM インターフェース QoS 構成をリストします。
Set	ATM インターフェース QoS パラメーターを設定します。
Remove	ATM インターフェースの QoS 構成を除去します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、この ATM インターフェースの QoS 構成をリストするのに使用します。 QoS パラメーターは、少なくとも 1 つのパラメーターが構成されている場合にのみリストされます (下の例を参照)。そうでない場合には、パラメーターはリストされません。

構文:

list

例:

```
ATM-I/F 0 QoS> list

          ATM Interface 'Quality of Service' Configuration
          ================================================
                    (ATM interface number = 0  )

     Maximum Reserved Bandwidth for a VCC = 15000 Kbps
     VCC Type ........................... = RESERVED-BANDWIDTH
     Peak Cell Rate ..................... = 20000 Kbps
     Sustained Cell Rate ................ = 5000 Kbps
     QoS Class .......................... = 4
     Maximum Burst Size ................. = 5 frames
ATM-I/F 0 QoS>
```

Set

set コマンドは、ATM クライアントの QoS パラメーターを指定するのに使用します。

構文:

set max-burst-size
max-reserved-bandwidth
peak-cell-rate
qos-class
sustained-cell-rate
traffic-type

max-burst-size

フレームの最大バースト・サイズを設定します。このパラメーターの詳しい説明は、882ページの『最大バースト・サイズ (max-burst-size)』 を参照してください。

有効値:

整数のフレーム数。0 より大きいことが必要です。

デフォルト値:

1 フレーム

例:

```
ATM-I/F 0 QoS Config> se ma
Maximum Burst Size in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

max-reserved-bandwidth

このオプションは、各データ・ダイレクト VCC に許容される最大予約帯域幅を設定するのに使用します。このパラメーターの詳しい説明は、880ページの『最大予約帯域幅 (max-reserved-bandwidth)』 を参照してください。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

0

例:

```
ATM-I/F 0 QoS> se max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]? 15000
ATM-I/F 0 QoS>
```

peak-cell-rate

データ・ダイレクト VCC のピーク・セル速度を設定します。このパラメーターの詳しい説明は、881ページの『ピーク・セル速度 (peak-cell-rate)』 を参照してください。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

LEC ATM 装置の回線速度 (Kbps)

例:

```
ATM-I/F 0 QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
ATM-I/F 0 QoS Config>
```

qos-class

データ・ダイレクト VCC の QoS クラスを設定します。このパラメーターの詳しい説明は、882ページの『QoS クラス (qos-class)』 を参照してください。

有効値:

0: 未指定 QoS クラスの場合

1: 指定 QoS クラス 1 の場合

2: 指定 QoS クラス 2 の場合

3: 指定 QoS クラス 3 の場合

4: 指定 QoS クラス 4 の場合

デフォルト値:

0 (未指定 QoS クラス)

例:

```
ATM-I/F 0 QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
ATM-I/F 0 QoS Config>
```

sustained-cell-rate

データ・ダイレクト VCC の持続セル速度を設定します。このパラメーターの詳しい説明は、881ページの『持続セル速度 (sustained-cell-rate)』 を参照してください。

有効値:

0 から最大予約帯域幅とピーク・セル速度の最小値までの範囲内の整数値 (Kbps)

デフォルト値

なし

例:

```
ATM-I/F 0 QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

traffic-type

データ・ダイレクト VCC のトラフィックを設定します。このパラメーターの詳しい説明は、880ページの『トラフィック・タイプ (traffic-type)』 を参照してください。

有効値:

BEST_EFFORT または RESERVED_BANDWIDTH

デフォルト値:

BEST EFFORT

例:

```
ATM-I/F 0 QoS> set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved Bandwidth
Traffic Type of VCCs [1]? 0
ATM-I/F 0 QoS>
```

Remove

remove コマンドは、この ATM インターフェースの QoS 構成を除去するのに使用します。

構文:

remove

例:

```
ATM-I/F 0 QoS> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the ATM Interface QoS configuration be deleted? [No]: yes
Deleted QoS SRAM record successfully
ATM-I/F 0 QoS>
```

QoS 監視コマンドへのアクセス

サービス品質コマンドにアクセスするには、GWCON プロセスから **feature** コマンドを入力します。 **feature** と入力し、その後に機能番号 (6) または短縮名 (QOS) を入力します。たとえば、次のように入力します。

```
+feature qos
Quality of Service (QoS) - User Monitoring
QoS+
```

QoS 監視プロンプトにアクセスしたら、特定の LE クライアントを監視することを選択できます。 QoS 監視プロンプトで exit コマンドを入力すれば、いつでも GWCON プロンプトに戻ることができます。

あるいは、次のようにして、LE クライアントの QoS 監視にアクセスすることもできます。

1. GWCON プロンプト (+) で、network コマンドと LE クライアントのインターフェース番号を入力する。
2. LE クライアント監視プロンプトで、**qos-information** と入力する。

   例:

   ```
   +network 3
   ATM Emulated LAN Monitoring
   LEC+qos information
   LE Client QoS Monitoring
   LEC 3 QoS+
   ```

サービス品質監視コマンド

この節では、QoS 監視コマンドの要約を示します。これらのコマンドは QoS+ プロンプトで入力します。

表 117. サービス品質 (QoS) 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
le-client	選択された LE クライアントの `LE Client QoS console +` プロンプトを表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

LE クライアント QoS 監視コマンド

この節では、LE クライアント QoS 監視コマンドの要約を示します。コマンドは `LEC num QoS+` プロンプトから入力します。

表 118. LE クライアント QoS 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	現行の LE クライアント QoS 情報をリストします。オプションには、構成パラメーター、TLV、VCC、および統計が含まれます。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、この LE クライアントの QoS 関連情報をリストするのに使用します。

構文:

list configuration-parameters
data-direct-VCCs (Detailed Information)
statistics
tlv-information
vcc-information

configuration-parameters

QoS 構成パラメーターをリストします。パラメーターは、LE クライアント、ATM インターフェース、または ELAN に対して構成できるので、これらのパラメーターは LE クライアントが使用する解決済み パラメーター・セットとともに表示されます。

le-client

SRAM レコードから入手された、この LE クライアントに構成され

ているパラメーター。 SRAM レコードに無効なパラメーター・セットが入っている場合、この欄にはパラメーター値は表示されません。

ATM Interface
この LE クライアントが使用する ATM インターフェースに構成されているパラメーター。これらのパラメーターは、ローカル SRAM レコードから入手されます。 SRAM レコードに無効なパラメーター・セットが入っている場合、この欄にはパラメーター値は表示されません。

From LECS
この LE クライアントが LE 構成サーバーから受信したパラメーター。パラメーターは、LE_CONFIGURE_RESPONSE 制御メッセージ内の個々の TLV として受信されます。

used データ・ダイレクト VCC に使用される解決済みトラフィック・パラメーター・セット。どのエンティティーにも QoS パラメーターが構成されていない場合、USED パラメーターはデフォルト・パラメーターを表します。少なくとも 1 つのエンティティーが構成されている場合は、以下のように解決されます。

- LE クライアントまたは ATM インターフェースのどちらか一方にのみパラメーターが構成されており、accept-parms-from-lecs が FALSE であるか、 LECS からパラメーターを受信しなかった場合は、構成された LE クライアントまたは ATM インターフェースのパラメーターが使用されます。
- LE クライアントと ATM インターフェースの両方にパラメーターが構成されている場合は、LE クライアントのパラメーターが使用されます。
- accept-parms-from-lecs が TRUE であり、LECS からパラメーターを受信した場合は、LE クライアントのパラメーター (または、LE クライアントが構成されていない場合は、デフォルト値) と LECS から受信したパラメーターが結合されて、879ページの『QoS 構成パラメーター』 に記述されている最初の 6 つの QoS パラメーターの完全なセットが作成されます。
- 879ページの『QoS 構成パラメーター』 に記述されている最初の 6 つの QoS パラメーター・セットに無効な組み合わせが含まれている場合、 LECS からのパラメーターはリジェクトされます。 2 つのフラグ negotiate-qos と validate-pcr-of-best-effort-vccs は、独立して検証されます。

例:

```
LEC 1 QoS+ list configuration parameters

                ATM LEC Configured QoS  Parameters
                ==================================

     QoS                                        |    LEC      ATM-IF    FROM

   PARAMETER                             USED    |    SRAM     SRAM      LECS

 ------------------------------------------------------------------------------
 Max Reserved Bandwidth (cells/sec) :    23584   |    23584        0     none
                       (Kbits/sec) :    10000   |    10000        0     none
```

```
 VCC Type ........................ :   ResvBW   |   ResvBW   BstEft        0
 Peak Cell Rate ........(cells/sec) :    18867   |    18867   365566   365566
                        (Kbits/sec) :     8000   |     8000   155000   155000
 Sustained Cell Rate ...(cells/sec) :    18867   |    18867   365566     none
                        (Kbits/sec) :     8000   |     8000   155000     none
 QoS Class ....................... :        4   |        4        0     none
 Max Burst Size .............(cells) :       95   |       95        0     none
                             (frames) :        1   |        1        0     none
 Validate PCR of Best-Effort VCCs . :       NO   |       NO      n/a     none
 Enable QoS Negotiation ........... :      YES   |      YES      n/a     none
 Accept QoS Parameters from LECS .. :      YES   |      YES      n/a      n/a
 ------------------------------------------------------------------------------
(BstEft = Best Effort, ResvBW = Reserved Bandwidth)
(n/a = not applicable, none = no value is specified)

LEC 1 QoS+
```

data-direct-vccs (Detailed Information)

このオプションは、この LE クライアントのデータ・ダイレクト VCC 情報をリストします。 **list vcc-information** を使用した場合も、同様の情報がリストされます。

例:

```
LEC 1 QoS+ list data direct vccs

          LEC Data Direct VCCs - QoS Information
          ======================================

Conn Handle = 80, VPI = 0, VCI = 546
        Connection Type = RETRIED CONNECTION PARAMETERS
          TrafficType    = BEST EFFORT VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 58962 (25 Mbps)
          QoS Class      = 0
          Max Burst Size = 0

Conn Handle = 78, VPI = 0, VCI = 544
        Connection Type = PARAMETERS SET BY DESTINATION
          TrafficType    = RESERVED BANDWIDTH VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 16509 (7 Mbps)
          QoS Class      = 1
          Max Burst Size = 95

LEC 1 QoS+
```

statistics

以下の統計のカウンターが維持されています。

Successful QoS Connections

LE クライアントによって確立された RESERVED-BANDWIDTH 接続の数

Successful Best-Effort Connections

LE クライアントによって確立された BEST-EFORT 接続の数

Failed QoS Connections

LE クライアントが行い、失敗した RESERVED-BANDWIDTH 接続要求の数

Failed Best-Effort Connections

LE クライアントが行い、失敗した BEST-EFFORT 接続要求の数

QoS Negotiation Applied

QoS ネゴシエーション拡張が適用された回数。パラメーターのネゴシエーションが行われるのは、LE クライアントが LE_ARP_RESPONSE 制御メッセージで着信先 LE クライアントのパラメーターを受信した場合です。

PCR Proposal (IBM) Applied
IBM ピーク・セル速度が適用された回数。この提案は、BEST-EFFORT 接続で 100 Mbps または 155 Mbps でシグナルする場合は、特定の速度パラメーターを使用することを推奨しています。これにより、参加している他の IBM プロダクト (たとえば、25-Mbps ATM アダプター) は、シグナルされたピーク・セル速度に基づいて接続をリジェクトすることができます。

QoS Connections Accepted
この LE クライアントによって受け入れられた RESERVED-BANDWIDTH 接続の数。

Best-Effort Connections Accepted
この LE クライアントによって受け入れられた BEST-EFFORT 接続の数

QoS Connections Rejected
この LE クライアントが受信し、リジェクトした RESERVED-BANDWIDTH 接続要求の数。

Best-Effort Connections Rejected
この LE クライアントが受信し、リジェクトした BEST-EFFORT 接続要求の数

Rejected due to PCR Validation
validate-pcr-of-best-effort-vccs parameter が TRUE の場合、ピーク・セル速度の検証が原因で LE クライアントによってリジェクトされた BEST-EFFORT 接続の数。

例:

```
LEC 1 QoS+  li stat

QoS Statistics: of Data Direct Calls Placed by the LEC
------------------------------------------------------
    Successful QoS Connections          = 0
    Successful Best-Effort Connections  = 1
    Failed QoS Connections              = 1
    Failed Best-Effort Connections      = 1
    Qos Negotiation Applied             = 0
    PCR Proposal (IBM) Applied          = 0

QoS Statistics: of Data Direct Calls Received by the LEC
--------------------------------------------------------
    QoS Connections Accepted            = 1
    Best-Effort Connections Accepted    = 0
    QoS Connections Rejected            = 0
    Best-Effort Connections Rejected    = 0
    Rejected due to PCR Validation      = 0

LEC 1 QoS+
```

tlv-information
この LE クライアントが LE サーバーに登録した IBM トラフィック情報 TLV をリストします。 TLV が登録されるのは、LE クライアントが QoS ネゴシエーションに参加している場合だけです。

例:

```
LEC 1 QoS+ list tlv

  Traffic Info TLV of the LEC (registered with the LES)
  =====================================================
    TLV Type .........................= 268458498
    TLV Length .......................= 24
    TLV Value:
           Maximum Reserved Bandwidth = 23584 cells/sec (10 Mbps)
```

```
Data Direct VCC Type..... = RESERVED BANDWIDTH VCC
Data Direct VCC PCR..... = 18867 cells/sec (8 Mbps)
Data Direct VCC SCR..... = 18867 cells/sec (8 Mbps)
Data Direct VCC QoS Class  = 4
Maximum Burst Size         = 95 cells (1 frames)

LEC 1 QoS+
```

vcc-information

LE クライアントのすべてのアクティブ VCC をリストします。この情報には、接続のトラフィック・パラメーターが入っています。ベストエフォート接続の場合は、持続セル速度が表示されますが、これはピーク・セル速度、QoS クラス、および最大バースト・サイズが 0 として表示されるのと同じことです。

パラメーター記述子エントリーは、次のとおりです。

SrcParms
この LE クライアントによって確立された接続のパラメーター

DestParms
この LE クライアントが受信した接続のパラメーター

NegoParms
QoS ネゴシエーションを使用して LE クライアントが確立した接続のパラメーター

RetryParms
少なくとも 1 回失敗した後で、この LE クライアントによって確立された接続のパラメーター

例:

```
LEC 1 QoS+ li vcc

                          LEC VCC Table
                          =============

                                                                        Burst
Conn   Conn              Conn          VCC    PCR    SCR   QoS   Size    Parameters
Index  Handle VPI   VCI   Type  Status  Type  (kbps) (kbps) Class (cells) Descriptor
-------------------------------------------------------------------------------------
   2)     69    0   535  Cntrl  Ready  BstEft 155000 155000    0      0   SrcParms
   3)     71    0   537  Cntrl  Ready  BstEft      0      0    0      0   DestParms
   4)     72    0   538  Mcast  Ready  BstEft 155000 155000    0      0   SrcParms
   5)     74    0   540  Mcast  Ready  BstEft      0      0    0      0   DestParms
   6)     78    0   544  Data   Ready  ResvBW  25000   7000    1     95   DestParms

LEC 1 QoS+
```

第69章 IP セキュリティーの使用

インターネット・プロトコル (IP) を使用して送信されるパケットは、2210 の IP セキュリティー機能を使用して保護することができます。この保護は、認証および暗号化と呼ばれるプロセスによって提供されます。

注: 暗号化サポートはオプションです。ロードしたソフトウェアに暗号化が含まれていない場合、暗号化関連パラメーターはありません。

セキュリティー (インターネット・プロトコルの RFC 1825 セキュリティー体系によって定義) は、以下の特性から構成されています。

認証 受信したデータは送信されたデータと同じであること、および主張している送信側が確かに実際の送信側であることが分かっていること。

保全性 変更が検出されることなくデータが送信元から宛先に転送されることが保証されること。

機密性 指定された受信側は何が送信されたのかを知っているが、当事者以外は何が送信されたのかを判別できない方法で通信すること。

非否認 後で送信側がそのデータを送信したことを否定しても、受信側は送信側が確かに所定のデータを送信したことを証明できる方法で通信すること。

2210 の IP セキュリティー機能は、これらの特性のうちの 3 つ (認証、保全性、および機密性) を提供します。

保護トンネル

別のホスト、ルーター、またはファイアウォールに送信するデータを保護するために、保護トンネルを構成することができます。 IP 保護 (IPsec) トンネルは、保護 IP パケットを転送するための、リモート・ホスト、ルーター、またはファイアウォールへの両方向論理接続です。 IP 認証ヘッダー (AH) および IP カプセル化セキュリティー・ペイロード (ESP) は、トンネルのセキュリティーを確保するために認証と暗号化を含む特殊な IP ヘッダーを使用する技法です。

保護トンネルは、トンネル ID やトンネルの反対側の宛先ホストのアドレスなど、さまざまなパラメーターによって識別されます。 IP セキュリティーは、保護する必要がある各 IP ルートごとに手動で保護トンネルを構成するという手法で、2210 上に作成します。指定された 1 組のパラメーターが、1 つの保護トンネルを作成します。

注: 各保護トンネルでは、以下にリストするパラメーターが保護トンネルの両側で一致していなければなりません。すなわち、受信側と受信側に同じ値を構成することが必要です。

- AH アルゴリズムと AH 認証キー (902ページの『アルゴリズムの構成』を参照してください)。
- ESP 暗号化アルゴリズムおよび ESP 暗号化キーと暗号化解除キー (902ページの『アルゴリズムの構成』を参照してください)。
- セキュリティー・パラメーター・インデックス (SPI) (900ページの『セキュリティー・アソシエーション』を参照してください)。

トンネル・ポリシー

保護トンネルは、AH、ESP、AH-ESP、または ESP-AH のいずれか 1 つから成るトンネル・ポリシーを使用して構成します。

AH と ESP の両方が構成されている場合、次の関係が適用されます。

- ポリシー AH-ESP は、発信パケットは認証より前に暗号化を実行するように構成されることを意味しています。この場合、着信パケットは最初に AH 認証によって検査されます。 AH 認証に合格したパケットだけが ESP に転送されて、暗号化解除されます。
- ポリシー ESP-AH は、発信パケットは暗号化より前に認証を実行するように構成されることを意味しています。この場合、着信パケットは最初に ESP によって暗号化解除されます。暗号化解除が正常に行われたパケットだけが AH 認証に転送されます。

セキュリティー・アソシエーション

セキュリティー・アソシエーション (SA) は、AH または ESP が接続トラフィックを保護するために使用する単方向セキュリティー接続です。各保護トンネルに 2 つのセキュリティー・アソシエーション (SA バンドル) を構成します。1 つは着信用、1 つは発信用です。各セキュリティー・アソシエーションは、独自のセキュリティー・パラメーター・インデックス (SPI) (任意の 32 ビット値) によって識別されます。

トランスポート・モードおよびトンネル・モード

各保護トンネルに対して、トランスポート・モードまたはトンネル・モードを構成します。トランスポート・モードまたはトンネル・モードは、AH または ESP が IP パケットを扱う方法を決めます。トンネル・モードがデフォルトです。トランスポート・モードは、ルーターがホストとして動作している場合にのみ使用できます。ルーターがセキュリティー・ゲートウェイとして動作している場合は、トンネル・モードが必須です。

AH を使用するモード

トランスポート・モードでは、AH は IP ヘッダーの後と高位レイヤー・プロトコル (TCP または UDP など) のヘッダーの前に挿入されます。このモードでは、AH は高位レイヤー・プロトコル・ヘッダーと IP パケットの内容を認証します。ただし、IP パケットの可変フィールド (たとえば、存続期間 [TTL]、チェックサム、フラグメント・フラグ、フラグメント・オフセット、およびサービス・タイプ [TOS] など) は除きます。

トンネル・モードでは、AH の直後に IP パケット全体が続き、新規の IP ヘッダーが作成されて AH の前に置かれます。トンネル伝送されるパケットの IP ヘッダー (内部 IP ヘッダーと呼ばれます) は、パケットの最終的な送信元と宛先のアドレスを伝送します。新規 IP ヘッダー (外部 IP ヘッダーと呼ばれます) には、セキュリティー・ゲートウェイ (トンネルのエンドポイント) のアドレスを入れることができます。AH は、新規 IP ヘッダー内の可変フィールドを除いて、新規 IP ヘッダーとトンネル伝送される IP パケットの両方を含めた新規パケット全体を保護します。

ESP を使用するモード

ESP を使用するトランスポート・モードでは、ペイロード・データ・フィールドに、高位レイヤー・プロトコル・データ (TCP または UDP データ) が入ります。 ESP は、高位レイヤー・プロトコル・データ (および、IP セキュリティー・バージョン 2 の場合は、 ESP トレーラー) を暗号化します。認証が使用されている場合には、ESP ヘッダー、高位レイヤー・プロトコル・データ、および ESP トレーラーが認証されます。

トンネル・モードでは、ペイロード・データ・フィールドに IP パケット全体が入り、新規の IP ヘッダーが作成されて ESP の前に置かれます。トンネル伝送されるパケットの IP ヘッダー (内部 IP ヘッダーと呼ばれます) は、パケットの最終的な送信元と宛先のアドレスを伝送し、新規 IP ヘッダー (外部 IP ヘッダーと呼ばれます) には、セキュリティー・ゲートウェイのアドレスが入ります。 ESP は、トンネル伝送 IP パケット (および、IP セキュリティー・バージョン 2 の場合は、 ESP トレーラー) を暗号化します。認証が使用されている場合には、ESP ヘッダー、トンネル伝送 IP パケット、および ESP トレーラーが認証されます。

IP 認証ヘッダー (AH)

AH は、draft-ietf-ispe-auth-header-05 Authentication Header に記述されています。このヘッダーには、IP データグラムの認証データが入っています。データグラムの送信側は、秘密の認証キーに依存する暗号認証機能を使用します。この暗号認証機能は、データグラムの内容に適用されます。

AH 認証アルゴリズム

AH トンネル・ポリシーを使用する保護トンネルは、次の 2 つの認証アルゴリズムのうちの 1 つを使用することが必要です。

- 再生防止付き HMAC-MD5 IP 認証
- 再生防止付き HMAC-SHA-1 IP 認証

これらのアルゴリズムは両方とも、再生防止を備えた暗号ハッシュ機能 (略語 HMAC) を使用して、キー付きメッセージ認証を結合します。再生防止 (オプション機能) は、AH によって提供されたシーケンス番号を使用して、このパケットが以前に受信されていないことを確認します。再生防止機能は、同じパケットが繰り返し受信側に送られるというサービス拒否 (denial-of-service) アタックから受信側を守るために使用されます。ルーターが重複パケットの処理に忙殺されて、正当なトラフィックを処理できなくなる可能性があるからです。スライディング・ウィンドウを使用して、このシーケンス番号を以前に受信したかどうかを調べるのに十分なシーケンス番号が保管されます。

IP カプセル化セキュリティー・ペイロード (ESP)

ESP は、draft-ietf-ipsec-esp-v2-04 Encapsulating Security Payload に記述されています。ESP は、IP パケットの一部または全部を暗号化して、ユーザーに機密性、認証、および保全性を提供します。 ESP では、認証機能はオプション機能です。

ESP 認証アルゴリズム

ESP 認証に利用可能な認証アルゴリズムは、AH の場合と同じです。詳細については、901ページの『AH 認証アルゴリズム』を参照してください。

ESP 暗号化アルゴリズム

ESP を構成するには、次の 3 つの暗号化アルゴリズムのうちの 1 つを選択することが必要です。

- 暗号化ブロック・チェーン方式のデータ暗号化規格 (DES-CBC)
- 商業データ・マスキング・ファシリティー (CDMF)
- トリプル DES (3DES)

注: ESP 暗号化アルゴリズムは、米国の輸出規制の対象になっています。 2210 にこれらのアルゴリズムの一部または全部を構成することが許可されていない場合は、これらのアルゴリズムの販売が禁止されている可能性があります。詳細については、IBM 担当者にお尋ねください。

アルゴリズムの構成

トンネル・ポリシーに基づいて、アルゴリズムは表119 のように構成されます。

表 119. 各種のトンネル・ポリシーを使用して構成されたアルゴリズム

トンネル・ポリシー	アルゴリズム
AH、AH-ESP、または ESP-AH	• ローカル AH 認証アルゴリズム - 必須 • リモート AH 認証アルゴリズム - オプション
ESP、AH-ESP、または ESP-AH	• ローカル暗号化アルゴリズム - 必須 • リモート暗号化アルゴリズム - オプション • ローカル ESP 認証アルゴリズム - オプション • リモート ESP 認証アルゴリズム - オプション **注:** ソフトウェア・ロードに暗号化が含まれていない場合は、暗号化関連のパラメーターは表示されません。

ローカル・アルゴリズムは発信パケットに適用され、リモート・アルゴリズムは着信パケットに適用されます。各リモート・アルゴリズムは対応するリモート・アルゴリズムの値をデフォルトとして取るので、リモート・アルゴリズムの値はオプションです。 ESP の一部としての認証はオプション機能なので、ローカル認証アルゴリズムはオプションです。

特定の保護トンネルに対して送信側によって構成されたローカル・アルゴリズムは、その保護トンネルの反対側の受信側によって構成されたリモート・アルゴリズムと一致していなければなりません。たとえば、送信側のトンネル・ポリシーが AH で、 AH ローカル認証アルゴリズムが HMAC-MD5 である場合、受信側のトンネル・ポリシーの 1 つとして AH が構成されていることが必要であり、受信側の AH リモート認証アルゴリズムは HMAC-MD5 でなければなりません。

キーの構成

構成された各アルゴリズムごとに、キーを構成することが必要です。各キーは、トンネルの反対側のホスト内の同じアルゴリズムのキーと一致していなければなりません。たとえば、発信パケットのローカル暗号化キーが 0098B1C588A109D5 の場合、保護トンネルの反対側のホストの着信パケットの暗号化キーも同じ番号に構成されていることが必要です。詳細については、911ページの『第70章 IP セキュリティーの構成および監視』 の **add tunnel** コマンドの項のキーの説明を参照してください。

例: IPsec トンネルの構成

図49 のネットワークは、IPsec を備えたルーターと、IPsec およびネットワークアドレス変換 (NAT) を備えたルーターを接続する IPsec トンネルの例を示しています。

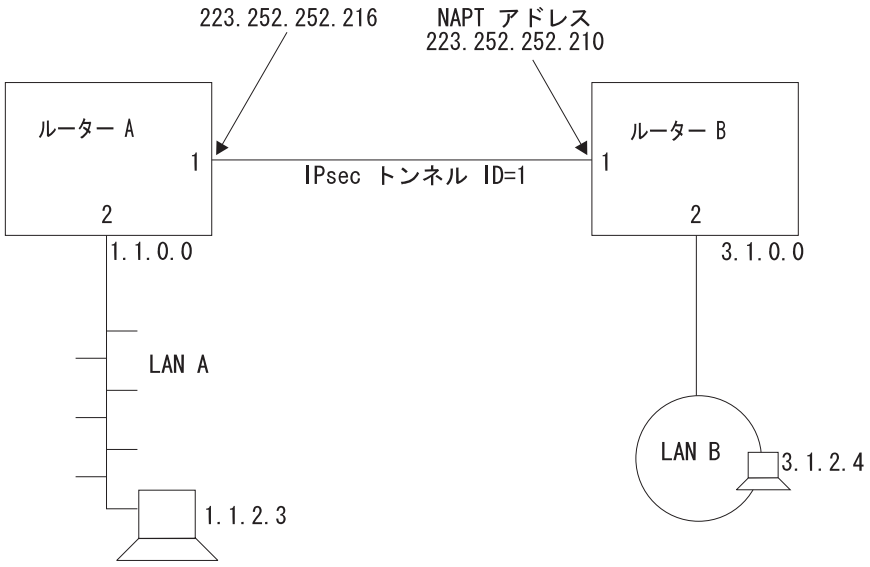


図 49. IPsec と NAT を備えたルーター

このネットワークでは、IPsec トンネル ID 1 をもつ IPsec トンネルが、ルーター A の IP アドレス 223.252.252.216 からルーター B の IP アドレス 223.252.252.210 に構成されています。ルーター A は IPsec 用に構成されています。ルーター B は、IPsec と NAT の両方用に構成されています。このネットワークを構成するプロセスを、以下で説明します。

注: ユーザーのネットワークで NAT を使用する計画がない場合は、ルーター B よりもルーター A の方に関心をお持ちと思いますが、ルーター B の構成の説明も通してお読みになると、IPsec トンネルの各端のパラメーターの関係をよく理解することができます。

ルーター A の構成 (IPsec のみ)

最初に、以下のステップに従って、ルーター A を構成します。

- IPsec トンネルを作成する。

- IPsec トンネルのエンドポイントのルーター・インターフェース上に、1 つの発信パケットと 1 つの着信パケットを作成する。
- パケット・フィルターのアクセス制御規則を作成する。
- IPsec をリセットする。
- IP をリセットする。

ルーター A の IPsec トンネルの作成: 下の例は、ルーター A 用の IPsec トンネル 1 を構成する方法を示しています。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> add tunnel
IPsec Tunnel ID (1 - 65535) [1]
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600)[46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]? AH
Local IP Address [1.1.1.1]? 223.252.252.216
Local Authentication SPI (256-65535)[256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 223.252.252.210
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
Ipsec config>
```

この例から分かるように、ユーザーが提供する必要があるパラメーターを入力するようにプロンプトで指示されます。 ESP、AH-ESP、または ESP-AH 保護トンネルの構成でも、同様のパラメーターが要求されます。

注: キーの値は、入力したときには表示されないので、この例には示されていません。 HMAC-MD5 認証のキーが表示されるとすれば、32 桁の 16 進文字で示されます。たとえば、キーは X'1234567890ABCDEF1234567890ABCDEF' のような値を持っています。

ルーター A のパケット・フィルターの構成: ルーター A 用の IPsec トンネルを作成した後で、2 つの IP パケット・フィルターを設定する必要があります。1 つは発信パケット・フィルターで、もう 1 つは着信パケット・フィルターです。下の例は、パケット・フィルター *out-router-A* の作成を示しています。 IP パケット・フィルターの構成およびアクセス制御規則についての詳細は、*プロトコルの構成と監視 解説書、第 1 巻* の IP の章の IP アクセス制御の節を参照してください。

```
* talk 6
Config> Protocol IP
Internet protocol user configuration
IP Config> set access-control on
IP Config> add packet-filter
Packet-filter name [ ]? out-router-A
Filter incoming or outgoing traffic? [IN]? OUT
Which interface is this filter for [0]? 1
IP Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config>
```

同様の方法で、ルーター A のインターフェース 1 上に、ルーター A の着信パケット・フィルター *in-router-A* を作成します。パケット・フィルターはインターフェース 1 上に作成します。これが IPsec トンネル 1 のエンドポイントであるからです。

ルーター A のパケット・フィルター・アクセス制御規則の構成: 次のステップは、パケット・フィルター・アクセス制御規則を構成することです。発信パケット・フィルター *out-router-A* に関する 2 つのアクセス制御規則と、着信パケット・フィルター *in-router-A* に関する 2 つのアクセス制御規則を作成する必要があります。

注: 各 IPsec トンネルには、着信パケット・フィルターと発信パケット・フィルターが構成され、それぞれのパケット・フィルターに 2 つのアクセス制御規則が構成されていなければなりません。

発信パケット・フィルターのアクセス制御規則は、以下の機能を実行します。

- 1 つのアクセス制御規則は、IPsec トンネルに渡されるパケットの発信元および宛先アドレスの範囲を定義します。
- もう 1 つのアクセス制御規則は、パケット・フィルターを通して IPsec トラフィックを渡せるようにします。

着信パケット・フィルターのアクセス制御規則は、以下の機能を実行します。

- 1 つのアクセス制御規則は、パケット・フィルターを通して着信 IPsec トラフィックを渡せるようにします。
- もう 1 つのアクセス制御規則は、IPsec によって処理済みのパケットの送信元および宛先アドレスを調べる冗長検査機能です。このアクセス制御規則により、これらの送信元および宛先アドレスが、IPsec トンネルの反対側から発信されたパケットの送信元および宛先アドレスに一致していることが保証されます。

in-router-A の最初のアクセス制御規則は、IPsec トンネルの 2 つのエンドポイントを識別し、IPsec トンネルを介してトラフィックを渡します。プロトコル範囲 50 - 51 は、IPsec を識別します。

```
IP Config> update packet-filter
Packet-filter name [ ]? in-router-A
Packet-filter 'in-router-A' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 223.252.252.210
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 223.252.252.216
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
(Enable logging? (Yes or [No]):
Packet-filter 'in-router-A' Config>
```

in-router-A の 2 番目のアクセス制御規則は、ルーター A の IPsec 処理済みパケットの発信元および宛先アドレスを検査して、それらがルーター B から送信されたパケットの送信元および宛先アドレスと同じであることを確認します。ルーター A 上の発信パケット・フィルターは、ルーター B 上で予想されている送信元および宛先アドレスと一致しない送信元および宛先アドレスをもつパケットは決して通過させるはずがないので、この IPsec トンネルのセキュリティーに関する追加検査は冗長ですが、IETF セキュリティー体系の草案では、これが推奨されています。

注: ルーター B は NAT を使用しているので、ルーター A はルーター B の 3.1.0.0 アドレスにはアクセスできません。そのため、*in-router-A* の 2 番目のアクセス制御規則は、リモート送信元アドレスとして、サブネット 3.1.0.0 ではなく、アドレス 223.252.252.210 を使用しています。

```
Packet-filter 'in-router-A' Config> add access
Enter type [E]? IS
Internet source [0.0.0.0]? 223.252.252.210
Source mask [255.255.255.255]?
```

```
Internet destination [0.0.0.0]? 1.1.0.0
Destination mask [255.255.255.255]? 255.255.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
(Enable logging? (Yes or [No]):
Packet-filter 'in-router-A' Config> exit
```

どのアクセス制御規則にも一致しないすべてのパケットを、廃棄せずに通過させたい場合は、これらのパケットを通過させるための包括的ワイルドカード・アクセス制御規則を構成することができます。ただし、このアクセス制御規則は、着信パケット・フィルターに対する 2 番目の着信アクセス制御規則で廃棄するように設計されているパケットを通過させるので、2 番目の着信アクセス制御規則は無効になります。次の例は、このようなアクセス制御規則を示しています。

```
Packet-filter 'in-router-A' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]?
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]?
Destination mask [255.255.255.255]? 0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable Logging (Yes or [No]):
Packet-filter 'in-router-A' Config> exit
```

次に、パケット・フィルター *out-router-A* の最初のアクセス制御規則を構成します。このアクセス制御規則は、パケットをサブネット 1.1.0.0 からルーター B の宛先アドレス 223.252.252.210 に渡します。

```
IP Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config> add access
Enter type [E]? IS
Internet source [0.0.0.0]? 1.1.0.0
Source mask [255.255.255.255]? 255.255.0.0
Internet destination [0.0.0.0]? 223.252.252.210
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
(Enable logging? (Yes or [No]):
Packet-filter 'out-router-A' Config>
```

out-router-A の 2 番目のアクセス制御規則は、IPsec トンネルの 2 つのエンド間でパケットを渡せるようにします。

```
Packet-filter 'out-router-A' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 223.252.252.216
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 223.252.252.210
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
(Enable logging? (Yes or [No]):
Packet-filter 'out-router-A' Config>
```

他のパケット・フィルターと同様に、*out-router-A* に対してワイルドカード・アクセス制御規則を構成して、どのアクセス制御規則にも一致しないトラフィックを渡せるようにすることもできます。

ルーター A 上の IPsec と IP のリセット: IPsec 構成が完了したら、Talk 5 で **reset ipsec** コマンドを使用して、Talk 6 で作成した新規の IPsec 構成を SRAM に再ロードします。**reset ipsec** コマンドは、IP 構成には影響を与えません。次に、Talk 5 で **reset ip** コマンドを使用して、ルーター内の IP を動的にリセットします。代わりに、各コンポーネントをリセットするために、ルーターをリスタートすることもできます。パケット・フィルターおよびアクセス規則が再ロードされたことを保証するためには、IPsec と IP をリセットするか、ルーターをリスタートすることが必要です。

そうしないと、構成がインターフェース上で正しくサポートされない可能性があります。詳細については、911ページの『第70章 IP セキュリティーの構成および監視』、および*プロトコルの構成と監視 解説書、第 1 巻* の **reset ip** コマンドの項を参照してください。

ルーター B の構成 (IPsec および NAT)

IPsec トンネル 1 は、ルーター B のインターフェース 1 にエンドポイントがあります。ルーター B は、IPsec および NAT の両方用に構成します。 NAT が構成されている場合、ルーター上の発信パケット・フィルターを使用して、NAT 変換および IPsec カプセル化を通して発信パケットを渡すことができます。着信パケットは、最初に IPsec を通って暗号化解除され、次に NAT に渡されて変換されます。

以下のステップに従って、ルーター B を構成します。

- NAT を構成する。
- IPsec トンネルを作成する。
- IPsec トンネルのエンドポイントのルーター・インターフェース上に、1 つの発信パケットと 1 つの着信パケットを作成する。
- パケット・フィルターのアクセス制御規則を作成する。
- IPsec をリセットする。
- NAT をリセットする。
- IP をリセットする。

ルーター B の NAT の構成については、ここでは説明しません。 NAT の構成についての詳細は、927ページの『第71章 ネットワーク・アドレス変換の使用』、および935ページの『第72章 ネットワーク・アドレス変換の構成および監視』を参照してください。この例では、NAT は構成済みであり、NAPT アドレス 223.252.252.210 は IPsec トンネルのエンドポイントでもあるものと想定します。この例の NAT 私設アドレス・プールは 3.1.0.0 で、サブネットは 255.255.0.0 です。 IPsec トンネル 1 から到着した着信トラフィックは IPsec によって処理され、次に NAT に渡されて、これらのアドレスの 1 つに変換されます。

注:

1. この例では、IPsec トンネルのエンドポイント・アドレスと NAPT アドレスが同一ですが、この例の場合のように IPsec と NAT が一緒に使用されている場合は、IPsec トンネルのエンドポイント・アドレスは任意の有効な IP アドレスを使用することができ、必ずしも NAPT アドレスまたは NAT 公衆アドレスの 1 つに一致している必要はありません。
2. NAT に関心がない場合は、アドレス 223.252.252.210 を IPsec トンネル 1 のエンドポイントとみなし、アドレス範囲 3.1.0.0 は単に IPsec に渡すパケットのアドレス範囲とみなすことができます。

ルーター B の IPsec トンネルの作成: ルーター B 内に、ルーター A に構成したのと同じ IPsec トンネル (IPsec トンネル 1) を構成する必要があります。ルーター B 内のこのトンネルのローカル IP アドレスは 223.252.252.210 で、リモート IP アドレスは 223.252.252.216 です。その他のすべての IPsec トンネル・パラメーターは、ルーター A に構成されたパラメーターと一致していなければなりません。

ルーター B のパケット・フィルターの構成: ルーター A で行ったのと同様に、インターフェース 1 (IPsec トンネル 1 のエンドポイントであるルーター B 内のインターフェース) に、着信パケット・フィルター (*in-router-B*) と発信パケット・フィルター (*out-router-B*) を構成します。

ルーター B のパケット・フィルター・アクセス制御規則の構成: 最初に、ルーター B 上の着信パケット・フィルター *in-router-B* 用の着信アクセス制御規則を構成します。このアクセス制御規則は IPsec の 2 つのエンドポイントを識別し、ルーター B がトンネルからパケットを受信できるようにします。このパケット・フィルター *in-router-B* のタイプは、包含 (I) です。

```
IP Config> update packet-filter
Packet-filter name [ ] in-router-B
Packet-filter 'in-router-B' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 223.252.252.216
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 223.252.252.210
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
Enable logging? (Yes or [No]):
Packet-filter 'in-router-B' Config>
```

次に、2 番目のアクセス制御規則を *in-router-B* に追加することができます。

IPsec トンネルのセキュリティーに関するこの追加検査は IPsec 内で冗長ですが、この追加アクセス制御規則は NAT によって必要とされます。アクセス制御規則は、タイプ I、N、および S です。

```
Packet-filter 'in-router-B' Config> add access
Enter type [E]? INS
Internet source [0.0.0.0]? 1.1.0.0
Source mask [255.255.255.255]? 255.255.0.0
Internet destination [0.0.0.0]? 223.252.252.210
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable logging? (Yes or [No]):
Packet-filter 'in-router-B' Config>
```

どのアクセス制御規則にも一致しないすべてのパケットを、廃棄せずに通過させたい場合は、これらのパケットを通過させるために *in-router-B* 用の包括的ワイルドカード・アクセス制御規則を構成することができます。ただし、このアクセス制御規則は、着信パケット・フィルターに対する 2 番目の着信アクセス制御規則で廃棄するように設計されているパケットを通過させるので、2 番目の着信アクセス制御規則は無効になります。

次に、*out-router-B* に対するアクセス制御規則を構成して、サブネット 3.1.0.0 からの発信パケットを NAT に渡して変換し、次に IPsec に渡して処理し、IPsec トンネル 1 を通して伝送するようにします。アクセス制御規則は、タイプ I、N、および S です。

```
Packet-filter name [ ]? out-router-B
Packet-filter 'out-router-B' Config> add access
Enter type [E]? INS
Internet source [0.0.0.0]? 3.1.0.0
Source mask [255.255.255.255]? 255.255.0.0
Internet destination [0.0.0.0]? 1.1.0.0
Destination mask [255.255.255.255]? 255.255.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enter IPsec Tunnel ID [1]?
Enable logging? (Yes or [No]):
Packet-filter 'out-router-B' Config>
```

ここで、*out-router-B* に対して包括的アクセス制御規則を作成して、IPsec によって処理されたパケットを IPsec トンネル 1 を通して渡すようにします。

```
Packet-filter 'out-router-B' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 223.252.252.210
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]? 223.252.252.216
Destination mask [255.255.255.255]?
Enter starting protocol number ([0] for all protocols) [0]? 50
Enter ending protocol number [50]? 51
(Enable logging? (Yes or [No]):
Packet-filter 'out-router-B' Config>
```

out-router-B に対しては、2 つのアクセス制御規則のいずれにも一致しないパケット (たとえば、IPsec トンネル 1 向けでないトラフィック) を廃棄せずに通過させたい場合は、包括的ワイルドカード・アクセス制御規則を作成します。

ルーター B の NAT、IPsec、および IP のリセット: NAT および IPsec 機能を動作し、IP アクセス制御規則をアクティブにする前に、NAT、IPsec、および IP をリセットする必要があります。 NAT および IPsec をリセットするには、talk 5 **reset NAT** および **reset IPsec** コマンドを使用します。 NAT のリセットについては、935ページの『第72章 ネットワーク・アドレス変換の構成および監視』を参照してください。 IPsec のリセットについては、906ページの『ルーター A 上の IPsec と IP のリセット』を参照してください。 NAT と IPsec をリセットした後で、talk 5 **reset IP** コマンドを使用して、IP をリセットします。代わりに、各コンポーネントをリセットするために、ルーターをリスタートすることもできます。

第70章 IP セキュリティーの構成および監視

この章では、IP セキュリティーの構成および監視の方法、および IP セキュリティー監視コマンドの使用法について説明します。本章には、以下の節が含まれています。

- 『IP セキュリティー構成環境へのアクセス』
- 『IP セキュリティー構成コマンド』
- 919ページの『IP セキュリティー監視環境へのアクセス』
- 919ページの『IP セキュリティー監視コマンド』

注: TN3270、APPN-ISR、または APPN-HPR トラフィックを伝送するために IPsec トンネルを作成し、BRS を使用してそのトラフィックに優先順位を付ける計画の場合は、BRS の IPv4 優先順位ビット設定機能を使用することが必要です。詳細については、710ページの『IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィックのための IP バージョン 4 優先順位ビット処理の使用』を参照してください。

IP セキュリティー構成環境へのアクセス

IP セキュリティー構成環境にアクセスするには、`Config>` プロンプトで以下のコマンドを入力します。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>
```

IP セキュリティー構成コマンド

この節では、IP セキュリティー構成コマンドについて説明します。これらのコマンドは `IPsec config>` プロンプトで入力します。

表 120. IP セキュリティー構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add tunnel	保護トンネルを追加します。
Change tunnel	保護トンネル構成パラメーター値を変更します。
Delete tunnel	保護トンネルを削除します。
Disable	安全な方法でのすべての IP セキュリティー処理 (パケット・フィルターに一致するパケットを廃棄する) を使用不可にする、非安全な方法でのすべての IP 処理 (パケット・フィルターに一致するパケットを通過させる) を使用不可にする、または保護トンネルを使用不可にします。
Enable	すべての IP セキュリティー処理を使用可能にする、または保護トンネルを使用可能にします。
List	グローバル IP セキュリティー情報、または定義されたトンネルに関する情報をリストします。

表 120. IP セキュリティー構成コマンドの要約 (続き)

コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add Tunnel

add tunnel コマンドは、IPsec トンネルを定義するためのパラメーターを追加するのに使用します。

注: 以下のパラメーターを使用する場合は、AH、ESP、AH-ESP、および ESP-AH トンネル・ポリシーの値と同じでなければなりません。

- ローカル SPI
- ローカル認証アルゴリズム
- ローカル認証キー
- リモート SPI
- リモート認証アルゴリズム
- リモート認証キー

構文:

add tunnel...

tunnel-id

追加する保護トンネルの識別子を指定する必須の番号。各トンネル ID は、2210 内で固有でなければなりません。

有効値: 1 ～ 65536

デフォルト値: なし

tunnel-name

トンネルにラベルを付けるためのオプション・パラメーター。これは 2210 内で固有でなければなりません。

有効値: 最大 15 文字。最初の字は文字でなければなりません。ブランクは使用できません。

デフォルト値: なし

lifetime

トンネルがアクティブでいられる時間数 (分)。値 0 は、トンネルの存続時間は満了しないことを示します。

有効値: 0 ～ 525600 (0 = 満了しない、525600 = 365 日)

デフォルト値: 46080 (32 日)

encapsulation-mode

IP パケットをカプセル化する方法。トンネル・モードでは、IP パケット全体がカプセル化され、新規の IP ヘッダーが作成されます。トランスポート・モードでは、IP ヘッダーはカプセル化されません。保護トンネルの一端がルーターの場合は、インターネット技術作業部会 (IETF) セキュリティー体系草案に準拠して、トンネル・モードを使用することが***必須*** です。

有効値: トンネル (*TUNN*) またはトランスポート (*TRANS*)

デフォルト値: トンネル (*TUNN*)

tunnel-policy
トンネル・ポリシーを定義する 4 つの選択項目のうちの 1 つ。すなわち、IP 認証ヘッダー (AH)、IP カプセル化セキュリティー・ペイロード (ESP)、またはこれらのプロトコルの組み合わせ (AH-ESP および ESP-AH)。 AH-ESP では、発信パケットで ESP 暗号化が最初に実行されます。ESP-AH では、発信パケットで AH 認証が最初に実行されます。一部のパラメーターは、ESP または AH のどちらかに固有です。暗号化パラメーターは、ESP、AH-ESP、または ESP-AH を選択した場合にのみ構成します。認証パラメーターは、AH、AH-ESP、または認証付き ESP を選択した場合にのみ構成します。

有効値: AH、ESP、AH-ESP、ESP-AH

デフォルト値: AH-ESP

local-IP-address
トンネルのこちら側 の IP アドレス

有効値: インターフェースに対して構成された、または 2210 の内部アドレスとして構成された、有効な IP アドレス

デフォルト値: 1.1.1.1

local-spi
セキュリティー・アソシエーションは、AH または ESP を使用してコネクションのトラフィックを保護する単方向セキュリティー・コネクションです。セキュリティー・パラメーター・インデックス (SPI) は、この保護トンネルに対応する 2 つのセキュリティー・アソシエーション (着信または発信) の 1 つを固有に識別する任意の 32 ビット値です。このパラメーターは必須であり、トンネルのローカル側で受信される着信パケットに対してこのトンネルで期待される SPI を識別します。この値は、同じローカル IP アドレスをもつ別のトンネルのローカル SPI と一致していてはなりません。トンネル・ポリシー (ESP、AH、AH-ESP、または ESP-AH) に関係なく、1 つの保護トンネルの着信トラフィックに対して 1 つだけローカル SPI を構成します。

有効値: 256 ～ 65535

デフォルト値: 256

local-encryption-algorithm
ローカル・ルーターから送信される発信パケットの ESP に使用される暗号化アルゴリズム。ESP を構成する場合は必須です。このアルゴリズムは、トンネルの反対側のワークステーションで使用される暗号化と一致していなければなりません。一部の国では、米国の輸出規制のため、このアルゴリズムの一部または全部を使用できない場合があります。

有効値: DES-CBC、CDMF、または 3DES

デフォルト値: DES-CBC

local-encryption-key
ローカル ESP 暗号化アルゴリズムで使用される 1 つまたは複数のキー。これらは、保護トンネルの反対側に構成された等価キーと一致していなければなりません。

有効値:

- DES-CBC の場合: 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- CDMF の場合: 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- 3DES の場合: どれも同じでない 3 つの別々のキー、それぞれ 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)

デフォルト値: なし

padding-for-local-encryption

発信 ESP パケットに追加される追加埋め込みのサイズ (バイト)。追加埋め込みは、暗号化アルゴリズムの結果、暗号化されたパケットが元のパケットと同じサイズになる場合、暗号化される IP パケットのサイズを偽装するために使用できます。 ESP 埋め込み値は 8 の倍数でなければなりません。

有効値: 0 ～ 120

デフォルト値: 0

local-ESP-authentication

ローカル ESP 認証を選択します (必要な場合)。

有効値: Yes または No

デフォルト値: Yes

local-authentication-algorithm

発信パケットで使用される認証アルゴリズム。これは ESP 用のオプション・パラメーターで、ESP 認証を選択しない限り必要ではありません。AH、AH-ESP、または ESP-AH の場合、このパラメーターは必須です。使用される認証アルゴリズムは、IPsec トンネルの反対側で使用されるリモート認証アルゴリズムと一致していなければなりません。

有効値: HMAC-MD5 または HMAC-SHA

デフォルト値: HMAC-MD5

local-authentication-key

ローカル認証アルゴリズムで使用されるキー。これは、IPsec トンネルの反対側に構成される等価キーと一致していなければなりません。ポリシーが AH、AH-ESP、または ESP-AH の場合、またはポリシーが ESP で、ローカル ESP 認証アルゴリズムが構成されている場合には、このパラメーターは必須です。

有効値:

- HMAC-MD5 の場合: 32 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- HMAC-SHA の場合: 40 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)

デフォルト値: なし

remote-IP-address

トンネルのリモート側の IP アドレス。これは必須パラメーターです。

有効値: 有効な IP アドレス

デフォルト値: 1.1.1.3

remote-spi

セキュリティー・アソシエーションは、AH または ESP を使用してコネクシ

ョンのトラフィックを保護する単方向セキュリティー・コネクションです。セキュリティー・パラメーター・インデックス (SPI) は、この保護トンネルに対応する 2 つのセキュリティー・アソシエーション (着信または発信) の 1 つを固有に識別する任意の 32 ビット値です。このパラメーターは必須であり、リモート・ホストあての発信パケットの ESP または AH に期待される SPI を識別します。この値は、同じリモート IP アドレスをもつ別のトンネルのリモート SPI と一致していてはなりません。トンネル・ポリシー (ESP、AH、AH-ESP、または ESP-AH) に関係なく、1 つの IPsec トンネルの発信トラフィックに対して 1 つだけローカル SPI を構成します。

有効値: 1 ～ 65535

デフォルト値: 256

remote-encryption-algorithm
リモート・ホストから受信する着信パケットで使用される暗号化解除アルゴリズム。

有効値: DES-CBC、CDMF、または 3DES

デフォルト値: ローカル暗号化アルゴリズムの値

remote-encryption-key
リモート ESP 暗号化アルゴリズムで使用される 1 つまたは複数のキー。これらは、保護トンネルの反対側に構成された等価キーと一致していなければなりません。

有効値:

- DES-CBC の場合: 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- CDMF の場合: 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- 3DES の場合: どれも一致しない 3 つの別々のキー、それぞれ 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)

デフォルト値: なし

verification-of-remote-encryption-padding
受信パケットの暗号化埋め込みのサイズを検査するかどうかを決めます。

有効値: Yes または No

デフォルト値: No

padding-for-remote-encryption
受信 ESP パケットに期待される追加埋め込みのサイズ (バイト)。このパラメーターは必須であり、*verification-of-remote-encryption-padding* の値が Yes の場合にのみ有効です。 ESP 埋め込み値は 8 の倍数でなければなりません。8 で割り切れない値が構成されている場合、その値は 8 で割り切れる次の値に切り上げられます。

有効値: 0 ～ 120

デフォルト値: 0

remote-ESP-authentication
着信パケットのリモート ESP 認証を選択します (必要な場合)。

有効値: Yes または No

デフォルト値: Yes

remote-authentication-algorithm

着信パケットに使用される認証アルゴリズム。これは ESP 用のオプション・パラメーターで、ESP 認証を選択しない限り必要ではありません。 AH または AH と ESP の組み合わせ (AH-ESP または ESP-AH) の場合、このパラメーターは必須です。使用される認証アルゴリズムは、IPsec トンネルの反対側で使用されるローカル認証アルゴリズムと一致していなければなりません。

有効値: HMAC-MD5 または HMAC-SHA

デフォルト値: HMAC-MD5

remote-authentication-key

リモート認証アルゴリズムで使用されるキー。これは、保護トンネルの反対側に構成された等価キーと一致していなければなりません。これは、AH、AH-ESP、ESP-AH、および ESP 認証アルゴリズムが構成されている場合は ESP で必須です。

有効値:

- HMAC-MD5 の場合: 32 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- HMAC-SHA の場合: 40 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)

デフォルト値: なし

enable-replay-prevention

再生防止が使用可能かどうかを指定します。再生防止が使用可能の場合、IP セキュリティー・ヘッダー内のシーケンス番号を監視して、トンネルの受信側によって重複パケットが処理されるのを防止します。再生防止の使用は推奨できません。送信側のシーケンス番号カウンターが限界に達すると、トンネル・セキュリティー・アソシエーションを停止しなければならないからです。これが起こると、既存のセキュリティー・アソシエーションをリスタートするか、新規のものを作成するために、手動による介入が必要になります。

さらに、再生防止が使用可能のときに、**reset ipsec** コマンドを使用して IPsec をリセットした場合は、必ず IPsec トンネルの反対側のルーター上の IPsec もリセットする必要があります。これは、トンネルの両側でシーケンス番号を再初期化するために必要です。トンネルの一端で IPsec がリセットされ、他端はリセットされていない場合、トンネルの各端のルーターは、シーケンス番号不一致によりパケットを廃棄する可能性があります。

有効値: Yes または No

デフォルト値: No

enable-tunnel

このトンネルが使用可能かどうかを指定します。パケット・フィルターを構成して、この IPsec トンネルで使用するインターフェースを定義し、IP をリセットするか 2210 をリスタートするまでは、使用可能にされたトンネルはパケットをフィルターに掛けません。 IP をリセットするには、**reset ip** コマンドを使用します。

有効値: Yes または No

デフォルト値: Yes

Change Tunnel

change tunnel コマンドは、**add tunnel** コマンドを使用して以前に構成した IPsec トンネル・パラメーターを変更するのに使用します。

構文:

change tunnel... 変更できるパラメーターのリストは、**add tunnel** コマンドの項を参照してください。

Delete Tunnel

delete tunnel コマンドは、IPsec トンネルを削除するのに使用します。

構文:

delete tunnel *tunnel-id tunnel-name* **all**

tunnel-id

削除する IPsec トンネルの識別子を指定します。

有効値: 1 ～ 65536

デフォルト値: 1

tunnel-name

削除する IPsec トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all このインターフェース上のすべての IPsec トンネルを削除することを指定します。

Disable

disable コマンドは、IPsec トンネルを使用不可にするか、あるいはすべての IPsec トンネルを安全な方法 (IPsec フィルターに一致するパケットを廃棄する) または非安全な方法 (IPsec フィルターに一致するパケットを通過させる) で使用不可にするのに使用します。

構文:

disable ipsec drop

ipsec pass

tunnel ...

ipsec drop

ルーター上の IP セキュリティーを安全な方法で使用不可にします。すべての IPsec トンネルが使用不可にされますが、パケット・フィルター規則の保護トンネル情報を使用して、IPsec トンネル・パケット・フィルターに一致するパケットを識別します。一致するパケットは廃棄されます。

ipsec pass
ルーター上の IP セキュリティーを非安全な方法で使用不可にします。すべての IPsec トンネルが使用不可にされます。 IPsec トンネル・パケット・フィルターに一致するパケットは、通常のトラフィックとして転送されます。

tunnel *tunnel-id* **all**
指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用不可にします。

tunnel-id
使用不可にする保護トンネルの識別子を指定します。

有効値: 1 ～ 65536

デフォルト値: 1

all すべてのトンネル

Enable

enable コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを使用可能にするのに使用します。ルーター上の IPsec をグローバルに使用可能にしないと、個々の使用可能にされた IPsec トンネルはアクティブになりません。

構文:

enable ipsec
tunnel ...

ipsec ルーター全体の IP セキュリティーを使用可能にします。

tunnel *tunnel-id* **all**
指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用可能にします。

tunnel-id
使用可能にする保護トンネルの識別子を指定します。

有効値: 1 ～ 65536

デフォルト値: 1

all すべてのトンネル

List

list tunnel コマンドは、現行の IP セキュリティー構成を表示するのに使用します。グローバル・トンネル (global tunnels) には、ルーター上のすべてのトンネル (アクティブと定義済みの両方) が含まれます。すべてのトンネル (all tunnels) には、このインターフェースに構成されたすべてのトンネル (アクティブと定義済みの両方) が含まれます。アクティブ・トンネル (active tunnels) は、現在アクティブのトンネルです。定義済みトンネル (defined tunnels) は、定義されているがアクティブではないトンネルです。

構文:

list ... all
global
tunnel
active *tunnel-id tunnel-name* all
defined *tunnel-id tunnel-name* all

例:

```
IPsec
config>list all

IPsec is ENABLED

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      1  test                    1.1.1.1          2.1.1.1  TUNN   Enabled
      2  test2                   1.1.1.1          1.1.1.3  TRANS  Enabled

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  ------------------
    2          1.1.1.1          1.1.1.3  TRANS  ESP     ******************
    1          1.1.1.1          2.1.1.1  TUNN   AH      ******************
```

IP セキュリティー監視環境へのアクセス

IP セキュリティー監視環境にアクセスするには、OPCON prompt (*) プロンプトで **t 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで、次のようなコマンドを入力します。

```
+ feature ipsec
IPsec>
```

IP セキュリティー監視コマンド

この節では、IP セキュリティー監視コマンドについて説明します。これらのコマンドは IPsec> プロンプトで入力します。

表 121. IP セキュリティー監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Add tunnel	保護トンネルを動的に追加します。
Change tunnel	保護トンネル構成パラメーター値を動的に変更します。
Delete tunnel	保護トンネルを動的に削除します。

表 121. IP セキュリティー監視コマンドの要約 (続き)

コマンド	機能
Disable	安全な方法でのすべての IP セキュリティー処理 (パケット・フィルターに一致するパケットを廃棄する) を動的に使用不可にする、非安全な方法でのすべての IP セキュリティー処理 (パケット・フィルターに一致するパケットを通過させる) を動的に使用不可にする、または特定の保護トンネルを動的に使用不可にします。
Enable	すべての IP セキュリティー処理を動的に使用可能にする、または保護トンネルを動的に使用可能にします。
List	グローバル IP セキュリティーに関する情報、またはアクティブおよび定義済みのトンネルに関する情報をリストします。
Reset	IP セキュリティーをリセットするか、または保護トンネルをリセットします。このコマンドは、Talk 6 で作成された構成を再ロードします。リセットすると、Talk 5 を使用して構成されたパラメーター値は、Talk 6 を使用して構成されたパラメーター値でオーバーライドされます。
Restart	IP セキュリティーをリスタートするか、保護トンネルをリスタートします。このコマンドは、Talk 5 コマンドを使用して動的に構成された構成情報を再ロードします。
Stats	すべてのトンネルまたはアクティブ・トンネルの統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Add Tunnel

保護トンネルを動的に追加します。

構文:

add tunnel ...

パラメーターの説明は、911ページの『IP セキュリティー構成コマンド』の **add tunnel** コマンドの項を参照してください。

Change Tunnel

保護トンネルを動的に変更します。

構文:

change tunnel ...

パラメーターの説明は、911ページの『IP セキュリティー構成コマンド』の **add tunnel** コマンドの項を参照してください。

Delete Tunnel

delete は、1 つの保護トンネルまたはすべての保護トンネルを動的に削除するのに使用します。

構文:

delete tunnel *tunnel-id tunnel-name* **all**

tunnel-id
削除する IPsec トンネルの識別子を指定します。

有効値: 1 ～ 65536

デフォルト値: 1

tunnel-name
削除する IPsec トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all このインターフェース上のすべての IPsec トンネルを削除することを指定します。

Disable

disable コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを使用不可にするのに使用します。

構文:

disable ipsec drop
ipsec pass
tunnel ...

ipsec drop
ルーター上の IP セキュリティーを安全な方法で使用不可にします。すべての IPsec トンネルが使用不可にされますが、パケット・フィルター規則の保護トンネル情報を使用して、IPsec トンネル・パケット・フィルターに一致するパケットを識別します。一致するパケットは廃棄されます。

ipsec pass
ルーター上の IP セキュリティーを非安全な方法で使用不可にします。すべての IPsec トンネルが使用不可にされます。 IPsec トンネル・パケット・フィルターに一致するパケットは、通常のトラフィックとして転送されます。

tunnel *tunnel-id* **all**
指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用不可にします。

tunnel-id
使用不可にする保護トンネルの識別子を指定します。

有効値: 1 ～ 65536

デフォルト値: 1

all すべてのトンネル

Enable

enable コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを動的に使用可能にするのに使用します。ルーター上の IPsec をグローバルに使用可能にしないと、個々の使用可能にされた IPsec トンネルはアクティブになりません。

注: IPsec を使用不可に設定してルーターをリスタートした場合は、IPsec を動的に使用可能にすることはできません。

構文:

enable ipsec
tunnel ...

ipsec ルーター全体の IP セキュリティーを使用可能にします。

tunnel *tunnel-id* **all**

tunnel-id
使用可能にする保護トンネルの識別子を指定します。

有効値: 1 ～ 65536

デフォルト値: 1

all すべてのトンネル

List

list コマンドは、現行の IP セキュリティー構成を表示するのに使用します。グローバル・トンネル (global tunnels) には、ルーター上のすべてのトンネル (アクティブと定義済みの両方) が含まれます。すべてのトンネル (all tunnels) には、このインターフェースに構成されたすべてのトンネル (アクティブと定義済みの両方) が含まれます。アクティブ・トンネル (active tunnels) は、現在アクティブのトンネルです。定義済みトンネル (defined tunnels) は、定義されているがアクティブではないトンネルです。

構文:

list ... all
global
tunnel
active *tunnel-id tunnel-name* all
defined *tunnel-id tunnel-name* all

例:

```
IPsec>li tunnel ?
ACTIVE
DEFINED
IPsec>li tunnel active
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all

Tunnel Cache:
```

```
 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  --------------  --------------  -----  ------  ------------------
    2         1.1.1.1         1.1.1.3  TRANS  ESP     ******************
    1         1.1.1.1         2.1.1.1  TUNN   AH      ******************
```

Reset

reset コマンドは、ルーター上または 1 つのトンネル上の IP セキュリティーを動的にリセットするのに使用します。 IPsec またはトンネルをリセットした後で、必ず **reset IP** コマンドを使用して、IP 構成をリセットしてください。これは、パケット・フィルターやそのアクセス制御規則などのアクセス制御情報を再ロードするために必要です。 IP をリセットしないと、パケット・フィルターおよびアクセス制御規則が、新規の IPsec 構成をサポートしない可能性があります。

reset コマンドを使用する代わりに、ルーターをリブートすることもできます。ただし、ルーターをリブートするとネットワークがしばらく切断されますが、**reset** コマンドは IP 機能だけを中断します。

構文:

reset ipsec

tunnel *tunnel-id tunnel-name* all

ipsec 2210 上の IP セキュリティーをリセットします。 IP セキュリティーは一時的に使用不可になった後、リスタートします。 IP セキュリティーが使用不可の間、通常は IPsec トンネルによって処理されるパケットは、リセットが完了するまで廃棄されます。 IP セキュリティーをリセットしても、2210 上の他の機能には影響を与えません。このコマンドは、Talk 6 を使用して作成された IP セキュリティー構成を起動します。Talk 6 IP セキュリティー構成は Talk 5 構成を上書きします。

tunnel 指定されたトンネルの IP セキュリティーをリセットします。リセット時にトンネルが使用不可にされている場合、トンネル構成は SRAM 構成から再作成されますが、リセット後もトンネルは使用不可のままです。

tunnel-id
リセットする保護トンネルの識別子を指定します。

有効値: 1 〜 65536

デフォルト値: 1

tunnel-name
リセットする保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all すべてのトンネル

Restart

restart コマンドは、ルーター上または 1 つのトンネル上の IP セキュリティーを動的にリスタートするのに使用します。これは Talk 5 を使用して作成された一時構成をリスタートします。Talk 6 IP セキュリティー構成は Talk 5 構成を上書きしません。

構文:

restart ipsec

tunnel *tunnel-id tunnel-name* all

ipsec 2210 上の IP セキュリティーをリスタートします。

tunnel 指定されたトンネルの IP セキュリティーをリスタートします。

tunnel-id
リセットする保護トンネルの識別子を指定します。

有効値: 1 ～ 65536

デフォルト値: 1

tunnel-name
リセットする保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all すべてのトンネル

Stats

stats コマンドは、特定のトンネルまたはすべてのトンネルに関する統計を表示するのに使用します。たとえば、**stats** コマンドは、送受信されたパケットを表示します。

構文:

stats *tunnel-id tunnel-name* **all**

tunnel-id
保護トンネルの識別子を指定します。

有効値: 1 ～ 65536

デフォルト値: 1

tunnel-name
構成された保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all 2210 上に構成されたすべてのトンネルの統計を表示します。

例:

```
IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all
```

```
                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           0            0             0             0            0            0

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           0            0             0             0            0            0

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0
```

第71章 ネットワーク・アドレス変換の使用

ネットワーク・アドレス変換 (NAT) とその拡張機能であるネットワーク・アドレスおよびポート変換 (NAPT) は、組織の利用可能な IP アドレスの数を拡張することができ、また公衆網のユーザーに私設ネットワークの一部のアドレスを知られるのを防止することができます。 NAT では、公衆 IP アドレスを使用して私設 IP アドレスを表します。

公衆 IP アドレスとは、IP 公衆網のホストの有効なアドレスであり、公衆網内で固有であることが必要です。公衆網がインターネットの場合、公衆 IP アドレスは、ネットワーク情報センター (NIC) によって提供される固有のインターネット・アドレスでなければなりません。

私設アドレスはルーターには分かりますが、公衆網には分かりません。各私設ネットワーク内ではアドレスは固有であることが必要ですが、2 つの異なる私設ネットワークに同じアドレスが重複して存在しても構いません。私設アドレスは、スタブ・ネットワーク内のホストに割り当てられます。スタブ・ネットワークというのは、1 つのルーターのみを通して公衆網にアクセスできるネットワークのことです。

NAT は、いくつかの方法で、利用可能な IP アドレスを拡張します。

- 公衆アドレスを回転して使用することにより、1 つの公衆アドレスで複数の私設アドレスを表すことができる。
- アドレスの重複が可能である (重複アドレスがそれぞれ異なる私設ネットワークで使用されている場合に限られる)。
- ネットワーク管理者が、資源が限られてきている NIC アドレスの代わりに、任意の IP アドレスを私設ネットワークで使用することができる。

私設アドレスを使用すれば、アドレスを外界から隠すこともできます。 NAT のこの機能は、私設アドレスが知られるのを防止するための 1 種のファイアウォールとして役立ちます。

重要: NAT を定義しているインターネット草案のセクション 5.4 に、“アプリケーション内の IP アドレス (および、NAPT の場合は、TCP/UDP ポート) を持つ (および、使用する) アプリケーションは、NAT を通すと機能しない...” と記述されています。 DLSw および XTP は、エンドポイント IP アドレスに基づいて (特に、どの相手がより高いアドレスを持っているかに基づいて) 決定することに注意する必要があります。 NAT を通して実行されているアプリケーション (DLSw や XTP など) は、そのアドレスは私設アドレスであると考えているのに対して、他のルーター内の相手のアプリケーションは、そのアプリケーションのアドレスは公衆アドレスであると考えるので、間違った決定がなされる可能性があります。

928ページの図50 に示されている、スタブ・ネットワーク内のワークステーションの図を見てください。この例では、スタブ・ネットワークは IP アドレスが 10.33.96.0、サブネット・マスクが 255.255.255.0 の IP サブネットから構成されています。

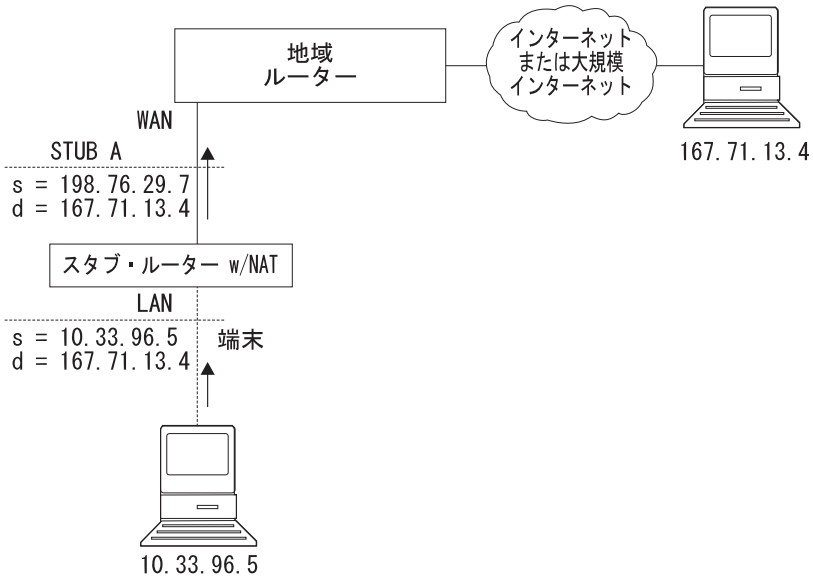


図 50. NAT を実行するネットワーク

NAT を使用するには、ネットワーク管理者は 1 つまたは複数の公衆 IP アドレスを 2210 内の公衆アドレス・プールに割り当て、私設 IP アドレスをスタブ・ネットワーク内の各ワークステーションに割り当てます。公衆 IP アドレスは *reserve pool* に割り当てられ、私設 IP アドレスは *translate range* に割り当てられます。

NAT 機能は、最初に私設ネットワーク内のステーションの私設アドレスを公衆アドレスの 1 つに結合します。結合とは、その私設アドレスをもつパケットはすべて、パケットが発信されるときに、その公衆 IP アドレスに変換されることを意味しています。着信パケットは、宛先として公衆 IP アドレスを持っています。 NAT は公衆アドレスを認知し、それを私設 IP アドレスに変換して、パケットを転送します。トラフィックが停止した後、ユーザーが設定できるタイマーがタイムアウトになるまで、結合は維持されます。タイムアウトになった時点で、NAT は結合を終了し、その公衆アドレスを再利用できるようにします。

この例では、パケットは、送信元私設アドレス 10.33.96.5 からインターネット内の宛先アドレス 167.71.13.4 に転送されます。 2210 内の NAT は、私設アドレス 10.33.96.5 を公衆アドレス 198.76.29.7 に変換します。この変換によって、私設アドレス 10.33.96.5 は公衆網から隠されるので、私設アドレス 10.33.96.5 を直接アドレス指定する着信パケットはありません。代わりに、167.71.13.4 からの着信パケットは公衆アドレス 198.76.29.7 あてに送られます。 NAT ルーターは 198.76.29.7 をアドレス指定したパケットを受信すると、その宛先公衆アドレスを私設アドレス 10.33.96.5 に変換し、パケットを転送します。

ネットワーク・アドレス・ポート変換

NAPT は、TCP および UDP トラフィックにのみ使用できます。 NAPT では、複数の私設アドレスが 1 つの公衆アドレスを同時に使用することができます。 NAT は、1 つの公衆アドレスを 1 つの私設アドレスにマップするのに対して、NAPT は、NAPT 公衆アドレス***および*** 公衆ポート番号を、私設アドレスおよび私設ポート番号にマップします。各公衆アドレス・プールごとに 1 つの NAPT アドレスしか構成できません。

NAPT の構成は、NAPT トラフィックに使用する 1 つの公衆アドレスを構成するだけです。 NAPT の利点は、公衆 IP アドレス・プールからの 1 つのアドレスが複数の私設 IP アドレスを同時にサポートできることです。

静的アドレス・マッピング

ときには、公衆網から直接アクセスできるステーションまたはサーバーを私設ネットワーク内に構成したい場合があります。その場合には、ステーションの私設アドレスを特定の公衆アドレスに静的にマッピングする必要があります。私設アドレスから発信されるすべてのメッセージは、宛先の公衆アドレスに変換され、公衆アドレスあての着信メッセージはすべて、対応する私設アドレスに自動的に転送されます。静的アドレス・マッピングには、NAT と NAPT の 2 種類があります。

NAT 静的アドレス・マッピング

NAT マッピングでは、すべての IP プロトコルがホストにアクセスできます。以下に示すのは、NAT マッピングの構成例です。

私設アドレス	10.1.1.2
私設ポート	0
公衆 NAT アドレス	9.67.1.1
公衆ポート	0

NAPT 静的アドレス・マッピング

TCP または UDP アプリケーションを指定する場合、割り当て済みの私設ポートを含む NAPT マッピングを指定するオプションがあります。 NAPT 静的アドレス・マッピングでは、NAPT 公衆アドレスを構成する必要があります。たとえば、私設アドレス 10.1.1.1 の Telnet ホストが NAPT 公衆アドレス 9.67.1.2 を使用するように構成する場合、静的マッピングは以下のように構成します。

私設アドレス	10.1.1.1
私設ポート	23
公衆 NAPT アドレス	9.67.1.2
公衆ポート	23

私設ポートと公衆ポートは、Telnet 用に割り当て済みのポートであるポート 23 にマップされます。この管理者は、同じ私設アドレス 10.1.1.1 に FTP サーバー (割り当て済みアドレス 21) も持っており、これを NAPT 公衆アドレス 9.67.1.2 にマップする場合、このマッピングは以下のようになります。

私設アドレス	10.1.1.1
私設ポート	21
公衆 NAPT アドレス	9.67.1.2
公衆ポート	21

アドレス 10.1.1.1 のサーバーは、両方のアプリケーションに同じ NAPT 公衆アドレス (9.67.1.2) を使用していますが、NAPT は異なるポート番号 (23 と 21) を使用することによって、この 2 つを区別することができます。しかし NAPT は、2 つのサーバーが同じ NAPT 公衆アドレスを使用し、同じアプリケーションおよびポート番号を持っている場合は、それらを区別することはできません。たとえば、NAPT 公衆アドレスと割り当て済みポート番号が、10.1.1.3 ポート 21 と 10.1.1.1 ポート 21 とで同じである場合、NAPT は着信 FTP トラフィックをサーバー 10.1.1.3 と 10.1.1.1 のどちらに送るのか判断できません。同じ NAPT アドレスとアプリケーションを使用するサーバーを 2 つ以上構成する場合は、サーバーの割り当て済みポート以外のポートを使用する必要があります (たとえば、FTP デーモンをポート 200 で開始するなど)。

NAT 用のパケット・フィルターおよびアクセス制御規則の設定

管理者は、NAT または NAPT によって変換される私設アドレスの範囲を識別するのに加えて、2210 内の IP 用のパケット・フィルターとアクセス制御規則も設定する必要があります。 NAT 構成では、公衆網に接続されているインターフェースに、1 つの着信パケット・フィルターと 1 つの発信パケット・フィルターを構成することが必要です。また、着信パケット・フィルターに対して 1 つまたは複数のアクセス制御規則を構成し、発信パケット・フィルターに対しても 1 つまたは複数のアクセス制御規則を構成する必要があります。着信フィルター・アクセス制御規則は、該当する定義済み公衆アドレスをもつ着信パケットを NAT に渡します。発信フィルター・アクセス制御規則は、該当する定義済み私設アドレスをもつ発信パケットを NAT に渡します。

NAT に適用されるアクセス制御規則は、アクセス制御規則タイプ ***I*** (包括的) および ***N*** (NAT) を持っています。 IP アクセス制御の構成については、*プロトコルの構成と監視 解説書、第 1 巻* を参照してください。

注: NAT は、IPsec トンネルと合わせて構成することもできます。この構成の例は、905ページの『ルーター A のパケット・フィルター・アクセス制御規則の構成』にあります。

例: IP フィルターとアクセス制御規則をもつ NAT の構成

この例は、931ページの図51 に示したネットワーク内のスタブ・ルーターの NAT を構成する方法を示しています。コマンドの説明は、935ページの『第72章 ネットワーク・アドレス変換の構成および監視』を参照してください。

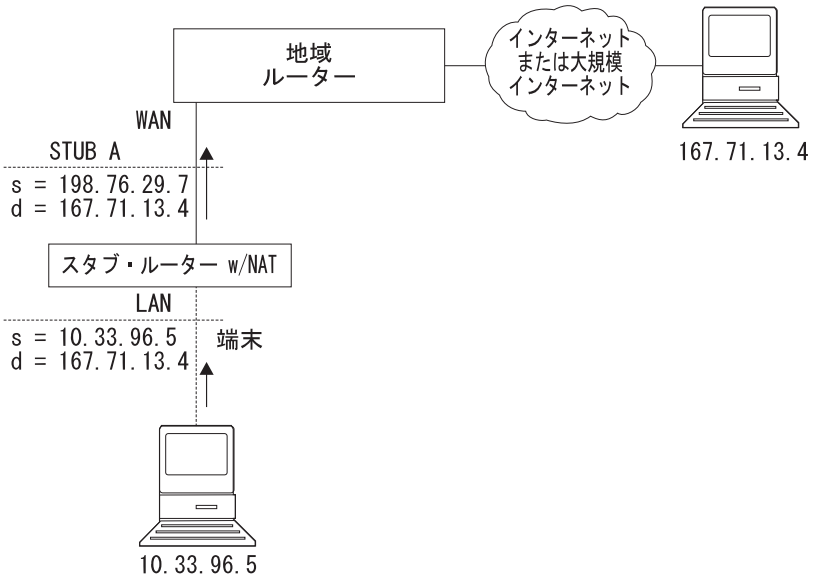


図 51. NAT を実行するネットワーク

以下の手順で行います。

1. NAT および NAPT によって使用される公衆アドレスのプールを設定します。これには **reserve** コマンドを使用します。

```
NAT config> reserve 198.76.29.7 255.255.255.0 6 pool1 198.76.29.7
NAT config> reserve 198.76.29.15 255.255.255.0 3 pool1 0.0.0.0
```

   この例では、*pool1* と呼ばれるプールが設定されました。プール内の NAPT アドレスは 198.76.29.7 です。アドレス 198.76.29.13 および 198.76.29.14 は利用不能なので、プールはそれら除外するするように設定されています。入力するパラメーターは *public-address*、*mask*、*number-in-group*、*name*、および *napt-address* です。 NAPT アドレスの値 0.0.0.0 は、このグループ内のアドレスはどれも NAPT アドレスではないことを意味しています。プールに NAPT を構成しない場合は、すべてのグループに NAPT アドレス 0.0.0.0 を使用します。

2. **translate** コマンドを使用して、pool1 内の公衆アドレスに変換される私設アドレスの範囲を設定します。入力するパラメーターは、*private-address*、*mask*、および *name* です。

```
NAT config> translate 10.33.96.0 255.255.255.0 pool1
```

3. 公衆アドレスの 1 つに固定的にマップする、私設ネットワーク内部のステーションの静的マッピングを設定します。以下のコマンドは、公衆網から任意のタイプのトラフィックを受信するマシン (10.33.96.5) を識別します。 2 番目のマシン (10.33.96.4) は、Telnet サーバーと HTTP サーバーの両方です。パラメーターは、*private-address*、*private-port-number*、*public-address*、および *public-port-number* です。 pool1 の NAPT アドレスは、2 つのポート番号を持つように構成されているホストの公衆アドレスとして使用されていることに注意してください。

```
NAT config> map 10.33.96.5 0 198.76.29.8 0
NAT config> map 10.33.96.4 23 198.76.29.7 23
NAT config> map 10.33.96.4 80 198.76.29.7 80
```

4. NAT を使用可能にします。

```
NAT config> enable NAT
```

5. 2 つの IP パケット・フィルターを作成して、IP がパケットを NAT に渡すようにします。これらは、インターフェース 0 (公衆網に接続されているインターフェース) の着信パケット・フィルターと発信パケット・フィルターです。

```
IP Config> add packet-filter outbound out-0 0
IP Config> add packet-filter inbound in-0 0
```

6. **update** コマンドを使用して、packet-filter '*filter-name*' Config> プロンプトを表示します。 NAT 用のアクセス制御規則を着信フィルターに追加します。公衆インターフェース (ネット 0) を介して受信した NAT の予約済み公衆アドレス・プールあてのパケットを、NAT に渡す必要があります。 NAT は公衆アドレス (および、パケットが NAPT アドレスあての場合は、公衆ポート) を正しい私設アドレス (および、パケットが NAPT アドレスあての場合は、私設ポート) で置き換えます。インターネット送信元の 0.0.0.0 のアドレスとマスクは、公衆網からのすべての送信元アドレスを NAT に渡すことを示しています。

```
IP Config> update packet-filter
Packet-filter name [ ]? in-0
Packet-filter 'in-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]?
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 198.76.29.0
Destination mask [255.255.255.255]?255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

   アクセス制御規則の範囲は、pool1 に定義されたアドレスの範囲より大きくなっています。 NAT に渡されたパケットのアドレスが、アクセス制御規則に定義された範囲内であるが、公衆アドレス・プール内のアドレスの 1 つではない場合、NAT はそのパケットを変更せずに IP に戻します。

7. ルーターが、アクセス制御規則に一致しないパケットを廃棄せずに渡すようにしたい場合は、ワイルドカード・アクセス制御規則を作成することができます。次の例は、このようなアクセス制御規則を示しています。

```
Packet-filter 'in-0' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 0.0.0.0
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 0.0.0.0
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

8. NAT 用のアクセス制御規則を発信フィルターに追加します。ネット 0 インターフェースから転送された、私設ネットワーク上の送信元アドレスを持っているパケットを識別し、IP がそれらを NAT に渡せるようにします。 NAT は私設アドレスを pool1 内の公衆アドレスの 1 つで置き換えます。

```
Packet-filter 'out-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]? 10.33.96.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]?
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'out-0' Config>
```

   アクセス制御規則に一致しないパケットを転送する計画の場合は、フィルター *in-0* の場合と同様に、このパケット・フィルターを使用して、ワイルドカード包括的アクセス制御規則を最後のアクセス制御規則として追加することができます。

9. IP Config> プロンプトから **list packet-filter** *filter-name* コマンドを使用して、各パケット・フィルターのアクセス制御規則の正確性とシーケンスを検査することができます。
10. IP 用のアクセス制御を使用可能にします。

    ```
    IP Config> set access-control on
    ```

11. talk 5 を使用して、IP および NAT をリセットします。ここまでは、ルーター構成の変更を作成してきましたが、これらの変更はルーターには影響を与えていません。 IP および NAT の reset コマンドにより、ルーターは新規構成を読み取り、構成に定義された規則を使用して稼働するようになります。

    ```
    NAT> reset NAT
    IP> reset IP
    ```

第72章 ネットワーク・アドレス変換の構成および監視

この章では、ネットワーク・アドレス変換 (NAT) 構成コマンドおよび監視コマンドについて説明し、以下の節が含まれています。

- 『ネットワーク・アドレス変換の構成環境へのアクセス』
- 『ネットワーク・アドレス変換構成コマンド』
- 942ページの『ネットワーク・アドレス変換監視環境へのアクセス』
- 942ページの『ネットワーク・アドレス変換監視コマンド』

ネットワーク・アドレス変換の構成環境へのアクセス

NAT 構成環境にアクセスするには、Config> プロンプトで、次のようなコマンドを入力します。

```
Config> feature nat
Network Address Protocol user configuration
NAT config>
```

ネットワーク・アドレス変換構成コマンド

この節では、ネットワーク・アドレス変換 (NAT) 構成コマンドについて説明します。NAT を構成するには、これらのコマンドを NAT config> プロンプトで入力します。

表 122. NAT 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
Change	公衆 IP アドレス予約プール、私設アドレス変換範囲、および静的マッピングを変更します。
Delete	公衆 IP アドレス予約プール、私設アドレス変換範囲、および静的マッピングを削除します。
Disable	NAT を使用不可にします。
Enable	NAT を使用可能にします。
List	NAT 構成に関する情報をリストします。
Map	ステーションまたはサーバーの静的 NAT または NAPT 結合を作成します。
Reserve	公衆 IP アドレス・プールを作成し、そのプールにアドレスを追加します。
Reset	ルーターが NAT 構成を読み込み、構成された NAT 規則に従って稼働するようにします。
Set	タイムアウトを設定します。
Translate	NAT 公衆アドレス・プールによって変換される私設 IP アドレスを識別します。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

Change

change コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、および静的マッピングを変更するのに使用します。

構文:

change reserve
translate
mappings

reserve *pools*
公衆 IP アドレス予約プールの特性 (IP アドレスおよびマスクなど) を変更することができるプロンプトを表示します。

有効値: 構成されたプールを識別するインデックス番号。この番号は、**list reserve pools** コマンドを入力すると表示されます。

デフォルト値: なし

translate *ranges*
私設 IP アドレス変換範囲の特性 (IP アドレスおよびマスクなど) を変更することができるプロンプトを表示します。

有効値: 構成された変換範囲を識別するインデックス番号。この番号は、**list translate** コマンドを入力すると表示されます。

デフォルト値: なし

mappings
静的アドレス・マッピングの特性 (IP アドレスおよびポートなど) を変更することができるプロンプトを表示します。

有効値: 構成されたマッピングを識別するインデックス番号。この番号は、**list mappings** コマンドを入力すると表示されます。

デフォルト値: なし

Delete

delete コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、およびマッピングを削除するのに使用します。

構文:

delete reserve
translate
mappings

reserve *pools*
公衆 IP アドレス予約プールを削除することができるプロンプトを表示します。

有効値: 構成されたプールを識別するインデックス番号。この番号は、**list reserve pools** コマンドを入力すると表示されます。

デフォルト値: なし

translate *ranges*

私設 IP アドレス変換範囲を削除することができるプロンプトを表示します。

有効値: 構成された変換範囲を識別するインデックス番号。この番号は、**list translate** コマンドを入力すると表示されます。

デフォルト値: なし

mappings

静的アドレス・マッピングを削除することができるプロンプトを表示します。

有効値: 構成されたマッピングを識別するインデックス番号。この番号は、**list mappings** コマンドを入力すると表示されます。

デフォルト値: なし

Disable

disable コマンドは、NAT を使用不可にするのに使用します。変換を必要とするパケットを廃棄するようにして NAT を使用不可にすることも、変換を必要とするパケットを通過させるようにして NAT を使用不可にすることもできます。

構文:

disable nat

drop

pass

drop 変換を必要とするパケットを廃棄するようにして NAT を使用不可にします。

pass 変換を必要とするパケットを通過させるようにして NAT を使用不可にします。

Enable

enable コマンドは、NAT を使用可能にするのに使用できます。 NAT を使用可能にすると、実行の準備が整いますが、**reset** コマンドを使用するか、ルーターをリスタートするまでは実行されません。

構文:

enable nat

List

list コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、マッピング、グローバル設定値、またはすべての NAT 情報をリストするのに使用します。

構文:

list reserve

addresses

pools

translate

mappings

global

all

次の例では、時間は、時、分、および秒で表示されます。エントリー経過時間は、そのエントリーが最後に使用されてから経過した時間です。結合は、これらの 2 つのアドレス間をトラフィックが流れることを意味しています。タイムアウトは、結合を除去する前の、最後の通信後に経過した時間を決めます。タイムアウトについての詳細は、**set** コマンドの項を参照してください。

例:

```
NAT config>list all
NAT Globals:
NAT is ENABLED
Tcp Timeout....:   24:00:00
Non-Tcp Timeout:    0:01:00
NAT Reserved Address Pool(s):
Index First Address    Mask             Count NAPT Address     Pool Name
1     9.8.7.1          255.255.255.0    3     0.0.0.0          pool1
2     9.8.7.6          255.255.255.0    12    9.8.7.9          pool1
NAT Translate Range(s):
Index IP Address       IP Mask          Associated Pool Name
1     7.1.1.0          255.255.255.0    pool1
2     10.0.0.0         255.0.0.0        pool1
NAT Static Mapping(s):
Index Private Address:Port    Public Address.:Port
1     10.1.2.3        0       9.8.7.1        0
2     7.1.1.1         21      9.8.7.9        21
```

Map

map コマンドは、私設ネットワーク内のホストまたはサーバーを公衆アドレスに静的に結合するのに使用します。このコマンドは、私設ネットワークのサーバーを設定するのに使用することができ、変更されることのない NAT の始動時のアソシエーションを確立します。

公衆および私設ポート番号 0 をもつ静的マッピングは NAT マッピングです。ポート番号に他の値をもつ静的マッピングは NAPT マッピングです。

構文:

map *private-address private-port-number public-address public-port-number*

private-address

ワークステーションの私設アドレス

有効値: 有効な IP フォーマットのインターネット・ホスト・アドレス。これは、公衆網から永続的にアクセスする必要があるスタブ・ネットワーク内のステーション (サーバーなど) に割り当てられたアドレスでなければなりません。

デフォルト値: なし

private-port-number

私設アドレスをもつ装置で実行されているアプリケーションの TCP/UDP ポート番号。 **0** を入力すると NAT 結合が作成され、それ以外の値を入力すると NAPT 結合が作成されます。 NAPT の一般的なポート値は、Telnet は 23、FTP は 21、HTTP は 80 です。

有効値: 0 ～ 65535

デフォルト値: 0

public-address

この私設アドレスがマップされる公衆 IP アドレス。これは、NAPT マッピングの場合は NAPT アドレス、NAT マッピングの場合は NAT アドレスでなければなりません。

有効値: 公衆網に固有の有効な IP アドレス。公衆網は、ネットワークの設計に応じて、インターネットまたはイントラネットが可能です。

デフォルト値: なし

public-port-number

公衆アドレスで変換されるパケットのポート番号。値 0 は、すべてのポートを表します。一般的な値は、Telnet は 23、FTP は 21、HTTP は 80 です。

有効値: 0 ～ 65535

デフォルト値: 0

この例では、私設 IP アドレス 10.11.12.200 をもつサーバーは、インターネットからのすべてのトラフィックを受け入れます。私設アドレス 10.11.12.199 をもつサーバーは、Telnet サーバーおよび FTP サーバーです。

例:

```
map 10.11.12.200 0 9.8.7.2 0
map 10.11.12.199 23 9.8.7.9 23
map 10.11.12.199 21 9.8.7.9 21
```

Reserve

reserve コマンドは、一定範囲の IP アドレスを作成し、公衆アドレス・プールに追加するのに使用します。

構文:

reserve *public-address mask number-in-group name napt-address*

public-address

プール内のこの範囲またはグループを構成する一連のアドレスの最初の公衆 IP アドレス。たとえば、プール内のこのグループに 9.8.7.6 ～ 9.8.7.17 の一連の 12 のアドレスが含まれている場合、この値は 9.8.7.6 になります。

注: 別の範囲のアドレスを公衆アドレス・プールに追加するには、各グループごとに別々に **reserve** コマンドを使用し、同じプール名を使用して各グループを対応付けます。たとえば、9.8.7.6 ～ 9.8.7.17 のアドレスを pool1 内の 1 つのグループとして構成し、アドレス 9.8.7.1 ～ 9.8.7.3 を

同じプール内の別のグループとして構成するといったことが可能です。その場合、アドレス 9.8.7.4 と 9.8.7.5 は構成されず、そのプールでは使用されません。

有効値: 公衆網に固有の有効な IP アドレス

デフォルト値: なし

mask IP アドレスからビットを選択するマスク。このマスクは、インターネット・アドレスと同様に、32 ビットの長さです。マスク内の 1 は、アドレスのネットワークまたはサブネット部分を選択します。 0 はホスト部分を選択します。たとえば、アドレスが 9.8.7.6 でマスクが 255.255.0.0 の場合は、最初の 2 バイトが 9.8 であるすべてのアドレス範囲 (つまり、9.8.0.0 〜 9.8.255.255) が含まれます。

有効値: 任意の有効な IP マスク

デフォルト値: なし

number-in-group

グループ内に *public-address* から始まる順次アドレスがいくつ含まれるかを指定しますアドレス 9.8.7.6 〜 9.8.7.17 の場合、この値は 12 です。

有効値: 1 〜 IP マスクによって定義できる値

デフォルト値: なし

name 公衆アドレス予約プールの名前。この文字列は、対応する **translate** コマンドのプール名と一致していることが必要です。

有効値: 最大 16 字の印刷可能文字を使用した任意の名前。先頭と末尾のブランクは無視されます。

デフォルト値: なし

napt-address

ネットワーク・アドレス・ポート変換 (NAPT) によって使用される公衆アドレス・プールからの 1 つの IP アドレス。このアドレスは、TCP および UDP トラフィックで、プロトコル・ポート番号に従って複数の私設アドレスを 1 つの NAPT アドレスにマップするのに使用されます。 NAPT の使用はオプションです。これを使用する場合、1 つの公衆アドレス・プールには 1 つの NAPT アドレスしか入れることができません。プールまたはグループに NAPT アドレスが存在しない場合は、値 **0.0.0.0** を入力します。 NAPT アドレスは 1 回だけプールに入力すれば済みます。

有効値: 公衆 IP アドレスの 1 つ。必ずしも公衆アドレス・プールに定義された値の範囲に含まれている必要はありませんが、同じサブネット内に存在することが必要です。

デフォルト値: 0.0.0.0 (NAPT がないことを意味します。)

例:

```
reserve 9.8.7.1 255.255.255.0 3  pool1 0.0.0.0
reserve 9.8.7.6 255.255.255.0 12 pool1 9.8.7.9
```

Reset

reset コマンドは、NAT をリセットするのに使用します。このコマンドは、すべての結合を削除し、NAT が使用しているすべてのメモリーを解放し、現行の Talk 6 構成に基づいて NAT をリスタートします。 NAT をリセットしても、2210 の他のコンポーネントを中断させることはありません。

構文:

reset nat

NAT が無効な構成を検出すると、それを知らせるメッセージを出します。 NAT ELS メッセージを検討して、NAT 初期化に失敗した理由を調べてください。

Set

set コマンドは、TCP および非 TCP タイムアウトを設定するのに使用します。

構文:

set **tcp**

nontcp

tcp *timeout*
2 つの結合されたワークステーション間で最後のメッセージを渡した後、NAT が TCP 結合を維持する時間。結合とは、私設アドレスと公衆 IP アドレスの 1 つとの間の関係を維持することです。

有効値: 0 ～ 65535 分 (0 分 ～約 45 日間)

デフォルト値: 1440 分 (24 時間)

nontcp *timeout*
2 つの結合されたワークステーション間で最後のメッセージを渡した後、NAT が非 TCP 結合を維持する時間。結合とは、私設アドレスと公衆 IP アドレスの 1 つとの間の関係を維持することです。

有効値: 0 ～ 65535 分 (0 分 ～約 45 日間)

デフォルト値: 1 分

Translate

translate コマンドは、NAT が変換するアドレスのリストにサブネットを追加するのに使用します。各サブネットは、1 つの変換範囲です。 NAT が知っている必要がある各変換範囲ごとに、このコマンドを 1 回入力する必要があります。任意の個数の変換範囲が、1 つの公衆アドレス予約プールを使用できます。

構文:

translate *private-address mask name*

private-address
変換する必要がある IP ホストまたはサブネットのアドレス。

有効値: 有効な小数点付き 10 進数の IP フォーマットのアドレス。サブネット・マスクと AND すると、このアドレスはスタブ・サブネット内のすべてのアドレスを識別します。スタブ・サブネットとは、そのルーターを介してのみ公衆網にアクセスするネットワークのことです。

デフォルト値: なし

mask **有効値**: 変換するスタブ・ネットワークに対応したネットワーク・マスクまたはサブネット・マスク

デフォルト値: 私設アドレスのクラス・マスク

name この範囲の私設アドレスのために NAT が使用する必要がある公衆アドレス・プールの名前

有効値: 最大 16 字の印刷可能文字を使用した任意の名前。これは **reserve** コマンドによって作成された公衆アドレス・プール名と一致していることが必要です。

デフォルト値: なし

ネットワーク・アドレス変換監視環境へのアクセス

NAT 監視環境にアクセスするには、次のように入力します。

```
* t 5
```

次に、**+** プロンプトで、次のようなコマンドを入力します。

```
+ feature NAT
NAT>
```

NAT> プロンプトが表示されます。

ネットワーク・アドレス変換監視コマンド

この節では、IP セキュリティー監視コマンドについて説明します。これらのコマンドは NAT> プロンプトで入力します。

表 123. NAT 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) をリストします。 13ページの『ヘルプの入手』 を参照してください。
List	NAT に関する情報を表示します。
Reset	ルーターが NAT 構成を読み込み、構成された NAT アクセス規則に従って稼働するようにします。 **reset NAT** コマンドを入力するまでは、NAT はルーターの稼働に影響を与えません。
Exit	直前のコマンド・レベルに戻ります。 13ページの『下位レベル環境の終了』 を参照してください。

List

list コマンドは、NAT 構成に関する情報を表示するのに使用します。

構文:

list
- all
- binding
- fragment
- global
- reserve
  - pools
  - addresses
- statistics
- translate

次の例では、時間は、時、分、および秒で表示されます。エントリー経過時間は、そのエントリーが最後に使用されてから経過した時間です。結合は、これらの 2 つのアドレス間にセッションが確立されることを意味しています。タイムアウトは、結合を除去する前の、最後の通信後に経過する時間を決めます。タイムアウトについての詳細は、Talk 6 の **set** コマンドの項を参照してください。

例:

```
NAT>list all
NAT Globals:
Current State    Tcp Timeout    Non-Tcp Timeout    Memory Usage (in bytes)
ENABLED            24:00:00           0:01:00           408

NAT Statistics:
Requests :     Passes      Drops      Holds
       0 :          0          0          0

NAT Address Binding(s):
Private Address//Port  Public Address//Port  Bind Type  Entry Age
        7.1.1.1    21         9.1.1.1    21  STATIC       0:00:13
       10.1.2.3     0         9.1.1.2     0  STATIC       0:00:13

NAT TCP Session Information:
Private Address//Port  Public Address//Port  Tcp State  Data Delta  Entry Age
        7.1.1.1    21         9.1.1.1    21  ESTAB'ED      0        0:00:56

NAT Translate Range(s):
Base Ip Address        Range Mask      Associated Reserve Pool
       7.1.1.0         255.255.255.0   carol
      10.0.0.0         255.0.0.0       carol

NAT Reserve Pool(s):
Reserve Pool     Pool Size    NAPT Address   1st Available Address
carol               21           9.1.1.1          9.1.1.12
------------------------------------------------------------
Number of Reserve Pools using NAPT.....:     1
Number of configured Reserved Addresses:    21

NAT Fragment Information:
Number of Entries    Number of Saved Fragments
           0                          0
```

Reset

reset コマンドは、NAT をリセットするのに使用します。このコマンドは、すべての結合を削除し、NAT が使用しているすべてのメモリーを解放し、現行の Talk 6 構成に基づいて NAT をリスタートします。 NAT をリセットしても、2210 の他のコンポーネントを中断させることはありません。

構文:

reset nat

第5部 付録および後付け

付録A. クィック構成リファレンス

重要

IBM 2210 の構成および監視を試みているときに、サービス端末が読み取り不能の場合は、 IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual の “Service Terminal Display Unreadable” の項を参照してください。

クィック構成に関する注記

選択

クイック構成プログラムの使用時に表示されるパネルで、大括弧 [ ] で囲んで示されている情報は、デフォルト値です。たとえば、次のように入力します。

```
Configure Bridging? (Yes, No, Quit): [Yes]
```

- デフォルト値の `Yes` を使用する場合は、**Enter** を押します。
- デフォルト以外の値 (`No` または `Quit`) を使用する場合は、小括弧の中の値から選択します。
- 大括弧の中に値が表示されない場合は、デフォルトがないので、値を入力する必要があります。

内蔵モデム

内蔵モデムは自動的に構成されます。

終了とリスタート

- **r** を入力すれば、いつでも現行のクイック構成セクションを最初からやり直すことができます。たとえば、インターフェース構成セクションにいるときに、**r** と入力して **Enter** を押すと、そのセクションの始めに戻ります。
- クイック構成を終了するには、**q** と入力して **Enter** を押します。 `Config>` プロンプトが表示されます。
- `Config>` プロンプトからクイック構成をリスタートするには、**qc** と入力して **Enter** を押します。

完了

- 構成を完了したら、構成を有効にするために、IBM 2210 をリスタートする必要があります。クイック構成プログラムの終わりに、このオプションが与えられます。

クイック構成プログラムの開始

以下の節では、クィック構成プログラム (**qconfig**) を使用したサンプル構成について説明します。

クィック構成プログラムを開始するには、Config> プロンプトで **qc** と入力します。

開始すると、プログラムは次のようなパネルを表示します。

```
Router Quick Configuration for the following:

o   Interfaces
o   Multilink PPP (w/o DIALs)
o   Dial Circuits (w/o DIALs)
o   Dial-in Access to LANs (DIALs)
o Bridging
        Spanning Tree Bridge (STB)
        Source Routing Bridge (SRB)
        Source Routing/Transparent Bridge (SR/TB)
        Source Routing Transparent Bridge (SRT)
o   Protocols
        IP (including OSPF, RIP, and SNMP)
        IPX
        DNA
o   Booting

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note: Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
```

イベント・ログ は、システム・アクティビティー、状態の変更、データの送受信、データ誤りと内部誤り、およびサービス要求を記録します。ログ・レベルは標準 (デフォルト) に設定されます。エラー・ログについての詳細は、 *イベント・ログ・システム メッセージの手引き* を参照してください。

クィック構成では、次のことが行えます。

1. インターフェースを構成する
2. マルチリンク PPP インターフェースを構成する
3. ダイヤル回線を構成する
4. ダイヤルイン回線およびダイヤルアウト回線を構成する
5. LAN へのダイヤルイン・アクセス (DIALs) 情報を構成する
6. ブリッジングを構成する
7. プロトコルを構成する
8. ブートを構成する
9. コンソール・モデム制御を使用可能にする
10. ルーターをリスタートする

LAN エミュレーションの構成

ATM 装置を追加した場合、次のようなプロンプトが表示されます。

```
*********************************************************
LAN Emulation Configuration
*********************************************************

Type 'Yes' to Configure LAN Emulation
Type 'No' to skip LAN Emulation Configuration
Type 'Quit' to exit Quick Config

Configure LAN Emulation? (Yes, No, Quit): [Yes]
```

この画面からトークンリングまたはイーサネット LAN エミュレーション・クライアントのいずれも構成することができます。

インターフェースの構成

```
*********************************************
Interface Configuration
*********************************************

Type 'Yes' to Configure Interfaces
Type 'No' to skip Interface Configuration
Type 'Quit' to exit Quick Config

Configure Interfaces? (Yes, No, Quit): [Yes]
```

1. 次の処置のいずれかを行います。
   - **y** と入力して、インターフェース構成プロンプトを表示する。
   - **n** と入力して、インターフェース構成を飛ばし、クィック構成を継続する。
   - **q** と入力して、クイック構成を終了する。これにより、Config> プロンプトが表示されます。このプロンプトからクィック構成をリスタートする場合は、**qc** と入力します。

インターフェース構成が開始したら、このレベルで何度でも 'r' を入力して、インターフェース構成をやり直すことができます。

クィック構成を使用して構成できる WAN インターフェースは、PPP、フレーム・リレー、および V34 だけです。 IBM 2210 がクロックを提供している場合、PPP およびフレーム・リレーに構成できるパラメーターは、ケーブル・タイプと回線速度だけです。 V34 インターフェースの場合、ケーブル・タイプは RS-232 DTE、クロック速度は 115200 に設定されます。

注: 一部のモデムは、DTE シリアル速度として 115200 をサポートしません。その場合は、その V34 ネットのネットワーク構成に入って、DTE 速度を下げる必要があります。

構成時に表示される次の画面は、IBM 2210 がイーサネット版であるか、トークンリング版であるかによって異なります。

イーサネット

イーサネット版の IBM 2210 の場合、構成は次のようなプロンプトを表示します。

1. インターフェースの確認:

```
Intf 0 is Ethernet

Intf 1 is WAN PPP
Encapsulation for WAN 1 (PPP, Frame Relay, V34):  [PPP] PPP
```

2. カプセル化タイプを指定するために、以下の値の 1 つを入力します。

   ppp　ポイント・ポイント・プロトコル

   fr　フレーム・リレー

   V34　V.34 モデム・ハンドラー

   PPP およびフレーム・リレーの場合は、次のようなメッセージが表示されます。

```
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
X.21 DCE: [RS-232 DTE] V.35 DCE
```

   注: DTE ケーブル・タイプは、モデムまたは DSU に接続するときに使用します。DCE ケーブル・タイプは、別の DTE 装置に直接接続し、2210 がクロックを提供するようにする場合に使用します。

3. 使用する、またはこの WAN ポートに接続するケーブル・タイプを入力します。

```
Internal clock speed (decimal) (2400 - 2048000): [0] 1544000
```

   内部クロック速度は、DCE ケーブルを入力した場合にのみ表示されます。

   WAN は、WAN Port 2 について繰り返すようにプロンプトで指示します。

```
Intf 2 is WAN PPP
Encapsulation for WAN 2 (PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
X.21 DCE: [RS-232 DTE] V.35 DCE
This is all configured device information:

Intf 0 is Ethernet, Connector (10BaseT, AUI) autoconfigured
Intf 1 is WAN 1 with PPP Encapsulation, V.35 direct attach cable
  internal clock speed 1544000 bits/second
Intf 2 is WAN 2 with PPP Encapsulation, V.35 modem cable

Save this configuration? (Yes, No): [Yes]
```

4. 構成を保管し、クィック構成を続ける場合は、**y** を入力します。インターフェース構成プロンプトを再表示する場合は、**n** を入力します。

トークンリング

トークンリング版の IBM 2210 の場合、構成は次のようなプロンプトを表示します。

1. インターフェースの確認:

```
Intf 0 is Token Ring
Speed in Mb/sec (4,16): [16]
```

2. 媒体転送速度を MB/秒単位で指定するために、**4** または **16** を入力します。媒体転送速度は、リングの速度に一致していることが必要です。

```
Connector (STP, UTP): [STP]
```

3. 使用している媒体を指定するために、以下の値の 1 つを入力します。

STP　シールド付き対より線

UTP　シールドなし対より線

WAN プロンプトの説明は、イーサネット構成プロンプトの項を参照してください。

```
Intf 1 is a WAN PPP
Encapsulation for WAN 1
(PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
X.21 DCE: [RS-232 DTE] V.35 DCE
Intf 2 is a WAN PPP
Encapsulation for WAN 2
(PPP, Frame Relay, V34): [PPP]
Cable type (RS-232 DTE, RS-232 DCE, V.35 DTE, V.35 DCE, V.36 DTE, X.21 DTE,
X.21 DCE: [RS-232 DTE] V.35 DCE
Internal clock speed (decimal) (4800 - 2048000): [0]

This is all configured device information:

Intf 0 is Token--Ring, Speed 16 Mb/sec, Connector UTP
Intf 1 is WAN1 with PPP Encapsulation, V.35 modem cable
Intf 2 is WAN2 with PPP Encapsulation, V.35 direct attach cable
   internal clock speed 0 bits/second

Save this configuration? (Yes, No): [Yes]
```

4. 構成を保管し、クィック構成を続ける場合は、**y** を入力します。インターフェース構成プロンプトを再表示する場合は、**n** を入力します。

マルチリンク PPP (MP) インターフェースの構成

ISDN 機能を備えたルーターを使用している場合は、次のような構成質問が表示されます。

注: 次の例は、1 次 ISDN アダプターが 2210 モデル 24x またはモデル 14x に接続されているものと想定しています。

```
*********************************************************
Multilink PPP Configuration (w/o DIALs)
*********************************************************

 Type 'Yes' to Configure Multilink PPP
 Type 'No' to skip Multilink PPP Configuration
 Type 'Quit' to exit Quick Config

 Configure Multilink PPP? (Yes, No, Quit): [Yes]
```

1. 次の処置のいずれかを行います。
   - y と入力して、マルチリンク PPP 構成プロンプトを表示する
   - n と入力して、マルチリンク PPP 構成を飛ばし、クイック構成を継続する。
   - q と入力して、クイック構成を終了する。

   MP 構成が現行の MP 構成を表示し始めると、次のような状態メッセージが現れます。既存の MP インターフェース構成を編集するため、または新規の MP バンドルを開始するための選択項目が得られます。

```
Current Multilink PPP Configuration:
Num    Intf#    Direction  Max Links  Link Intf#  Base Intf#  Destination
1      New Multilink PPP

Choose the Multilink PPP you wish to edit/add:  (1 - 1): [1]
```

2. 項目の番号を選択します。新規の MP インターフェース構成を開始する場合は、リストの最後の番号を入力し、構成を変更する場合は、既存の MP インターフェースの番号を選択します。 (注: 上の例には、既存の MP インターフェースはありません。) 新規 MP インターフェースを追加することを選択した場合は、次のような質問が出されます。質問は、INBOUND と OUTBOUND の MP インターフェースで、いくぶん異なります。

```
Enter maximum number of active links (2 - 23): [2] 3
Set Call Direction (Inbound, Outbound, Both): [Inbound] Inbound
Enter Idle timer (seconds, 0 means always active) (0 - 65535): [0] 0
```

3. 次に、MP インターフェースが使用できる ISDN ダイヤル回線を追加/編集するようにプロンプトで指示されます。下の例は、1 つのダイヤル回線を追加する場合を示していますが、1 つの MP インターフェースにつき複数のダイヤル回線を追加することも可能です。ダイヤル回線を追加する場合は、リストの最後の ″New Circuit″ と示されている番号を選択し、既存のダイヤル回線構成を編集する場合は、対応する番号を入力します。 (注: 下の例には、既存のダイヤル回線構成は表示されていません。)

```
Current Dial Circuit Configuration:

Num Intf# Intf Type               BaseIntf# MP  Direction  Destination
1   New Circuit

Choose a Dial Circuit Link you wish to edit/add:  (1 - 1): [1]
Enter interface # of Base Net, "?" for List,"Q" to quit: (6)

Address assigned name             Network Address  Network Subaddress
----------------------            ---------------  ------------------
default_address                   9999999
Assign Line ID *In* Network Address:
     Network Address name ([1-23] chars): LID_IN
     Enter Network Address [1-26 digits]: 1234
     Enter Network Subaddress [0-21 digits]:


Interface #:                8
Interface Type:             PPP Dial Circuit
Base Intferface #:          6 (ISDN Base Net)
Multilink PPP Interface #:  7
Call Direction:             Inbound only
Destination Name:           default_address
Line ID *IN* Name:          LID_IN

Is this correct (Yes, No): [Yes] Yes
Add another Dial Circuit Link (Yes, No): [Yes] No
```

4. 次に、確認のために、MP インターフェースとそのインターフェースのすべてのダイヤル回線がリストされます。この例の場合、MP インターフェースには 1 つのダイヤル回線しかありません。

```
 Multilink PPP Interface #:  7
 Call Direction:             Inbound only
 Idle timer:                 0 (fixed circuit)
 Maximum Number of links:    3
 Dial Circuit Link
      Interface #:           8
      Interface Type:        PPP Dial Circuit
      BASE Interface #:      6 (ISDN Base Net)
      Destination Name:      default_address
      Line ID *In* Name:     LID_IN
Is this correct (Yes, No): [Yes] Y
```

5. 別の MP インターフェースを追加/編集する場合は、次の質問に対して y と入力します。 n と応答すると、MP 構成セクションを終了します。

```
Add another Multilink PPP Interface (Yes, No): [Yes] n
```

6. すべての MP インターフェースを構成し終わると、構成されたすべての MP インターフェースがリストされた MP 確認画面が表示されます。変更を保管する場合は y と入力し、新規の MP 構成を廃棄する場合は n と入力します。

```
Current Multilink PPP Configuration:
Num    Intf#    Direction  Max Links  Link Intf#  Base Intf#  Destination
1      7        In         3          8           6           default_ad

Save this configuration (Yes, No): [Yes] y

Multilink PPP configuration saved.
```

ダイヤル回線の構成

ダイヤル回線の構成の場合は、次のような構成質問が表示されます。

```
************************************************************
Dial Circuit Configuration (w/o DIALs)
************************************************************

Type 'Yes' to Configure Dial Circuits
Type 'No' to skip Dial Circuits Configuration
Type 'Quit' to exit Quick Config

Configure Dial Circuits? (Yes, No, Quit): [Yes] y
```

1. 次の処置のいずれかを行います。
   - y と入力して、ダイヤル回線構成プロンプトを表示する。
   - n と入力して、ダイヤル回線構成を飛ばし、クイック構成を継続する。
   - q と入力して、クイック構成を終了する。

   ダイヤル回線構成に入ると、次のような状態メッセージが表示されます。この例には、既存のダイヤル回線構成はありません。

```
Current Dial Circuit Configuration:
Num Intf# Intf Type               BaseIntf# MP  Direction ...
Destination
1   New Circuit

Choose the circuit you wish to edit/add:  (1 - 1): [1] 1
```

2. 新規のダイヤル回線を追加する場合は、リストの最後の ″New Circuit″ と示されている番号を選択します。既存のダイヤル回線の構成を編集する場合は、編集した

いダイヤル回線の番号を選択します (注: 上の例では、既存のダイヤル回線はありません)。下の例は、新規の PPP 着信ダイヤル回線を追加する場合に表示されるプロンプトを示しています。

```
Enter interface # of Base Net, "?" for List,"Q" to quit: (6)
Enter type of dial circuit for this net: (PPP, FRAME-RELAY): [FRAME-RELAY] PPP

Set Call Direction (Inbound, Outbound, Both): [Both] Inbound
Accept ANY INBOUND call (Yes, No): [No] Yes
```

3. すべての質問に応答し終わると、下のように、そのダイヤル回線について確認を求める画面が表示されます。

```
Interface #:                13
Interface Type:             PPP Dial Circuit
Base Intferface #:          6 (ISDN Base Net)
Idle timer:                 0 (fixed circuit)
Call Direction:             Inbound only
Destination Name:           default_address
Line ID *IN* Name:          * ANY *

Is this correct (Yes, No): [Yes] Yes
```

4. 次に、上の例と同じ方法で、さらにダイヤル回線を追加/編集することができます。

```
Add another Dial Circuit (Yes, No): [Yes] No
```

5. 最後に、ダイヤル回線の構成を確認するように求められ、ダイヤル回線構成セクションが終了します。 y と応答すると、ダイヤル回線構成が保管され、n と応答すると、この構成セッションで行われた変更は廃棄されます。

```
Current Dial Circuit Configuration:
Num Intf# Intf Type               BaseIntf# MP  Direction
Destination
1   13    PPP Dial Circuit        6/ISDN    No  In
default_addre

Save this configuration (Yes, No): [Yes] Yes

Dial circuit configuration saved.
```

LAN へのダイヤルイン・アクセス (DIALs) インターフェースと DIALs サーバー情報の構成

構成しているルーターが DIALs 機能を備えている場合、DIALs インターフェースおよび DIALs サーバー情報を構成するかどうかを尋ねられます。 DIALs インターフェースの構成について尋ねられるのは、基本 WAN インターフェース上に V34 を構成した場合、またはルーター内に ISDN インターフェースが存在する場合だけです。 DIALs の構成は、以下のプロンプトによって導かれます。

```
*********************************************************
Dial-in Access to LANs (DIALs) Configuration
*********************************************************

Type 'Yes' to Configure DIALs Configuration
Type 'No' to skip DIALs Configuration Configuration
Type 'Quit' to exit Quick Config

Configure DIALs Interfaces? (Yes, No, Quit): [Yes]
```

1. 次の処置のいずれかを行います。
   - y と入力して、DIALs インターフェース・プロンプトを表示する。
   - n と入力して、DIALs インターフェース構成を飛ばす。
   - q と入力して、クイック構成を終了する。

   yes と応答し、装置に ISDN がロードされている場合には、次のような画面が表示されます。

```
Current Multilink PPP Configuration:
Num  Intf#   Direction   MaxLinks  DIALs
1    8       In          2         No

Enter the number of Multilink PPP DIALs interfaces:(0-23) 2
Enter maximum number of active links per Multilink PPP interface: 3
```

   次に、次のようなプロンプトが表示されます。

```
For Base Interface #1 (V.34 Base Net) no Dial Circuits are configured!
Add a DIALs (Dial-in) Interface for this Base Interface? (Yes, No): [No]y
Add a Dial-out DIALs Interface for this Base Interface? (Yes, No): [No] y

Num Intf# Intf Type                BaseIntf#  MP  Direction  Destination

 1   3     PPP Dial-in Circuit      1/V34     No  In         N/A


 2   4     Dial-out Dials Circuit   1/V34     No  Out        N/A


Save this configuration (Yes, No): [Yes]

Dial circuit configuration saved.
```

   no と応答すると、ユーザーは DIALs サーバー構成から出ます。

2. ルーター内の有効な基本 WAN インターフェース (V34 または ISDN) のそれぞれについて、この基本ネットに DIALs ダイヤルイン・インターフェースを追加したいかどうかを尋ねられます。
   - 基本ネットが ISDN BRI または ISDN PRI の場合、その ISDN 基本ネットに対して、それぞれ最大 2 または 23 のダイヤルイン・インターフェースを追加したいかどうかを尋ねられます。
   - 基本ネットが V34 の場合には、この基本ネットに対して DIALs ダイヤルアウト回線を追加したいかどうかも尋ねられます (ISDN 上ではダイヤルアウトはサポートされません)。
3. これらの質問に yes または no と応答し終わると、その基本ネットの現行ダイヤル回線構成が表示されます。 yes と応答して、構成を保管することも、no と応答して、その基本ネットの構成をやり直すこともできます。

4. すべての DIALs インターフェースを構成した後、または DIALs インターフェースの質問に no と応答すると、DIALs サーバー構成に進みます。ここでは、DIALs サーバーのグローバル設定値に関する情報の入力を求められます。

```
Configure DIALs Server? (Yes, No, Quit): [Yes] yes
Type 'r' any time at this level to restart Dial-in Access to LANs
Configuration.
```

5. 次の処置のいずれかを行います。
   - y と入力して、DIALs サーバー・プロンプトを表示する。
   - n と入力して、DIALs サーバー構成を飛ばす。
   - q と入力して、クイック構成を終了する。

   yes と応答すると、次のようなプロンプトが表示されます。 no と応答すると、次の構成セクションに進みます。

```
Default number of minutes a user is allowed before being
disconnected, 0 is unlimited: (0)
```

6. オンラインのデフォルト分数 (default number of minutes) は、ダイヤルインおよびダイヤルアウト・ユーザーの最大接続時間を決めます。この時間を無制限に設定したい場合は、0 を入力します。この情報を以前に構成していない場合、デフォルトはゼロになります。

```
Enter DIALs Server name - up to 30 chars: (2210_DIALS_SERVER)
```

7. DIALs サーバーの名前を入力します。デフォルトは 2210_DIALS_SERVER です。これは、DIALs クライアントの CHOOSER アプリケーションを起動した場合、ダイヤルアウト・クライアントがネットワーク上で DIALs ダイヤルアウト・サーバーを ″発見″ したときに表示されるサーバーの名前です。

```
Dial-out client type(s) supported (DIALs, TELNET, BOTH): [BOTH]
```

8. 前の質問によって、そのルーターでオンにされるダイヤルアウト・サポートのレベルが決まります。 DIALs は、IBM DIALs ダイヤルアウト・クライアントをサポートすることを示しています。 Telnet ダイヤルアウトは、telnet アプリケーションまたは telnet シリアル・ポート・アプリケーションを使用して、LAN を基本ネットとするクライアントからダイヤルアウトすることができることを示しています。デフォルト設定では、両方とも使用可能になります。

```
Inactive time before a connection is dropped, 0 is unlimited: (30)
```

9. 前の質問は、データの送受信が行われずにダイヤルアウト回線がアクティブに保持される時間の長さに関するものです。これは、ダイヤルアウト回線を介する接続をトラフィックがない状態でアクティブに保つことができる分数を設定します。デフォルト値は 30 分です。

```
Configure Proxy DHCP? (Yes, No, Quit): [Yes]
How many DHCP Servers do you wish to use? (Maximum is 20) : (1) 2
Enter DHCP Server Address: [] 10.0.0.1
Enter DHCP Server Address: [] 10.0.0.2
```

10. DHCP ゲートウェイ・インターフェース、または giaddr (RFC1531 の定義) は、DHCP サーバーがアドレスを提供するサブネットに対応した IP アドレスです。これは、DHCP サーバーが複数のサブネットにアドレスをリースする場合に必要

です。 giaddr は、DHCP サーバーがアドレスを提供するサブネットを区別できるようにするだけでなく、応答先のアドレスも提供します。

ここで、クイック構成は、ダイヤルイン・ユーザーに対応するサブネットとして構成するインターフェースの番号を尋ねます。 LAN インターフェースが 1 つだけの場合、そのインターフェースの番号は、たいていはゼロです。

```
 DHCP Gateway (giaddr) interface: (0)

Do you want to use Dynamic DNS with your DHCP server? (Yes, No): [Yes]
```

11. 次の一連の質問は、動的ホスト構成プロトコル (DHCP) 構成を決めます。

    DHCP を使用してダイヤルイン・ユーザーへの IP アドレスを管理する場合は、この質問に yes と答える必要があります。 yes と応答すると、DHCP サーバー・アドレスと、ダイヤルイン・ユーザーがアクセスする LAN に接続されているネットワーク番号の入力を求められます。

```
This is all the configured Dial-in Access to LANs information:

Default number of minutes allowed per connection:  15
Inactive timer:                                    Unlimited
LAN Protocols enabled for dial-out:                TELNET SHIVA
DIALs Server name:                                 2210_DIALS_SERVER

DIALs client IP address specification:
Client     : Disabled
UserID     : Disabled
Interface  : Disabled
DHCP Proxy : Enabled

Configured DHCP Servers :           10.0.0.1          10.0.0.2

DHCP Gateway (giaddr) interface: 0
Lease addresses will be associated with the
network (subnet) accessed via 10.0.0.2

Dynamic DNS: Enabled


Is this information correct? (Yes, No, Quit): [Yes]
```

12. DIALs 構成の情報の要約が表示され、それが正しいかどうかを尋ねられます。情報が正しい場合は、yes と応答します。情報が正しくなく、再入力したい場合は、no と応答します。

ブリッジングの構成

```
*********************************************
Bridging Configuration
*********************************************

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes]
```

1. Configure Bridging に応答して、以下の処置の 1 つを行います。
   - **y** と入力して、ブリッジング構成プロンプトを表示する。表示されるプロンプトは、ネットワーク構成によって異なります。
   - **n** と入力して、ブリッジング構成を飛ばし、クイック構成を継続する。

- **q** と入力して、クイック構成を終了する。これにより、Config> プロンプトが表示されます。クイック構成に再び入るには、このプロンプトの後に **qc** と入力します。

2. DIALs ダイヤルイン回線用に構成した場合は、次のようなパネルが表示されます。

```
Transparent bridging automatically enabled
on DIALs ports? (Yes, No, Quit): [Yes]
```

   各 DIAL インターフェースのブリッジ構成に透過ブリッジ・ポートを自動的に追加する場合は、**y** と入力します。

   各 DIALs ダイヤルイン・インターフェース上のブリッジングを自動的に使用不可にする場合は、**n** と入力します。

3. ブリッジングを構成することを選択すると、すべての LAN インターフェース上のスパンニング・ツリー・ブリッジング (STB) が使用可能になります。次のようなパネルが表示されます。

```
Type 'r' any time at this level to restart Bridging Configuration

STB will be enabled on all LAN interfaces
```

   SRT ブリッジングを構成する場合は、**y** と入力します。そうでない場合は、**n** と入力します。構成内の各トークンリング・インターフェースごとに、インターフェース上のソース・ルーティングを使用可能にするように求めるプロンプトが出ます。

```
Configure SRT Bridging? (Yes, No): [Yes]
You are now configuring the Source Routing part of SRT Bridging
Bridge Number (hex) of this Router (1-F): [A]
```

4. ブリッジ番号を入力します。これは、2 つの並列セグメント間で固有の 1 ～ F の 16 進値です。

```
Interface 0 (Port 1) is of type Token Ring
Configure Source Routing on this interface (Yes, No): [Yes]
```

5. **y** と入力して、インターフェース上のソース・ルーティングを構成します。コンソールに、次の 2 行が表示されます。

```
Configuring Interface 0 (Port 1)
Segment Number (hex) of this Interface (1-FFF): [A1]
```

   注: ソース・ブリッジングではゼロのポート番号は使用できないので、ポート番号が 1 だけ増えます。

   各インターフェースに、1 ～ FFF の固有の 16 進値が割り当てられます。各リング (セグメント) 上のインターフェースは同じセグメント番号を持ちますが、セグメント番号は各リングに固有です。

   各トークンリング・インターフェースごとに、次のようなプロンプトが表示されます。

```
Interface 1 (Port 2) is of type Token Ring
Configure Source Routing on this interface? (Yes, No): [Yes]
Configuring Interface 1 (Port 2)
Segment Number (hex) of this Interface (1-FFF): [A2]
```

3 つ以上のインターフェースをソース・ルーティング用に構成する場合は、内部バーチャル・セグメントに対して固有の 1 ～ FFF の 16 進値を入力します。

```
Virtual Segment Number (hex) of this Router (1-FFF): [A4]
```

6. 次のようなパネルが表示されます。

```
This is all configured bridging information:

       Interfaces configured for STB:

       Interface #    Port #     Interface Type

           0          1          Token Ring
           1          2          Token Ring

The Source Routing part of SRT Bridging has been enabled

Bridge Number of this Router: A

Interfaces configured for Source Routing:

       Interface #     Port#      Segment #   Interface Type

           0             1          A1        Token Ring
           1             2          A2        Token Ring

Virtual Segment Number of this Router:  A4

Save this Configuration? (Yes, No): [Yes]
```

7. ブリッジング構成を保管し、クイック構成を継続する場合は、**y** と入力します。ブリッジング構成プロンプトを再表示する場合は、**n** と入力します。

   y と入力すると、次のようなメッセージが表示されます。

```
Bridging configuration saved
```

プロトコルの構成

ブリッジング構成を保管すると、次のようなパネルが表示されます。

```
*********************************************
Protocol Configuration
*********************************************

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]
```

次の処置のいずれかを行います。

- **y** と入力して、プロトコルを構成する。
- **n** と入力して、プロトコル構成を飛ばし、クイック構成を継続する。
- **q** と入力して、クイック構成を終了する。

最初に IP を構成し、次に IPX、その後で DECnet を構成します。

IP の構成

Configure Protocol パネルに **y** と応答すると、クイック構成は次のようなメッセージを表示します。

```
Type 'r' any time at this level to restart Protocol configuration
Configure IP? (Yes, No): [Yes]
```

1. 次の処置のいずれかを行います。
   - **y** と入力して、IP を構成する。
   - **n** と入力して、IP 構成を飛ばし、クイック構成を継続する。

DIALs ダイヤルイン・インターフェース用に構成した場合は、次のようなパネルが表示されます。

```
Automatically configure IP on DIALs dial-in interfaces (this will
also enable ARP subnet routing)? (Yes, No, Quit): [Yes]
```

2. 次の処置のいずれかを行います。
   - **y** と入力して、各 DIAL インターフェースの非番号制 IP アドレスを自動的に追加する。これにより、ルーターの ARP サブネット・ルーティングが使用可能にされ、DIAL インターフェース上の RIP パケットの送信はオフにされます。これらはすべて LAN へのダイヤルイン・アクセス インターフェースに必要なオプションです。 DIAL インターフェース上の IP を使用可能にしたい場合は、この質問に yes と応答することをお勧めします。
   - **n** と入力して、各 DIALs ダイヤルイン・インターフェース上の IP を自動的に使用不可にする。

各インターフェースごとに、次のような行が表示されます。

```
Configuring Per-Interface IP Information

Configuring Interface 0 (Token Ring)
Configure IP on this interface? (Yes, No): [Yes]
IP Address: [ ] 128.185.141.1
Address Mask: [255.255.0.0]
```

3. IP アドレスを 10 進表記法 (たとえば、128.185.142.20) で入力します。無効な IP アドレスを入力すると、以下のエラー・メッセージの 1 つがコンソールに表示されます。

   ```
   Bad address, please try again.

   This address has already been assigned.  Enter a different address
   ```

   アドレス・マスクは、このインターフェースが接続する IP ネットワークまたはサブネットワークを表す 10 進値です。

   IP アドレッシングまたはアドレス・マスクについての詳細は、*プロトコルの構成と監視 解説書* を参照するか、あるいはネットワーク管理者に相談してください。

```
Per-Interface IP Configuration complete

Configuring IP Routing Information
Enable Dynamic Routing (Yes, No): [Yes]
```

4. ルーティング・プロトコル (RIP または OSPF) がルーティング・テーブルを作成する必要がある場合は、**y** と入力します。手動で IP アドレスをルーティング・テーブルに追加する場合 (静的ルート) は、**n** と入力します。

```
Enable OSPF? (Yes, No): [Yes]
```

5. OSPF ルーティング・プロトコルを 1 次動的 IP ルーティング・プロトコルとして使用可能にする場合は、**y** と入力します。 RIP は、公示の受信ではなく、公示の送信についてのみ使用可能にされます。 OSPF を使用したくない場合は、**n** と入力します。 RIP は、公示の送信および受信に対して使用可能にされます。

```
OSPF Enabled with Max routes = 1000  and Max routers = 50
```

Max routes は、OSPF ルーティング・ドメインにインポートされる自律システム (AS) 外部ルートの最大数です。 Max routers は、ルーティング・ドメイン内の OSPF ルーターの最大数です。

```
Routing Configuration Complete

SNMP will be configured with the following parameters:

Community: public
Access:    READONLY

If you plan to use the graphical configuration tool
to download a configuration, it requires the definition
of a community name with read_write_trap access.

Define community with read_write_trap access ? (Yes, No):  [Yes]


This is the information you have entered:

          Interface #        IP Address     Address Mask

             0               128.185.141.1  255.255.255.0
             1               128.185.142.1  255.255.255.0
             2               128.185.143.1  255.255.255.0

OSPF is configured, and RIP is configured only for 'sending'

SNMP has been configured with the following parameters:

Community: public
     Access:    read_trap

     Community: dana
     Access:    read_write_trap

Save this configuration? (Yes, No): [Yes]
```

6. IP 構成を保管し、クイック構成を継続する場合は、**y** と入力します。プロトコル構成プロンプトを再表示する場合は、**n** と入力します。

IPX の構成

IP 構成を保管すると、次のようなメッセージが表示されます。

```
Configure IPX? (Yes, No): [Yes]
```

1. IPX を構成する場合は、**y** と入力します。 IPX 構成を飛ばして、クイック構成を継続する場合は、**n** と入力します。

   次のようなメッセージが表示されます。

   ```
   Type 'r' any time at this level to restart IPX Configuration
   IPX Configuration is already present
   Configure IPX anyway? (Yes, No): [No] yes
   ```

2. 既存の構成を置き換える場合は、**y** と入力します。現行の構成を保持し、継続する場合は、**n** と入力します。

DIALs ダイヤルイン・インターフェース用の構成を行った場合は、次のようなパネルが表示されます。

```
Enable IPX on DIALs interfaces? (Yes, No): [Yes]
```

3. 各 DIAL インターフェース上の IPX を自動的に使用可能にする場合は、**y** と入力します。インターフェースに対してランダムの IPX ネットワーク番号が生成され、DIAL インターフェースの IPXWAN は使用不可にされます。 DIAL インターフェースの IPXWAN を使用不可にすることは必須条件です。

   各 DIALs ダイヤルイン・インターフェース上の IPX を自動的に使用不可にする場合は、**n** と入力します。

```
Configuring Per-Interface IPX Information

Configuring Interface 0 (Token Ring)
Configure IPX on this interface? (Yes, No): [Yes]
```

4. 次のメッセージとユーザーの応答は、トークンリングまたはイーサネットのいずれを構成しているかによって異なります。

   トークンリングの IPX の構成:

   a. 次のようなプロンプトが表示されます。

      ```
      Token Ring encapsulation (frame) type? (TOKEN--RING MSB, TOKEN--RING LSB,
          TOKEN--RING_SNAP MSB, TOKEN--RING_SNAP LSB): [TOKEN--RING MSB]
      ```

   b. トークンリング・エンド・ステーション上の IPX プロトコルが使用するカプセル化タイプを入力します。

`Token--Ring MSB:` これは最も一般的なカプセル化タイプで、これがデフォルトです。IBM 2210 は、3 バイト 802.2 ヘッダー (0xE0, 0xE0, 0x03) を付けて発信パケットを作成します。これは、発信元および宛先アドレスを MSB (最上位ビット) に入れて、つまり非標準フォーマット (トークンリングに固有のアドレス・フォーマット) で送信します。

`Token--Ring LSB` IBM 2210 がアドレスを LSB (最下位ビット) に入れて、つまり標準フォーマットで送信する点を除いて、Token-Ring MSB と同じです。

`Token-Ring SNAP MSB` IBM 2210 は、8 バイトの 802.2/SNAP ヘッダー (0xAA, 0xAA, 0x03, 0x00, 0x00, 0x00, 0x81, 0x37) を付けて発信パケットを作成します。これは、発信元および宛先アドレスを MSB (最上位ビット) に入れて、つまり、非標準フォーマットで送信します。

Token-Ring SNAP LSB　IBM 2210 がアドレスを LSB (最下位ビット) に入れて、つまり標準フォーマットで送信する点を除いて、Token-Ring SNAP MSB と同じです。

イーサネットの IPX の構成:

a. 次のようなプロンプトが表示されます。

```
Ethernet encapsulation type? (ETHERNET_8022, ETHERNET_8023, ETHERNET_ii,
ETHERNET_SNAP): [ETHERNET_8023]
```

b. イーサネット・エンド・ステーション上の IPX プロトコルが使用するカプセル化タイプを入力します。

Ethernet_8022　パケットには 802.2 ヘッダーが含まれています。

Ethernet_8023　802.2 ヘッダーが付かない IEEE 802.3 パケット・フォーマットを使用します。これがデフォルトで、NetWare バージョン 4.0 より前のバージョンのデフォルトです。イーサネット 802.3 は、802.2 ヘッダーを含まないので、 IEEE 802 標準に合致しません。これは、ネットワーク上の他のノードとの問題の原因になることがあります。

Ethernet_II　イーサネット・タイプ 8137 をパケット・フォーマットとして使用します。イーサネット上で NetWare VMS を使用している場合は、このフォーマットが必要です。これは、NetWare バージョン 4.0 以上のデフォルトです。

Ethernet_SNAP　SNAP ヘッダーが付いた 802.2 形式を使用します。このカプセル化タイプは、トークンリング SNAP カプセル化との互換性のためのものです。ただし、IEEE 標準には違反しており、この標準に準拠するブリッジを介しての相互運用は不可です。

```
Network Number (hex) (1-FFFFFFFD):[1] 1
```

5. 対応する直接接続ネットワークに IPX ネットワーク番号を割り当てます。各 IPX インターフェースには、固有のネットワーク番号が必要です。

```
Configuring Interface 1 (WAN PPP)
Configure IPX on this interface? (Yes, No): [Yes]
Network Number (hex) (1-FFFFFFFD): [1] 2

Enable IPXWAN? (Yes, No): [No] yes
Configuring Interface 2 (WAN PPP)
Configure IPX on this interface? (Yes, No): [Yes]
Network Number (hex) (1-FFFFFFFD):[1] 3

Enable IPXWAN? (Yes, No): [No] yes
Host Number for Serial Lines: (000000000000) 1

Configure IPXWAN NodeID? (Yes, No): [Yes]
NodeID (hex) (1 - FFFFFFFD): [1] 4
```

使用可能にされている場合、IPXWAN プロトコルは、IPX パケットの転送を開始する前に、PPP シリアル・インターフェースで使用するルーティング・パラメーターを交渉します。 IPXWAN は、PPP シリアル・インターフェース上で IPX パケットを転送する必要はありません。 IPXWAN Node ID は、ルーターを識別する固有の IPX ネットワーク番号で、ネットワーク・インターフェース上で IPXWAN が使用可能にされている場合に必要です。

6. ホスト番号は、IPX ルーターに割り当てられた固有の 12 桁の 16 進値です。シリアル・ラインにはホスト番号を作成する元になるハードウェア・ノード・アドレスがないので、これが必要になります。

```
This is the information you have entered:

               Per-Interface Configuration Information

Ifc   IPX Net (hex)   Encapsulation       IPXWAN

0     1               TOKEN-RING MSB      Not Configured
1     2                                   Enabled
2     3                                   Enabled

  Host Number for Serial Lines: 000000000001
  IPXWAN Node ID = 4
  IPX Router Name = ipx_router-4
Save this configuration? (Yes, No): [Yes]
```

7. IPX 構成を保管し、クイック構成を継続する場合は、**y** と入力します。 IPX 構成プロンプトを再表示する場合は、**n** と入力します。

   y と入力すると、次のようなメッセージが表示されます。

```
IPX configuration saved
```

DECnet (DNA) の構成

IPX 構成を保管すると、次のようなメッセージが表示されます。

```
IPX Configuration saved

Configure DNA? (Yes, No): [Yes]
```

1. DNA を構成する場合は、**y** と入力します。 DNA 構成を飛ばして、クイック構成を継続する場合は、**n** と入力します。

```
Type 'r' any time at this level to restart DNA Configuration

Configuring Global DNA information

Highest Node Number (decimal) (1-1023): [32]
Router Level (Level1, Level2, DEC Level1, DEC Level2):
  [ Level2]
Highest Area (decimal) (1-63): [63]
Node Address (area.node): (63.32)
```

   上の構成フィールドは、以下を考慮して構成します。

   Highest Node Number
   ルーターのエリアの最高ノード・アドレス。これを高く設定しすぎると、ルーターの効率に悪影響を与え、余分な記憶域が必要になります。

   Router Level
   ルーターがレベル 1 またはレベル 2 のどちらのルーターであるかを識別します。レベル 1 のルーターは、そのエリア内のすべてのノードを追跡しますが、エリア外のノードには関与しません。レベル 2 のルーターは、エリア間のトラフィックをルートします。

通常は Level1 または Level2 を選択します。ただし、ルーターが X.25 ネットワークを介して DEC X.25 標準準拠のルーターと通信する必要がある場合は例外で、その場合にのみ DEC Level1 または DEC Level2 を選択します。

Highest Area

この番号は、少なくともネットワーク全体で最も高いエリア番号と同じ値にすることが必要です。

Node Address

このルーターのノード ID で、ネットワーク内で固有であることが必要です。

Enter を押すと、次のようなパネルが表示されます。

```
Configuring Per-Interface DNA Information

Configuring Max Routers on each interface

Configuring Interface 0 (Ethernet)
Configure DNA on this interface? (Yes, No) [YES]
Max Routers (decimal) (1-33): [16]

Configuring Interface 1 (WAN PPP)
Configure DNA on this interface? (Yes, No) [Yes]

Configuring Interface 2 (Token Ring)
Configure DNA on this interface? (Yes, No) [Yes]
Max Routers (decimal) (1-33): [16]
```

2. DECnet ネットワークに接続されるすべてのインターフェースに対して **y** と入力します。 LAN の場合、Max Routers はこの回線上に存在できる他のルーターの数を指定します。ルーターの効率とメモリー所要量を考慮して、この引き数はこの回線上の隣接ルーターの合計数より少し多めに設定します。

   次のようなパネルが表示されます。

```
This is the information you have entered:

        Global Configuration Information

           Highest Node Number:       32
           Router Level:              Level2
           Highest Area:              63
           Node Address:              63.32

        Pre-Interface Configuration Information
      Interface Number           Max Routers

              0                         16
              1                         1
              2                         16

Save this configuration? (Yes, No): [Yes]
```

3. DECnet 構成を保管し、クイック構成を継続する場合は、**y** と入力します。 DECnet 構成プロンプトを再表示する場合は、**n** と入力します。

   y と入力すると、次のようなメッセージが表示されます。

```
DNA Configuration Saved
```

ブートの構成

```
*********************************************
Boot Configuration
*********************************************

Type 'Yes' to Configure Booting
Type 'No' to skip Booting Configuration
Type 'Quit' to exit Quick Config

Configure Booting? (Yes, No, Quit): [Yes]
```

1. ブート構成プロンプトを表示する場合は、**y** と入力します。ブート構成を飛ばす場合は、**n** と入力します。クリック構成を終了する場合は、**q** と入力します。

   下の例に示されているように、以前のブート情報が表示されます。

```
Type 'r' any time at this level to restart Boot configuration


Previous Boot information

Booting Method:TFTP Boot
Interface Number:0
Interface IP Address:128.185.133.18
Address Mask:255.255.255.0
Host IP Address:128.185.120.120
Gateway IP Address:128.185.133.7
Boot file Name:ibm2210.ldc
Create a boot record using this information? (yes, No): [Yes]
```

2. 以前のブート情報が入っているブート・レコードを作成する場合は、**y** と入力します。次のようなプロンプトが表示されます。

```
Boot Configuration saved

Enable Console Modem-Control  (Yes, No, Quit): [No]
```

3. 次の処置のいずれかを行います。
   - モデムを介してコンソールを IBM 2210 に接続する場合、または電話接続が失われたら自動的にログアウトしたい場合は、**y** と入力します。
   - コンソールを直接 IBM 2210 に接続する場合は、**n** と入力します。
   - クイック構成を終了する場合は、**q** と入力します。

   no と入力した場合、次のプロンプトから別のブート・オプションを選択することができます。

```
Select Booting Method (TFTP Boot, BOOTP Boot, IBD Boot): [ ]
```

4. IBM 2210 をブートするのに使用するブート方式を入力します。
   - TFTP
   - BOOTP
   - IBD

以下では、各方式で表示されるプロンプトについて説明します。

TFTP ブート

```
Select Booting Method (TFTP Boot, BOOTP Boot, IBD Boot): [ ]
```

1. TFTP ホスト・サーバーを使用してブートする場合は、**TFTP** と入力し、以下のプロンプトに応答します。

`Interface Number ( ):[0]`	ブートに使用する LAN インターフェースの番号。このバージョンの IBM 2210 では、デフォルトの 0 を使用する必要があります。
`Interface IP Address: [0.0.0.0]`	ブートに使用するインターフェースの IP アドレス。IP アドレスを 10 進表記法で入力します。
`Address Mask: [255.255.0.0]`	アドレス・マスクは、IP アドレス・クラス・タイプを識別します。クラス A は 255.0.0.0、クラス B は 255.255.0.0、およびクラス C は 255.255.255.0 です。
`Host IP Address:[ ]`	ブート・ファイルが収容されているホストの IP アドレス。
`Via Gateway:[ ]`	ホストが IBM 2210 と同じ (サブ) ネットワーク上にない場合は、中間ルーターの IP アドレスを入力します。
`Boot File Name:` (*/path/filename.ext*)	ブートに使用するファイルの名前。ブート・ファイルの完全なパス (たとえば、 `/usr/2210/bootfile.name`) を指定する必要があります。

```
TFTP Boot Configuration Complete

This is the information you have entered:

       Booting Method:TFTP Boot
       Interface Number:0
       Interface IP Address:128.185.141.1
       Address Mask:255.255.255.0
       Host IP Address:128.185.120.120
       Gateway IP Address:128.185.141.7
       Boot File Name:ibm2210.ldc

Save this configuration? (Yes, No): [Yes]
```

2. ブート・レコードを作成する場合は、**y** と入力します。ブート構成プロンプトを最初からやり直す場合は、**n** と入力します。

BOOTP ブート

```
Select Booting Method (TFTP Boot, BOOTP Boot, IBD Boot): [ ]
```

1. **BOOTP** と入力すると、ブートに使用するインターフェース番号を入力するためのプロンプトがコンソールに表示されます。

   その後、次に似たメッセージが表示されます。

```
BOOTP Boot Configuration Complete

This is the information you have entered:

       Booting Method:BOOTP Boot
       Interface Number:    1

Save this configuration? (Yes, No): [Yes]
```

2. ブート・レコードを作成する場合は、**y** と入力します。ブート構成プロンプトを最初からやり直す場合は、**n** と入力します。

IBD ブート

```
Select Booting Method (TFTP Boot, BOOTP Boot, IBD Boot): [ ]
```

1. **IBD** と入力すると、IBD 内のソフトウェア・ロードのリストがコンソールに表示されます。

```
The following # loads(s) exist in the IBD
load.name load.name load.name load.name

You may use only these loads to configure an IBD boot record
IBD Load Name: (load.name) [ ]
```

2. ブートしたときに IBM 2210 がロードするソフトウェア・ロードの名前を入力します。

```
IBD Boot Configuration Complete

This is the information you have entered:

       Booting Method:        IBD Boot
       IBD Load Name:         load.name
```

IBD 内にロードが存在しない場合は、次のようなメッセージが表示されます。

```
There are no loads in the IBD. Select another booting
method
```

3. 別のブート方式を使用するために、**TFTP** または **BOOTP** を入力してください。

コンソールのモデム制御の使用可能化

```
Enable Console Modem-Control  (Yes, No, Quit): [No]
```

次の処置のいずれかを行います。

- モデムを介してコンソールを IBM 2210 に接続する場合、または電話接続が失われたら自動的にログアウトしたい場合は、**y** と入力します。
- コンソールを直接 IBM 2210 に接続する場合は、**n** と入力します。
- クイック構成を終了する場合は、**q** と入力します。

ルーターのリスタート

構成が完了すると、次のようなメッセージを受け取ります。

```
Quick Config Done
Restart the router? (Yes, No): [Yes]
```

1. 新しい構成を使用してルーターをリスタートするために **y** と入力すると、次のような情報が表示されます。

```
RESTARTING THE ROUTER........

Copyright IBM Corp. 1994, 1996
MOS Operator Control

*
```

2. **n** と入力すると、次のようなメッセージがコンソールに表示されます。

```
Type RESTART at the Config> prompt for the configuration to take effect
Config>
```

3. 新しい構成を使用して IBM 2210 をリスタートするには、Config> プロンプトの後に **restart** コマンドを入力します。現行の構成を変更または表示するには、**qc** と入力します。

付録B. X.25 ナショナル・パーソナリティー

この付録では、GTE-Telenet および DDN の省略時設定値をリストします。

GTE-Telenet

以下のパラメーターは GTE-Telenet の省略時設定値です。

- 発呼要求（Callreq): 20
- 復旧要求（Clearreq):
  - 再試行（Retries): 1
  - タイマー（Timer): 18
- 切断（Disconnect): Passive
- DP タイマー（DP-timer): 500 ミリ秒
- フレーム・ウィンドウ・サイズ（Frame window size): 7
- ネットワーク・タイプ（Network Type): CCITT
- N2 タイムアウト（N2 timeouts): 20
- パケット（Packet):
  - 省略時サイズ（Default size): 128
  - 最大サイズ（Maximum size): 256
  - ウィンドウ・サイズ（Window size): 2
- リセット（Reset)
  - 再試行（Retries): 1
  - タイマー（Timer): 18
- 再始動(Restart)
  - 再試行（Retries): 1
  - タイマー（Timer): 18
- 標準（Standard): 1984
- T1 タイマー（T1-timer): 4
- T2 タイマー（T2-timer): 2

DDN

以下のパラメーターは DDN の省略時設定値です。

- 発呼要求（Callreq): 20
- 復旧要求（Clearreq):
  - 再試行（Retries): 1
  - タイマー（Timer): 18
- 切断（Disconnect): Passive
- DP タイマー（DP-timer): 500 ミリ秒
- フレーム・ウィンドウ・サイズ（Frame window size): 7

- ネットワーク・タイプ（Network Type): CCITT
- N2 タイムアウト（N2 timeouts): 20
- パケット（Packet):
  - 省略時サイズ（Default size): 128
  - 最大サイズ（Maximum size): 256
  - ウィンドウ・サイズ（Window size): 2
- リセット（Reset)
  - 再試行（Retries): 1
  - タイマー（Timer): 18
- 再始動(Restart)
  - 再試行（Retries): 1
  - タイマー（Timer): 18
- 標準（Standard): 1984
- T1 タイマー（T1-timer): 4
- T2 タイマー（T2-timer): 2

付録C. 複数のディスクからのルーター・ロード・ファイルの作成

ソフトウェア・ロードが複数のディスクで到着した場合、以下の手順を使用して、ロードを結合して 1 つのロード・ファイルを作成し、ルーターがブート時に使用できるようにします。

最初のディスクには、既存のロードを分割して複数のディスケットでトランスポートするのに必要な、次の 4 つのファイルが入っています。

cutup.c
(標準 C コンパイラーを使用してコンパイルできる UNIX C ソース・ファイル)

cutup.exe
(DOS)

以下のファイルは、分割されたロードを再アセンブルして、DOS または UNIX サーバーにロードするのに使用します。

kopy.bat
(DOS)

kopy (UNIX シェル・スクリプト)

DOS でのロード・ファイルのアセンブル

2 枚のディスケットからロードをアセンブルするには、ディスケット 1 (KOPY.BAT) で提供された DOS バッチ・ファイルを使用し、次の構文を用いて行います。

kopy <*installation_drive***><***destination_directory***>**

ロードをアセンブルする前に、宛先ディレクトリーを作成したこと、および installation_diskette_drive パラメーターで指定されたドライブに最初のディスケットが挿入されていることを確認してください。次の例は、これらの手順を示しています。

```
B:\>kopy b: c:\source\cutup\tmp
B:\>copy c:\gw0/B c:\source\cutup\tmp\gw.tmp
1 file(s) copied
.
Please mount the second diskette
Press any key to continue . . .
Copying the second load file fragment
B:\>
B:\>copy c:\source\cutup\tmp\gw.tmp/B + b:\gw1
c:\source\cutup\tmp\gw.tmp  c:\SOURCE\CUTUP\TMP\GW.TMP
B:\GW1
1 file(s) copied
B:\>rename c:\source\cutup\tmp\gw.tmp  gw.ldc
Load file reassembly was successful
B:>
```

UNIX でのロード・ファイルのアセンブル

2 枚の UNIX ディスケットからロードをアセンブルするには、ディスケット 1 で提供された UNIX Bourne シェル・スクリプト (kopy) を使用し、次の構文を用いて行うことができます。

kopy<*installation_drive*><*diskette_directory*><*destination_directory*

ロードをアセンブルする前に、宛先ディレクトリーを作成したこと、および installation_diskette_drive パラメーターで指定されたドライブに最初のディスケットが挿入されていることを確認してください。次の例は、これらの手順を示しています。

```
kopy /dev/fd0 /kew /pcfs

Please insert the first diskette

Copying the first load file fragment

Please mount the second diskette

Copying the second load file fragment

Load file reassembly was successful

# ls /kew

gw0   gw1   gw.ldc
```

UNIX Bourne シェル・スクリプトを使用できない場合は、以下の手順を使用して、手動でロードをアセンブルすることができます。

1. 2 枚のディスケット (gw0 および gw1) に分割されたロードを、UNIX ファイル・システム上のディレクトリーにコピーする。
2. 次の UNIX コマンドを入力する。

   ```
   cat gw0 gw1 > gw.ldc
   ```

   得られたファイル (gw.ldc) は、アセンブルされたルーター・ロードです。

DOS でのロード・ファイルの分割

DOS のもとでロードを分割するには、CUTUP.EXE ファイルを使用して、次のようにして行います。

cutup<*file_extension*><*file_name*><*cut_length*>

file_extension は、分割する必要がある各スライスの先頭に付加されます。 file_name は、分割されるファイルの DOS ファイル名です。 cut_length は、CUTUP.EXE がファイルを分割するときの各フラグメントの長さです。次の例は、これらの手順を示しています。

```
C: \source\cutup>dir
Volume in drive C has no label
Volume Serial Number is XXXXXXXX
Directory of C: \SOURCE\CUTUP
.0730934:46p
..0730934:46p
GW      LDC     10225660728931:22p
CUTUP   EXE   105410902939:38a
2 file(s)   1033107 bytes
14811136 bytes free
C: \source\cutup>cutup gw.ldc gw 1000000
.....................................................
```

```
.....................
.............................
c: \SOURCE\CUTUP>dir
Volume in drive C has no label
Volume Serial Number is XXXXXXXX
Directory of C: \SOURCE\CUTUP
.0730934:46p
..0730934:46p
GW      0 10000000801931:22p
GW      LDC     10225660728931:22p
CUTUP   EXE   105410902939:38a
GW      1   225660801931:22p
4 file(s)   2055673 bytes
14811136 bytes free
```

UNIX でのロード・ファイルの分割

ロードの分割は、cutup.c を使用して行います。始めに、UNIX コンパイラーを使用してプログラムをコンパイルし、分割実行可能ファイルを作成します。その後で、次の構文を使用します。

cutup<*file_extension*><*file_name*><*cut_length*>

file_extension は、分割する必要がある各スライスの先頭に付加されます。 file_name は、分割されるファイルの DOS ファイル名です。 cut_length は、ファイルを分割するのに使用される長さ CUTUP.EXE です。次の例は、これらの手順を示しています。

```
#  ls -la
total 658
drwxrxrx   2 root    512 Aug  114:41  .
drwxrxrx  26 root   1024 Aug  114:41  ..
drwxrxrx   2 root  24576 Aug  114:41  cutup
drwxrxrr   2 root1022566 Aug  114:41  gw.ldc

#  cutup gw.ldc gw 100000

#  ls -la

total 658
drwxrxrx   2 root    512 Aug  114:41  .
drwxrxrx  26 root   1024 Aug  114:41  ..
drwxrxrx   2 root  24576 Aug  114:41  cutup
drwxrxrr   2 root1022566 Aug  114:41  gw.ldc
drwxrxrr   2 root1000000 Aug  114:41  gw0
drwxrxrr   2 root  22566 Aug  114:41  gw1
```

付録D. リモート AAA 属性

ここには、Radius、TACACS、および TACACS+ サーバーによって使用されるリモート AAA 属性が収められています。

Radius

IBM ベンダー ID: 211

認証属性

標準の草案

TUNNEL_TYPE	64
TUNNEL_MEDIUM_TYPE	65
TUNNEL_CLIEN_TYPE	66
TUNNEL_SERVER_EP	67
TUNNEL_CONN_ID	68
TUNNEL_PASSWORD	69

値

TUNNEL_TYPE		整数
	3	L2TP
TUNNEL_MEDIUM_TYPE		整数
	1	IP
TUNNEL_SERVER_EP		文字列
		IP アドレス

IBM ベンダー特有

NAS_TUNNEL_PASSWORD	101
CALLBACK_FLAGS	210
ENCRYPTION	211
HOSTNAME	213
DIALOUT	214
SUBNETMASK	215
PRIVILEGE	216

キーワード

Radius サーバーでは、ベンダー特有のフィールド `<keyword>=<value>` に入力できるキーワードが使用されます。

KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN

KWD_DIALOUT	DOF
KWD_SUBNETMASK	SNM
KWD_PRIVELGE	PRV

値

PRIVILEGE:
- ADMIN
- OPER
- MONITOR

CALLBACKFLAGS

REQ	必須コールバック
ROAM	ローミング・コールバック

DIALOUT

TRUE	このユーザーのダイヤルアウトが使用可能
FALSE	このユーザーのダイヤルアウトが使用不可
ONLY	このユーザーのダイヤルアウトのみ許可 (ダイヤルインは不許可)

TACACS+

認証

承認

PPP service=ppp protocol=ip
LOGIN service=shell cmd=null pri_lvl*0

標準 TACACS+ 属性
- service
- protocol
- cmd
- addr
- timeout
- priv_lvl
- callback-dialstring

IBM 特有の属性

encryption_key	16 進文字
dial_out	TRUE FALSE ONLY

会計

- task_id
- start_time

stop_time
elasped_time
timezone
event
reason
bytes
bytes_in
bytes_out
paks
paks_in
paks_out
status
err_msg

略語集

AARP AppleTalk アドレス解決プロトコル (AppleTalk Address Resolution Protocol)

ABR エリア・ボーダー・ルーター (area border router)

ack 確認応答 (acknowledgment)

AIX 拡張対話式エグゼクティブ (Advanced Interactive Executive)

AMA 任意 MAC アドレス指定 (arbitrary MAC addressing)

AMP アクティブ・モニター・プレゼント (active monitor present)

ANSI 米国規格協会 (American National Standards Institute)

AP2 AppleTalk フェーズ 2 (AppleTalk Phase 2)

APPN 拡張対等通信ネットワーキング機能 (Advanced Peer-to-Peer Networking)

ARE 全ルート探索 (all-routes explorer)

ARI ATM 実インターフェース (ATM real interface)

ARI/FCI
アドレス認知標識/フレーム複写標識 (address recognized indicator/frame copied indicator)

ARP アドレス解決プロトコル（Address Resolution Protocol）

AS 自律システム (autonomous system)

ASBR 自律システム境界ルーター (autonomous system boundary router)

ASCII 情報交換用米国標準コード (American National Standard Code for Information Interchange)

ASN.1 抽象構文表記法 1 (abstract syntax notation 1)

ASRT 適応ソース・ルーティング透過 (adaptive source routing transparent)

ASYNC
非同期 (asynchronous)

ATCP AppleTalk 制御プロトコル (AppleTalk Control Protocol)

ATP AppleTalk トランザクション・プロトコル（AppleTalk Transaction Protocol）

AUI 接続装置インターフェース (attachment unit interface)

AVI ATM バーチャル・インターフェース (ATM virtual interface)

ayt are you there (相手確認)

BAN 境界アクセス・ノード（Boundary Access Node）

BBCM ブリッジング・ブロードキャスト・マネージャー (Bridging Broadcast Manager)

BECN 逆方向明示的輻輳 (ふくそう) 通知（backward explicit congestion notification）

BGP ボーダー・ゲートウェイ・プロトコル（Border Gateway Protocol）

BNC bayonet Niell-Concelman

BNCP ブリッジング・ネットワーク制御プロトコル (Bridging Network Control Protocol)

BOOTP
BOOT プロトコル (BOOT protocol)

BPDU ブリッジ・プロトコル・データ単位（bridge protocol data unit）

bps ビット/秒 (bits per second)

BR ブリッジング/ルーティング (bridging/routing)

BRS 帯域幅予約システム (bandwidth reservation system)

BSD Berkeley ソフトウェア配布 (Berkeley software distribution)

BTP BOOTP リレー・エージェント (BOOTP relay agent)

BTU 基本伝送単位 (basic transmission unit)

CAM コンテンツ・アドレス可能メモリー (content-addressable memory)

CCITT 国際電信電話諮問委員会 (Consultative Committee on International Telegraph and Telephone)

CD 衝突検出 (collision detection)

CGWCON
ゲートウェイ・コンソール (Gateway Console)

CIDR 無クラス・ドメイン間ルーティング (Classless Inter-Domain Routing)

CIP クラシカル IP (Classical IP)

CIR 認定情報速度 (committed information rate)

CLNP コネクションレス型モード・ネットワーク・プロトコル (Connectionless-Mode Network Protocol)

CPU 中央演算処理装置 (central processing unit)

CRC 巡回冗長検査 (cyclic redundancy check)

CRS 構成報告書サーバー（configuration report server）

CTS 送信可 (clear to send)

CUD 起呼ユーザー・データ (call user data)

DAF 宛先アドレス・フィルター (destination address filtering)

DB データベース (database)

DBsum
データベース要約 (database summary)

DCD データ・チャネル受信回線信号検出器 (data channel received line signal detector)

DCE データ回線終端装置 (data circuit-terminating equipment)

DCS 直接接続サーバー (Directly connected server)

DDLC デュアル・データ・リンク制御装置 (dual data-link controller)

DDN 国防データ・ネットワーク (Defense Data Network)

DDP データグラム送達プロトコル (Datagram Delivery Protocol)

DDT 動的デバッグ・ツール (Dynamic Debugging Tool)

DHCP 動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)

dir 直接接続 (directly connected)

DL データ・リンク (data link)

DLC データ・リンク制御 (data link control)

DLCI データ・リンク接続識別子 (data link connection identifier)

DLS データ・リンク交換 (data link switching)

DLSw データ・リンク交換 (data link switching)

DMA 直接メモリー・アクセス (direct memory access)

DNA ディジタル・ネットワーク体系 (Digital Network Architecture)

DNCP DECnet プロトコル制御プロトコル (DECnet Protocol Control Protocol)

DNIC データ・ネットワーク識別子コード (Data Network Identifier Code)

DoD 米国国防総省 (Department of Defense)

DOS ディスク・オペレーティング・システム (Disk Operating System)

DR 指定ルーター (designated router)

DRAM 動的ランダム・アクセス・メモリー (Dynamic Random Access Memory)

DSAP 宛先サービス・アクセス・ポイント (destination service access point)

DSE データ交換装置 (data switching equipment)

DSE データ交換機 (data switching exchange)

DSR データ・セット・レディ (data set ready)

DSU データ・サービス装置 (data service unit)

DTE データ端末装置 (data terminal equipment)

DTR データ端末レディー (data terminal ready)

Dtype 宛先タイプ (destination type)

DVMRP
距離ベクトル・マルチキャスト・ルーティング・プロトコル (Distance Vector Multicast Routing Protocol)

E1 2.048 Mbps 伝送速度 (2.048 Mbps transmission rate)

EDEL 終了区切り文字 (end delimiter)

EDI エラー検出標識 (error detected indicator)

EGP 外部ゲートウェイ・プロトコル (Exterior Gateway Protocol)

EIA 米国電子工業会 (Electronics Industries Association)

ELAN エミュレート LAN (Emulated LAN)

ELAP EtherTalk リンク・アクセス・プロトコル (EtherTalk Link Access Protocol)

ELS イベント・ログ・システム (Event Logging System)

ESI エンド・システム識別子 (End system identifier)

EST 東部標準時 (Eastern Standard Time)

Eth イーサネット

fa-ga 機能アドレス・グループ・アドレス (functional address-group address)

FCS フレーム検査シーケンス (frame check sequence)

FECN 順方向明示的輻輳 (ふくそう) 通知 (forward explicit congestion notification)

FIFO 先入れ先出し (first in, first out)

FLT フィルター・ライブラリー (filter library)

FR フレーム・リレー (Frame Relay)

FRL フレーム・リレー (Frame Relay)

FTP ファイル転送プロトコル (File Transfer Protocol)

GMT グリニッジ標準時 (Greenwich Mean Time)

GOSIP
米国政府 OSI 調達仕様 (Government Open Systems Interconnection Profile)

GTE 一般電話会社 (General Telephone Company)

GWCON
ゲートウェイ・コンソール (Gateway Console)

HDLC ハイレベル・データ・リンク制御 (high-level data link control)

HEX 16 進法 (hexadecimal)

HPR 高性能ルーティング (high-performance routing)

HST TCP/IP ホスト・サービス (TCP/IP host services)

HTF ホスト・テーブル形式 (host table format)

IBD 統合ブート装置 (Integrated Boot Device)

ICMP インターネット制御メッセージ・プロトコル (Internet Control Message Protocol)

ICP インターネット制御プロトコル (Internet Control Protocol)

ID 識別 (identification)

IDP イニシアル・ドメイン・パート (Initial Domain Part)

IDP インターネット・データグラム・プロトコル (Internet Datagram Protocol)

IEEE 米国電気電子学会 (Institute of Electrical and Electronics Engineers)

Ifc# インターフェース番号 (interface number)

IGP 内部ゲートウェイ・プロトコル (interior gateway protocol)

InARP 逆アドレス解決プロトコル (Inverse Address Resolution Protocol)

IP インターネット・プロトコル (Internet Protocol)

IPCP IP 制御プロトコル (IP Control Protocol)

IPPN IP プロトコル・ネットワーク (IP Protocol Network)

IPX インターネットワーク・パケット交換 (Internetwork Packet Exchange)

IPXCP IPX 制御プロトコル (IPX Control Protocol)

ISDN サービス総合ディジタル網 (integrated services digital network)

ISO 国際標準化機構 (International Organization for Standardization)

Kbps キロビット/秒 (kilobits per second)

LAC L2TP ネットワーク・アクセス集線装置 (L2TP Network Access Concentrator)

LAN ローカル・エリア・ネットワーク (local area network)

LAPB リンク・アクセス・プロトコル (link access protocol-balanced)

LAT ローカル・エリア・トランスポート (local area transport)

LCP リンク制御プロトコル (Link Control Protocol)

LED 発光ダイオード (light-emitting diode)

LF 最大フレーム、改行 (largest frame; line feed)

LIS 論理 IP サブネット (Logical IP subnet)

LLC 論理リンク制御 (logical link control)

LLC2 論理リンク制御 2 (論理リンク制御 2)

LMI ローカル管理インターフェース (local management interface)

LNS L2TP ネットワーク・サーバー (L2TP Network Server)

LRM LAN 報告機構 (LAN reporting mechanism)

LS リンク状態 (link state)

LSA リンク状態公示 (link state advertisement)

LSB 最下位ビット (least significant bit)

LSI LAN ショートカット・インターフェース (LAN shortcuts interface)

LSreq リンク状態要求 (link state request)

LSrxl リンク状態再送リスト (link state retransmission list)

LU 論理装置 (logical unit)

MAC 媒体アクセス制御 (medium access control)

Mb メガビット (megabit)

MB メガバイト (megabyte)

Mbps メガビット/秒 (megabits per second)

MBps メガバイト/秒 (megabytes per second)

MC マルチキャスト (multicast)

MCF MAC フィルター (MAC filtering)

MIB 管理情報ベース (Management Information Base)

MIB II 管理情報ベース II (Management Information Base II)

MILNET
軍用ネットワーク (military network)

MOS マイクロ・オペレーティング・システム (Micro Operating System)

MOSDDT
マイクロ・オペレーティング・システム動的デバッグ・ツール (Micro Operating System Dynamic Debugging Tool)

MOSPF
マルチキャスト拡張付き最短パス最優先オープン (Open Shortest Path First with multicast extensions)

MSB 最上位ビット (most significant bit)

MSDU MAC サービス・データ単位 (MAC service data unit)

MRU 最大受信単位 (maximum receive unit)

MTU 最大伝送単位 (maximum transmission unit)

nak 否定応答 (not acknowledged)

NBMA 非同報通信マルチアクセス (Non-Broadcast Multiple Access)

NBP ネーム・バインディング・プロトコル (Name Binding Protocol)

NBR 近隣、ネイバー (neighbor)

NCP ネットワーク制御プロトコル (Network Control Protocol)

NCP ネットワーク・コア・プロトコル (Network Core Protocol)

NetBIOS
ネットワーク基本入出力システム (Network Basic Input/Output System)

NHRP ネクスト・ホップ解決プロトコル (Next Hop Resolution Protocol)

NIST 米国連邦情報技術局 (National Institute of Standards and Technology)

NPDU ネットワーク・プロトコル・データ単位 (Network Protocol Data Unit)

NRZ 非ゼロ復帰 (non-return-to-zero)

NRZI 非ゼロ復帰反転 (non-return-to-zero inverted)

NSAP ネットワーク・サービス・アクセス・ポイント (Network Service Access Point)

NSF 米国科学財団 (National Science Foundation)

NSFNET
米国科学財団ネットワーク (National Science Foundation NETwork)

NVCNFG
不揮発性構成 (nonvolatile configuration)

OPCON
オペレーター・コンソール (Operator Console)

OSI 開放型システム間相互接続 (open systems interconnection)

OSICP
OSI 制御プロトコル (OSI Control Protocol)

OSPF 最短パス最優先オープン (Open Shortest Path First)

OUI 組織固有識別子 (organization unique identifier)

PC パーソナル・コンピューター (personal computer)

PCR ピーク・セル速度 (peak cell rate)

PDN 公衆データ網 (public data network)

PING パケット・インターネット・グローパー (packet internet groper)

PDU プロトコル・データ単位 (protocol data unit)

PID プロセス識別 (process identification)

P-P ポイント・ポイント (Point-to-Point)

PPP ポイント・ポイント・プロトコル (Point-to-Point Protocol)

PROM プログラム式読み取り専用メモリー (programmable read-only memory)

PU 物理装置 (physical unit)

PVC パーマネント・バーチャル・サーキット (permanent virtual circuit)

RAM ランダム・アクセス・メモリー (random access memory)

RD ルート記述子 (route descriptor)

REM リング・エラー監視 (ring error monitor)

REV 受信 (receive)

RFC Request for Comments (コメント要求)

RI リング標識、ルーティング情報 (ring indicator; routing information)

RIF ルーティング情報フィールド (routing information field)

RII ルーティング情報標識 (routing information indicator)

RIP ルーティング情報プロトコル (Routing Information Protocol)

RISC 縮小命令セット・コンピューター (reduced instruction-set computer)

RNR 受信不可 (receive not ready)

ROM 読み取り専用メモリー (read-only memory)

ROpcon
リモート・オペレーター・コンソール (Remote Operator Console)

RPS リング・パラメーター・サーバー (ring parameter server)

RTMP ルーティング・テーブル保守プロトコル (Routing Table Maintenance Protocol)

RTP ルーティング更新プロトコル (RouTing update Protocol)

RTS 送信要求 (request to send)

Rtype ルート・タイプ (route type)

rxmits 再送 (retransmissions)

rxmt 再送する (retransmit)

SAF 送信元アドレス・フィルター (source address filtering)

SAP サービス・アクセス・ポイント (Service access point)

SAP サービス公示プロトコル (Service Advertising Protocol)

SCR 持続セル速度 (Sustained cell rate)

SCSP サーバー・キャッシュ同期プロトコル (Server Cache Synchronization Protocol)

sdel 開始区切り文字 (start delimiter)

SDLC SDLC リレー、同期データ・リンク制御 (SDLC relay, synchronous data link control)

seqno シーケンス番号 (sequence number)

SGID サーバー・グループ ID (sever group id)

SGMP シンプル・ゲートウェイ監視プロトコル (Simple Gateway Monitoring Protocol)

SL シリアル・ライン (serial line)

SMP 待機モニター・プレゼント (standby monitor present)

SMTP シンプル・メール転送プロトコル (Simple Mail Transfer Protocol)

SNA システム・ネットワーク体系 (Systems Network Architecture)

SNAP サブネットワーク・アクセス・プロトコル (Subnetwork Access Protocol)

SNMP シンプル・ネットワーク管理プロトコル (Simple Network Management Protocol)

SNPA サブネットワーク接続ポイント (subnetwork point of attachment)

SPF OSPF エリア内ルート (OSPF intra-area route)

SPE1 OSPF 外部ルート・タイプ 1 (OSPF external route type 1)

SPE2 OSPF 外部ルート・タイプ 2 (OSPF external route type 2)

SPIA OSPF エリア間ルート・タイプ (OSPF inter-area route type)

SPID サービス・プロファイル ID (service profile ID)

SPX 順次パケット交換 (Sequenced Packet Exchange)

SQE 信号品質エラー (signal quality error)

SRAM 静的ランダム・アクセス・メモリー (static random access memory)

SRB ソース・ルーティング・ブリッジ (source routing bridge)

SRF 特定ルート・フレーム (specifically routed frame)

SRLY SDLC リレー (SDLC relay)

SRT ソース・ルーティング透過 (source routing transparent)

SR-TB
ソース・ルーティング - 透過型ブリッジ (source routing-transparent bridge)

STA 静的 (static)

STB スパンニング・ツリー・ブリッジ (spanning tree bridge)

STE スパンニング・ツリー探索 (spanning-tree explorer)

STP シールド付き対より線、スパンニング・ツリー・プロトコル (shielded twisted pair; spanning tree protocol)

SVC スイッチド・バーチャル・サーキット (switched virtual circuit)

TB 透過型ブリッジ (transparent bridge)

TCN トポロジー変更通知 (topology change notification)

TCP 伝送制御プロトコル (Transmission Control Protocol)

TCP/IP
伝送制御プロトコル/インターネット・プロトコル (Transmission Control Protocol/ Internet Protocol)

TEI 端末終端点識別子 (terminal endpoint identifier)

TFTP トリビアル・ファイル転送プロトコル (Trivial File Transfer Protocol)

TKR トークンリング (token ring)

TMO タイムアウト (timeout)

TOS サービスのタイプ (type of service)

TSF 透過スパンニング・フレーム (transparent spanning frames)

TTL 活動時間 (time to live)

TTY テレタイプライター (teletypewriter)

TX 送信 (transmit)

UA 非番号制確認 (unnumbered acknowledgment)

UDP ユーザー・データグラム・プロトコル (User Datagram Protocol)

UI 非番号制情報 (unnumbered information)

UTP シールドなし対より線 (unshielded twisted pair)

VCC バーチャル・チャネル・コネクション (Virtual Channel Connection)

VINES バーチャル・ネットワーキング・システム (VIrtual NEtworking System)

VIR 可変情報速度 (variable information rate)

VL バーチャル・リンク (virtual link)

VNI バーチャル・ネットワーク・インターフェース (Virtual Network Interface)

VR バーチャル・ルート (virtual route)

WAN 広域ネットワーク (wide area network)

WRS WAN 復元/再ルート (WAN restoral/reroute)

X.25 パケット交換網 (packet-switched networks)

X.251 X.25 物理レイヤー (X.25 physical layer)

X.252 X.25 フレーム・レイヤー (X.25 frame layer)

X.253 X.25 パケット・レイヤー (packet layer)

XID 交換 ID (exchange identification)

XNS Xerox ネットワーク・システム (Xerox Network Systems)

XSUM チェックサム (checksum)

ZIP AppleTalk ゾーン情報プロトコル (AppleTalk Zone Information Protocol)

ZIP2 AppleTalk ゾーン情報プロトコル 2 (AppleTalk Zone Information Protocol 2)

ZIT ゾーン情報テーブル (Zone Information Table)

用語集

この用語集には、以下からの用語および定義が含まれています。

- *American National Standard Dictionary for Information Systems*、ANSI X3.172-1990 (米国規格協会 (ANSI) が 1990 年に著作権を取得)。この複写版が米国規格協会 (ANSI: 11 West 42nd Street, New York, New York 10036)から発売されています。定義の後に記号 (A) を付けて出典を示してあります。
- ANSI/EIA Standard--440-A、*Fiber Optic Terminology*。この複写版が米国電子工業会 (2001 Pennsylvania Avenue, N.W., Washington, DC 20006) から発売されています。定義の後に記号 (E) を付けて出典を示してあります。
- *Information Technology Vocabulary*。国際標準化機構および国際電気標準会議の第 1 合同技術委員会第 1 分科会 (ISO/IEC JTC1/SC1) によって編さんされたものです。この語い集の刊行部分から転載した定義については、その後に記号 (I) を付けて示してあります。また、ISO/IEC JTC1/SC1 で編さん中の国際規格草案、分科会草案、および作業文書から採用した定義については、その後に記号 (T) を付けて、SC1 の加盟各国諸団体間で最終合意がなされていないことを示してあります。
- *IBM Dictionary of Computing* , New York: McGraw-Hill, 1994
- Internet Request for Comments: 1208、*Glossary of Networking Terms*
- Internet Request for Comments: 1392、*Internet Users' Glossary*
- *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

この用語集では、以下の形で相互参照しています。

と対比:
反対の意味または実質的に異なる意味をもつ用語を示します。

の同義語:
この用語集の該当箇所に記述されている、優先的に使用してほしい、同じ意味をもつ用語を示します。

と同義:
逆方向参照として、定義の対象となっている用語から、同じ意味をもつ他の用語をすべて参照します。

を参照:
一部の語 (特に最後の語) が同じ複数語からなる用語を参照します。

も参照:
関連する意味 (同義ではない) をもつ用語を参照します。

A

AAL. ATM アダプテーション・レイヤー (ATM Adaptation Layer)。ヘッダーを追加/除去し、セルへ/からのデータを細分化/再組み立てすることにより、ATM ネットワークへ/からのユーザー・データを適応させるレイヤー。

AAL-5. ATM アダプター・レイヤー 5 (ATM Adaptation Layer 5)。複数ある標準 AAL の 1 つ。 AAL-5 はデータ通信用に設計されたもので、LAN エミュレーションおよびクラシカル IP によって使用される。

抽象構文 (abstract syntax). データ伝送に必要な特性はすべて含んでいるが、その他の明細 (たとえば、特定のコンピューター・アーキテクチャーに依存する明細など) は省略 (抽象化) されているデータ仕様。*抽象構文表記法 (ASN.1) (abstract syntax notation 1 (ASN.1))* および*基本符号化規則 (BER) (basic encoding rules (BER))* も参照。

抽象構文表記法 1 (ASN.1) (abstract syntax notation 1 (ASN.1)). 次の標準で指定されている抽象構文の開放型システム間相互接続 (OSI) 方式。

- ITU-T 勧告 X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T 勧告 X.680 (1994) | ISO/IEC 8824-1: 1994

基本符号化規則 (BER) (basic encoding rules (BER)) も参照。

ACCESS. シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理ノードがオブジェクトに対して提供する最小レベルのサポートを定義する、管理情報ベース (MIB) モジュール内の文節。

確認応答 (acknowledgment). (1) 受信側が送信側に肯定応答として確認応答文字を伝送すること。 (T) (2) 送信された項目が受信されたことを示すこと。

アクティブ (active). (1) 運用可。 (2) 別のノードまたは装置に接続された、またはそれへの接続が利用可能なノードまたは装置に関する用語。

アクティブ・モニター (active monitor). トークンリング・ネットワークにおいて、一度に 1 つのリング・ステーションによって実行される機能で、トークンの伝送を開始し、トークン誤り回復機能を提供する。現在のアクティブ・モニターに障害が起こった場合、リング上の任意のアクティブ・アダプターが、アクティブ・モニター機能を提供することができる。

アドレス (address). データ通信において、通信ネットワークに接続された各装置、ワークステーション、またはユーザーに割り当てられる固有のコード。

アドレス・マッピング・テーブル (AMT) (address mapping table (AMT)). 現在のノード・アドレスとハードウェア・アドレスのマッピングを提供する、AppleTalk ルーター内に維持されているテーブル。

アドレス・マスク (address mask). インターネット・サブネットワークにおいて、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットを識別するために使用される、32 ビットのマスク。サブネット・マスク *(subnet mask)* およびサブネットワーク・マスク *(subnetwork mask)* と同義。

アドレス解決 (address resolution). (1) ネットワーク・レイヤー・アドレスを媒体特有アドレスにマッピングする方法。 (2) *アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP))* および *AppleTalk アドレス解決プロトコル (AARP) (AppleTalk Address Resolution Protocol (AARP))* も参照。

アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP)). (1) インターネット・プロトコルにおいて、サポートされる大都市圏ネットワークやローカル・エリア・ネットワーク (イーサネットやトークンリングなど) が使用するアドレスに、IP アドレスを動的にマップするプロトコル。 (2) *逆アドレス解決プロトコル (RARP) (Reverse Address Resolution Protocol (RARP))* も参照。

アドレッシング (addressing). データ通信において、端末局がデータの送信先の端末局を選択する方法。

隣接ノード (adjacent nodes). 他のノードとは接続していない少なくとも 1 つのパスによって相互に接続されている 2 つのノード。 (T)

管理ドメイン (Administrative Domain). 1 つの管理機関によって管理される、ホストとルーターおよび相互接続ネットワークの集合。

拡張対等通信ネットワーキング機能 (Advanced Peer-to-Peer Networking) (APPN). SNA の拡張機能で、次の特長を備えている。(a) 重大な階層間の依存関係を回避することによって、単一点の障害の影響を分離できるようにした、分散ネットワーク制御の機能強化。(b) 接続、再構成、および柔軟なルート選択を容易に実現できる、動的なネットワーク・トポロジー情報の交換。(c) ネットワークの資源の動的定義。(d) 資源の登録およびディレクトリー検索の自動化。 APPN は、エンド・ユーザー・サービス向けの LU 6.2 同位間通信機能をネットワークの制御に拡張し、LU 2、LU 3、および LU 6.2 を含む複数の LU タイプをサポートする。

拡張対等間通信ネットワーキング機能 (APPN) エンド・ノード (Advanced Peer-to-Peer Networking (APPN) end node). 広範囲のエンド・ユーザー・サービスを提供し、そのローカル・コントロール・ポイント (CP) と隣接するネットワーク・ノード内の CP との間のセッションをサポートするノード。このノードは、これらのセッションを使用して、隣接 CP (ネットワーク・ノード・サーバー) に資源を動的に登録し、ディレクトリー検索要求を送受信し、管理サービスを受ける。 APPN エンド・ノードは、サブエリア・ネットワークに周辺ノードまたは他のエンド・ノードとして接続することもできる。

拡張対等間通信ネットワーキング機能 (APPN) ネットワーク (Advanced Peer-to-Peer Networking (APPN) network). 相互接続されたネットワーク・ノードとそれらのクライアント・エンド・ノードの集合。

拡張対等間通信ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node). 広範囲のエンド・ユーザー・サービスを提供するノードで、次のものを提供することができる。

- 分散ディレクトリー・サービス (中央ディレクトリー・サーバーへの領域の資源の登録を含む)
- トポロジー・データベースは他の APPN ネットワーク・ノードと交換し、そのネットワーク・ノード内のネットワーク・ノードが、要求されたサービス・クラスに基づいて LU-LU セッションの最適ルートを選択できるようにする。
- そのローカル LU とクライアント・エンド・ノードのセッション・サービス
- APPN ネットワーク・ノードの中間ルーティング・サービス

拡張対等間通信ネットワーキング機能 (APPN) ノード (Advanced Peer-to-Peer Networking (APPN) node). APPN ネットワーク・ノードまたは APPN エンド・ノード。

エージェント (agent). エージェントの役割を果たすシステム。

アラート (alert). 問題または切迫した問題を識別するためにネットワーク・ノード内の管理サービス中心拠点に送られるメッセージ。

全ステーション・アドレス (all-stations address). 通信において、*同報通信アドレス (broadcast address)* の同義語。

米国規格協会 (ANSI) (American National Standards Institute (ANSI)). 認定組織が米国の自主業界標準を作成して維持するための手順を決める、生産者、消費者、および一般の関係団体から構成される組織。 (A)

アナログ (analog). (1) 連続的に変化する物理量から構成されるデータに関する用語。 (A) (2) *ディジタル (digital)* と対比。

AppleTalk. Apple Computer, Inc. によって開発されたネットワーク・プロトコル。このプロトコルは、ネットワーク上の装置を相互接続するために使用される。装置は、Apple 製品と非 Apple 製品を混合して使用できる。

AppleTalk アドレス解決プロトコル (AARP) (AppleTalk Address Resolution Protocol (AARP)). AppleTalk ネットワーク・ノードにおいて、(a) AppleTalk ノード・アドレスをハードウェア・アドレスに変換し、(b) 複数のプロトコルをサポートするネットワーク・ノード内のアドレッシングの矛盾を調整するプロトコル。

AppleTalk トランザクション・プロトコル (ATP) (AppleTalk Transaction Protocol (ATP)). AppleTalk ネットワーク・ノードにおいて、ゾーン情報を得るためにゾーン情報プロトコル (ZIP) にアクセスするホストに対して、クライアント/サーバー要求・応答機能を提供するプロトコル。

APPN ネットワーク (APPN network). *拡張対等間通信ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network)* を参照。

APPN ネットワーク・ノード (APPN network node). *拡張同位間通信ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node)* を参照。

任意 MAC アドレッシング (AMA) (arbitrary MAC addressing (AMA)). DECnet 体系において、一元管理アドレスとローカル管理アドレスをサポートする、 DECnet フェーズ IV-Prime によって使用されるアドレッシング機構。

エリア、区域 (area). インターネットおよび DECnet ルーティング・プロトコルにおいて、ネットワーク・ノードの通信事業者の定義によってグループ化された、ネットワーク・ノードまたはゲートウェイのサブセット。各エリアは自己完結型で、あるエリアのトポロジーは他のエリアからは見えない。

非同期 (ASYNC) (asynchronous (ASYNC)). 共通タイミング信号のような特定の事象の発生に依存しない 2 つ以上のプロセス。 (T)

ATM. 非同期転送モード (Asynchronous Transfer Mode)。セル交換を基礎とした、コネクション型高速ネットワーキング・テクノロジー。

ATMARP. クラシカル IP 内の ARP。

接続ユニット・インターフェース (attachment unit interface (AUI)). ローカル・エリア・ネットワークにおいて、媒体接続ユニットとデータ・ステーション内のデータ端末装置間のインターフェース。 (I) (A)

属性値対 (Attribute Value Pair) (AVP). メッセージのタイプと本体を符号化する汎用方式。この方式によって、L2TP は相互運用性が許容されると同時に、拡張性が最大化される。

属性値ペア (AVP) (Attribute Value Pair (AVP)). メッセージ・タイプおよび本文をコード化する一律的な方法。この方式は、 L2TP の相互運用性を可能にすると同時に、拡張性を最大化する。

認証障害 (authentication failure). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、要求側クライアントが SNMP コミュニティーのメンバーでない場合に、認証エンティティーが生成するトラップ。

自律システム (autonomous system). TCP/IP において、1 つの管理機関の下にあるネットワーク・ノードとルーターの集まり。このようなネットワーク・ノードとルーターは緊密に協力し、自ら選択した内部ゲートウェイ・プロトコルを使用して、相互にネットワークの到達可能性とルーティングの情報を伝送する。

自律システム番号 (autonomous system number). TCP/IP において、IP アドレスの割り当てを行うのと同じ中央電気通信事業者が自律システムに割り当てる番号。自律システム番号により、自動ルーティング・アルゴリズムは、自律システムを区別することができる。

B

バックボーン (backbone). (1) ローカル・エリア・ネットワークのマルチ・ブリッジ・リング構成において、ブリッジまたはルーターを用いてリングが接続されている高速リンク。バックボーンは、バスまたはリングとして構成することができる。 (2) 広域ネットワーク・ノードにおいて、ノードまたはデータ交換機 (DSE) が接続されている高速リンク。

バックボーン・ネットワーク (backbone network). より小規模の (通常は、より低速の) ネットワーク・ノードを接続する中央のネットワーク。バックボーン・ネットワークは通常、相互接続するネットワークよりもはるかに高容量の通信ネットワーク、あるいは公用パケット交換データグラム・ネットワークのような広域ネットワーク (WAN) である。

バックボーン・ルーター (backbone router). (1) エリア間でデータを転送するのに使用されるルーター。 (2) ネットワーク・ノードをより大規模なネットワーク・ノードに接続するのに使用される、一連のルーターの中の 1 つ。

帯域幅 (Bandwidth). 光リンクの帯域幅は、リンクが情報を運ぶ容量を表し、光リンクがサポートできる最大ビット・レートを示す。

基本伝送単位 (BTU) (basic transmission unit (BTU)). SNA において、パス制御コンポーネント間で受け渡されるデータと制御情報の単位。 BTU は、1 つまたは複数のパス情報単位 (PIU) から構成される。

ボー (baud). 非同期伝送において、1 秒当りの変調速度の単位。つまり、サイクル間隔が 20 ミリ秒の場合、変調速度は 50 ボーになる。 (A)

ブートストラップ (bootstrap). (1) コンピューター・プログラムが完全に記憶装置に入り終わるまで、後に続く命令をロードして実行させる一連の命令。 (T) (2) それ自体の働きによって望ましい状態に到達するように設計された技法または装置。たとえば、最初の幾つかの命令が、残りの命令を入力装置からコンピューターに読み込むようになっている機械ルーチン。 (A)

ボーダー・ゲートウェイ・プロトコル (BGP) (Border Gateway Protocol (BGP)). 領域 (ドメイン) と自律システムの間で使用されるインターネット・プロトコル (IP) ルーティング・プロトコル。

ボーダー・ルーター (border router). インターネット通信において、自律システムの端に位置し、別の自律システムの端にあるルーターと通信するルーター。

ブリッジ (bridge). 複数の LAN を (ローカルまたはリモート側で) 相互接続する機能を持った装置で、同じ論理リンク制御プロトコルを使用するが、異なる媒体アクセス制御プロトコルを使用することができる。ブリッジは、媒体アクセス制御 (MAC) アドレスに基づいてフレームを別のブリッジに転送する。

ブリッジ識別子 (bridge identifier). スパンニング・ツリー・プロトコルで使用される、最下位ポート識別子をもつポートの MAC アドレスとユーザー定義の値から構成される 8 バイトのフィールド。

ブリッジング (bridging). LAN では、フレームを 1 つの LAN セグメントから別のセグメントに転送すること。着側は、フレーム・ヘッダーの着信アドレス・フィールドに符号化された媒体アクセス制御 (MAC) サブレイヤー・アドレスによって指定される。

同報通信 (broadcast). (1) すべての着信先に同じデータを伝送すること。 (T) (2) 複数の着信先に同時にデータを伝送すること。 (3) マルチキャスト *(multicast)* と対比。

同報通信アドレス (broadcast address). 通信において、リンク上のすべてのステーションに共通のアドレスとして確保されているステーション・アドレス (8 桁の 1 で構成)。全ステーション・アドレス *(all-stations address)* と同義。

C

キャッシュ (cache). (1) 主記憶装置から読み出した、プロセッサーが次に必要になる可能性がある命令とデータのコピーを入れておくために使用される、主記憶装置より小さくて高速の特殊用途バッファー記憶装置。 (T) (2) 頻繁にアクセスされる命令とデータを入れておくバッファー記憶装置。アクセス時間を短縮するために使用される。 (3) ディレクトリーの検索速度を上げるために、頻繁に使用されるディレクトリー情報を入れておくことができる、ネットワーク・ノード内のディレクトリー・データベースのオプション部。 (4) キャッシュに入れる、または保管すること。

発呼要求パケット (call request packet). (1) 呼のための接続を確立することを要求するために、データ端末装置 (DTE) がネットワーク全体に伝送する発呼監視パケット。 (2) X.25 通信において、ネットワークを通して呼設定を要求するために、DTE によって伝送される発呼監視パケット。

標準アドレス (canonical address). LAN において、トークンリングまたはイーサネット・アダプターの媒体アクセス制御 (MAC) アドレスを伝送するための IEEE 802.1

形式。標準形式では、各アドレス・バイトの最下位 (右端) ビットが最初に伝送される。*非標準アドレス (noncanonical address)* と対比。

キャリア (carrier). 通信システムを介して伝送される情報を運ぶ信号によって変化する電波、電磁波、またはパルス列。 (T)

キャリア検出 (carrier detect). *受信回線信号検出器 (RLSD) (received line signal detector (RLSD))* の同義語。

キャリア・センス (carrier sense). ローカル・エリア・ネットワークにおいて、別のステーションが伝送中であるかどうかを検出する、データ・ステーションの機能。 (T)

搬送波検知多重アクセス/衝突検出 (CSMA/CD) (carrier sense multiple access with collision detection (CSMA/CD)). キャリア・センスを必要とするプロトコル。送信側データ・ステーションは、伝送中に別の信号を検出すると、送信を停止し、ジャム信号を送り、可変時間待ってから再試行する。 (T) (A)

CCITT. 国際電信電話諮問委員会 (International Telegraph and Telephone Consultative Committee)。 以前は国際電気通信連合 (ITU) の組織であったが、 1993 年 3 月 1 日に ITU は再編成され、標準化の任務は、電気通信連合の電気通信標準化部門 (ITU-TS) という名前の下部組織に移管された。 『CCITT』 という用語は、再編成の前に承認さた勧告を表すのに引き続き使用される。

チャネル (channel). (1) 信号を送ることができるパス。たとえば、データ・チャネル、出力チャネル。 (A) (2) 主記憶装置とローカル周辺装置との間のデータ転送を扱う、処理装置によって制御される装置。

チャネル・サービス・ユニット (CSU) (channel service unit (CSU)). ディジタル・ネットワークへのインターフェースを提供する装置。 CSU は、チャネル帯域幅内で信号の効率を一定に保つ伝送路調整 (等化) 機能、バイナリー・パルス・ストリームを構成する信号再編成機能、および CSU と通信事業体のオフィス・チャネル装置間のテスト信号伝送を含めたループバック・テスト機能を提供する。*データ・サービス装置 (DSU) (data service unit (DSU))* も参照。

チェックサム (checksum). (1) グループに関連し、検査目的で使用される、データのグループの合計。 (T) (2) 誤り検出において、ブロック内の全ビットを対象とする。書き込まれて計算された合計に一致しない場合は、誤りが指示される。 (3) ディスケットにおいて、誤り検出の目的でセクターに書き込まれるデータ。計算されたチェックサムが、セクターに書き込まれたデータのチェックサムに一致しない場合は、不良セクターを示している。データは、数字またはチェックサムの計算では数字とみなされる他の文字列のいずれかである。

サーキット交換 (circuit switching). (1) 必要に応じて、2 つ以上のデータ端末装置 (DTE) を接続し、その接続が解放されるまで、それらの装置間のデータ回線を専用に使用することができるプロセス。 (I) (A) (2) *回線交換 (line switching)* と同義。

クラス A ネットワーク (class A network). インターネット通信において、IP アドレスの上位 (最上位) ビットが 0 に設定され、ホスト ID が下位の 3 オクテットを占めるネットワーク。

クラス B ネットワーク (class B network). インターネット通信において、IP アドレスの 2 つの上位 (最上位と最上位の次の) ビットがそれぞれ 1 と 0 に設定され、ホスト ID が下位の 2 オクテットを占めるネットワーク。

サービス・クラス (COS) (class of service (COS)). セッションのパートナー間のルートを確立するために使用される一組の特性（ルートのセキュリティー、伝送の優先順位、帯域幅など)。サービス・クラスは、セッションの開始プログラムによって指定されたモード名から導出される。

クライアント (client). (1) サーバーから共用サービスを受け取る機能単位。 (T) (2) ユーザーのこと。

クライアント/サーバー (client/server). 通信において、一方の側のプログラムが相手側のプログラムに要求を送信して応答を待つという、分散データ処理における対話のモデル。要求側プログラムをクライアントといい、応答側プログラムをサーバーという。

クロッキング、刻時 (clocking). (1) 2 進データ同期通信において、クロック・パルスを使用して、データおよび制御文字の同期を制御すること。 (2) 一定時間に通信回線上で送信するデータ・ビット数を制御する方法。

衝突 (collision). チャネル上の同時伝送によって生じる望ましくない状態。 (T)

衝突検出 (collision detection). 搬送波検知多重アクセス/衝突検出 (CSMA/CD) において、2 台以上のステーションが同時に伝送していることを示す信号。

認定情報速度 (Committed information rate). ネットワークが送達することに同意した、ビットで表されたデータの最大量。

コミュニティー (community). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、エンティティー間の管理関係。

コミュニティー名 (community name). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、コミュニティーを識別するオクテット列。

圧縮 (compression). (1) レコードまたはブロックの長さを短縮するために、ギャップ、空のフィールド、冗長要素、および不必要なデータを除去する処理。 (2) メッセージまたは記録を表すのに使用するビット数を減らすために符号化すること。

構成 (configuration). (1) 情報処理システムのハードウェアとソフトウェアを編成し、相互に接続する方法。 (T) (2) システム、サブシステム、またはネットワークを構成する装置とプログラム。

構成データベース (CDB) (configuration database (CDB)). 1 つまたは複数の装置の構成パラメーターを保管するデータベース。構成プログラムを使用して作成し、更新する。

構成ファイル (configuration file). システム装置またはネットワーク・ノードの特性を指定するファイル。

構成パラメーター (configuration parameter). 構成定義内の変数で、その値により、あるプロダクトと同じネットワーク・ノード内の別のプロダクトの特性を表したり、プロダクト自体の特性を定義する。

構成報告書サーバー (CRS) (configuration report server (CRS)). IBM トークンリング・ネットワーク・ブリッジ・プログラムにおいて、 LAN ネットワーク・マネージャー (LNM) からのコマンドを受け入れて、ステーション情報を入手する、ステーション・パラメーターを設定する、およびステーションをリングから除去するサーバー。また、このサーバーは、リング上のステーションによって生成された構成報告書の収集および転送も行う。構成報告書には、新しいアクティブ・モニター報告書および最近隣アクティブ・アップストリーム (NAUN) 報告書が含まれる。

輻輳 (ふくそう) (congestion). *ネットワーク輻輳 (ふくそう) (network congestion)* を参照。

接続、コネクション (connection). データ通信において、情報を伝達するために装置間に設定される関係。 (I) (A)

コントロール・ポイント (CP) (control point (CP)). (1) ノードの資源を管理する、APPN ノードまたは LEN ノードのコンポーネント。 APPN ノードでは、CP は他の APPN ノードとの CP-CP セッションを行うことができる。 APPN ネットワーク・ノードでは、CP は APPN ネットワーク・ノードの隣接エンド・ノードへのサービスも提供する。 (2) ノードの資源を管理し、オプションでネットワークの他のノードにサービスを提供する、該当ノードのコンポーネント。その例としては、タイプ 5 サブエリア・ノードのシステム・サービス・コントロール・ポイント (SSCP)、APPN ネットワーク・ノードのネットワーク・ノード・コントロール・ポイント (NNCP)、および APPN または LEN エンド・ノードのエンド・ノード・コントロール・ポイント (ENCP) がある。 SSCP および NNCP は、他のノードへのサービスを提供することができる。

コントロール・ポイント管理サービス (CPMS) (control point management services (CPMS)). 管理サービス機能から構成され、問題管理、効率および会計管理、変更管理、および構成管理を実行するのに役立つ機能を提供する、コントロール・ポイントの構成要素。 CPMS によって提供される機能には、システム資源をテストするために要求を物理装置管理サービス (PUMS) に送信する機能、システム資源に関する統計情報 (たとえば、誤りデータやパフォーマンス・データ) を PUMS から収集する機能、およびテスト結果と収集されたシステム資源に関する統計情報を分析および表示する機能が含まれる。問題判別およびパフォーマンス監視を分析および表示する機能は、複数の CPMS 間に分散することができる。

コントロール・ポイント管理サービス単位 (CP−MSU) (control point management services unit (CP-MSU)). 管理サービス機能セット間を流れる、管理サービス・データが入っているメッセージ単位。このメッセージ単位は、汎用データ・ストリーム (GDS) 形式である。*管理サービス単位 (MSU) (management services unit (MSU))* および*ネットワーク・ノード管理ベクトル移送 (NMVT) (network management vector transport (NMVT))* も参照。

D

D ビット (D-bit). 送達確認ビット (Delivery-confirmation bit)。 X.25 通信において、受信側からのエンド・エンド確認 (送達確認) が必要な場合に 1 にセットされる、データ・パケットまたは発呼要求パケット内のビット。

デーモン (daemon). 標準サービスを行うために無人で実行されるプログラム。デーモンには、そのタスクを実行するために自動的に起動されるものと、定期的に動作するものがある。

データ・キャリア検出 (DCD) (data carrier detect (DCD)). *受信回線信号検出器 (RLSD) (received line signal detector (RLSD))* の同義語。

データ回線 (data circuit). (1) 両方向データ通信の手段を提供する、関連付けられた一対の送信チャネルと受信チャネル。 (I) (2) SNA においては、*リンク接続 (link*

connection) の同義語。 (3) *物理サーキット (physical circuit)* およびバーチャル・サーキット *(virtual circuit)* も参照。

注:

1. データ交換装置相互間では、データ回線は、データ交換装置で使用するインターフェースのタイプによって、データ回線終端装置 (DCE) を含むことがある。
2. データ端末とデータ交換装置またはデータ集線装置との間では、データ回線は、データ装置側のデータ回線終端装置を含み、またデータ交換装置またはデータ集線装置側の DCE と類似の装置を含むことがある。

データ回線終端装置 (DCE) (data circuit-terminating equipment (DCE)). データ端末において、データ端末装置 (DTE) と回線の間で信号変換および符号化を行う装置。 (I)

注:

1. DCE は、独立した機器であるか、DTE または中間装置に組み込まれている。
2. DCE は、伝送路のネットワーク・ノード側で一般的に必要とされる機能を果す。

データ・リンク接続識別子 (DLCI) (data link connection identifier (DLCI)). フレーム・リレー・サブポート、またはフレーム・リレー・ネットワークの PVC セグメントの数字識別子。 1 つのフレーム・リレー・ポート内の各サブポートは、固有の DLCI を持っている。下表 (米国規格協会 (ANSI) 標準 T1.618 および国際電信電話諮問委員会 (ITU-T/CCITT) 標準 Q.922 から抜粋) は、特定の DLCI 値に関連する機能を示している。

DLCI 値	機能
0	チャネル内信号
1-15	未使用
16-991	フレーム・リレー接続手順を用いて割り当て
992-1007	フレーム・リレー・ベアラー・サービスのレイヤー 2 管理
1008-1022	未使用
1023	チャネル内のレイヤー管理

データ・リンク制御 (DLC) (data link control (DLC)). データ・リンク (SDLC リンクまたはトークンリングなど) 上のノードが、情報を正確に交換するために使用する規則。

データ・リンク制御 (DLC) レイヤー (data link control (DLC) layer). SNA において、2 つのノード間のリンクを介するデータ転送をスケジュールし、そのリンクの誤り制御を行うリンク・ステーションから構成されるレイヤー。データ・リンク制御の例としては、ビット順次リンク接続の SDLC や、システム/370 チャネルのデータ・リンク制御がある。

注: 通常、DLC レイヤーは物理トランスポート機構から独立しており、上位レイヤーに送るデータの保全性が確保される。

データ・リンク・レイヤー (data link layer). 開放型システム間相互接続参照モデルにおいて、ネットワーク・レイヤー内のエンティティーが通信リンクを通して相互にデータを転送するサービスを提供するレイヤー。データ・リンク・レイヤーは、物理レイヤーで発生した誤りを検出し、訂正する。 (T)

データ・リンク・レベル (data link level). (1) データ・ステーションの階層構造において、ハイレベル論理とデータ・リンクの制御を維持するデータ・リンクとの間の、制御または処理論理の概念的レベル。データ・リンク・レベルは、送信ビットの挿入および受信ビットの削除、アドレス・フィールドおよび制御フィールドの解釈、コマンドとレスポンスの生成、送信、および解釈、フレーム・チェック・シーケンスの計算と解釈といった機能を実行する。*パケット・レベル (packet level)* および *物理レベル (physical level)* も参照。 (2) X.25 通信において、*フレーム・レベル (frame level)* の同義語。

データ・リンク交換 (DLSw) (data link switching (DLSw)). IEEE 802.2 論理リンク制御 (LLC) タイプ 2 を使用する、ネットワーク・プロトコルの伝達方法。 SNA および NetBIOS は、LLC タイプ 2 を使用する例である。*カプセル化 (encapsulation)* およびスプーフィング *(spoofing)* も参照。

データ・パケット (data packet). X.25 通信において、DTE/DCE インターフェースのバーチャル・サーキット上でユーザー・データを伝送するために使用されるパケット。

データ・サービス装置 (DSU) (data service unit (DSU)). データ端末装置にディジタル・データ・サービス・インターフェースを直接提供する装置。 DSU は、ループ等化機能、リモートおよびローカル・テスト機能、および標準 EIA/CCITT インターフェース機構を提供する。

データ・セット・レディ (DSR) (data set ready (DSR)). *DCE レディー (DCE ready)* の同義語。

データ交換機 (DSE) (data switching exchange (DSE)). 1 つの場所に設置され、回線交換、メッセージ交換、およびパケット交換などの交換機能を提供する装置。 (I)

データ端末装置 (DTE) (data terminal equipment (DTE)). データ・ステーションにおいて、データ送信側、データ受信側、またはその両方として動作する部分。 (I) (A)

データ端末レディー (DTR) (data terminal ready (DTR)). EIA 232 プロトコルで使用されるモデムへの信号。

データ転送速度 (data transfer rate). データ伝送システムの通信している装置の間を単位時間に通過するビット、文字、またはブロックの数の平均値。 (I)

注:

1. 速度は、秒、分、または時間当たりのビット数、文字数、またはブロック数で表す。
2. 通信する装置、たとえば、モデム、中間装置、または送信側と受信側を示す必要がある。

データグラム (datagram). (1) パケット交換において、発信データ端末装置 (DTE) から着信 DTE までのルーティングに必要な十分な情報を伝達し、前もって DTE とネットワーク・ノード間で情報交換をする必要がない、他のパケットから独立した自己完結型パケット。 (I) (2) TCP/IP においては、インターネット環境で受け渡される情報の基本単位。データグラムには、データの他に発信元アドレスと着信先アドレスが入っている。インターネット・プロトコル (IP) データグラムは、IP ヘッダーと後続のトランスポート・レイヤー・データによって構成される。 (3) *パケット (packet)* および *セグメント (segment)* も参照。

データグラム送達プロトコル (DDP) (Datagram Delivery Protocol (DDP)). AppleTalk ネットワーク・ノードおいて、インターネット・レイヤーのコネクションレス・ソケット間送達サービスによってネットワークの接続性を提供するプロトコル。

DCE レディー (DCE ready). EIA 232 標準において、ローカル・データ回線終端装置 (DCE) が通信チャネルに接続され、データ送信が可能になっていることを、データ端末装置 (DTE) に知らせる信号。データ・セット・レディー *(DSR) (data set ready (DSR))* と同義。

DECnet. 通常は資源の共用、分散計算、またはリモート・システム構成の目的で、Digital Equipment Corporation のシステムを相互連結するのに使用される、一連のソフトウェア・モジュール、データベース、およびハードウェア・コンポーネント動作を定義するネットワーク体系。 DECnet ネットワーク・ノードの実現方式は、ディジタル・ネットワーク体系 (DNA) モデルに準拠している。

デフォルト (default). 明示的に指定されていない場合に仮定される属性、状態、値、またはオプション。 (I)

従属 LU リクエスター (dependent LU requester) (DLUR). APPN エンド・ノードまたは APPN ネットワーク・ノードで、従属 LU を所有するが、従属 LU サーバーがそれらの従属 LU に SSCP サービスを提供することを要求する。

指定ルーター (designated router). 他のルーターの存在とアイデンティティーをエンド・ノードに知らせるルーター。指定ルーターの選択は、最高の優先順位をもつルーターに基づいて行われる。最高の優先順位をもつルーターが複数ある場合は、最高のステーション・アドレスをもつルーターが選択される。

宛先ノード (destination node). 要求またはデータの送信先のノード。

宛先ポート (destination port). 順次サービスを提供するコネクション・ポイントとして機能する 8 ポート非同期アダプター。

宛先サービス・アクセス・ポイント (DSAP) (destination service access point (DSAP)). SNA および TCP/IP において、システムがリモート装置からのデータを該当する通信サポートにルーティングするのに使用される論理アドレス。*送信元サービス・アクセス・ポイント (SSAP) (source service access point (SSAP)* と対比。

装置 (device). 特定の目的をもつ機械的、電気的、または電子的な仕組み。

ディジタル (digital). (1) 数字からなるデータを表わす用語。 (T) (2) 数字の形をしたデータを表わす用語。 (A) (3) *アナログ (analog)* と対比。

ディジタル・ネットワーク体系 (DNA) (Digital Network Architecture (DNA)). すべての DECnet ハードウェアおよびソフトウェア実現モデル。

直接メモリー・アクセス (DMA) (direct memory access (DMA)). マイクロチャネル・バス上の装置が、システム処理装置を介さずに、システムまたはバス・メモリーに直接アクセスできるシステム機能。

ディレクトリー (directory). 識別子およびそれに対応するデータ項目への参照からなるテーブル。 (I) (A)

ディレクトリー・サービス (DS) (directory service (DS)). アプリケーション・プロセスによって使用される記号名を、OSI 環境で使用される完全なネットワーク・アドレスに変換するアプリケーション・サービス要素。 (T)

ディレクトリー・サービス (DS) (directory services (DS)). ネットワーク・リソースの場所に関する情報を維持する、APPN ノードのコントロール・ポイント・コンポーネント。

使用不可 (disable). 機能しないようにすること。

使用不可の (disabled). (1) 特定のタイプの割り込みの発生を防止する処理装置の状態を表わす用語。 (2) 伝送制御装置または音声応答装置が線路上の着呼を受け入れることができない状態を表わす用語。

定義域、ドメイン (domain). (1) データ処理資源が共通制御下に置かれているコンピューター・ネットワーク部分。 (T) (2) 開放型システム間相互接続 (OSI) において、共通のポリシーが適用される、分散システムの部分または管理オブジェクトの集合。 (3) *管理領域 (Administrative Domain)* および*ドメイン名 (domain name)* を参照。

ドメイン名 (domain name). インターネット・プロトコルにおける、ホスト・システムの名前。ドメイン名は、区切り文字によって区切られた一連のサブネームから構成される。たとえば、ホスト・システムの完全修飾ドメイン名 (FQDN) が `ralvm7.vnet.ibm.com` である場合、以下がそれぞれドメイン名である。

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

ドメイン名サーバー (domain name server). インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップすることにより名前からアドレスへの変換を行うサーバー・プログラム。ネーム・サーバー *(name server)* と同義。

ドメイン名システム (DNS) (Domain Name System (DNS)). インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップするために使用される分散データベース・システム。

ドット 10 進表記 (dotted decimal notation). 基底を 10 とし、ピリオド (ドット) で相互を分離して書かれた、4 つの 8 ビット数字からなる 32 ビット整数の構文表記。 IP アドレスを表すのに使用される。

ダンプ (dump). (1) ダンプしたデータ。 (T) (2) 誤り情報を収集するために、バーチャル記憶装置のコンテンツの全部または一部をコピーすること。

動的再構成 (DR) (dynamic reconfiguration (DR)). 完全な構成テーブルを再生成したり、影響を受けるメジャー・ノードを停止せずに、ネットワーク構成 (周辺 PU および LU) を変更するプロセス。

動的ルーティング (Dynamic Routing). 初期化時に静的に構成されたルートではなく、動的に確認されたルートを使用するルーティング。

E

エコー (echo). データ通信において、通信チャネル上の反射信号。たとえば、通信端末装置では各信号は 2 度表示される。ローカル端末に入ったときに一度表示され、通信リンクを経由して戻ってきたときに再度表示される。これにより、信号が正確であるかどうかを検査することができる。

EIA 232. データ通信において、順次 2 進データ交換を使用して、データ端末装置 (DTE) とデータ回線終端装置 (DTE) 間のインターフェースを定義する米国電子工業会 (EIA) の仕様。

米国電子工業会 (EIA) (Electronic Industries Association (EIA)). 業界の技術成長を促進し、各メンバーの意見を代表し、業界標準を開発するために組織された電子機器製造業者の団体。

EIA 単位 (EIA unit). 米国電子工業会で確立された測定単位で、44.45 mm (1.7 インチ) に等しい。

カプセル化 (encapsulation). (1) 通信において、階層化されたプロトコルによって使用される技法で、これを用いて各レイヤーはサポートするレイヤーからのプロトコル・データ単位 (PDU) に制御情報を追加する。この場合、このレイヤーは、サポートするレイヤーからのデータをカプセル化する。インターネット・プロトコルでは、たとえば、パケットには、物理レイヤーからの制御情報が入り、その後にネットワーク・レイヤーからの制御情報が続き、その後にアプリケーション・プロトコル・データが入っている。 (2) *データ・リンク交換 (data link switching)* も参照。

コード化 (encode). 元の形に再び変換できるような方法で、規則を使用してデータを変換すること。 (T)

エンド・ノード (EN) (end node (EN)). (1) *拡張対等間通信ネットワーキング (APPN) エンド・ノード (Advanced Peer-to-Peer Networking (APPN) end node)* および*ローエントリー・ネットワーキング (LEN) エンド・ノード (low-entry networking (LEN) end node)* を参照。 (2) 通信において、頻繁に 1 つのデータ・リンクに接続されるノードで、中間ルーティング機能を実行できないもの。

入り口点 (EP) (entry point (EP)). SNA において、分散ネットワーク・ノード管理サポートを提供する、タイプ 2.0、タイプ 2.1、タイプ 4、またはタイプ 5 ノード。それ自体に関するネットワーク管理データとそれが制御する資源を、集中処理のために中心拠点に送り、中心拠

点が開始したコマンドを受け取って実行することによって、その資源を管理および制御する。

イーサネット(Ethernet). 複数の端末が事前の調整なしに伝送媒体に自由にアクセスできる、10 Mbps のベースバンド・ローカル・エリア・ネットワーク。搬送波検知/延期を使用して競合を回避し、衝突検出/遅延再送を使用して競合を解決する。イーサネットは、搬送波検知多重アクセス/衝突検出 (CSMA/CD) を使用する。

例外 (exception). データ・セットまたはファイルの処理中に見付かった入出力誤りのような異常な状態。

例外応答 (ER) (exception response (ER)). SNA において、受信した要求が受付不能または処理不能の場合にのみ応答を戻すように受信側に指示する (つまり、否定応答は戻すことができるが肯定応答は戻せない)、要求ヘッダーの「要求された応答形式」フィールドで指定されたプロトコル。*固定応答 (definite response)* および*応答なし (no response)* と対比。

交換 ID (XID) (exchange identification (XID)). 隣接ノード間でノードおよびリンクの特性を伝達するために使用される、基本リンク単位の 1 つのタイプ。 XID は、リンク起動の前と起動中はリンクおよびノード特性の設定と交渉を行うためにリンク・ステーション間で交換され、またリンク起動後はそれらの特性の変更を通知する。

明示ルート (ER) (explicit route (ER)). SNA において、2 つのサブエリア・ノードを接続する 1 つまたは複数の伝送グループ。明示ルートは、発側サブエリア・アドレス、着側サブエリア・アドレス、明示ルート番号、および逆明示ルート番号によって識別される。*バーチャル・ルート (VR) (virtual route (VR))* と対比。

探索フレーム (explorer frame). *探索パケット (explorer packet)* を参照。

探索パケット (explorer packet). LAN において、発信元ホストによって生成され、LAN のソース・ルーティング全体を探索して、ホストが利用可能なパスに関する情報を収集するパケット。

外部ゲートウェイ (exterior gateway). インターネット通信において、ある自律システム上の、別の自律システムと通信するゲートウェイ。*内部ゲートウェイ (interior gateway)* と対比。

外部ゲートウェイ・プロトコル (EGP) (Exterior Gateway Protocol (EGP)). インターネット・プロトコルにおいて、領域 (ドメイン) と自律システム間で使用され、ネットワーク到達可能性情報を公示および交換することができるプロトコル。ある自律システム内の IP ネットワーク・アドレスが、EGP に参加しているルーターによって、別の自律システムに公示される。 EGP の例としては、ボーダー・ゲートウェイ・プロトコル (BGP) がある。内部ゲートウェイ・プロトコル (IGP) (Interior Gateway Protocol (IGP)) と対比。

F

ファックス (fax). ファクシミリ機から受け取ったハードコピー。***テレコピー (telecopy)*** と同義。

ファイル転送プロトコル (FTP) (File Transfer Protocol (FTP)). インターネット・プロトコルにおいて、TCP および Telnet サービスを使用して、計算機間またはホスト間で大量データ・ファイルを転送する、アプリケーション・レイヤー・プロトコル。

フラッシュ・メモリー (flash memory). プログラム式で、消去可能で、連続的な電力を必要としない、データ記憶装置。他のプログラム式、消去可能データ記憶装置と比べたフラッシュ・メモリーの主な長所は、回路ボードから取り外さずに再プログラムできることである。

フロー制御 (flow control). (1) SNA において、データ・トラフィックがネットワークのコンポーネント間を通過する速度を管理するプロセス。フロー制御の目的は、メッセージの流れを最適化してネットワーク輻輳 (ふくそう) を最小にすることである。つまり、受信側または中間ルーティング・ノードのバッファーがオーバーフローせず、また受信側が追加メッセージ単位の到着を待つこともないようにする。 (2) *ペーシング (pacing)* も参照。

フラグメント (fragment). *分割 (fragmentation)* を参照。

断片化 (fragmentation). (1) 伝送する物理媒体の容量に合わせるために、データグラムをより小さい部分つまり断片に分割する処理。 (2) *分割 (segmenting)* も参照。

フレーム (frame). (1) ある特別な情報で構成されるデータ構造。特別な情報とは、いくつかのスロットで成り立ち、各スロット内の属性値を読むことにより適切な接続手順が決められる。 (T) (2) IBM トークンリング・ネットワークなどのローカル・エリア・ネットワークにおける伝送単位。区切り文字、制御文字、情報、および検査文字が含まれる。 (3) SDLC において、SDLC 手順を使用して伝送される、コマンド、レスポンス、およびすべての情報を運ぶ手段。

フレーム・レベル (frame level). *データ・リンク・レベル (data link level)* と同義。*リンク・レベル (link level)* を参照。

フレーム・リレー (frame relay). (1) ユーザーの装置と高速パケット・ネットワークの境界を記述したインターフェース標準。フレーム・リレー・システムでは、無効

なフレームは廃棄される。回復はホップごとではなく、エンド・エンドで行われる。 (2) サービス総合ディジタル網 (ISDN) D チャネル標準から導出された技法。接続は高信頼性で、ネットワークの誤り検出と制御のオーバーヘッドはないものと想定している。

フロントエンド・プロセッサー (front-end processor). メインフレームの通信制御タスクを軽減する、IBM 3745 または 3174 のようなプロセッサー。

G

ゲートウェイ (gateway). (1) ネットワーク体系が異なる 2 つのコンピューター・ネットワークを相互に接続する機能単位。ゲートウェイは、異なる体系をもつネットワークまたはシステムを接続する。ブリッジは、同一または類似の体系をもつネットワークまたはシステムを接続する。 (T) (2) IBM トークンリング・ネットワークにおいて、ローカル・エリア・ネットワークを、異なる論理リンク・プロトコルを使用する別のローカル・エリア・ネットワークまたはホストに接続する、装置と関連ソフトウェア。 (3) TCP/IP においては、*ルーター (router)* の同義語。

汎用データ・ストリーム (GDS) (general data stream (GDS)). LU 6.2 セッション内の会話に使用されるデータ・ストリーム。

汎用データ・ストリーム (GDS) 変数 (general data stream (GDS) variable). 識別子と長さフィールドで始まり、アプリケーション・データ、ユーザー制御データ、または SNA 定義制御データのいずれかを持つ RU 副構造の 1 タイプ。

H

ヘッダー (header). (1) ユーザー・データの前に置かれるシステムが定めた制御情報。 (2) 1 つまたは複数の着信先フィールド、発信元ステーションの名前、入力シーケンス番号、メッセージのタイプを示す文字列、メッセージの優先順位レベルなどの制御情報が入っているメッセージの部分。

ヒープ・メモリー (heap memory). データ構造を動的に割り振るために使用される RAM の量。

ハロー (Hello). 協働する承認ルーターが最小遅延ルートを見付けるために使用するプロトコル。

ハロー・メッセージ (hello message). (1) ルーター相互間またはルーターとホスト間の到達可能性を設定し、テストするために定期的に送られるメッセージ。 (2) インターネット・プロトコルにおいて、ハロー・プロトコルによって内部ゲートウェイ・プロトコル (IGP) として定義されるメッセージ。

ヒューリスティック (heuristic). 最終結果に向けての進展状況を評価することによって解答を見付けるという、問題解決の探索的方法を表わす用語。

ハイレベル・データ・リンク制御 (HDLC) (high-level data link control (HDLC)). データ通信において、HDLC 国際規格 ISO 3309 フレーム構造および ISO 4335 手順要素に準拠して、指定された一連のビットを使用してデータ・リンクを制御すること。

高性能ルーティング (high-performance routing (HPR)). 特に高速リンクの使用時に、データ・ルーティングの効率と信頼性を高める、同位間通信ネットワーキング機能 (APPN) 体系の追加機能。

ホップ (hop). (1) APPN において、中間ノードを含まないルート部分。隣接ノード間を接続する 1 つの伝送グループだけで構成される。 (2) ルーティング・レイヤーにおいては、ネットワークの 2 つのノード間の論理距離。

ホップ・カウント (hop count). (1) 2 点間の距離の尺度。 (2) インターネット通信において、着信先までの線路でデータグラムが通過するルーターの数。 (3) SNA において、着信先までのパスで通過するリンク数の尺度。

ホスト (host). インターネット・プロトコルにおいて、エンド・システムのこと。エンド・システムはどのワークステーションでも構わず、必ずしもメインフレームである必要はない。

ハブ (インテリジェント) (hub (intelligent)). 異なるケーブルおよびプロトコルをもつ LAN に対してブリッジングおよびルーティング機能を提供する、IBM 8260 のような集線装置。

ヒステリシス (hysteresis). アラート条件がクリアされる前に、設定されたアラート限界値を超過して変化する必要がある温度の量。

I

I フレーム (I-frame). 情報フレーム (Information frame)。

情報 (I) フレーム (information (I) frame). 番号制情報転送に使用される I フォーマットのフレーム。

入出力チャネル (input/output channel). データ処理システムにおいて、内部機器と周辺機器の間のデータ転送を扱う装置。 (I) (A)

統合ディジタル網交換機 (IDNX) (Integrated Digital Network Exchange (IDNX)). 音声、データ、および画像アプリケーションを統合する処理装置。伝送資源の管理や、マルチプレクサーおよびネットワーク管理支援システムへの接続も行う。異なるベンダーからの装置を統合することができる。

サービス総合ディジタル網 (ISDN) (integrated services digital network (ISDN)). 音声やデータも含めた多数のサービスをサポートするディジタル・エンド・エンド通信ネットワーク・ノード。

注: ISDN は公衆網および私設網体系で使用される。

インターフェース (interface). (1) 機能特性、信号特性、またはその他の該当する特性によって定義された、2 つの機能単位間の共有された境界。この概念には、異なる機能をもつ 2 つの装置を接続するための仕様も含まれる。 (T) (2) システム、プログラム、または装置をつなぐハードウェア、ソフトウェア、またはその両方。

内部ゲートウェイ (interior gateway). インターネット通信において、専用の自律システムとのみ通信するゲートウェイ。*外部ゲートウェイ (exterior gateway)* と対比。

内部ゲートウェイ・プロトコル (IGP) (Interior Gateway Protocol (IGP)). インターネット・プロトコルにおいて、自律システム内部でネットワーク到達可能性およびルーティングに関する情報を伝送するのに使用されるプロトコル。 IGP の例としては、ルーティング情報プロトコル (RIP) および最短パス優先オープン (OSPF) がある。

中間ノード (intermediate node). 複数の分岐の終端にあるノード。 (T)

中間セッション・ルーティング (ISR) (intermediate session routing (ISR)). そのノードを通過するが、エンドポイントは別の場所にあるすべてのセッションに対して、セッション・レベルのフロー制御と障害報告を提供する、APPN ネットワーク・ノード内のルーティング機能の 1 タイプ。

国際標準化機構 (ISO) (International Organization for Standardization (ISO)). 製品やサービスの国際的な交流を容易にするため、また知的、科学的、技術的、経済的活動の分野における相互協力を進めるための標準化を推進するために設立された国際的な組織。

国際電気通信連合 (ITU) (International Telecommunication Union (ITU)). 世界の周波数割り振りおよび無線規制を含めて、標準化された通信手順および実施要領を提供するために設立された米国の特殊通信機関。

インターネット (internet). 一組のルーターによって相互接続され、1 つの大規模ネットワーク・ノードとして機能することができるネットワーク・ノードの集合体。インターネット *(Internet)* も参照。

インターネット (Internet). 世界中の大規模な国営バックボーン・ネットワークと、多数の地域や構内のネットワークから構成される、インターネット体系委員会 (IAB) によって管理されるインターネット。インターネットでは、1 組のインターネット・プロトコルを使用する。

インターネット・アドレス (Internet address). *IP アドレス (IP address)* を参照。

インターネット体系委員会 (IAB) (Internet Architecture Board (IAB)). TCP/IP として知られるインターネット・プロトコルの開発を監督する技術団体。

インターネット制御メッセージ・プロトコル (ICMP) (Internet Control Message Protocol (ICMP)). インターネット・プロトコル (IP) レイヤーの誤りを処理し、メッセージを制御するために使用されるプロトコル。問題の報告と誤っているデータグラム着信先が、データグラムの発信元に戻される。 ICMP は、インターネット・プロトコルの一部である。

インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP)). 例外通知、メトリック通知、および PING サポートを提供するバーチャル・ネットワーキング・システム (VIrtual NEtworking System (VINES))。*ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP))* も参照。

インターネット技術特別調査委員会 (IETF) (Internet Engineering Task Force (IETF)). インターネットの短期的な技術問題の解決を担当する、インターネット体系委員会 (IAB) の特別調査委員会。

インターネットワーク・パケット交換機能 (IPX) (Internetwork Packet Exchange (IPX)). (1) Novell のサーバー、または IPX を実装したワークステーションまたはルーターと、他のワークステーションを接続するために使用される、ネットワーク・プロトコル。 IPX は、インターネット・プロトコル (IP) に類似しているが、異なるパケット・フォーマットおよび用語を採用している。 (2) *Xerox ネットワーク・システム (XNS) (Xerox Network Systems (XNS))*も参照。

インターネット・プロトコル (IP) (Internet Protocol (IP)). 1 つのネットワークまたは相互接続ネットワークを通してデータをルーティングするコネクションレス・プロトコル。 IP は、上位のプロトコル・レイヤーと物理ネットワーク・ノードの間の中間層として働く。ただ

し、このプロトコルは、誤り回復やフロー制御は行わず、また物理ネットワーク・ノードの信頼性も保証しない。

相互運用性 (interoperability). ユーザーが装置固有の特性をほとんど (または、まったく) 知らなくても、種々の機能単位間で通信したり、プログラムを実行したり、あるいはデータを転送できること。 (T)

エリア内ルーティング (intra-area routing). インターネット通信において、エリア内部でデータをルーティングすること。

逆アドレス解決プロトコル (InARP) (Inverse Address Resolution Protocol (InARP)). インターネット・プロトコルにおいて、事前設定されたハードウェア・アドレスを使用してプロトコル・アドレスを見付けるために使用されるプロトコル。フレーム・リレー文脈において、データ・リンク・コネクション識別子 (DLCI) は、事前設定ハードウェア・アドレスと同義。

IPPN. 他のプロトコルが IP を通してデータをトランスポートする場合に使用するインターフェース。

IP アドレス (IP address). インターネット・プロトコル、標準 5、Request For Comments (RFC) 791 によって定義された 32 ビット・アドレス。通常は、ドット付き 10 進表記で示される。

IP データグラム (IP datagram). インターネット・プロトコルにおいて、インターネットを通して伝送される情報の基本単位。発信元と着信先のアドレス、ユーザー・データ、および制御情報 (データグラムの長さ、ヘッダー・チェックサム、データグラムの分割が可能かどうか、あるいは分割されているかどうかを示すフラグなど) が入っている。

IP ルーター (IP router). ネットワーク上のトラフィックが流れるパスを決定する、IP インターネット内の装置。ルーティング・プロトコルを使用して、ネットワーク・ノードに関する情報を収集し、データグラムを最終着側に転送する最善ルートを決める。データグラムは、IP 着信アドレスに基づいてルーティングされる。

IPXWAN. 広域ネットワーク・ノード (WAN) を介してインターネットワーク・パケット交換機能 (IPX) ルーティング情報を交換する前に、ルーター相互間で情報を交換するために使用される Novell プロトコル。

L

L2TP アクセス集線装置 (L2TP Access Concentrator) (LAC). PPP プロトコルと L2TP プロトコルの両方の取り扱いが可能な 1 本または複数本の公衆交換電話網 (PSTN) または ISDN 伝送路に接続された集線装置。装置 には、L2TP が稼働する媒体をインプリメントする必要がある。 L2TP は 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) にトラフィックを渡す。L2TP は、PPP ネットワークが伝えるプロトコルであれば、いずれもトンネル伝送することができる。

L2TP ネットワーク・サーバー (L2TP Network Server) (LNS). LNS は、PPP エンド・ステーションとなりうるプラットフォームであればどこでも動作する。 LNS は L2TP プロトコルのサーバー側を処理する。 L2TP では到着する L2TP トンネル経路が通る媒体は 1 つだけなので、 LNS には単一の LAN または WAN インターフェースしかないが、LAC でサポートされる全範囲の PPP インターフェースのどれから到着する呼でも終了することができる。これには非同期 ISDN、同期 ISDN、 V.120、およびその他のタイプの接続が含まれる。

L2TP アクセス集線装置 (LAC) (L2TP Access Concentrator (LAC)). PPP プロトコルと L2TP プロトコルの両方を扱うことができる 1 つまたは複数の公衆サービス電話網 (PSTN) 回線または ISDN 回線に接続される集線装置。装置には、L2TP が稼働するためのメディアをサポートする必要がある。L2TP はトラフィックを 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) に渡す。L2TP は、PPP ネットワークによって搬送されたプロトコルをトンネルすることができる。

L2TP ネットワーク・サーバー (LNS) (L2TP Network Server (LNS)). LNS は PPP エンド・ステーションなど任意のプラットフォーム上で稼働する。 LNS は L2TP プロトコルのサーバー側を扱う。L2TP は、L2TP トンネルを通じて到着する単一の媒体にだけ依存しているので、LNS は単一の LAN または WAN インターフェースだけをもつが、LAC によってサポートされる全範囲の PPP インターフェースのうちどのインターフェースから到着する呼び出しも着信する。これらには、非同期 ISDN、同期 ISDN、V.120、およびその他のタイプの接続が含まれる。

LAN ブリッジ・サーバー (LBS) (LAN bridge server (LBS)). IBM トークンリング・ネットワーク・ブリッジ・プログラムにおいて、2 つ以上のリング間で (ブリッジを介して) 転送されたフレームに関する統計情報を保持しているサーバー。 LBS は、LAN 報告機構 (LRM) を通して、これらの統計を該当の LAN マネージャーに送信する。

LAN エミュレーション (LE) (LAN Emulation (LE)). ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

LAN エミュレーション・クライアント (LEC) (LAN Emulation Client (LEC)). エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

LAN エミュレーション構成サーバー (LECS) (LAN Emulation Configuration Server (LECS)). 構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

LAN エミュレーション・サーバー (LES) (LAN Emulation Server (LES)). LAN 着信先を ATM アドレスにする、LAN エミュレーション・サービス・コンポーネント。

LAN ネットワーク管理プログラム (LNM) (LAN Network Manager (LNM)). ユーザーが中央のワークステーションから LAN 資源を管理および監視できるようにする、IBM ライセンス・プログラム。

LAN セグメント (LAN segment). (1) 独立して動作することができるが、ブリッジによってネットワークの他の部分に接続されている LAN の部分 (たとえば、バスまたはリング)。 (2) ブリッジのない環状ネットワークまたはバス・ネットワーク。

レイヤー (layer). (1) ネットワーク体系において、階層式に配列された一組のグループのうちの 1 つで、ネットワーク体系に一致するすべてのシステム間にまたがっている、概念的に完全なサービス・グループ。 (T) (2) 開放型システム間相互接続参照モデルにおいて、7 つの概念的に完全な、階層式に配列されたサービス、機能、およびプロトコルのグループのうちの 1 つで、すべての開放型システム間にまたがっている。 (T) (3) SNA において、他のグループの機能からは論理的に分離されている、関連する機能の集まり。あるレイヤーの機能の実現方式を変更しても、他のレイヤーの機能には影響を与えない。

LE. LAN エミュレーション (LAN Emulation)。 ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

LEC. LAN エミュレーション・クライアント (LAN Emulation Client)。エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

LECS. LAN エミュレーション構成サーバー (LAN Emulation Configuration Server)。構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

LES. LAN エミュレーション・サーバー (LAN Emulation Server)。 LAN 着信先を ATM アドレスにする、LAN エミュレーション・サービス・コンポーネント。

回線交換 (line switching). サーキット交換 *(circuit switching)* の同義語。

リンク (link). リンク接続機構 (伝送媒体) と、2 つのリンク局 (リンク接続機構の両側に 1 つずつ) の組み合わせ。多地点構成またはトークンリング構成では、1 つのリンク接続を複数のリンクで共用できる。

平衡型リンク・アクセス・プロトコル (LAPB) (link access protocol balanced (LAPB)). リンク・レベルで X.25 ネットワークにアクセスするのに使用されるプロトコル。 LAPB は、ポイント・ポイント通信に使用される全二重、非同期、対称プロトコルである。

リンク接続 (link-attached). (1) データ・リンクによって制御装置に接続されている装置を表わす用語。 (2) チャネル接続 *(channel-attached)* と対比。 (3) リモート *(remote)* と同義。

リンク接続機構 (link connection). (1) 1 つのリンク局と他の 1 つまたは複数のリンク局の間で両方向通信を提供する物理装置。たとえば、通信回線およびデータ回線終端装置 (DCE)。 (2) SNA においては、データ回線 *(data circuit)* と同義。

リンク・レベル (link level). (1) 加入者の機械をネットワーク・ノードに接続する全二重リンクを通してネットワークとの間でデータを受け渡しするのに使用されるリンク・プロトコルを定義している X.25 勧告の部分。 LAP および LAPB は、CCITT によって推奨されているリンク・アクセス・プロトコルである。 (2) データ・リンク・レベル *(data link level)* も参照。

リンク状態 (link-state). ルーティング・プロトコルにおいて、ルーターまたはネットワーク・ノードの使用可能なインターフェースおよび到達可能な近隣ノードに関する、公示された情報。プロトコルのトポロジー・データベースは、収集されたリンク状態公示から作成される。

リンク・ステーション (link station). (1) 特定のリンクを介した隣接ノードへの接続を表す、ノード内のハードウェアおよびソフトウェア・コンポーネント。たとえば、ノード A が 3 つの隣接ノードに接続する多地点回線の 1 次エンドのとき、ノード A は隣接ノードへの接続を表す 3 つのリンク・ステーションをもつことになる。 (2) 隣接リンク・ステーション *(ALS) (adjacent link station (ALS))* も参照。

ローカル (local). (1) 通信回線を使用しないで直接アクセスされる装置を表わす用語。 (2) リモート *(remote)* と対比。 (3) チャネル接続 *(channel-attached)* の同義語。

ローカル・エリア・ネットワーク (LAN) (local area network (LAN)). (1) 地理的に限定された区域内にある、ユーザーの構内に置かれているコンピューター・ネット

ワーク。ローカル・エリア・ネットワーク内部の通信は、外部の規制の対象にはならないが、LAN の境界を越えた通信は、何らかの形で規制を受ける場合がある。 (T)　(2) 1 組の装置が相互通信を目的として接続されているネットワーク・ノードで、さらに大きなネットワーク・ノードに接続することができる。 (3) *イーサネット (Ethernet)* およびトークンリング *(token ring)* も参照。 (4) *大都市圏ネットワーク・ノード (MAN) (metropolitan area network (MAN))* および*広域ネットワーク・ノード (WAN) (wide area network (WAN))* と対比。

ローカル・ブリッジング (local bridging). 通信リンクを使用せずに 1 つのブリッジが複数の LAN セグメントを接続することができるブリッジ・プログラムの機能。*リモート・ブリッジング (remote bridging)* と対比。

ローカル管理インターフェース (LMI) (local management interface (LMI)). *ローカル管理インターフェース (LMI) プロトコル (local management interface (LMI) protocol)* を参照。

ローカル管理インターフェース (LMI) プロトコル (local management interface (LMI) protocol). NCP において、DLCI X'00' を介して回線状況の情報を交換するために隣接フレーム・リレー・ノードが使用する、1 組のフレーム・リレー・ネットワーク管理手順とメッセージ。NCP は、米国規格協会 (ANSI) と国際電信電話諮問委員会 (ITU-T/CCITT) の両方のバージョンの LMI プロトコルをサポートする。これらの標準では、LMI プロトコルをリンク保全検査テスト *(LIVT) (link integrity verification tests (LIVT))* として参照している。

ローカル管理アドレス (locally administered address). ローカル・エリア・ネットワークにおいて、出荷時設定アドレスを指定変更するためにユーザーが割り当てることができるアダプター・アドレス。*出荷時設定アドレス (universally administered address)* と対比。

論理チャネル (logical channel). パケット交換モードの動作において、データ・リンクを介して同時にデータの送信と受信を行うために一緒に使用される、送信チャネルと受信チャネル。パケットの伝送をインターリーブすることにより、同じデータ・リンク上に複数の論理チャネルを確立することができる。

論理リンク (logical link). 1 対のリンク・ステーション (2 つの隣接ノードのそれぞれに 1 つ) とその基礎になるリンク接続。2 つのノード間に 1 つのリンク・レイヤー接続機構を提供する。 2 つのノードを接続する同一の物理媒体を共用しながら、複数の論理リンクを区別することができる。その例としては、ローカル・エリア・ネットワーク (LAN) ファシリティーで使用される 802.2 論理リンクと、2 つのノード間の同じポイント・ポイント物理リンクを使用する LAP E 論理リンクがある。論理リンクという用語には、DTE から X.25 ネットワークへのアクセス・リンクを共用する複数の X.25 論理チャネルも含まれる。

論理リンク制御 (LLC) (logical link control (LLC)). 情報を正確に交換するために、2 種類のデータ・リンク制御 (DLC) 動作を提供するデータ・リンク制御 (DLC) LAN サブレイヤー。最初のタイプはコネクションレス・サービスで、リンクを確立せずに情報を送受信することができる。コネクションレス・サービスの場合、LLC サブレイヤーは誤り回復またはフロー制御を行わない。 2 番目のタイプはコネクション指向のサービスで、情報を交換する前にリンクを確立する必要がある。コネクション指向のサービスは、順序保存情報転送、フロー制御、および誤り回復を提供する。

論理リンク制御 (LLC) プロトコル (logical link control (LLC) protocol). ローカル・エリア・ネットワークにおいて、伝送媒体の共用方法からは独立して、データ・ステーション間の伝送フレームの交換を規定するプロトコル (T)　LLC プロトコルは IEEE 802 委員会によって開発されたもので、すべての LAN 標準に共通である。

論理リンク制御 (LLC) プロトコル・データ単位 (logical link control (LLC) protocol data unit). 異なるノードのリンク・ステーション間で交換される情報の単位。LLC プロトコル・データ単位には、送信先サービス・アクセス・ポイント (DSAP)、送信元サービス・アクセス・ポイント (SSAP)、制御フィールド、およびユーザー・データが入っている。

論理装置 (LU) (logical unit (LU)). ユーザーがネットワーク・リソースにアクセスし、相互に通信することができる、ネットワーク・アクセス可能単位の一種。

ループバック・テスト (loopback test). テスターからの信号をモデムや他のネットワーク・ノード要素でループさせてテスターに戻し、それを計測して通信パスの品質を調べたり、確認したりするテスト。

ローエントリー・ネットワーキング (LEN) (low-entry networking (LEN)). 論理装置間の複数の並列セッションをサポートするために、基本同位間プロトコルを使用して相互に直接接続することができるノードの機能。

ローエントリー・ネットワーキング (LEN) エンド・ノード (low-entry networking (LEN) end node). 隣接 APPN ネットワーク・ノードからネットワーク・サービスを受ける LEN ノード。

ローエントリー・ネットワーキング (LEN) ノード (low-entry networking (LEN) node). 一連のエンド・ユーザー・サービスを行い、同位プロトコルを使用して他のノードと直接接続し、隣接 APPN ネットワーク・ノ

ードから暗黙に (すなわち、CP-CP セッションを直接使用せずに) ネットワーク・サービスを受けるノード。

M

管理情報ベース (MIB) (Management Information Base (MIB)). (1) ネットワーク管理プロトコルによってアクセスできるオブジェクトの集合。 (2) ホストやゲートウェイから入手できる情報および許容される動作を指定する管理情報の定義。 (3) OSI では、開放型システム内の管理情報の概念的リポジトリー。

管理ステーション (management station). インターネット通信において、ネットワーク・ノード全体 (または、一部) を管理するシステム。管理ステーションは、シンプル・ネットワーク・マネージメント・プロトコル (SNMP) のようなネットワーク管理プロトコルを使用して、被管理ノードに常駐するネットワーク管理エージェントと通信する。

マッピング (mapping). あるフォーマットで送信側から伝送されたデータを、受信側が受け入れられるデータ形式に変換するプロセス。

マスク (mask). (1) 他の文字パターンの一部を保持または削除することを制御するために使用する文字パターン。 (I) (A) (2) 他の文字パターンの一部を保持または削除することを制御するために、文字パターンを使用すること。 (I) (A)

最大伝送単位 (MTU) (maximum transmission unit (MTU)). LAN において、1 つのフレームに入れて所定の物理媒体で送信できる最大可能データ単位。たとえば、イーサネットの MTU は 1500 バイトである。

媒体アクセス制御 (MAC) (medium access control (MAC)). LAN において、媒体に依存する機能をサポートし、物理レイヤーのサービスを使用して論理リンク制御 (LLC) サブレイヤーにサービスを提供する、データ・リンク制御レイヤーのサブレイヤー。 MAC サブレイヤーには、装置が伝送媒体にアクセスできる時期を判別する方法が含まれている。

媒体アクセス制御 (MAC) プロトコル (medium access control (MAC) protocol). ローカル・エリア・ネットワークにおいて、データ・ステーション間でデータを交換できるようにするために、ネットワーク・ノードのトポロジーを考慮に入れて、伝送媒体へのアクセスを規制するプロトコル。 (T)

媒体アクセス制御 (MAC) サブレイヤー (medium access control (MAC) sublayer). ローカル・エリア・ネットワークにおいて、媒体アクセス方式に適用されるデータ・リンク・レイヤーの部分。 MAC サブレイヤーは、トポロジー依存の機能をサポートし、物理レイヤーのサービスを使用して、論理リンク制御サブレイヤーにサービスを提供する。 (T)

メトリック (metric). インターネット通信において、同じ自律システムへの複数の出入口ポイントを区別するために使用される、ルートに関連する値。最低のメトリックをもつルートが優先される。

大都市圏ネットワーク・ノード (MAN) (metropolitan area network (MAN)). 2 つ以上のネットワーク・ノードを相互接続して形成された通信ネットワーク。個々のネットワーク・ノードより高速で動作すること、行政の境界にまたがること、および複数のアクセス方式を使用することが可能になる。 (T) *ローカル・エリア・ネットワーク (local area network (LAN))* および*広域ネットワーク・ノード (wide area network (WAN))* と対比。

MIB. (1) MIB モジュール。 (2) 管理情報ベース (Management Information Base)。

MIB オブジェクト (MIB object). *MIB 変数 (MIB variable)* の同義語。

MIB 変数 (MIB variable). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、MIB モジュールに定義されているデータの特定インスタンス。*MIB オブジェクト (MIB object)* と同義。

MIB ビュー (MIB view). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、特定のコミュニティーに見える、エージェントと呼ばれる管理オブジェクトの集合。

MILNET. 本来は ARPANET の一部であった軍用ネットワーク・ノード。 1984 年に ARPANET から分割された。 MILNET は、軍用施設に高信頼性のネットワーク・ノード・サービスを提供している。

モデム (変復調装置) (modem (modulator/demodulator)). (1) 信号を変調および復調する装置。モデムの機能の 1 つは、ディジタル・データをアナログ伝送ファシリティーを介して伝送できるようにすることである。 (T) (A) (2) コンピューターからのディジタル・データを、通信回線上で伝送できるアナログ信号に変換し、また受信したアナログ信号をコンピューターのためのデータに変換する装置。

モジュロ (modulo). (1) モジュラスに関する用語。たとえば、9 は 4 モジュロ 5 と同等。 (2) モジュラス *(modulus)* も参照。

モジュラス (modulus). 剰余を残さずに 2 つの関連する数値の差を除算する関係式における、正整数のような

数。たとえば、9 と 4 はモジュラス 5 をもつ （9 - 4 = 5、4 - 9 = -5、かつ 5 は 5 と -5 の両方とも割りきれる)。

モニター (monitor). (1) 分析するために、データ処理システムの中の選ばれた活動を監視し、記録する機能。基準から著しく逸脱していることを示すため、または特定の機能の利用度を測るために使用する。 (T) (2) システムの操作を観察、監視、制御、検査するソフトウェアまたはハードウェア。 (A) (3) リング上のトークンの伝送を開始し、トークンの紛失、フレームの循環、またはその他の問題が生じた場合にソフト誤り回復を提供するために必要な機能。この機能は、すべてのリング・ステーションに存在する。

マルチキャスト (multicast). (1) 選択された着信先グループに同じデータを伝送すること。 (T) (2) パケットのコピーが可能なすべての着信先のサブセットだけに伝達される、特殊な形式の同報通信。

マルチドメイン・サポート (MDS) (multiple-domain support (MDS)). LU-LU および CP-CP セッションを介して管理サービス機能セット相互間で管理サービス・データを伝達する手法。*マルチドメイン・サポート・メッセージ単位 (MDS-MU) (multiple-domain support message unit (MDS-MU))* も参照。

マルチドメイン・サポート・メッセージ単位 (MDS-MU) (multiple-domain support message unit (MDS-MU)). 管理サービス・データが入っているメッセージ単位で、マルチドメイン・サポートによって使用される LU-LU および CP-CP セッションを介して管理サービス機能セット相互間に流される。このメッセージ単位およびその中に入っている実際の管理サービス・データは、一般データ・ストリーム (GDS) 形式である。*コントロール・ポイント管理サービス単位 (CP－MSU) (control point management services unit (CP-MSU))*、*管理サービス単位 (MSU) (management services unit (MSU))*、および*ネットワーク管理ベクトル伝達 (NMVT) (network management vector transport (NMVT))* も参照。

N

ネーム・バインディング・プロトコル (NBP) (Name Binding Protocol (NBP)). AppleTalk ネットワークにおいて、AppleTalk エンティティー (資源) 名 (文字列) からトランスポート・レイヤーの AppleTalk IP アドレス (16 ビットの数字) へのネーム変換機能を提供するプロトコル。

ネーム・レゾリューション (name resolution). インターネット通信において、機械名を対応するインターネット・プロトコル （IP) アドレスにマップする処理。*ドメイン名システム (DNS) (Domain Name System (DNS))* も参照。

ネーム・サーバー (name server). インターネット・プロトコルにおいて、*ドメイン名サーバー (domain name server)* の同義語。

最近隣活動アップストリーム (NAUN) (nearest active upstream neighbor (NAUN)). IBM トークンリング・ネットワークにおいて、リング上の所定のステーションにデータを直接送信するステーション。

近隣 (neighbor). ネットワーク管理者によってルーティング情報を受信するように指定された、共通サブネットワーク上のルーター。

NetBIOS. ネットワーク基本入出力システム (Network Basic Input/Output System)。メッセージ、プリンター・サーバー、およびファイル・サーバーの機能を提供するために LAN 上で使用される、ネットワーク、IBM パーソナル・コンピューター (PC)、および互換 PC への標準インターフェース。 NetBIOS を使用するアプリケーション・プログラムは、LAN データ・リンク制御 （DLC) プロトコルの詳細を処理する必要がない。

網、ネットワーク (network). (1) 情報交換のために接続されたデータ処理装置とソフトウェアの構成。 (2) ノードとそれを相互接続するリンクの集合。

ネットワーク・アクセス・サーバー (Network Access Server) (NAS). ユーザーに一時的なオンデマンド・アクセスを提供する装置。このアクセスは、PSTN または ISDN 伝送路を使用するポイント・ポイントです。

ネットワーク・アクセス可能単位 (NAU) (network accessible unit (NAU)). 論理装置 (LU)、物理装置 (PU)、コントロール・ポイント (CP)、またはシステム・サービス・コントロール・ポイント (SSCP)。パス制御ネットワークによって伝送される情報の発側または着側となる。 *ネットワーク・アドレス可能単位 (network addressable unit)* と同義。

ネットワーク・アドレス (network address). ISO 7498-3 によると、1 組のネットワーク・サービス・アクセス・ポイントを識別する、OSI 環境内であいまいさのない名前。

ネットワーク・アドレス可能単位 (NAU) (network addressable unit (NAU)). *ネットワーク・アクセス可能単位 (network accessible unit)* の同義語。

ネットワーク体系 (network architecture). コンピューター・ネットワークの論理構造と運用原則。 (T)

注: 運用原則には、サービス、機能、およびプロトコルが含まれる。

ネットワーク輻輳 (ふくそう) (network congestion). 通信量がネットワークで処理できる量を上回ったことによって起こる望ましくない過負荷状態。

ネットワーク識別子 (network identifier). (1) TCP/IP において、ネットワークを定義する IP アドレスの部分。ネットワーク ID の長さは、ネットワーク・クラス (A、B、または C) のタイプによって異なる。 (2) 特定のサブネットワークを固有に識別する、1〜8 バイトのユーザーが選択した名前、または 8 バイトの IBM 登録名。

ネットワーク情報センター(NIC) (Network Information Center (NIC)). インターネット通信において、ユーザーに援助、資料、訓練、およびその他のサービスを提供する、全世界の局所的、地域的、および国家的なグループ。

ネットワーク・レイヤー (network layer). 開放型システム間相互接続 (OSI) 体系において、OSI 環境全体のルーティング、交換、およびリンク・レイヤー・アクセス機能を提供するレイヤー。

ネットワーク管理 (network management). 通信用のデータ処理または情報システムを計画、組織、および制御するプロセス。

ネットワーク管理ステーション (network management station). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、ネットワーク要素を監視、制御する管理アプリケーション・プログラムを実行する端末。

ネットワーク管理ベクトル転送 (NMVT) (network management vector transport (NMVT)). 物理装置管理サービスとコントロール・ポイント管理サービス間のアクティブ・セッション (SSCP-PU セッション) を介して流される、管理サービス要求応答単位 (RU)。

ネットワーク管理プログラム (network manager). ネットワーク・ノードの問題を監視、管理、および診断するプログラムまたはプログラムの集まり。

ネットワーク・ノード (NN) (network node (NN)). *拡張同位間通信ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node)* を参照。

ネットワーク・ユーザー・アドレス (NUA) (network user address (NUA)). X.25 通信において、最大 15 桁の 2 進コード数字を含む X.121 アドレス。

ノード (node). (1) ネットワーク・ノードにおいて、1 台または複数の装置がチャネルまたはデータ回線を接続する点。 (I) (2) ネットワークに接続された、データを送受信する装置。

非標準アドレス (noncanonical address). LAN において、トークンリング・アダプターの媒体アクセス制御 (MAC) アドレスを伝送するためのフォーマットの 1 つ。非標準フォーマットでは、各アドレス・バイトの最上位 (左端) ビットが最初に伝送される。*標準アドレス (canonical address)* と対比。

非ゼロ復帰 (1) 記録 (NRZ-1) (Non-Return-to-Zero Changes-on-Ones Recording (NRZ-1)). 磁化状態の変化が 1 を表し、変化しないことが 0 を表す記録方式。 1 の信号のみが明示的に記録される。 (以前は***非ゼロ復帰反転 (NRZI)*** 記録と呼ばれていた。)

非シード・ルーター (nonseed router). AppleTalk ネットワークにおいて、同じネットワークに接続されているシード・ルーターからネットワーク番号範囲とゾーン・リスト情報を獲得するルーター。

O

最短パス優先オープン (OSPF) (Open Shortest Path First (OSPF)). インターネット・プロトコルにおいて、領域 (ドメイン) 内の情報転送を行う機能。ルーティング情報プロトコル (RIP) の代替として、OSPF は最低コストのルーティングが可能であり、大きい地域や企業ネットワークのルーティングを扱う。

開放型システム間相互接続 (OSI) (Open Systems Interconnection (OSI)). (1) 情報交換のための国際標準化機構 (ISO) の標準に準拠した開放型システムの相互接続。 (T) (A) (2) データ処理システムの相互接続を可能にする標準的手順の使用。

注: OSI 体系は、コンピューター・システムの相互接続のための現在および将来の標準の開発を統合するための枠組みを設定している。ネットワーク機能は 7 つのレイヤーに分けられている。各レイヤーは、異なるアプリケーションをサポートする標準的方法で実行できる、関連したデータ処理および通信機能の集まりを表している。

開放型システム間相互接続 (OSI) 体系 (Open Systems Interconnection (OSI) architecture). 開放型システム相互接続に関連する特定の一組の ISO 規格に準拠したネットワーク体系。 (T)

開放型システム間相互接続 (OSI) 参照モデル (Open Systems Interconnection (OSI)). 開放型システム相互接続、およびその 7 つのレイヤーの目的と階層式配列の一般原則を記述したモデル。 (T)

発信元 (origin). メッセージまたはその他のデータが発信された外部論理装置 (LU) またはアプリケーション・プログラム。*着信先 (destination)* も参照。

孤立回線 (orphan circuit). その利用可能性が動的に学習される未構成の回線。

P

ペーシング (pacing). (1) オーバーランまたは輻輳 (ふくそう) を防止するために、受信側コンポーネントが送信側コンポーネントの伝送速度を制御する方法。 (2) *フロー制御 (flow control)*、*受信ペーシング (receive pacing)*、*送信ペーシング (send pacing)*、*セッション・レベル・ペーシング (session-level pacing)*、およびバーチャル・ルート *(VR)* ペーシング *(virtual route (VR) pacing)* も参照。

パケット (packet). データ通信において、1 つのまとまりとして送信および交換される、データと制御信号を含む 2 進数の列。データ、制御信号、および誤り制御情報が、特定の形式に配列されている。 (I)

パケット・インターネット・グローパー (PING) (packet internet groper (PING)). (1) インターネット通信において、インターネット制御メッセージ・プロトコル (ICMP) エコー要求を宛先に送って応答を待つことにより、宛先に到達できるかどうかをテストする、TCP/IP ネットワーク・ノードで使用されるプログラム。 (2) 通信における、到達可能性のテスト。

パケット損失率 (packet loss ratio). パケットが指定の着信先に到達しない、または指定された時間内に到達しない確率。

パケット・モード動作 (packet mode operation). *パケット交換 (packet switching)* の同義語。

パケット交換 (packet switching). (1) アドレス指定されたパケットを用いてデータのルーティングと転送を行うことによって、パケットの伝送中だけチャネルが占有されるようにする処理。伝送が完了すると、そのチャネルは他のパケットの伝送に利用可能になる。 (I) (2) *パケット・モード動作 (packet mode operation)* と同義。*回線交換 (circuit switching)* も参照。

並列ブリッジ (parallel bridges). 同じ LAN セグメントに接続され、そのセグメントへの冗長パスを形成する 1 対のブリッジ。

並列伝送グループ (parallel transmission groups). 各グループが異なるグループ番号をもつ、隣接ノード間の複数の伝送グループ。

パス (path). (1) 通信ネットワークにおける 2 つのノード間のルート。パスは複数の分岐を含むことができる。 (T) (2) 2 つのネットワーク・アクセス可能装置間で交換される情報が通る、一連の伝送ネットワーク・コンポーネント (パス制御およびデータ・リンク制御)。*明示ルート (ER) (explicit route (ER))*、*ルート拡張 (route extension)*、およびバーチャル・ルート *(VR) (virtual route (VR))* も参照。

パス制御 (PC) (path control (PC)). 通信ネットワークのネットワーク・アクセス可能装置間でメッセージをルーティングし、相互間のパスを提供する機能。伝送制御からの基本情報単位 (BIU) を (場合によっては分割して) パス情報単位 (PIU) に変換し、1 つまたは複数の PIU を含む基本伝送単位をデータ・リンク制御と交換する。パス制御はノード・タイプによって異なる。あるノード (たとえば、APPN ノード) は、ローカルに生成されたセッション識別子をルーティングに使用し、あるノード (サブエリア・ノード) は、ネットワーク・アドレスをルーティングに使用する。

パス・コスト (path cost). リンク状態ルーティング・プロトコルにおいて、2 つのノードまたはネットワーク・ノード間のパス上のリンク・コストの合計。

パス情報単位 (PIU) (path information unit (PIU)). 伝送ヘッダー (TH) のみから成る、または TH の後に基本情報単位 (BIU) または BIU セグメントが続いているメッセージ単位。

パターン突き合わせ文字 (pattern-matching character). 1 文字または複数の文字を表すために使用できる、アスタリスク (*) や疑問符 (?) のような特殊文字。任意の 1 文字または一組の文字を、パターン突き合わせ文字と置き換えることができる。*グローバル文字 (global character)* および*ワイルドカード文字 (wildcard character)* と同義。

パーマネント・バーチャル・サーキット (PVC) (permanent virtual circuit (PVC)). X.25 およびフレーム・リレー通信で、各データ端末装置 (DTE) に論理チャネルが固定的に割り当てられているバーチャル・サーキット。呼設定プロトコルは不要である。*スイッチド・バーチャル・サーキット (SVC) (switched virtual circuit (SVC))* と対比。

物理回線 (physical circuit). 多重化なしで確立されている回路。*データ回線 (data circuit)* も参照。*バーチャル・サーキット (virtual circuit)* と対比。

物理レイヤー (physical layer). 開放型システム間相互接続参照モデルにおいて、伝送媒体を介して物理接続を確立、維持、および解放するための機械的、電気的、機能的、および手順的な手段を提供するレイヤー。 (T)

物理装置 (PU) (physical unit (PU)). (1) SSCP-PU セッションを介した SSCP の要求に応じて、ノードに関連する資源 (接続リンクや隣接リンク・ステーションなど) を管理および監視するコンポーネント。 SSCP は、接続リンクのようなノードの資源を PU を介して間接的に管理するために、物理装置をもつセッションを起動する。この用語は、タイプ 2.0, タイプ 4, およびタイプ 5 ノードにのみ適用される。 (2) *周辺 PU (peripheral PU)* およびサブエリア *PU (subarea PU)* も参照。

PING コマンド (ping command). インターネット制御メッセージ・プロトコル (ICMP) エコー要求パケットをゲートウェイ、ルーター、またはホストに送信し、その応答を待つコマンド。

ポイント・ポイント・プロトコル (PPP) (Point-to-Point Protocol (PPP)). パケットをカプセル化し、シリアル・ポイント・ポイント・リンクを介して伝送する方法を提供するプロトコル。

ポーリング (polling). (1) 多地点接続またはポイント・ポイント接続において、ステーションに対して一度に 1 台ずつ送信するように促す処理。 (I) (2) 競合を避けるため、動作状況を調べるため、またはデータの送信または受信が可能であるかどうかを調べるための、装置に対する問い合わせ。 (A)

ポート (port). (1) データを入出力するためのアクセス・ポイント。 (2) 他の装置 (ディスプレイ、プリンターなど) のケーブルが接続される装置上のコネクター。 (3) リンク・ハードウェアへの物理接続の表現。ポートはアダプターと呼ばれることもあるが、アダプターは 2 つ以上のポートをもつことができる。単一の DLC プロセスで、1 つまたは複数のポートを制御することができる。 (4) インターネット・プロトコルにおいて、TCP またはユーザー・データグラム・プロトコル (UDP) と、上位レベルのプロトコルまたはアプリケーションの間の通信に使用される 16 ビットの番号。ファイル転送プロトコル (FTP) やシンプル・メール転送プロトコル (SMTP) など一部のプロトコルでは、すべての TCP/IP 実装に同一の割り当て済みポート番号が使用される。 (5) ホスト計算機内の複数の宛先を区別するために、トランスポート・プロトコルが使用する抽象概念。 (6) ソケット *(socket)* と同義。

ポート番号 (port number). インターネット通信において、トランスポート・サービスに対してアプリケーション・エンティティーを識別するもの。

構内交換機 (PBX) (private branch exchange (PBX)). 公衆電話網と相互に呼を伝送する構内電話交換機。

問題判別 (problem determination). プログラムのコンポーネント、機械の障害、通信設備、ユーザー所有または外注のプログラムや機器、停電などの環境障害、あるいはユーザーの誤りなど、問題の原因を判別するプロセス。

プログラム一時修正 (PTF) (program temporary fix (PTF)). プログラムの未変更の現行リリースに含まれる、IBM によって診断された問題の一時的な解決策または迂回策。

プロトコル (protocol). (1) 機能単位が通信する方法を規定する、意味上および構文上の一組の規則。 (I) (2) 開放型システム間相互接続体系において、同じレイヤー内のエンティティーが通信機能を実行する方法を規定する、1 組の意味上および構文上の規則。 (T) (3) SNA において、ネットワーク管理、データ伝送、およびネットワーク・コンポーネントの状態の同期化を行うために使用する要求とレスポンスの意味と順序の規則。*回線制御規則 (line control discipline)* および*伝送制御手順 (line discipline)* と同義。*ブラケット・プロトコル (bracket protocol)* および*リンク・プロトコル (link protocol)* を参照。

プロトコル・データ単位 (PDU) (protocol data unit (PDU)). 特定のレイヤーのプロトコルに指定されており、このレイヤーのプロトコル制御情報 (および、このレイヤーのユーザー・データが含まれる場合もある) から構成されるデータの単位。 (T)

R

高速トランスポート・プロトコル (RTP) コネクション (Rapid Transport Protocol (RTP) connection). 高性能ルーティング (HPR) において、セッション・トラフィックを伝達するためにルートのエンドポイント間に確立される接続。

到達可能性 (reachability). ノードまたは資源が、別のノードまたは資源と通信できること。

読み取り専用メモリー (ROM) (read-only memory (ROM)). 特殊な条件下を除いて、保管されたデータをユーザーが変更できないメモリー。

リアルタイム処理 (real-time processing). 処理操作中に、ある処理が必要とするデータまたは生成するデータを処理すること。通常はその結果が、実行中の処理 (および、おそらく関連の処理にも) 使用され、それに影響を与える。

再組み立て (reassembly). 通信において、分割されたパケットを受信後に相互に結合して元に戻すプロセス。

受信不可 (RNR) (receive not ready (RNR)). 通信において、着信フレームを受け入れることができないという一時的な状態を示す、データ・リンク・コマンドまたはレスポンス。

受信不可 (RNR) パケット (receive not ready (RNR) packet). *RNR パケット (RNR packet)* を参照。

受信回線信号検出器 (RLSD) (received line signal detector (RLSD)). EIA 232 標準において、リモート・データ回線終端装置 (DCE) からの信号を受信中であることをデータ端末装置 (DTE) に示す信号。*キャリア検出 (carrier detect)* および*データ・キャリア検出 (DCD) (data carrier detect (DCD))* と同義。

認定私企業 (RPOA) (Recognized Private Operating Agency (RPOA)). 電気通信サービスを提供し、国際電信電話諮問委員会の定める義務と規則に従う、政府省庁や機関以外の個人、会社、または組織。たとえば、通信事業者。

縮小命令セット・コンピューター (RISC) (reduced instruction-set computer (RISC)). 実行速度を上げるために、少数の単純化された頻繁に使用される命令セットを使用するコンピューター。

リモート (remote). (1) 通信回線を介してアクセスされるシステム、プログラム、または装置を表わす。 (2) *リンク接続 (link-attached)* と同義。 (3) *ローカル (local)* と対比。

リモート・ブリッジング (remote bridging). 2 つのブリッジが通信リンクを使用して複数の LAN を接続することができる、ブリッジの機能。*ローカル・ブリッジング (local bridging)* と対比。

リモート実行プロトコル (REXEC) (Remote Execution Protocol (REXEC)). ネットワーク・ノード内の任意のホストからコマンドまたはプログラムを実行することができるプロトコル。ローカル・ホストは、コマンドの実行結果を受け取る。

コメント要求 (RFC)(Request for Comments (RFC)). インターネット通信において、インターネット・プロトコルの一部とそれに関連する実験を記述した文書シリーズ。すべてのインターネット標準は、RFC として文書化されている。

リセット (reset). バーチャル・サーキットにおいて、データ・フロー制御を再初期化すること。リセットすると、転送中のデータはすべて削除される。

リセット要求パケット (reset request packet). X.25 通信において、バーチャル・コールまたはパーマネント・バーチャル・サーキットのリセットを要求するために、データ端末装置 (DTE) またはデータ回線終端装置 (DCE) に送信するパケット。要求の理由もパケットに指定することができる。

リング (ring). *環状ネットワーク (ring network)* を参照。

環状ネットワーク (ring network). (1) 各ノードに正確に 2 本の分岐が接続されており、任意の 2 つのノード間には正確に 2 つのパスがあるネットワーク・ノード。 (T) (2) 装置が単方向伝送リンクで接続されて閉じたパスを形成しているネットワーク構成。

リング・セグメント (ring segment). リングの残りの部分から分離することができる (コネクターを引き抜くことによって) リングの区間。 *LAN セグメント (LAN segment)* を参照。

rlogin (リモート・ログイン) (rlogin (remote login)). Berkeley UNIX ベースのシステムによって提供されるサービス。ある機械の許可ユーザーがインターネットを介して他の UNIX システムに接続し、相互の端末が直接接続されているかのようにして対話することができる。 rlogin ソフトウェアは、ユーザーの環境に関する情報 (たとえば、端末タイプ) をリモートの機械に渡す。

RNR パケット (RNR packet). データ端末装置 (DTE) またはデータ回線終端装置 (DCE) が、バーチャル・コールまたはパーマネント・バーチャル・サーキットに対する追加パケットを一時的に受付不能であることを示すために使用するパケット。

ルート (根) ブリッジ (root bridge). ブリッジ・ネットワークにおいて、他のアクティブ・ブリッジとの間に形成されたスパンニング・ツリーのルート (根) となるブリッジ。ルート (根) ブリッジは、スパンニング・ツリー・トポロジーを維持するために、ブリッジ・プロトコル・データ単位 (BPDU) を発信し、他のアクティブ・ブリッジに転送する。これは、ネットワーク内の最高の優先順位をもつブリッジである。

ルート (route). (1) 発信ノードから着信ノードまでのパスを表し、相互間で交換されるトラフィックが通る、正しいシーケンスのノードと伝送グループ (TG)。 (2) ネットワークのトラフィックが発信元から着信先に達するために使用するパス。

ルート (経路) ブリッジ (route bridge). 2 つのブリッジ・コンピューターが通信リンクを使用して 2 つの LAN を接続することができる、IBM ブリッジ・プログラムの

機能。各ブリッジ・コンピューターは LAN の 1 つに直接接続されており、通信リンクが 2 つのブリッジ・コンピューターを接続する。

ルート拡張機能 (REX) (route extension (REX)). SNA において、サブエリア・ノードと隣接周辺ノード内のネットワーク・アドレス可能単位 (NAU) 間のパス部分を形成する、周辺リンクを含めたパス制御ネットワーク・コンポーネント。*明示ルート (ER) (explicit route (ER))*、*パス (path)*、および*バーチャル・ルート (VR) (virtual route (VR))* も参照。

ルート選択制御ベクトル (RSCV) (Route Selection control vector (RSCV)). APPN ネットワーク内のルートを記述する制御ベクトル。 RSCV は、発信元ノードから着信先ノードまでのパスを形成する TG とノードを識別する、正しいシーケンスの制御ベクトルから構成される。

ルーター (router). (1) ネットワークのトラフィックの流れのパスを決めるコンピューター。パスの選択は、特定のプロトコル、最短または最善パスを識別するアルゴリズム、およびその他の基準 (メトリックやプロトコル特有の着信先アドレスなど) から得られた情報に基づいて、複数のパスから選ばれる。 (2) 参照モデル・ネットワーク・レイヤーにおいて、類似または異なる体系を使用する 2 つの LAN セグメントを接続する装置。 (3) OSI 用語では、エンティティーに到達できるパスを判別する機能。 (4) TCP/IP では、*ゲートウェイ (gateway)* と同義。 (5) *ブリッジ (bridge)* と対比。

ルーティング (routing). (1) メッセージを着側に到達させるためのパスを割り当てること。 (2) SNA において、メッセージ単位で運ばれるパラメーター (伝送ヘッダー内の着信先ネットワーク・アドレスなど) によって決められた、ネットワークの特定パスを通ってメッセージ単位を転送すること。

ルーティング・ドメイン (routing domain). インターネット通信において、ルーティング・プロトコルを使用してネットワーク全体の表示が各中間システム内で同一になるようにしている、中間システムのグループ。ルーティング・ドメインは、外部リンクによって相互に接続されている。

ルーティング情報プロトコル (RIP) (Routing Information Protocol (RIP)). インターネット・プロトコルにおいて、領域間のルーティング情報を交換し、インターネット・ホスト間の最適ルートを決めるために使用される、内部ゲートウェイ・プロトコル。 RIP は、リンク伝送速度ではなく、ルート・メトリックに基づいて最適ルートを決める。

ルーティング・ループ (routing loop). コンバージェンスが起こるまで、あるいは関係のネットワークが到達不能とみなされるまで、ルーターが相互間で情報を循環するときに発生する状態。

ルーティング・プロトコル (routing protocol). ルーターが他のルーターを見付け、到達可能なネットワークに達する最善ルートに関する情報を最新に保つために使用される技法。

ルーティング・テーブル (routing table). データグラムを転送したり、接続を確立するために使用されるルートの集まり。この情報は、ネットワーク・トポロジーと着側への到達可能性を識別するために、ルーター間で受け渡される。

ルーティング・テーブル保守プロトコル (RTMP) (Routing Table Maintenance Protocol (RTMP)). AppleTalk ネットワークにおいて、AppleTalk ルーティング・テーブルを用いて、トランスポート・レイヤーでルーティング情報を生成し、保守する機能を提供するプロトコル。 AppleTalk ルーティング・テーブルは、インターネットを通して、発信元ソケットから着信先ソケットにパケットを伝送する。

ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP)). ルーティング・データベースを維持しているバーチャル・ネットワーキング・システム (VIrtual NEtworking System (VINES)) プロトコルで、VINES ノード間でのルーティング情報の交換を可能にする。*インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP))* も参照。

rsh. ログイン・ステップを完全に飛ばして、リモート UNIX 機械上のコマンド解釈プログラムを呼び出し、そのコマンド解釈プログラムにコマンド行引き数を渡す、rlogin コマンドの変数。

S

SAP. サービス・アクセス・ポイント (service access point) を参照。

シード・ルーター (seed router). AppleTalk ネットワークにおいて、ネットワーク構成データ (たとえば、ネットワーク範囲の数やゾーン・リスト) を維持するルーター。各ネットワークには、少なくとも 1 つのシード・ルーターがある。シード・ルーターは、構成ツールを使用して、最初に設定する必要がある。*非シード・ルーター (nonseed router)* と対比。

セグメント (segment). (1) コンポーネント間または装置の相互間のケーブル区間。セグメントは、1 本のパッチ・ケーブル、相互接続された複数のパッチ・ケーブ

ル、または相互接続された建物ケーブルとパッチ・ケーブルの組み合わせから成る。 (2) インターネット通信において、異なる機械にある TCP 機能の間の転送単位。各セグメントには、制御フィールドとデータ・フィールドが入っており、現在のバイト・ストリーム位置、実際のデータ・バイト、および受信データを妥当性検査するためのチェックサムが付加されている。

分割 (segmenting). OSI において、サポートするレイヤーからの 1 つのプロトコル・データ単位 (PDU) を複数の PDU にマップするためにレイヤーが実行する機能。

シーケンス番号 (sequence number). 通信において、伝送の流れやデータの受信を制御するために、フレームまたはパケットに割り当てられる番号。

シリアル・ライン・インターネット・プロトコル (Serial Line Internet Protocol) (SLIP). シリアル・ライン (たとえば、シリアル・ケーブルまたは電話回線を介したモデムへの RS232 接続) を介した 2 つの IP ホスト間のポイント・ポイント接続上で使用されるプロトコル。

サーバー (server). 通信ネットワークを通してワークステーションに共用サービスを提供する機能。たとえば、ファイル・サーバー、プリント・サーバー、メール・サーバー。 (T)

サービス・アクセス・ポイント (SAP) (service access point (SAP)). (1) 開放型システム間相互接続 (OSI) 体系において、あるレイヤーのサービスが、そのレイヤーのエンティティーによって、すぐ上のレイヤーのエンティティーに提供されるポイント。 (T) (2) アダプターによって提供される、情報を送受信することができる論理ポイント。 1 つのサービス・アクセス・ポイントで、多数のリンクを終端させることができる。

サービス公示プロトコル (SAP) (Service Advertising Protocol (SAP)). インターネットワーク・パケット交換機能 (IPX) において、以下を提供するプロトコル。

- インターネット上の IPX サーバーが、そのサービスの名前とタイプを公示することができる機構。このプロトコルを使用するサーバーの名前、サービス・タイプ、およびアドレスは、NetWare を稼働するすべてのファイル・サーバーに記録されている。
- ワークステーションが、すべてのタイプのすべてのサーバー、特定タイプのすべてのサーバー、または特定タイプの最近隣サーバーのアイデンティティーを見付けるために、照会を同報通信できる機構。
- ワークステーションが、特定タイプのすべてのサーバーの名前とアドレスを見付けるために、NetWare を稼働するすべてのファイル・サーバーを照会することができる機構。

セッション (session). (1) ネットワーク体系において、装置間のデータ通信を目的として、接続の確立、維持、および解放の過程で生じるすべての活動。 (T) (2) 要求に応じて、活動化し、さまざまのプロトコルを提供するように調整し、非活動化することができる、ネットワーク・アクセス可能単位 (NAU) 間の論理結合。 各セッションは、セッション中に交換されるすべての伝送を伴う伝送ヘッダー (TH) の中で固有に識別される。 (3) L2TP において、ダイヤル・ユーザーと LNS 間でエンドツーエンド PPP 接続が試行されるとき、ユーザーがセッションを開始したか、 LNS がアウトバウンド・コールを開始したかどうかにかかわらず、L2TP はセッションを生成する。そのセッション用のデータグラムは、LAC と LNS 間のトンネルを通じて送信される。 LNS および LAC は、LAC に接続された各ユーザーについての状態情報を保持する。

シンプル・ネットワーク管理プロトコル (SNMP) (Simple Network Management Protocol (SNMP)). インターネット・プロトコルにおいて、ルーターと接続ネットワークを監視するのに使用されるネットワーク管理プロトコル。 SNMP は、アダプテーション・レイヤー・プロトコルである。管理される装置に関する情報が定義され、そのアプリケーションの管理情報ベース (MIB) に保管される。

SNA 管理サービス (SNA/MS) (SNA management services (SNA/MS)). SNA ネットワークの管理を援助するために提供されるサービス。

ソケット (socket). (1) 処理間またはアプリケーション・プログラム間の通信のエンドポイント。 (2) カリフォルニア大学の Berkeley ソフトウェア配布 (一般には、 Berkeley UNIX または BSD UNIX と呼ばれる) によって提供される抽象概念で、プロセスまたはアプリケーション間の通信のエンドポイントとして働く。

ソース・ルート・ブリッジング (source route bridging). LAN において、フレームの IEEE 802.5 媒体アクセス制御 (MAC) ヘッダー内のルーティング情報を使用して、フレームが送信する必要があるリングまたはトークンリング・セグメントを判別するブリッジング方式。ルーティング情報は、送信元ノードによって MAC ヘッダーに挿入される。ルーティング情報フィールド内の情報は、送信元ホストが生成する探索パケットから取り出される。

ソース・ルーティング (source routing). LAN において、発信元ステーションがフレームの通るルートを決めて、そのルーティング情報をフレームに組み込む方式。ブリッジは、そのルーティング情報を読み取り、フレームを転送するかどうかを判別する。

送信元サービス・アクセス・ポイント (SSAP) (source service access point (SSAP)). SNA および TCP/IP において、システムがリモート装置にデータを送信することを可能にする論理アドレス。*宛先サービス・アクセス・ポイント (DSAP) (destination service access point (DSAP))* と対比。

スパンニング・ツリー (spanning tree). LAN において、ブリッジが自動的にルーティング・テーブルを作成し、トポロジーの変更に応じてそのテーブルを更新することによって、ブリッジ・ネットワーク内の任意の 2 つの LAN 間に 1 つしかルートが存在しないようにする方式。この方式により、パケットがルートを循環して送信元ルーターに戻るというパケットのループを防止することができる。

制御範囲 (SOC) (sphere of control (SOC)). 1 つの管理サービス中心拠点によってサービスされるコントロール・ポイント・ドメインの集合。

制御範囲 (SOC) ノード (sphere of control (SOC) node). 中心拠点の制御範囲内にあるノード。 SOC ノードは、その中心拠点と管理サービス機能を交換している。 APPN エンド・ノードは、管理サービス機能を交換する機能をサポートする場合は、SOC ノードになれる。

水平分割 (split horizon). ネットワークのコンバージェンスを達成する時間を最小化するための技法。ルーターは特定のルート (経路) を受信したインターフェースを記録し、そのルートに関する情報は再び同じインターフェースに伝送しないようにする。

スプーフィング (spoofing). データ・リンクにおいて、エンド・ステーションから開始されたプロトコルが、最終着側の代わりに中間ノードによって確認応答されて処理される技法。たとえば、IBM 6611 データ・リンク交換では、SNA フレームはカプセル化して TCP/IP パケットに入れられ、非 SNA 広域ネットワーク・ノードを通って伝送され、別の IBM 6611 によってアンパックされて、最終着側に渡される。スプーフィングの利点は、エンド・エンド・セッションのタイムアウトを防止できることである。

標準 MIB (standard MIB). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理情報構造 (SMI) の管理の下に置かれ、インターネット技術作業部会 (IETF) によって標準とみなされている MIB モジュール。

静的ルート (static route). ルーティング・テーブルに手入力される、ホスト間、ネットワーク・ノード間、またはその両方のルート。

ステーション (station). 通信機能を使用するシステムの入力または出力ポイント。たとえば、通信回線を通してデータを送信または受信することができる、ある特定の場所にある 1 台または複数のシステム、コンピューター、端末、装置、および関連のプログラム。

StreetTalk. バーチャル・ネットワーキング・システム (VINES) において、利用者がネットワークのトポロジーを知らなくても、ネットワーク上の任意のリソースを見付けてアクセスすることができる、ネットワーク全体の固有のネーミング/アドレッシング・システム。*インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP))* および *ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP))* も参照。

管理情報構造 (SMI) (Structure of Management Information (SMI)). (1) シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、ネットワーク管理プロトコルを用いてアクセスできるオブジェクトを定義するのに使用される規則。 (2) OSI において、情報の管理に関連する標準の集合。この集合には、*管理情報モデル (Management Information Model)*および*管理オブジェクト定義の指針 (Guidelines for the Definition of Managed Objects)*が含まれる。

サブエリア (subarea). サブエリア・ノード、接続された周辺ノード、および関連の資源から構成される SNA ネットワークの部分。サブエリア・ノード内では、すべてのネットワーク・アクセス可能単位 (NAU)、リンク、およびサブエリア内のアドレス可能な隣接リンク端末 (接続された周辺ノードまたはサブエリア・ノード内の) は、共通のサブエリア・アドレスを共用し、異なる要素アドレスを持っている。

サブネット (subnet). (1) TCP/IP において、IP アドレスの一部によって識別されるネットワークの部分。 (2) サブネットワーク *(subnetwork)* の同義語。

サブネット・アドレス (subnet address). インターネット通信において、ホスト・アドレスの一部がローカル・ネットワーク・アドレスとして解釈される、基本 IP アドレッシング機構の拡張。

サブネット・マスク (subnet mask). *アドレス・マスク (address mask)* の同義語。

サブネットワーク (subnetwork). (1) 1 組の共通特性 (同一ネットワーク ID など) を持つノードの集まり。 (2) サブネット *(subnet)* の同義語。

サブネットワーク・アクセス・プロトコル (SNAP) (Subnetwork Access Protocol (SNAP)). LAN において、パケットが属している非 IEEE 標準プロトコル・ファミリーを識別する、5 バイトのプロトコル識別子。 SNAP

値を使用して、$AA をサービス・アクセス・ポイント (SAP) 値として使用する各プロトコルを区別する。

サブネットワーク・マスク (subnetwork mask). *アドレス・マスク (address mask)* の同義語。

サブシステム (subsystem). 制御システムから独立して、または非同期で、動作することができる、2 次的または従属的なシステム。 (T)

スイッチド・バーチャル・サーキット (SVC) (switched virtual circuit (SVC)). 必要に応じて動的に確立される X.25 回線。交換回線と同等の X.25 回線。*パーマネント・バーチャル・サーキット (PVC) (permanent virtual circuit (PVC))* と対比。

同期 (synchronous). (1) 共通タイミング信号のような特定の事象の発生に依存する 2 つ以上のプロセス。 (T) (2) 規則的または予測可能な時間的関係をもって起こること。

同期データ・リンク制御 (SDLC) (Synchronous Data Link Control (SDLC)). (1) リンク接続上で同期、コード透過、ビット直列情報伝送を管理するための、米国規格協会 (ANSI) のアドバンスト・データ通信制御手順 (ADCCP) および国際規格のハイレベル・データ・リンク制御 (HDLC) のサブセットに従う規則。伝送交換は、交換回線または非交換回線上で、全二重または半二重で行われる。リンク接続の構成は、ポイント・ポイント、多地点、またはループのいずれかである。 (I) (2) *2 進データ同期通信 (BSC) (binary synchronous communication (BSC))* と対比。

SYNTAX. シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理オブジェクトに対応する抽象データ構造を定義する、MIB モジュール内の文節。

システム (system). データ処理において、特定の機能を達成するために組織された人間、機械、および方式の集まり。(I) (A)

システム構成 (system configuration). 特定のデータ処理システムを形成する装置とプログラムを指定するプロセス。

システム・サービス・コントロール・ポイント (SSCP) (system services control point (SSCP)). 構成の管理、ネットワーク運用者および問題判別の要求の調整、およびネットワーク利用者にディレクトリー・サービスやその他のセッション・サービスを提供するための、サブエリア・ネットワーク内のコンポーネント。相互に対等の立場で協働する複数の SSCP は、ネットワークを複数の制御領域に分割し、各 SSCP が自身の領域内の物理装置および論理装置に対して階層的な制御関係を持つようにすることができる。

システム・ネットワーク体系 (SNA) (Systems Network Architecture (SNA)). ネットワークを通して情報単位を伝送し、ネットワークの構成と運用を制御するための、論理構造、フォーマット、プロトコル、および動作手順の記述。 SNA の階層化された構造により、情報の最終的な発信元と着信先 (つまり、利用者) が、情報交換に使用される SNA ネットワークの特定のサービスや機能から独立し、その影響を受けなくすることができる。

T

TCP/IP. (1) 伝送制御プロトコル/インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)。(2) 本来は米国国防総省によって開発された UNIX に似ている、イーサネットを基礎にしたシステム相互接続プロトコル。 TCP/IP により、レイヤー 4 が TCP でレイヤー 3 が IP のパケット交換方式リサーチ・ネットワークである ARPANET (拡張研究プログラム機関ネットワーク (Advanced Research Projects Agency Network)) の便利性が向上した。

Telnet. インターネット・プロトコルにおいて、リモート端末接続サービスを提供するプロトコル。このプロトコルによって、あるホストのユーザーがリモート・ホストにログオンし、そのホストに直接接続されている端末ユーザーとして対話することができる。

しきい値 (threshold). (1) IBM ブリッジ・プログラムにおいて、『しきい値超過』 オカレンスがカウントされてネットワーク管理プログラムに通知される前に、誤りのためにブリッジを通過して転送されないフレームの最大数として設定される値。 (2) そこからカウンターが 0 まで減分される初期値、または初期値からカウンターが増分または減分されて到達する値。

スループット・クラス (throughput class). パケット交換において、データ端末装置 (DTE) パケットがパケット交換ネットワークを通過する速度。

活動回数 (TTL) (time to live (TTL)). ベストエフォート送達プロトコルが、パケットの無限ループを禁止するために使用する技法。 TTL カウンターが 0 に達すると、パケットは廃棄される。

タイムアウト (timeout). (1) 指定された事象の発生時から始まる事前定義された時間間隔の終了前に起こる別の事象。 (I) (2) システム操作を中断してリスタートするこ

とが必要になる前の、ポーリングまたはアドレッシングに対するレスポンスのような、特定の動作を起こすために割り当てられた時間。

トークン (token). (1) ローカル・エリア・ネットワークにおいて、あるデータ装置が一時的に伝送媒体を制御していることを示すために、そのデータ装置から別のデータ装置に連続的に渡される許可信号。各データ装置には、媒体を制御するためにトークンを獲得して使用する機会が与えられる。トークンというのは、伝送許可を示す特別のメッセージまたはビット・パターンである。 (T) (2) LAN において、伝送媒体上を、ある装置から別の装置に渡される一連のビット。トークンにデータが付加されるとフレームになる。

トークンリング (token ring). (1) IEEE 802.5 では、媒体に接続されたステーション間でトークン (特殊なパケットまたはフレーム) を渡すことによって媒体アクセスを制御するネットワーク技術。 (2) ある接続リング・ステーション (ノード) から別のノードにトークンを渡すリング・トポロジーを持つ、FDDI または IEEE 802.5 ネットワーク。 (3) *ローカル・エリア・ネットワーク (LAN) (local area network (LAN))* も参照。

トークンリング・ネットワーク (token-ring network). (1) トークン・パッシング手順により、データ・ステーション間で単方向のデータ伝送を行い、伝送されたデータが送信元ステーションに戻ってくる構造の環状ネットワーク。 (T) (2) ノードからノードへ順にトークンを渡すリング・トポロジーを使用するネットワーク。送信の準備ができているノードは、トークンを取り込み、伝送するデータを挿入することができる。

トポロジー (topology). 通信において、ネットワーク・ノード内のノードの物理的または論理的な配置。特に、ノードとそれを結ぶリンクの関係を表す。

トポロジー・データベース更新 (TDU) (topology database update (TDU)). ネットワーク・トポロジー・データベースを維持するために、APPN ネットワーク・ノード間に同報通信され、各ネットワーク・ノードに完全に複写される、新規または変更されたリンクまたはノードに関するメッセージ。 TDU には、以下のものを識別する情報が入っている。

- 送信元ノード
- ネットワークの各種資源のノード特性およびリンク特性
- 記述されている各資源の最新の更新のシーケンス番号

トレース (trace). (1) コンピューター・プログラムの実行の記録。命令が実行された順序を表す。 (A) (2) データ・リンクの場合は、送信または受信されたフレームとバイトの記録。

トランシーバー (送受信装置) (transceiver (transmitter-receiver)). LAN において、ホスト・インターフェースをイーサネットのようなローカル・エリア・ネットワークに接続する物理装置。イーサネット・トランシーバーには、ケーブルに信号を送って衝突を検出する電子機器が内蔵されている。

伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP)). インターネット、およびインターネットワーク・プロトコルに関する米国国防総省の規格に準拠するその他のすべての通信ネットワークで使用されている通信プロトコル。 TCP は、パケット交換通網のホストとそのネットワークの相互接続システムのホストとの間に、高信頼性ホスト間プロトコルを提供する。基礎となるプロトコルとして、インターネット・プロトコル (IP) を使用している。

伝送制御プロトコル/インターネット・プロトコル (TCP/IP) (Transmission Control Protocol/Internet Protocol (TCP/IP)). ローカル・エリア・ネットワークと広域ネットワーク・ノードの両方で、同位間接続機能をサポートする一組の通信プロトコル。

伝送グループ (TG) (transmission group (TG)). (1) 伝送グループ番号によって識別された隣接ノード間の接続。 (2) サブエリア・ネットワークにおいて、隣接ノード間の単一リンクまたはリンク群。伝送群がリンク群で構成される場合、リンクは単一の論理リンクと見なされ、伝送群は*マルチリンク伝送群 (MLTG)* と呼ばれる。*混合媒体マルチリンク伝送群 (MMMLTG)* とは、異なる媒体タイプのリンク (たとえば、トークンリング、交換 SDLC、非交換 SDLC、およびフレーム・リレー・リンク) を含むものを言う。 (3) APPN ネットワークにおいて、隣接ノード間の 1 つのリンク。 (4) *並列伝送群 (parallel transmission groups)* も参照。

伝送ヘッダー (transmission header) (TH). パス制御が、メッセージ単位をルーティングし、ネットワークの中の流れを制御するために作成して使用する制御情報。オプションでその後に基本情報単位 (BIU) または BIU セグメントを続けることができる。*パス情報単位 (path information unit)* も参照。

透過ブリッジング (transparent bridging). LAN において、媒体アクセス制御 (MAC) レベルを通して、個々のローカル・エリア・ネットワークを相互に結合する方式。透過型ブリッジには MAC アドレスが入ったテーブルが保管されており、テーブルに指示されている場合は、ブリッジが検出したフレームを別の LAN に転送することができる。

トランスポート・レイヤー (transport layer). 開放型システム間相互接続参照モデルにおいて、高信頼性エンド・エンド・データ転送サービスを提供するレイヤー。

パス内に中継開放型システムが存在する場合もある。 (T) *開放型システム間相互接続参照モデル (Open Systems Interconnection reference model)*も参照。

トラップ (trap). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、例外条件を報告するために、管理ノード (エージェント機能) が管理ステーションに送るメッセージ。

トンネル (Tunnel). トンネルとは、LNS-LAC の対によって定義されるもので、 LAC と LNS の間で PPP データグラムを伝える。単一のトンネル で多くのセッションを多重化することができる。制御接続が同じトンネルを介して作動する場合は、すべてのセッションおよびトンネル自体の設定、解放、および保守を制御する。

トンネル伝送 (tunneling). トランスポート・ネットワークを、単一の通信リンクまたは LAN のように扱うこと。*カプセル化 (encapsulation)* も参照。

T1. 米国では、1.544-Mbps の公衆アクセス回線。 24 個の 64 Kbps チャネルで利用可能。欧州方式 (E1) は 2.048 Mbps で伝送する。

U

出荷時設定アドレス (universally administered address). ローカル・エリア・ネットワークにおいて、製造時にアダプターに永久的に符号化されるアドレス。出荷時設定アドレスは固有である。*ローカル管理アドレス (locally administered address)* と対比。

ユーザー・データグラム・プロトコル (UDP) (User Datagram Protocol (UDP)). インターネット・プロトコルにおいて、低信頼性のコネクションレス・データグラム・サービスを提供するプロトコル。このプロトコルを使用して、ある計算機またはプロセス上のアプリケーション・プログラムが、別の計算機またはプロセス上のアプリケーション・プログラムに、データグラムを送信することができる。 UDP では、インターネット・プロトコル (IP) を使用してデータグラムを送達する。

V

V.24. データ通信において、データ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

V.25. データ通信において、手動および自動で設定された呼のエコー制御装置を使用禁止にする手順を含めた、一般交換電話ネットワークの自動応答装置および並列自動発呼装置を定義する CCITT の仕様。

V.35. データ通信において、種々のデータ転送速度のデータ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

V.36. データ通信において、48, 56, 64, または 72 キロビット/秒のデータ転送速度のデータ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

バージョン (version). 通常は重要な新しいコードまたは新しい機能を含む、別個のライセンス・プログラム。

VINES. バーチャル・ネットワーキング・システム (VIrtual NEtworking System)。

バーチャル・サーキット (virtual circuit). (1) パケット交換で、実際の接続箇所をユーザーに見えるようにする、ネットワークによって提供される機能。 (T) *データ回線 (data circuit)* も参照。*物理回線 (physical circuit)* と対比。 (2) 2 台の DTE 間に確立された論理接続。

バーチャル・コネクション (virtual connection). フレーム・リレーにおいて、ポテンシャル接続の戻りパス。

バーチャル・リンク (virtual link). 最短パス最優先オープン (OSPF) において、非バックボーン中継エリアによって分離されたボーダー・ルーターに接続する、ポイント・ポイント・インターフェース。エリア・ルーターは OSPF バックボーンの一部なので、バーチャル・リンクはバックボーンに接続する。バーチャル・リンクは、OSPF バックボーンが不連続にならないようにする。

バーチャル・ネットワーキング・システム (VINES) (VIrtual NEtworking System (VINES)). Banyan Systems, Inc. からのネットワーク運用システムとネットワーク・ソフトウェア。VINES ネットワークにおけるバーチャル・リンクでは、たとえ実際には数百マイル離れていても、すべての装置およびサービスが相互に直接接続されているように見える。 *StreetTalk* も参照。

バーチャル・ルート (VR) (virtual route (VR)). (1) SNA において、次のような論理接続。(a) 特定の明示ルートとして物理的に実現されている 2 つのサブエリア・ノード間の論理接続。または (b) ノード内のセッション用のサブエリア・ノード内に完全に収まっている論理接続。別個のサブエリア・ノードの間のバーチャル・ルートは、使用する明示ルートに伝送優先順位を定め、バーチャル・ルート・ペーシングよってフロー制御を行い、ルート情報単位 (PIU) にシーケンス番号を付けることによりデータ保全性を確保する。 (2) *明示ルート (ER) (explicit route (ER))* と対比。*パス (path)* および*ルート拡張 (REX) (route extension (REX))* も参照。

W

広域ネットワーク・ノード (WAN) (wide area network (WAN)). (1) ローカル・エリア・ネットワークや大都市圏ネットワークよりも広い地域に通信サービスを提供し、公衆通信施設を使用または提供することができるネットワーク。 (T) (2) 何百キロあるいは何千キロも離れた区域にサービスを行うように設計されたデータ通信ネットワーク。たとえば、公衆および私用パケット交換ネットワークや各国の電話網など。 (3) *ローカル・エリア・ネットワーク (local area network (LAN))* および*大都市圏ネットワーク (metropolitan area network (MAN))* と対比。

ワイルドカード文字 (wildcard character). *パターン突き合わせ文字 (pattern-matching character)* の同義語。

X

X.21. 公衆データ網上の同期動作のための、データ端末装置とデータ回線終端装置の間の汎用インターフェースに関する、国際電信電話諮問委員会 (CCITT) の勧告。

X.25. (1) データ端末装置とパケット交換データ網間のインターフェースに関する、国際電信電話諮問委員会 (CCITT) の勧告。 (2) *パケット交換 (packet switching)* も参照。

Xerox ネットワーク・システム (XNS) (Xerox Network Systems (XNS)). Xerox Corporation によって開発された一組のインターネット・プロトコル。 TCP/IP プロトコルに類似しているが、XNS は異なるパケット・フォーマットと用語を使用している。*インターネットワーク・パケット交換機能 (IPX) (Internetwork Packet Exchange (IPX))* も参照。

Z

ゾーン (zone). AppleTalk ネットワークにおいて、インターネット内部のノードのサブセット。

ゾーン情報プロトコル (ZIP) (Zone Information Protocol (ZIP)). AppleTalk プロトコルにおいて、セッション・レイヤーのインターネット全体のゾーン名とネットワーク番号のマッピングを維持してゾーン管理サービスを提供するプロトコル。

ゾーン情報テーブル (ZIT) (zone information table (ZIT)). インターネットのネットワーク番号と対応ゾーン・ネームのマッピングをリストしたもの。このリストは、AppleTalk インターネットの各インターネット・ルーターによって維持される。

索引

日本語, 英字, 数字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

［ア行］

［カ行］

［サ行］

［タ行］

［ナ行］

[ハ行]

［マ行］

［ヤ行］

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

Printed in Japan

SC88-6372-05

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12

Spine information:

IBM

Nways
マルチプロトコル・ルーティング・サービス

MRS V3.1 ソフトウェア使用者の手引き

SC88-6372-05