Nways
マルチプロトコル・ルーティング・サービス

フィーチャーの使用と構成
バージョン 3.4

SD88-6111-02
(英文原典：SC30-3992-02)

Nways
マルチプロトコル・ルーティング・サービス

フィーチャーの使用と構成
バージョン 3.4

SD88-6111-02
(英文原典：SC30-3992-02)

お願い

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

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 リリース 4 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。

本マニュアルについてご意見やご感想がありましたら

`http://www.ibm.com/jp/manuals/main/mail.html`

からお送りください。今後の参考にさせていただきます。
なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

`http://www.infocr.co.jp/ifc/books/`

をご覧ください。（URL は、変更になる場合があります）

原　典： SC30–3992–02
Nways Multiprotocol Routing Services
Using and Configuring Features
Version 3.4

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 2000.1

この文書では、平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財）日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

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

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律上の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

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。

Advanced Peer-to-Peer Networking
APPN
eNetwork
IBM
OS/2
SecureWay
VTAM

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

UNIX は X/Open Company Limited がライセンスしている米国ならびに他の国における登録商標です。

NetView は、米国あるいはその他の国々における Tivoli Systems, Inc. の商標です。

Java およびすべての Java ベースの商標とロゴは、米国またはその他の国々における Sun Microsystems の商標です。

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 装置に導入されたフィーチャー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。本書で説明しているフィーチャーが、どのNways 装置でもサポートされるわけではありません。装置特定のフィーチャーの場合は、以下の個所でそのことを示しています。

- 該当する章または節の中の注記
- 「まえがき」の中の、サポートするフィーチャーおよび装置をリストしているセクション

本書は、IBM 2210 をサポートし、それを “ルーター” または “装置” と呼びます。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。ここに示されている例は、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対象にしています。コンピューター・ネットワーキングのハードウェアおよびソフトウェアの使用経験は、プロトコル・ソフトウェアを使用する上で役立ちますが、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。追加情報をご利用いただける場合、または資料の印刷後に変更が必要になった場合は、CD-ROM 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 マルチプロトコル・ルーティング・サービスは、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、以下の構成要素が含まれています。

- 基本コード (次のものから構成されます)
  - 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でアクセスすることも、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することもできます。

  基本コードは工場で 2210 に導入済みです。

- IBM Nways マルチプロトコル・ルーティング・サービス用構成プログラム (本書では、*構成プログラム*と呼んでいます)。これは、独立型ワークステーションから装置を構成することを可能にする、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 マルチプロトコル・ルーティング・サービス用構成プログラムは、IBM ネットワーキング・テクニカル・サポートのホーム・ページからも入手できます。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・サービス製品 構成プログラム使用者の手引き*、GC88-6657 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の応答を示すために、以下の表記法を使用します。

1. コマンドの省略形は、以下のように下線を引いて表示しています。

   ```
   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。たとえば、次のように表記されます。

   ```
   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。たとえば、次のように表記されます。

   ```
   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、オプションのデフォルト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。たとえば、次のように表記されます。

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

   この例では、STP を指定しない限り、媒体はデフォルトの UTP に設定されます。

5. キーボードのキーの組み合わせは、次のように表示します。
   - **Ctrl-P**
   - **Ctrl -**

   キーの組み合わせ **Ctrl -** は、Ctrl キーとハイフンを同時に押す必要があることを示しています。ある状況では、このキーの組み合わせは、コマンド行プロンプトを変更します。

6. キーボードのキーの名前は、次のように表示します。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します。たとえば、次のように表記されます。

   File Name: *filename.ext*

IBM 2210 Nways マルチプロトコル・ルーターの資料

ライブラリーの変更: バージョン 3.2 より、ライブラリーは次のように変更されました:

- *ソフトウェア使用者の手引き* の **フィーチャーの理解、使用および構成** という表題で記述されていた内容は、*フィーチャーの使用と構成* という新しいマニュアルに移動しました。
- DIAL フィーチャーの使用、構成、監視に関する章は、 *フィーチャーの使用と構成* に移動しました。

情報の更新と訂正: 資料の印刷後に加えられた技術変更、説明、修正などを入手したい場合は、次の IBM ネットワーキングのホーム・ページにアクセスしてください。

http://www.networking.ibm.com

次のリストは、IBM 2210 のサポートとなる資料を示しています。

運用およびネットワーク管理

SC88-6372
ソフトウェア使用者の手引き

この資料では、次のことを説明しています。

- ルーターに付属の IBM Nways マルチプロトコル・ルーティング・サービス・ソフトウェアを構成し、監視し、使用する方法
- マルチプロトコル・ルーティング・サービスのコマンド行ルーター・ユーザー・インターフェースを使用して、ルーターに付属のネットワーク・インターフェースとリンク・レイヤー・プロトコルを構成し監視する方法

SD88-6111
フィーチャーの使用と構成

SC88-6371
プロトコルの構成と監視 解説書 第 1 巻

SC88-6687
プロトコルの構成と監視 解説書 第 2 巻

この 3 つの資料には、マルチプロトコル・ルーティング・サービスのコマンド行ルーター・ユーザー・インターフェースを使用して、ルーターに付属のルーティング・プロトコル・ソフトウェアとフィーチャーを構成し監視する方法が記載してあります。

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
イベント・ログ・システム・メッセージの手引き

この資料では、発生しうるエラー・コードのリストが、エラーの説明および推奨処置とともに記載されています。

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。

GC88-6657

Nways マルチプロトコル/アクセス・サービス製品 構成プログラム使用者の手引き

この資料には、構成プログラムの使用法が説明してあります。

GG24-4446

IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios

この資料には、IBM Nways マルチプロトコル・ルーティング・サービス を使用してプロトコルを構成する方法の例が記載されています。

安全

SD21-0030

Caution: Safety Information - Read This First

この資料では、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。

次のリストには、IBM 2210 Nways マルチプロトコル・ルーター・ライブラリー内の資料をタスクに応じて配列して示してあります。

計画および導入

GA88-6228

IBM 2210 入門と計画の手引き

GC88-6688

IBM 2210 Nways マルチプロトコル・ルーター導入と初期構成の手引き

この 2 つの資料は、2210 に付属しています (英語版のみ)。導入の準備、2210 の導入、初期構成の実行、導入が正常に行われたかどうかの確認を行う方法について説明してあります。

危険のただし書きと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 とともに出荷されます。この資料には、2210 に関する問題を診断し、修復する手順が記載されています。

IBM 2210 ソフトウェア・ライブラリーでの変更の要約

バージョン 3 リリース 4 でソフトウェアに加えられた変更が、以下に箇条書きで示してあります。

- フレーム・リレーの機能強化:
  - 新しいフレーム・ハンドラー (FH) のサポート
  - 3745 制御プログラムをサポートしたトラフィックのバーストを処理するための PU スロットル
  - 同じ物理インターフェース上でバーチャル・インターフェースを可能にする、新しいインターフェース・タイプ (Frame Relay サブインターフェース)
  - 非番号制 IP サポート
- VPN の機能強化:
  - CPE の機能強化:
    - LDAP サーバーからのポリシー情報が、ローカル側で保管されます。
    - ポリシーのクィック構成
    - ポリシーの整合性検査
    - ポリシー情報は、管理ドメイン内で LDAP サーバーから取り出すことができるようになりました。
    - IPSec トンネル PING
  - IP 機能強化:
    - 音声ルーティングの機能強化:
      - PPP 上での IP ヘッダー圧縮 (RFC 2507、2508、2509)
      - マルチリンク PPP 上で断片化されたデータ・パケット間の音声トラフィックのインターリービング
      - Frame Relay 上で断片化されたデータ・パケット間の音声トラフィックのインターリービング
      - 音声トラフィック用の PPP または Frame Relay パケット圧縮と暗号化のバイパス
    - IP ループバック・アドレス

      このサポートにより、ユーザーは、TN3270 ゲートウェイ、ネットワーク・ディスパッチャー、および IPSec の要件をサポートするために、特殊なインターフェース上で IP アドレスを定義することができます。
    - IPv6
      - IPv6 ルーティングとアドレッシング情報をサポートし、トランスポートに TCP6 を使用する、ドメイン間ルーティング機能 (BGP4+) が、IPv6 に提供されます。
      - IPv6 トラフィックが、カプセル化もトンネル伝送もなく、ATM イーサネット LAN エミュレーションを介してサポートされます。
    - 複数の転送パス

      IP ルーティングは、最高 4 つの等コスト静的ルートを使用して、特定のアドレスとマスクへの複数の並列リンクをサポートすることができます。
    - IP ルート集約
    - マルチキャストの機能強化:
      - IPv4 用のプロトコル独立マルチキャスト高密度モード (PIM-DM)

- ネットワーク管理者は、インバウンドとアウトバウンドのトラフィック・フィルターを使用して、ネットワークとの間の両方向の IP マルチキャスト・データ・フローを制御できるようになりました。

- Not-so-stubby エリア (NSSA)

  OSPF は、RFC 1587 で定義された not-so-stubby エリア (NSSA) をサポートし、最新のインターネット草案がサポートされます。

- Random Early Detection (RED)
- ディファレンシャル (差別化された) サービスのポリシング機能強化
- VRRP 機能強化:
  - ハードウェア MAC アドレスが、冗長ゲートウェイを識別するために、仮想 MAC アドレスの代わりに使用できます。これにより、パフォーマンスが向上します。
  - 複数のバックアップ候補が使用できる場合、優先使用オプションを構成することができます。
  - マスター IP ルーターを選択する場合、使用可能なルートやネットワーク・インターフェースなどの追加基準を使用して、非 IP 機能をサポートすることができます。

- WAN リルート用のダイヤル・オンデマンド代替インターフェース
- TN3270 機能強化
  - LU キャッピング
  - LU プールのロード・バランシング
  - TN3270 セッションの Talk 5 切断
  - 追加の報告情報
  - アドレス 1 と 255 のサポート
- ネットワーク・ディスパッチャーの機能強化
  - ルーティング・プロトコルによる、ネットワーク・ディスパッチャー・クラスター・アドレスの公示
  - 新しい SSL アドバイザー
- DLSw SDLC PU1 サポート
- 同じインターフェース上でのイーサネット・タイプ II (デフォルト) と 802.3 の両方に対する同時イーサネット・カプセル化サポート
- DHCP 機能強化:
  - リース情報のハード・ファイル・バックアップ
  - DHCP インターフェースに対する複数 IP アドレス・サポート
  - ショート・リース・サポート
- RADIUS 機能強化
  - Radius スケーラビリティー
  - Login of Last Resort
- L2TP スケーラビリティー
- シン・サーバーの機能強化

  代替サーバーまたはバックアップ・マスター・サーバーとの接続
- サービス・ファイル検索の機能強化

説明と訂正

ハードコピーおよび PDF では、技術的な変更および追加がある場合は、変更個所の左側余白に縦線 (|) を引いて示してあります。

ヘルプの入手

コマンド・プロンプトで、そのレベルで利用可能なコマンドのリストという形で、ヘルプを入手することができます。 これを行うには、**?** (**help** コマンド) を入力し、**Enter** を押します。 **?** は、現在のレベルから利用可能なコマンドのリストを入手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、そのオプションがリストされます。

下位レベル操作環境の終了

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、ASRT 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。

```
ASRT config> exit
Config>
```

1 次レベル (OPCON) に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。

変更の要約

第1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フィーチャー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

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。 2ページの図1 および 2ページの図2 を参照してください。

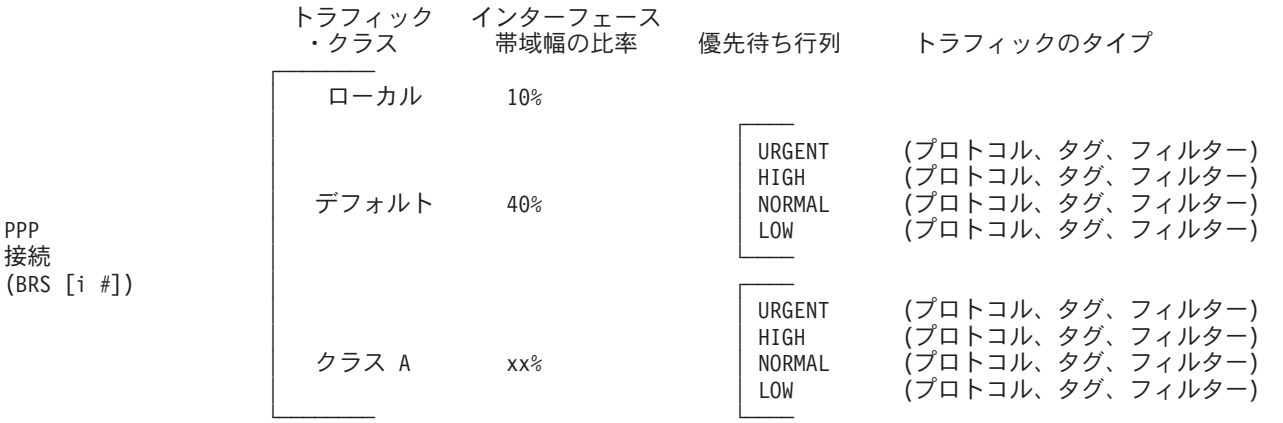
PPP インターフェースでは、トラフィック・クラス (t-classes) を定義し、各トラフィック・クラスに PPP インターフェースの帯域幅の比率を割り振ります。少なくとも 2 種類のトラフィック・クラスがあります。

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。 2ページの図1 を参照してください。

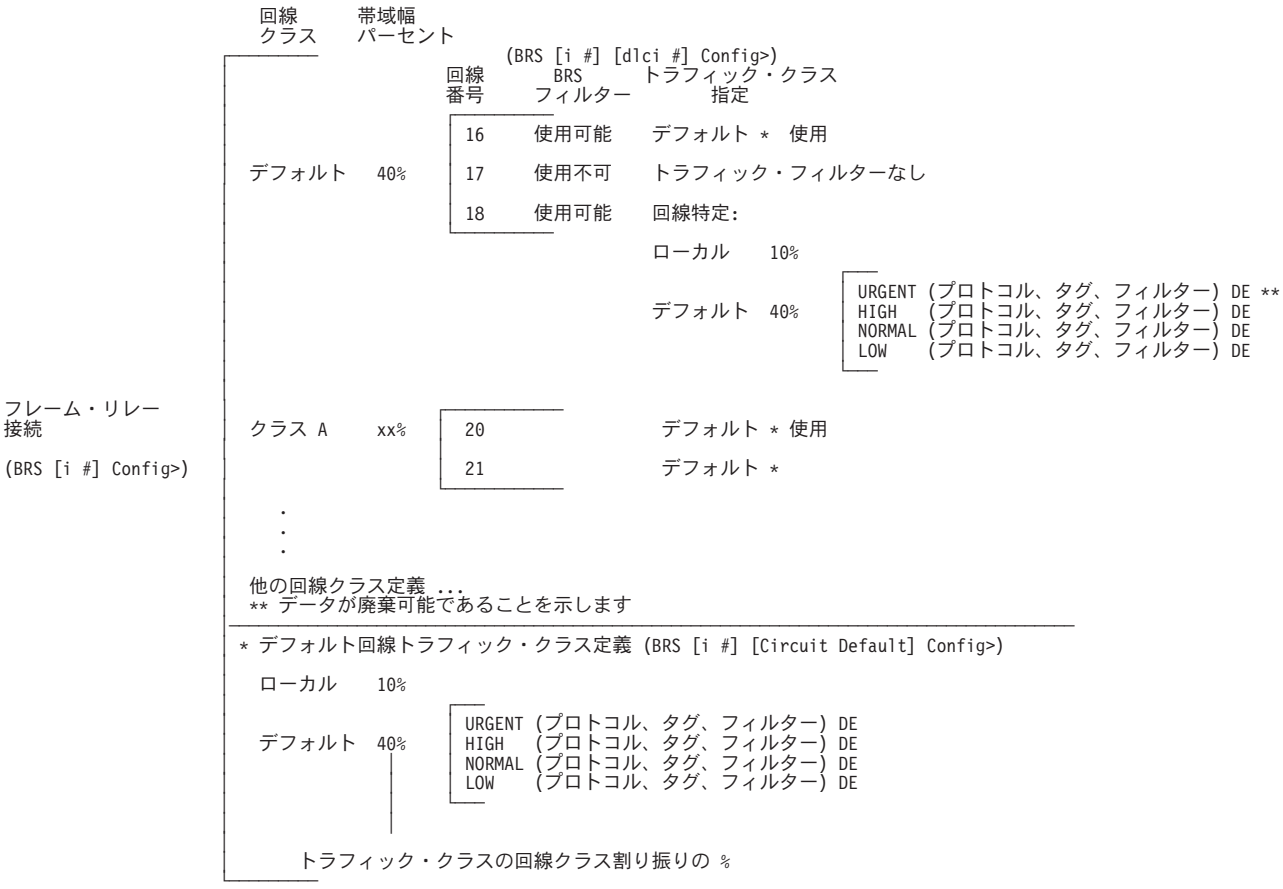
フレーム・リレー・インターフェースでは、回線クラス (c-classes) を定義し、各回線クラスに、フレーム・リレー・インターフェースの帯域幅の比率を割り振ります。少なくとも 1 つの回線クラス (DEFAULT 回線クラス) が存在し、すべての回線が最初はこのクラスに割り当てられます。ユーザーは追加の回線クラスを作成し、それらの回線クラス (c-classes) に回線を割り当てることができます。各フレーム・リレー回線では、トラフィック・クラス (t-classes) を定義し、各トラフィック・クラスに、そのフレーム・リレーの帯域幅の比率を割り振ることができます。フレーム・リレー回線のトラフィック・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、2ページの図2 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 1. 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 2. 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 (*t-classes*) 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。 (**create-super-class** コマンドで作成されるトラフィック・クラスは、どの帯域幅とも関連づけられてはいませんが、回路に定義されたその他のすべての t-classes よりも常に高い優先順位をとります。)

BRS がフレーム・リレーからパケットを受け取ると、構成済みの c-classes および t-classes を使って、パケットを送信するタイミングを決定します。 BRS は、c-class、回路、t-class、および t-class 内の優先順位を基準に、パケットを待ち行列に置きます。回路が割り当てられた c-class は、c-class の待ち行列に置かれ、c-class の待ち行列は、公正なウェイトを使用する待ち行列アルゴリズムによりソートを受けます。c-class のなかでは、送信するパケットがある回路がラウンドロビン方式によりサービスを受けます。各 c-class のなかの t-classes も公正なウェイトを使用する待ち行列アルゴリズムによりソートを受けます。t-class のなかでは、パケットが各優先順位にしたがって (緊急、高、中、低)、さらに待ち行列に置かれます。

パケットは、以下の基準をすべてクリアすると、待ち行列から取り外されて送信されます。
1. 次の c-class の次のパケットである
2. c-class 内の次の回路の次のパケットである
3. その c-class 内の次の t-class にあるパケットのうちの 1 つである
4. その t-class の次の優先グループの次のパケットである

インターフェースを使用可能にして、さらに BRS 用に 1 つまたは 2 つの回路を使用可能にし、c-classe および t-class をまったく構成しない場合、すべての回路は、*default* と呼ばれる 1 つの c-class に割り当てられます。この構成により、

BRS および優先待ち行列の使用

c-class の待ち行列上には、デフォルトの c-class だけが存在し、パケットがある c-class 内の回路は、それぞれラウンドロビン方式で処理されます。これを BRS に実行させる場合は、すべての回路をデフォルトの c-class に置いておき、ほかの回路クラスを作成しないでおきます。

オーファン回路と BRS のない回路は、確実に使用可能にしておけば、どんな条件でもこのデフォルト BRS 待ち行列環境を使用します。BRS は、これらをデフォルトの c-class に割り当てます。

BRS を構成するには、以下のようにします。

1. BRS をインターフェース上で使用可能にする。
2. BRS を回路上で使用可能にし、c-class を加える。
3. c-class に回路を割り当てる。
4. 必要であれば、各 c-class に t-class を定義する。

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、21ページの『第2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。

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、28ページの『Assign』を参照してください。音声トラフィック (VOFR プロトコルが認識する音声トラフィック) は、廃棄可能性を常に **not** にして構成します。

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。

フレーム・リレー上の音声に関する BRS の構成

音声フレームを専用回路上で伝送することができます。そのためには、インターフェースと回路の上で BRS を使用可能にし、音声に関連した回路上でデフォルトを受け入れます。複数の c-class を作成して、音声専用回路は帯域幅の割合が大きい c-class に割り当て、データ関連の回路は、帯域幅の割合の小さい回路クラスに割り当てることができます。

音声とその他のトラフィックを同一の回路上で伝送するときは、インターフェースと回路の上の BRS を使用可能にします。1 つか 2 つの回路を優先的に扱うのではなく、すべての回路をラウンドロビン方式で使用する場合は、デフォルトの c-class 以外に c-class を追加せずにおきます。次に、音声とデータをともに伝送する回路については、**create-super-class** コマンドで各回路ごとに t-class を 1 つ作り、このクラスに VOFR トラフィックを割り当てることを推奨します。必要に応じて、t-class をさらに作成し、t-class にほかのトラフィックを割り当てます。このように構成すると、その他のすべてのトラフィックに対して音声トラフィックが優先権を得ることができ、しかもセグメント化を使用可能にしておけば、セグメント化されていない音声フレームでも断片化したデータ・セグメントのあいだにはさみ込むことができます。音声とデータを同一のインターフェース上で伝送する場合は、フレーム・リレー・インターフェース上でセグメント化を使用可能にしておくことを勧めます。断片化が起こると、フレームが小さくなり、連続する音声フレームのあいだに小さな遅れが発生します。

断片化に関する詳細は、*ソフトウェア使用者の手引き* の “フレーム・リレー・インターフェースの構成と監視” の章にある **enable fragmentation** command を参照してください。

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。 **create-super-class**pubs コマンドで t-class を作成すると、ほかのすべての t-class よりも優先されますが、この t-class を除いて、BRS の t-class は帯域幅の割合と関連付けられます。プロトコルとフィルター・データは、t-class および t-class のなかの特定の優先待ち行列に割り当てられます。優先待ち行列を使うと、プロトコルやフィルターをトラフィック・クラス内の特定の待ち行列に設定で割り当てることができます。BRS の t-class は、同じ名前で認識されるパケットを集めたグループです。たとえば、すべての IPX パケットを指定するには “ipx” とします。

優先待ち行列を用いて、特定のトラフィック・クラス、または t-class やユーザーが指定するトラフィック・クラス、または t-class など、各帯域幅の t-class に対し、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 (デフォルト設定)
- Low

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、41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
- VOFR
- 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″ ことが可能です。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)
- IP 経由の BSC トンネル伝送 (BSC 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
- TOS バイト
- 優先順位ビット

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、51ページの『第3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 トンネルの終了点は、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フィーチャーによって、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、51ページの『第3章 MAC フィルターの使用』 および 55ページの『第4章 MAC フィルターの構成および監視』 を参照してください。

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、51ページの『第3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。

IPv4 TOS ビット・フィルター

サービス・タイプ (TOS) ビットの設定に基づいて、タイプの異なる IP トラフィックを区別するフィルターを作成することができます。このような TOS フィルターを使用すると、特定の TOS ビット設定値を持つ IPv4 トラフィックを、他のタイプの IP トラフィックとは異なるクラスおよび優先順位に割り当てることができます。各フィルターは、TOS バイト値が構成済み TOS フィルターに一致する IPv4 トラフィックを、固有のトラフィック・クラスと優先順位に割り当てます。 TOS フィルターの構成には、TOS バイト内のどのビットが一致しなければならないかを定義するマスク値の指定と、マスクに収まるビット範囲の下限値と上限値の指定が含まれます。このフィルター機構は IPv4 TOS 値にのみ基づいているので、他のほとんどの IP フィルターのように、IPv4 プロトコル・タイプやポート番号情報に依存することはありません。

このフィルターは、TOS バイトの高位 3 ビットのみを対象とする BRS IPv4 優先順位フィルターよりも広範な用途に使用できます。 BRS TOS ビット・フィルター・サポートは、TOS ビットを設定するための IP アクセス制御サポートと組み合わせて使用すると、保護トンネル経由で転送されるトラフィック (断片化されている)、あるいは BRS UDP および TCP ポート番号フィルター・サポートでは識別できないトラフィックをフィルター処理することが可能になります。また、IP アクセ

ス制御サポートは、BRS IPv4 優先順位ビット・フィルターに対応した APPN のハードコーディング優先順位ビット値を使用せずに、TOS ビット値をユーザー定義の値に設定することも可能にします。したがって、BRS IPv4 優先順位ビット・フィルターの代わりに、IP アクセス制御および BRS TOS フィルター・サポートをご使用になることをお勧めします。

12ページの『フィルターの優先順位』で説明しているように、TOS フィルターの一致は、IPv4 優先順位ビット・フィルターおよびその他の IP 特定フィルターより先に検査されます。 TOS1 フィルターから始めて、TOS1 ～ TOS5 フィルターの一致が順次に検査されます。最大 5 つの TOS フィルターを定義することができます。

重要: 特定の TOS 値を持つパケットは、値が一致した最初の TOS フィルター定義に従って処理されることを覚えておいてください。フィルターの設定は十分に注意して行い、特定の TOS バイトが意図したフィルターによって処理されるようにします。誤って優先順位の低いフィルターによって処理されることがないようにしてください。詳細については、*フィーチャーの使用と構成* の『IP の使用』 の節を参照してください。

IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィック用の 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送されたり、2 次 UDP または TCP フラグメントに入れて伝送される 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。 BRS が IP 保護トンネル伝送パケットや TCP および UDP 2 次フラグメント・パケットをフィルター処理できるようにするために、IP バージョン 4 優先順位ビット処理が BRS に追加されました。

注: IPv4 優先順位ビット処理の代わりに、BRS IPv4 TOS ビット・フィルター処理を使用することをお勧めします。詳細については、9ページの『IPv4 TOS ビット・フィルター』を参照してください。

APPN/HPR トラフィックが 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、優先順位レベルが 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処理される優先順位値の 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 2210 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。

ユーザーは、いろいろな場所で IPv4 優先順位ビット処理を構成することが必要になります。

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 保護トンネル伝送パケット、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、2210 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 で 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送されない、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を使用可能にする。

4. IPSec を構成するときに、DLSw、IP 経由 HPR、および TN3270 トラフィックを伝送する保護トンネルを作成する。

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 フィルターに一致する可能性があります。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ときのフィルターの評価順序は、次のとおりです。

1. TOS フィルター (IP)
2. IPv4 優先順位処理
3. ブリッジ・パケットの MAC フィルター・タグの一致 (IP/ASRT)
4. ブリッジングの NetBIOS (IP/ASRT)
5. ブリッジングの SNA/APPN-ISR (IP/ASRT)
6. HPR-Network (IP/ASRT/APPN-HPR)
7. HPR-High (IP/ASRT/APPN-HPR)
8. HPR-Medium (IP/ASRT/APPN-HPR)
9. HPR-Low (IP/ASRT/APPN-HPR)
10. APPN-HPR (IP/ASRT)
11. UDP/TCP ポート番号フィルター (IP)
12. IP トンネル伝送 (IP)
13. SDLC/BSC リレー (IP)
14. DLSw (IP)
15. マルチキャスト (IP)
16. SNMP (IP)
17. Rlogin (IP)
18. Telnet (IP)
19. 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 フィーチャー 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 VOFR 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 VOFR 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
 VOFR                 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 VOFR 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 VOFR 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
VOFR                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 VOFR 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 VOFR 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 VOFR 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 VOFR 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
VOFR                 DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEF2                 NORMAL            NO

BRS [i 1] [dlci 17] Config>exit
```

第2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。

この章は以下の節に分かれています。

- 『帯域幅予約構成の概説』
- 23ページの『帯域幅予約の構成コマンド』
- 44ページの『帯域幅予約監視プロンプトへのアクセス』
- 45ページの『帯域幅予約監視コマンド』
- 48ページの『帯域幅予約の動的再構成のサポート』

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。インターフェースは、ポイントツーポイント・インターフェースまたはフレーム・リレー・インターフェースでなければなりません。 BRS は、フレーム・リレー・サブインターフェース上で設定できません。詳細については、*ソフトウェア使用者の手引き* の『フレーム・リレー・インターフェースの使用』 の項を参照してください。
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、 24ページの表3 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、24ページの表2 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 24ページの表3 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 24ページの表3 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、フィーチャー名 (brs) またはフィーチャー番号 (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。ステップ 21ページの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。ステップ 21ページの4b 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>`、`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 1. 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
? (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。 xxxi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。 24ページの表2 および 24ページの表3 を参照してください。
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。

表 1. 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
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』を参照してください。

表 2. 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
? (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。 xxxi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3 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3 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。 xxxiページの『下位レベル操作環境の終了』 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 3. BRS トラフィック・クラス処理コマンド

コマンド	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。 xxxi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・クラスに割り当てます。
Create-super-class	*super-class* と呼ばれる t-class を定義します。

表 3. 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・フィーチャー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・フィーチャー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。 xxxiページの『下位レベル操作環境の終了』 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、10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 トラフィック用の 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。

構文:

add-class [*class-name* or *class#*] *%*

例 1 : フレーム・リレー回路上に CIRC17 という名前のクラスを 1 つ追加します。

```
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 VOFR 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
```

例 2 : フレーム・リレー回路上に class1 という名前のクラスを 1 つ追加します。

```
BRS [i 2] [dlci 128]>add
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults ?(Yes or [No]): y
Class name [DEFAULT]?
Class is already allocated.
BRS [i 2] [dlci 128]>add class1
Percent bandwidth to reserve [10]?
BRS [i 2] [dlci 128]>

BRS [i 2] [dlci 128]>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 2, circuit number 128
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 IP with default priority is not discard eligible
    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 VOFR 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 class1 has 10% bandwidth allocated
  no protocols or filters are assigned to this class.

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 2] [dlci 128]>
```

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

注: フレーム・リレー・インターフェース上に音声パケットが送信されたときに、Voice over Frame Relay (VOFR) というプロトコルを使います。音声パケットだけを回路で送信する場合は、回路に t-class を 1 つだけ割り当てて、VOFR プロトコルを指定します。 t-class を 1 つにするとほかとの優先順位がなくなるので、設定できる t-class の数は 1 つです。 t-class が 1 つ以上あると、音声を伝送しない t-class が音声トラフィックを伝送する帯域幅とインターフェースを制御します。音声トラフィックをすぐに伝送するためには、VOFR と VOFR のトラフィックだけに *Urgent* の優先順位を与えます。

音声とデータの両トラフィックを回路で伝送する場合は、*ソフトウェア使用者の手引き*の “Configuring and Monitoring Frame Relay Interfaces” の章の **enable fragmentation** command に説明がある Fragmentation over Frame Relay を構成

してください。このこと、帯域幅を大量のデータ・パケットで占領せず、音声パケットの通過が早過ぎないようにするために必要になります。

構文:

assign [*protocol-class* または TAG または *filter-class*] [*class-name* または *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。

例 1:

```
assign IPX test
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]? low
protocol IPX maps to class test with priority LOW Discard eligible <yes/no> [N]?
```

例 2: TOS フィルターを class1 に割り当てます。class1 は、前に *add class* コマンドを使用して構成に追加されています。

```
BRS [i 2] [dlci 128]>assign ?
IP
ARP
DNA
VINES
IPX
OSI
VOFR
AP2
ASRT
TUNNELING-IP
SDLC/BSC-IP
RLOGIN-IP
TELNET-IP
NETBIOS
SNA/APPN-ISR
SNMP-IP
MULTICAST-IP
DLSW-IP
TAG1
TAG2
TAG3
TAG4
TAG5
APPN-HPR
NETWORK-HPR
HIGH-HPR
MEDIUM-HPR
LOW-HPR
XTP-IP
UDP_TCP1
UDP_TCP2
UDP_TCP3
UDP_TCP4
UDP_TCP5
TOS1
TOS2
TOS3
TOS4
```

```
TOS5
Protocol or filter name [IP]? TOS1  1
Class name [DEFAULT]? class1  2
Priority  [NORMAL]?
Frame Relay Discard Eligible  [NO]?
TOS Mask [1-FF] [FF]?
TOS Range (Low) [0-FF] [0]? 1
TOS Range (High) [1]? 3
BRS [i 2] [dlci 128]> list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 2, circuit number 128
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 IP with default priority is not discard eligible
    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 VOFR 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 class1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    filter TOS1 with priority NORMAL is not discard eligible
       with TOS range x1 - x3 and TOS mask xFF

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 2] [dlci 128]>show

BANDWIDTH RESERVATION currently in RAM
interface number 2, circuit number 128
maximum queue length 10, minimum queue length 3
3 current defined classes:
class LOCAL has 10% bandwidth allocated
class DEFAULT has 40% bandwidth allocated
class class1 has 10% bandwidth allocated

protocol and filter assignments:

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   DEFAULT              NORMAL            NO
ARP                  DEFAULT              NORMAL            NO
DNA                  DEFAULT              NORMAL            NO
VINES                DEFAULT              NORMAL            NO
IPX                  DEFAULT              NORMAL            NO
OSI                  DEFAULT              NORMAL            NO
VOFR                 DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEFAULT              NORMAL            NO
TOS1                 class1               NORMAL            NO
   with TOS range x1 - x3
    and TOS mask xFF

BRS [i 2] [dlci 128]>
```

1 TOS フィルターを使用する場合は、3 つのパラメーターを入力する必要があります。つまり、TOS マスク、TOS 範囲-下限、および TOS 範囲-上限です。これらのパラメーターについての説明は、*プロトコルの構成と監視 解説書 第 1 巻* の『構成および監視』 の章の 『Add』 コマンドの項を参照してください。

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、指定された回線を指定された帯域幅 c-class に割り当てるのに使用します。 PVC を回線クラスに割り当てるときは DLCI を使用し、SVC を回線クラスに割り当てるときは回線名を使用します。

注: **circuit** コマンドを使用してバーチャル・サーキット上の BRS を使用可能にし、ルーターをリスタートまたは再ロード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。

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。

BRS と優先待ち行列の構成

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) またはスイッチド・バーチャル・サーキット (SVC) 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:

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または再ロードしておく必要があります。

PVC の例:

```
BRS [i 1] Config> circuit
Circuit (PVC number or SVC name) to reserve bandwidth:  [16]

BRS [i 1 ] [dlci 16] Config> enable
```

SVC の例:

```
BRS [i 1] Config> circuit
Circuit (PVC number or SVC name) to reserve bandwidth:  [16] svc01

BRS [i 1 ] [svc svc01] 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または再ロードすると、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または再ロードするまでは有効になりません。

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>
```

Create-super-class

create-super-class コマンドは、PPP インターフェースおよびフレーム・リレー回線の *super-class* と呼ばれる t-class を構成するときに使用します。 PPP インターフェースおよびフレーム・リレー回路で構成できる super-class は 1 つだけです。super-class に帯域幅の割合は関連付けされません。super-class に割り当てられたプロトコルやフィルターは、PPP インターフェースやフレーム・リレー回路にあるその他の t-class に割り当てられたプロトコルやフィルターよりも先に伝送されます。音声とデータの両方のパケットを回路で伝送するときは、Voice over Frame Relay (VOFR) プロトコルで super-class を構成します。この環境で、super-class を構成して音声を伝送すると、音声パケットに優先権を与える助けとなります。

構文:

create-super-class

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。

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孤立回線を含む) 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。

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。

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または再ロードするまでは有効になりません。

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または再ロードするまでは有効になりません。

BRS と優先待ち行列の構成

構文:

enable

注:

1. 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または再ロードした後で、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。
2. 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または再ロードしてから、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>
*restore
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。*

注: 帯域幅予約は、フレーム・リレー・サブインターフェース上ではサポートされません。詳細については、*ソフトウェア使用者の手引き* のフレーム・リレー・インターフェースの使用 の項を参照してください。

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 レストラルが使用されており、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 レストラル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フィーチャー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 Talk 6 **enable** 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 をリスタートまたは再ロードして、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: 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または再ロードする前に、**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 VOFR 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 VOFR 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 VOFR 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
VOFR                 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・フィーチャー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。

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。

BRS と優先待ち行列の構成

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または再ロード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>
 *restart
 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。 (45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、フィーチャー名 (brs) またはフィーチャー番号 (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、45ページの表4 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4 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 4. 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。 xxxi 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。 xxxiページの『下位レベル操作環境の終了』 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 number 1
Class            Pkt Xmit     Bytes Xmit     Bytes Ovfl     Pkt Ovfl    Q_len

LOCAL               10            914              0            0
   LOW               0              0              0            0        0
   NORMAL           10            914              0            0        0
   HIGH              0              0              0            0        0
   URGENT            0              0              0            0        0
DEFAULT             55           5555              0            0
   LOW               0              0              0            0        0
   NORMAL           20           5020              0            0        0
   HIGH              0              0              0            0        0
   URGENT           35            535              0            0        0
CLASS_1              5            910              0            0
   LOW               0              0              0            0        0
   NORMAL            5            910              0            0        0
   HIGH              0              0              0            0        0
   URGENT            0              0              0            0        0
CLASS_2             70           4123              0            0
   LOW              10            617              0            0        0
   NORMAL           55           3117              0            0        0
   HIGH              0              0              0            0        0
   URGENT            5            389              0            0        0

TOTAL              140          11502              0            0
```

Bytes Ovfl

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。

Pkt Ovfl

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。

Q_len 各トラフィック・クラス内の優先待ち行列で現在転送待ちになっているパケット数。

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。

BRS の監視

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

帯域幅予約の動的再構成のサポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

帯域幅予約では、制限なしに、CONFIG (Talk 6) **delete interface** コマンドをサポートします。

GWCON (Talk 5) Activate Interface

帯域幅予約では、制限なしに、GWCON (Talk 5) **activate interface** コマンドをサポートします。

帯域幅予約のインターフェース固有コマンドはすべて、GWCON (Talk 5) **activate interface** コマンドによってサポートされます。

GWCON (Talk 5) Reset Interface

帯域幅予約では、制限なしに、GWCON (Talk 5) **reset interface** コマンドをサポートします。

帯域幅予約のインターフェース固有コマンドはすべて、GWCON (Talk 5) **reset interface** コマンドによってサポートされます。

CONFIG (Talk 6) 即時変更コマンド

帯域幅予約では、装置の操作状態を即時に変更する次の CONFIG コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、これらの変更は保管され、保存されます。

コマンド
GWCON, feature brs, activate-ip-precedence-filtering
GWCON, feature brs, deactivate-ip-precedence-filtering
GWCON, feature brs, enable-hpr-over-ip-port-numbers
GWCON, feature brs, disable-hpr-over-ip-port-numbers
GWCON, feature brs, interface, add-circuit-class
GWCON, feature brs, interface, assign-circuit
GWCON, feature brs, interface, change-circuit-class
GWCON, feature brs, interface, deassign-circuit
GWCON, feature brs, interface, default-circuit-class
GWCON, feature brs, interface, del-circuit-class
GWCON, feature brs, interface, disable
GWCON, feature brs, interface, enable
GWCON, feature brs, interface, queue-length
GWCON, feature brs, interface, add-class **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
GWCON, feature brs, interface, assign **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
GWCON, feature brs, interface, change-class **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
GWCON, feature brs, interface, create-super-class **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
GWCON, feature brs, interface, deassign **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
GWCON, feature brs, interface, default-class **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
GWCON, feature brs, interface, del-class **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
GWCON, feature brs, interface, disable **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
GWCON, feature brs, interface, enable **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。

	GWCON, feature brs, interface, tag **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。
	GWCON, feature brs, interface, untag **注:** このコマンドは、フレーム・リレー・インターフェースの回線レベルで使用することもできます。

第3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。この章には次の節が含まれます。

- 『MAC フィルターと DLSw トラフィック』
- 52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扱い方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影響を与えます。

注: MAC フィルターはトンネル・トラフィックにも適用できます。

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、フィルターに掛けられるか、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、構成可能な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 フィルターを実装することにより、DLSw ネットワークの着信 LLC トラフィックをフィルターに掛けることができます。

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 `Config>` 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
- パケット内の照合するデータ
- 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
- 入力 / 出力の指定
- 包含 / 除外 / タグの指定
- タグ値 (タグが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するアドレス・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 進法で入力する数字の列で、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くなければならず、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 として想定されます。

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: *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、各フィルター項目を、リストに追加された順序で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、指定の番号のインターフェースで受信 (INPUT) または送信 (OUTPUT) される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。このデフォルト値は 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・フィーチャー (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、たとえばブリッジ・ トラフィックにタグを割り当て、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、このタグに関連する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、BRS **assign** 構成コマンドでこの 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。
- 最高 5 つのタグ付き MAC アドレスを、1 ～ 5 の値に設定することができます。 TAG1 が最初に探索され、次に TAG2 という具合に 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フィーチャーを使用して、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 トンネルの終了点を任意の数のグループに所属させることができます。

第4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フィーチャー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フィーチャー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 *フィーチャー番号* (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。

```
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・フィーチャーを構成します。

表 5. MAC フィルター構成コマンドの要約

コマンド	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。 xxxi 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。
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。

表 5. MAC フィルター構成コマンドの要約 (続き)

コマンド	機能
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。 xxxiページの『下位レベル操作環境の終了』 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 6. 更新サブコマンドの要約

サブコマンド	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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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・フィーチャーの監視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フィーチャー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、フィーチャー番号 (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。以下のコマンドは Filter> プロンプトで入力します。

表 7. MAC フィルター監視コマンドの要約

コマンド	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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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・フィーチャーを監視します。

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

MAC フィルター動的再構成のサポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

MAC フィルターでは、制限なしに、CONFIG (Talk 6) **delete interface** コマンドをサポートします。

GWCON (Talk 5) Activate Interface

MAC フィルターでは、GWCON (Talk 5) **activate interface** コマンドをサポートしますが、次の考慮事項があります。

新たに活動化されたインターフェースに対して MAC フィルターが定義されている場合、どのインターフェースの MAC フィルターもすべて再初期化されます。

MAC フィルターのインターフェース固有コマンドはすべて、GWCON (Talk 5) **activate interface** コマンドによってサポートされます。

GWCON (Talk 5) Reset Interface

MAC フィルターでは、GWCON (Talk 5) **reset interface** コマンドをサポートしますが、次の考慮事項があります。

新たにリセットされたインターフェースに対して MAC フィルターが定義されている場合、どのインターフェースの MAC フィルターもすべて再初期化されます。

MAC フィルターのインターフェース固有コマンドはすべて、GWCON (Talk 5) **reset interface** コマンドによってサポートされます。

GWCON (Talk 5) 構成要素リセット・コマンド

MAC フィルターでは、次の MAC フィルター固有の GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature MCF, Reinit コマンド

説明: 設定済みのすべての MAC フィルターを動的に再初期化します。

ネットワークの影響:
なし。

制限: なし。

MAC フィルター・コマンドはすべて、**GWCON, feature mcf, reinit** コマンドによってサポートされます。

CONFIG (Talk 6) Activate コマンド

MAC フィルターでは、次の CONFIG (Talk 6) **activate** コマンドをサポートします。

CONFIG, Feature MCF, Reinit コマンド

説明: 設定済みのすべての MAC フィルターを動的に再初期化します。

ネットワークの影響:
なし。

制限: なし。

MAC フィルター・コマンドはすべて、**CONFIG, feature mcf, reinit** コマンドによってサポートされます。

第5章 WAN レストラルの使用

本章には、以下の節が含まれています。

WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローの概説

WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローの各フィーチャーは、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 つのフィーチャーのすべての構成コマンドを、「WAN レストラルの構成」の章に収めてあります。 WAN リ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、97ページの『第7章 WAN リルート・フィーチャー』 を参照してください。

WAN レストラル

WAN レストラルは、最も基本的なフィーチャーです。 WAN レストラルを使用する場合は、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 レストラルの場合:

- 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 次リンクには、PPP シリアル・インターフェースまたはマルチリンク・インターフェースを使用することができます。 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 フィーチャー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。

WAN レストラルの使用

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 レストラルの 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 レストラル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 リルート

WAN リルートは、より拡張された機能です。 WAN リ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 リルートの場合:

- 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.25 bis 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.25 bis 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。ダイヤル回路をダイヤル・オンデマンド回路ではないように構成するには、その回路をダイヤルの `Circuit Config>` プロンプトで、**set idle 0** を使って構成します。詳しくは、*ソフトウェア使用者の手引き*の『ダイヤル回線の構成および監視』を参照してください。

  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。
- **enable wrs** コマンドを使用して、WRS フィーチャー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 リ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 リ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 リルートが引き継ぎ、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、そのルートを使い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 リ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 リルートの組みを構成する必要があり、WAN リ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 リルートの組みの 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)、ルーティング安定化時間 (routing-stabilization times)、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 リルートについての詳細は、97ページの『第7章 WAN リルート・フィーチャー』 を参照してください。

始める前に

WAN レストラルを構成する前に、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.25 bis 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。このコマンドは、ダイヤル回線がダイヤル・オンデマンドになるのを防止します。
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) が活動状態になると、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 レストラルの構成手順

この節では、WAN レストラル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 レストラルを構成します。

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 レストラルを使用可能にする。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 レストラル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.25 bis、 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) が活動状態になると、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、*ソフトウェア使用者の手引き* の 『ISDN インターフェースの使用』 の項を参照してください。
4. V.25 の構成方法については、*ソフトウェア使用者の手引き* の 『V.25 インターフェースの使用』 の項を参照してください。
5. V.34 の構成方法については、 *ソフトウェア使用者の手引き*の 『V.34 インターフェースの使用』の項を参照してください。

第6章 WAN レストラルの構成および監視

この章では、WAN レストラルの構成コマンドおよびオペレーショナル・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。

- 83ページの『WAN レストラル・インターフェース監視プロセスへのアクセス』
- 83ページの『WAN レストラル監視コマンド』
- 93ページの『WAN レストラルと WAN リルートの動的再構成のサポート』

注: ダイヤル回路に関する詳細は、*ソフトウェア使用者の手引き*の 『ダイヤル回線の構成および監視』を参照してください。 WAN レストラルを構成すると、ダイヤル回路をインターフェースとして使うことができます。

WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローの構成コマンド

WAN レストラル構成コマンドを用いて、WAN レストラル・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 レストラル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8 は、WAN レストラル構成コマンドとそのフィーチャー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 8. WAN レストラル構成コマンドの要約

コマンド	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。 xxxi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 レストラルの場合) または 1 次から代替へ (WAN リルートの場合) 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)、ルート安定化 (route-stabilization)、および復帰時刻 (time-of-day-revert-back) の各タイマー値を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 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 リルートのために、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、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 レストラルのために、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 レストラル・フィーチャー、WAN レストラルにおける 1 次 / 2 次の組み合わせ、WAN リルートにおける 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 リルートの 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 レストラル・フィーチャーをグローバルに使用不可にします。これは、WAN リ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 レストラル・フィーチャー、WAN レストラルにおける 1 次 / 2 次の組み合わせ、WAN リルートにおける 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リルートするときに、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 レストラルのフィーチャーを使用可能にします。これは、WAN リ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、そのフィーチャーのグローバル構成情報を表示したり、WAN レストラルの 1 次 / 2 次の組み、WAN リルートの 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 all
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  Stab
Primary Interface  Alternate Interface  Enabled  Stab  Stab  Start    Stop
-----------------  ---------------------  -------  ----  ----  -------  ------- ----

 1 - WAN Frame Re   2 - WAN Frame Relay      Yes    dflt  dflt  Not Set  Not Set 15


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または 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。

WAN レストラルの構成

構文:

remove alternate-circuit

secondary-circuit

alternate-circuit *alternate-interface# primary-interface#*

WAN リルートの代替 (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 レストラルの 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 リ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

routing-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。

routing-stabilization

ルーティング安定化の値を設定します。 このパラメーターは、1 次リンクがアップになっていることがわかり、安定化タイマーがある場合はこのタイマーの時間が過ぎた後、1 次リンクと代替リンクがともにアップの状態を継続する秒数を定義します。 ルーティング安定化時間は、OSPF や RIP などのルーティング・プロトコルが新しいルートの可用性を識別するために充分な時間を得られるようにするためのものです。 ルーティング安定化時間がないと、代替ルートが無効になってから 1 次ルートが見つかるまでの数秒間のあいだ、トラフィックが中断してしまいます。

リルート前に代替リンクがアップになっていると、代替リンクはアップのままになり、ルーティング安定化タイマーは無視されます。 リルート前あるいはリルート中に代替リンクがダウンされると、代替リンクはダウンのままになり、ルーティング安定化タイマーと安定化タイマーはともに無視されます。

```
WRS Config>set routing-stabilization
Primary interface number [0]? 1
Routing stabilization timer (0 - 3600 seconds) [0]?
```

Primary interface number

有効値 : 0 ～ ルーターに構成されたインターフェースの数

省略時値: 0

Routing-stabilization timer

有効値 : 1 ～ 3600

省略時値: 0

stabilization

1 次リンクがアップであることが最初に検出されてから、1 次リンクでルーティングの再初期化を開始するまでの秒数を設定します。 安定化タイマーの時間が過ぎると、ルーティング安定化タイマーを構成していなければ、代替リンクがダウンになります。 ルーティング安定化タイマーは、安定化タイマーの時間が過ぎるとすぐに開始し、OSPF や RIP などのルーティング・プロトコルが 1 次リンクのルートを再確立できるように、充分な時間にわたり 1 次リンクと代替リンクをともにアップにしておきます。

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 レストラル・インターフェース監視プロセスへのアクセス

WAN レストラル・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 レストラル監視コマンド

WAN レストラル (WRS) 監視コマンドを用いて、WAN レストラルの 1 次 / 2 次の組み、WAN リルートの 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 レストラル、WAN リルート、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保持されません。

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9 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 9. WAN レストラル監視コマンド

コマンド	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。 xxxi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。
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)、ルート安定化 (route-stabilization)、および復帰時刻 (time-of-day-revert-back) の各タイマー値を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 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 レストラル、WAN リルート、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 レストラル・フィーチャー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 リルートの 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 リルートの使用可能/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活動状態にされ、非活動状態のままになりますが、 WAN レストラルの 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。現行のコールだけを使用不可にします (つまり、活動状態のコールが切断されます)。 2 次回線を使用不可にするためには、WAN レストラル監視プロンプトで **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 レストラル、WAN リルート、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 レストラル・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 リルートの 1 次 / 代替の組み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 レストラルのフィーチャーを使用可能にします。WAN レストラル、WAN リルート、またはダイヤル・オン・オーバーフローを行うためには、このフィーチャーを使用可能にすることが必要です。

Set

set コマンドは、WAN リ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

routing-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。

routing-stabilization

ルーティング安定化の値を設定します。 このパラメーターは、1 次リンクがアップになっていることがわかり、安定化タイマーがある場合はこのタイマーの時間が過ぎた後、1 次リンクと代替リンクがともにアップの状態を継続する秒数を定義します。 ルーティング安定化時間は、OSPF や RIP などのルーティング・プロトコルが新しいルートの可用性を識別するために充分な時間を得られるようにするためのものです。 ルーティング安定化時間がないと、代替ルートが無効になってから 1 次ルートが見つかるまでの数秒間のあいだ、トラフィックが中断してしまいます。

リルート前に代替リンクがアップになっていると、代替リンクはアップのままになり、ルーティング安定化タイマーは無視されます。 リルート前あるいはリルート中に代替リンクがダウンされると、代替リンクはダウンのままになり、ルーティング安定化タイマーと安定化タイマーはともに無視されます。

```
WRS Config>set routing-stabilization
Primary interface number [0]? 1
Routing stabilization timer (0 - 3600 seconds) [15]?
```

Primary interface number

有効値 : 0 ～ ルーターに構成されたインターフェースの数

省略時値: 0

Routing-stabilization timer

有効値 : 1 ～ 3600

省略時値: 0

stabilization

1 次リンクがアップであることが最初に検出されてから、1 次リンクでルーティングの再初期化を開始するまでの秒数を設定します。 安定化タイマーの時間が過ぎると、ルーティング安定化タイマーを構成していなければ、代替リンクがダウンになります。 ルーティング安定化タイマーは、安定化タイマーの時間が過ぎるとすぐに開始し、OSPF や RIP などのルーティング・プロトコルが 1 次リンクのルートを再確立できるように、充分な時間にわたり 1 次リンクと代替リンクをともにアップにしておきます。

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 レストラルの 1 次 / 2 次の組みの 1 つまたはすべて、あるいは WAN リルートの 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
復元が活動状態かどうか (Yes または No) を示します。

Current/Longest Duration
現行の時間と、2 次ネットワーク・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
リ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
リルートおよびオーバーフローが活動状態かどうか (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リ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 リルートの状態、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)
Routing-stabilization time: 15 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リ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、ルーティングを代替リンクから 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。

Routing stabilization
ルーティングが 1 次リンクに戻ってから、代替リンクをダウンするまでの秒数。 このあいだ、1 次リンクと代替リンクはともにアップの状態になります。この時間は、OSPF and RIP などのルーティング・プロトコルに 1 次インターフェース上のルートの可用性を認識させる時間です。

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リ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 レストラルの状態、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 次の基本網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 次の基本ネットワーク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。

WAN レストラルと WAN リルートの動的再構成のサポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

WAN レストラルと WAN リルートでは、制限なしに、CONFIG (Talk 6) **delete interface** コマンドをサポートします。

GWCON (Talk 5) Activate Interface

WAN レストラルと WAN リルートでは、GWCON (Talk 5) **activate interface** コマンドをサポートしますが、次の考慮事項があります。

- 2 次インターフェースが別の 1 次インターフェースを復元している場合、WAN レストラル 1 次インターフェースを活動化できません。
- **activate interface** コマンドの前に、2 次インターフェースが WAN レストラル 1 次インターフェース、WAN リルート 1 次インターフェース、または WAN リルート代替インターフェースであった場合、WAN レストラル 1 次インターフェースを活動化できません。
- 1 次インターフェースが別の 2 次インターフェースによって復元されている場合、WAN レストラル 2 次インターフェースを活動化できません。
- **activate interface** コマンドの前に、1 次インターフェースが WAN レストラル 2 次インターフェース、WAN リルート 1 次インターフェース、または WAN リルート代替インターフェースであった場合、WAN レストラル 2 次インターフェースを活動化できません。
- **activate interface** コマンドの前に、代替インターフェースが WAN リルート 1 次インターフェース、WAN レストラル 1 次インターフェース、または WAN レストラル代替インターフェースとして使用された場合、WAN リルート 1 次インターフェースを活動化できません。
- 1 次インターフェースが、別の代替インターフェースの 1 次インターフェースであるか、WAN リルート代替インターフェースであるか、WAN レストラル 1 次インターフェースであるか、または WAN レストラル 2 次インターフェースである場合、WAN リルート代替インターフェースを活動化できません。

WAN レストラルと WAN リルートのインターフェース固有コマンドはすべて、GWCON (Talk 5) **activate interface** コマンドによってサポートされます。

GWCON (Talk 5) Reset Interface

WAN レストラルと WAN リルートは、GWCON (Talk 5) **reset interface** コマンドをサポートします。

GWCON (Talk 5) 一時変更コマンド

WAN レストラルと WAN リルートは、装置の操作状態を一時的に変更する次の GWCON コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、常にこれらの変更は失われます。

コマンド
GWCON, feature wan, disable alternate-circuit
GWCON, feature wan, disable dial-on-overflow
GWCON, feature wan, disable secondary-circuit

GWCON, feature wan, disable wrs
GWCON, feature wan, enable alternate-circuit
GWCON, feature wan, enable dial-on-overflow
GWCON, feature wan, enable secondary-circuit
GWCON, feature wan, set default
GWCON, feature wan, first-stabilization
GWCON, feature wan, stabilization
GWCON, feature wan, routing-stabilization
GWCON, feature wan, start-time-of-day-revert-back
GWCON, feature wan, stop-time-of-day-revert-back

第7章 WAN リルート・フィーチャー

この章では、WAN リルート・フィーチャー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 リルートの概説』
- 99ページの『WAN リルートの構成』

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活動状態の場合にのみ、WAN リルートを利用可能です。

WAN リルートの概説

WAN リルートは、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宛先への新しい接続を開始できるようにします。 WAN レストラルの説明、および WAN リ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、69ページの『WAN レストラル、WAN リルート、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 リルート・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.25 bis 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。ダイヤル回路がダイヤル・オンデマンドを実行しないようにするためには、 `Circuit Config>` プロンプトで、 **set idle 0** コマンドを使います。詳しくは、*ソフトウェア使用者の手引き*の 『ダイヤル回線の構成および監視』を参照してください。

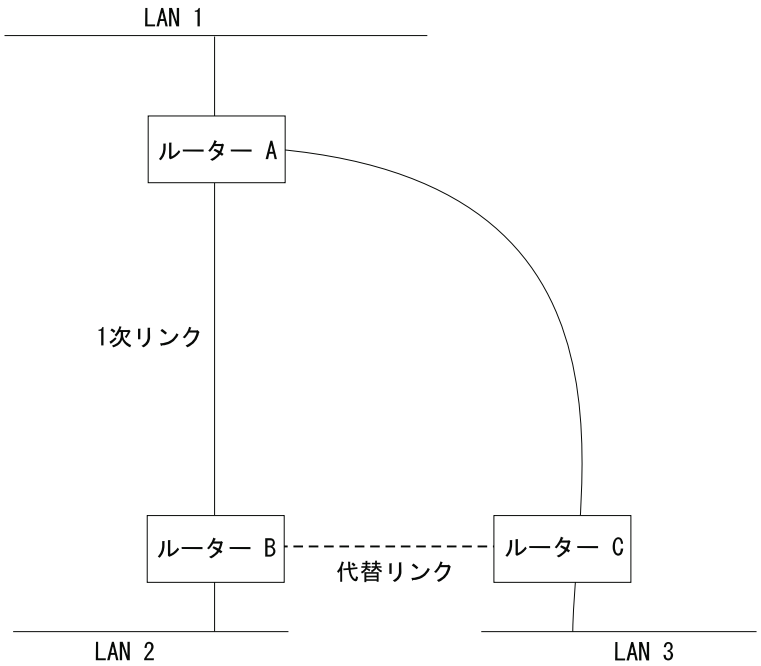


図3. WAN リルート. 通常は、ルーター A と B の間、およびルーター A と C の間にコネクションがあります。ルーター A と B のあいだの1 次リンクが失敗した場合、 WAN リルート機能により、ルーター B と C のあいだに代替リンクを確立するので、ルーター A と B は、ルーター C を介して通信できるようになります。

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 リ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、75ページの『WAN レストラル、WAN リルート、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 リルートの構成時に、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 リルート要求が生成されます。 WAN リルー

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 リ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、限界値を超過したとみなされます。

WAN リルートの構成

以下に示すのは、WAN リ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 リ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 リルート構成

100ページの図4 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 リ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 リ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。支社から本社への 1 次リンクの 1 つに障害が起きた場合、WAN リルートは別の支社を経由して本社に接続する代替ルートを確立します。

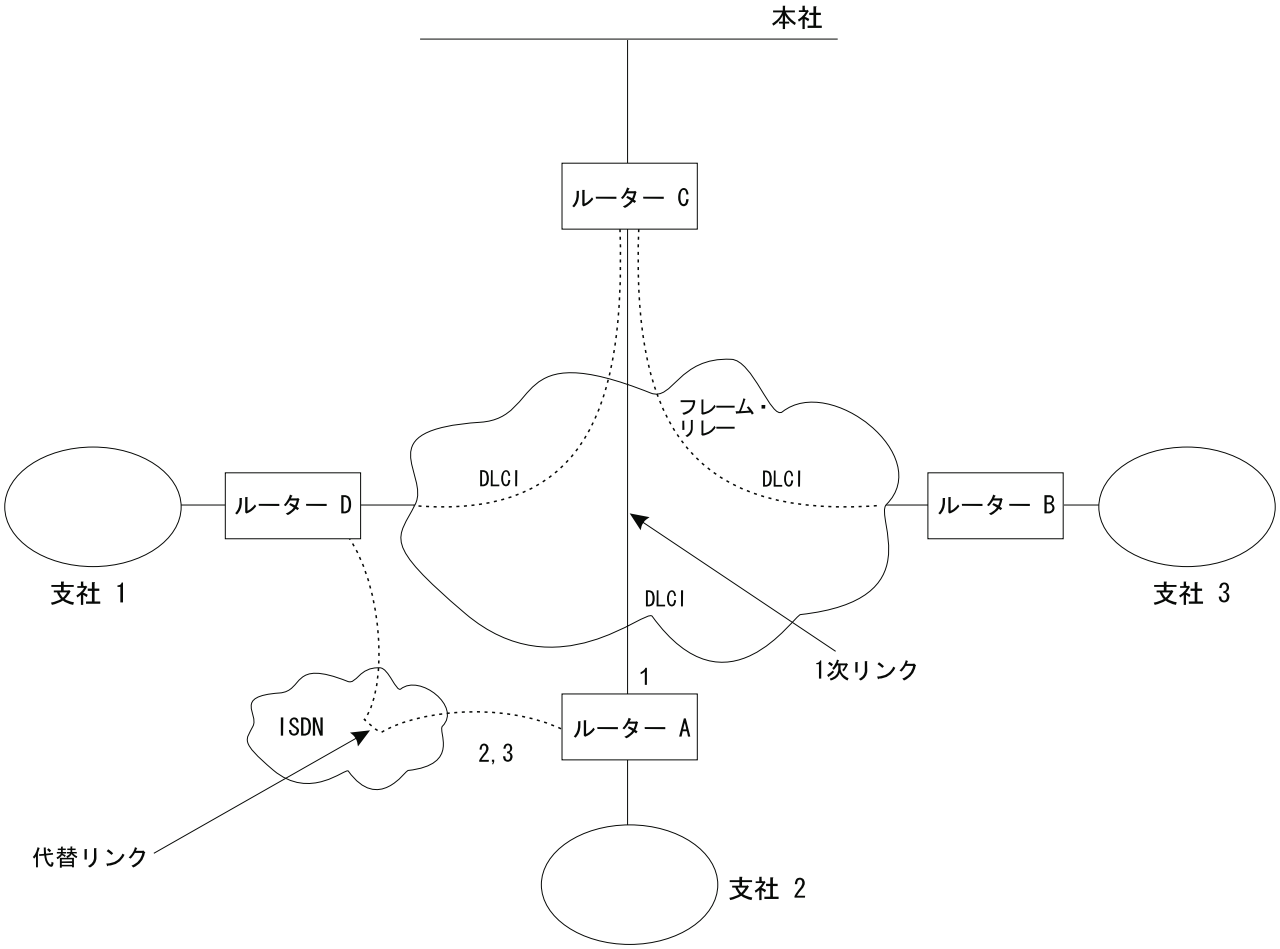


図 4. サンプル WAN リルート構成. 支社はフレーム・リレーを使用して本社に接続。

以下の節では、図4 のルーター A 上の WAN リ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 フィーチャーを使用可能にする。
- 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。
- この回路のダイヤル・オンデマンドを使用不可にするには、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`Circuit Config>` プロンプトで、 **set idle 0** コマンドを出す。
- 任意選択で、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 リ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 フィーチャーを使用可能にする。このフィーチャーが使用可能のとき、活動状態の 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 が非活動状態になると、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 が非活動状態になると、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. ISDN 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、*ソフトウェア使用者の手引き* の フレーム・リレー・インターフェースの使用 の項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 フィーチャーを使用可能にする。

   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、*ソフトウェア使用者の手引き* の ‘フレーム・リレーの使用’ の項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、*ソフトウェア使用者の手引き* の ‘ISDN インターフェースの使用’ の項を参照してください。

WAN レストラルとは異なり、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、代替リンクはリルートの必要がなくても接続を確立します。この場合、代替リンクをリ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活動状態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、最低優先順位の接続は終了され、高い優先順位の回線が接続を確立します。

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 リ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 3 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活動状態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 リ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。
- *ルーティング安定化期間 (Routing stabilization)*は、ルーターが代替リンクから 1 次リンクに戻ってから、1 次リンクと代替リンクをともにアクティブにしておく

時間の長さです。この時間は、代替リンクがダウンする前に、OSPF や RIP などのルーティング・プロトコルが 1 次リンクの新しいルートの可用性を確認するための時間です。

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 レストラル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、ルーティング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ルーティング安定化期間を設定するには、**set routing-stabilization** コマンドを使用します。

```
WRS Config>set routing-stabilization
Primary interface number [0]? 1
Routing stabilization time (0 - 3600 seconds) [15]?
```

7. オプションで、復帰の開始時刻と停止時刻 (time-of-day-revert-back) 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8章 ネットワーク・ディスパッチャー・フィーチャーの使用

この章では、ネットワーク・ディスパッチャー・フィーチャー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』
- 106ページの『ネットワーク・ディスパッチャーの使用による TCP および UDP トラフィックの平衡化』
- 107ページの『ネットワーク・ディスパッチャーの高可用性』
- 110ページの『ネットワーク・ディスパッチャーの構成』
- 119ページの『TN3270 でのネットワーク・ディスパッチャーの使用』
- 123ページの『クラスター・アドレス公示でのネットワーク・ディスパッチャーの使用』
- 124ページの『スケーラブル高可用性キャッシュ (SHAC) でのネットワーク・ディスパッチャーの使用』

ネットワーク・ディスパッチャーは、IBM が開発したロード・バランシング・テクノロジーを使用して、新規の接続のたびに、それ受け取るのに最も適したサーバーを判別します。これは、Solaris、Windows NT®、および AIX® 用の IBM の SecureWay ® ネットワーク・ディスパッチャー製品で使用される技術と同じものです。

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フィーチャーです。この転送は、ユーザーおよびアプリケーションには透過的に行われます。ネットワーク・ディスパッチャーは、E メール、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 アプリケーションなどのサーバー・アプリケーションに役立ちます。

また、ネットワーク・ディスパッチャーは、サーバー・グループへの状態なし UDP アプリケーション・トークンリングの負荷平衡を図るのにも役立ちます。

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、拡張が容易なソリューションを提供することにより、ユーザーのサイトの潜在的な能力を最大限に発揮させることができます。ネットワーク・ディスパッチャーは、ピーク需要時に、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、負荷平衡を図るのにドメイン名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、ネットワーク・ディスパッチャーが、動的に設定される重みに基づいて最適サ

ーバーと判断したサーバーに転送されます。これらの重みは、接続数、サーバーの負荷、およびサーバーの可用性を含めて、複数の因数に基づいて、ネットワーク・ディスパッチャーによって計算されます。

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、拡張が容易なサーバー・ネットワークを、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。世界からは、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、ドメイン名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・ディスパッチャーでは、SNMP ベースの管理アプリケーションを使用して、基本的な統計および潜在的なアラート状態を受信し、ネットワーク・ディスパッチャーを監視することができます。詳細については、*プロトコルの構成と監視 解説書 第 1 巻* の 『SNMP 管理』 の項を参照してください。

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・ディスパッチャーの使用による TCP および UDP トラフィックの平衡化

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を採用し、ドメイン名サーバーが、要求を処理するサーバーを選択します。この方法は比較的優れていますが、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一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・ディスパッチャーには、以下のコンポーネントが装備されています。

実行プログラム

受信した要求のタイプに基づいて、接続の負荷平衡を取ります。一般的な要求のタイプとしては、HTTP、FTP、および Telnet 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を用い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。ただし、アドバ

イザーを使用しない場合は、ネットワーク・ディスパッチャーは、サーバーに障害が起きても検出できないので、ダウンしたサーバーに新しい接続を引き続き送信します。

ネットワーク・ディスパッチャーは、FTP、HTTP、SMTP、NNTP、POP3、および Telnet 用のアドバイザー、IBM 2210、IBM 2212、および IBM 2216 内の TN3270 サーバーと協働する TN3270 アドバイザー、および MVS システム上のワークロード・マネージャー (WLM) と協働する MVS™ アドバイザーをサポートします。 WLM は、個々の MVS ID 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、WLM を利用して、OS/390® V1R3 以降のリリースを稼働する MVS サーバーへの要求の負荷平衡を図ることができます。

UDP プロトコル専用のプロトコル・アドバイザーはありません。 MVS サーバーを使用している場合は、MVS システム・アドバイザーを使用してサーバーの負荷情報を提供することができます。また、ポートが TCP および UDP トラフィックを扱っている場合は、適切な TCP プロトコル・アドバイザーを使用して、そのポートのアドバイザー入力を提供できます。ネットワーク・ディスパッチャーは、この入力を使用して、そのポート上の TCP および UDP の両方のトラフィックの負荷平衡を取ります。

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
- プロトコル・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・モニター (MVS アドバイザー) 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、ユーザーがマネージャーを使用しない場合、ネットワーク・ディスパッチャーは、ユーザーがサーバーごとに構成したサーバーの重みに基づいて、ラウンドロビン・スケジューリング方式で負荷の平衡を図ります。

ネットワーク・ディスパッチャーを使用して状態なし UDP トラフィックの負荷平衡を取る場合は、要求内の宛先 IP アドレスを使用してクライアントに応答したサーバーのみを使用する必要があります。詳細については、115ページの『ネットワーク・ディスパッチャー用のサーバーの構成』 を参照してください。

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リルートしません。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。標準 IP 回復機構を搭載したバックアップ用のネットワーク・ディスパッチャーを備えている場合でも、最善の場合でも、回復に時間がかかり、しかも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、同じサーバー・クラスターへの接続性、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
- 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 (特定のサーバー・クラスターを担当する) とスタンドバイ・ネットワーク・ディスパッチャー (そのサーバー・クラスタ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、迅速に 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、また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。

データベースの同期

1 次用とバックアップ用のネットワーク・ディスパッチャーは、″ハートビート″ 機構を使用して、双方のデータベースを同期化します。ネットワーク・ディスパッチャーのデータベースには、コネクション・テーブル、到達可能性テーブル、およびその他の情報が入っています。ネットワーク・ディスパッチャー高可用性機能は、データベース同期プロトコルを使用して、両方のネットワーク・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。この同期プロトコルは、既知の伝送遅延の誤差を考慮に入れます。プロトコルは、データベースの初期同期化を行い、その後は定期的に更新してデータベースの同期を維持します。

回復方法

ネットワーク・ディスパッチャーのマシンまたはインターフェース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るので、既存のクライアント・サーバー接続が保持されます。

IP 引き継ぎ

注: クラスター・アドレスの公示を使用する場合を除いて、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 (スタンドバイがアクティブになる) 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ブロードキャストされます。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・サイトにホスト名が 1 つしかなく、すべてのカスタマーがそれに接続する場合は、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5 に示します。

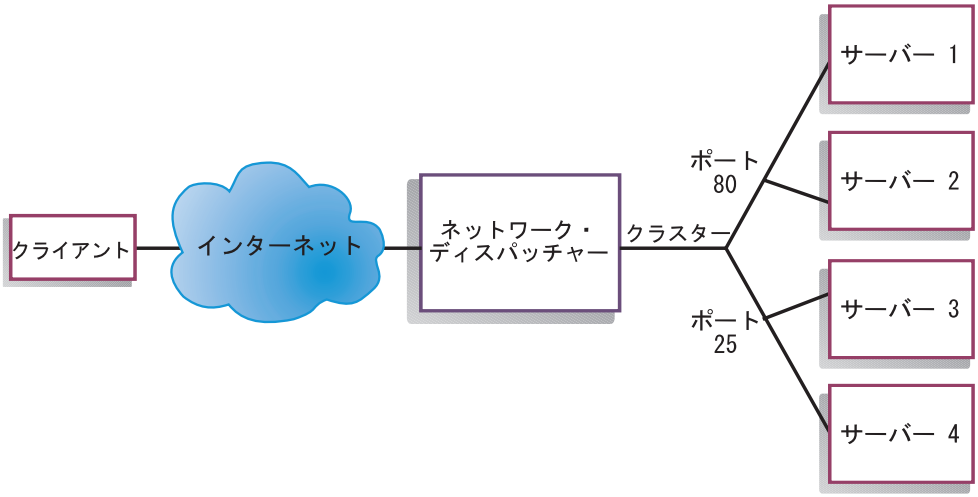


図5. 1 つのクラスターと 2 つのポートを持つように構成されたネットワーク・ディスパッチャーの例

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競合タイプのホスト接続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、111ページの図6 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。

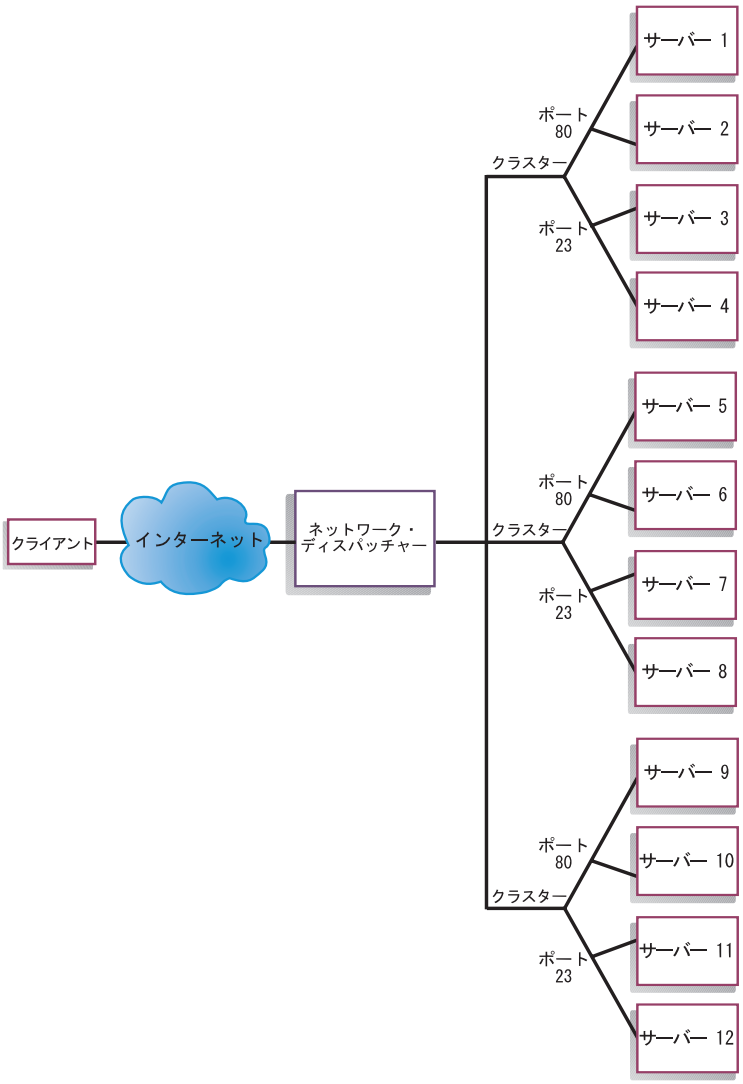


図 6. 3 つのクラスターと 3 つの URL を持つように構成されたネットワーク・ディスパッチャーの例

第 3 のネットワーク・ディスパッチャー構成方法は、サポートされる各プロトコル専用のサーバーが多数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専用の直接 T3 回線を、個別の FTP サーバーに構成するといったことが可能です。この場合は、112ページの図7 に示すように、各プロトコルについて、1 つのポートで複数のサーバーを持つクラスターを定義することができます。

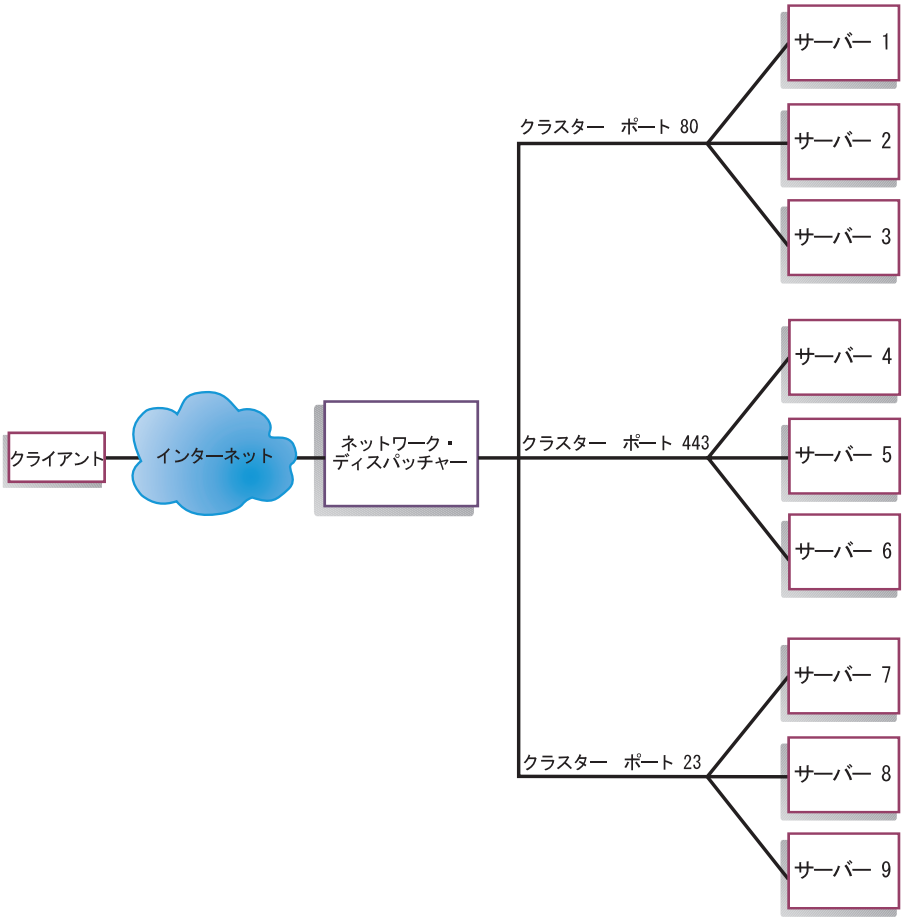


図7. 3 つのクラスターと 3 つのポートを持つように構成されたネットワーク・ディスパッチャーの例

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・ディスパッチャーにサーバーとの直接インターフェースがあることを確認する (つまり、各サーバー・マシンは、ネットワーク・ディスパッチャー・マシンにとってローカル側であるサブネットに直接接続されていなければなりません)。ネットワーク・ディスパッチャー・フィーチャーには、クライアントからサーバーに流れるトラフィックしか見えないので、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つことができ、これによりサーバーからクライアントへの発信トラフィックは、ネットワーク・ディスパッチャー・マシンをバイパスすることができます。こうしたタイプの発信コネクションを可能にするには、特別なネットワーク・ディスパッチャー構成は必要ありません。

   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は、113ページの図8に示した標準的な高可用性構成を参照してください。

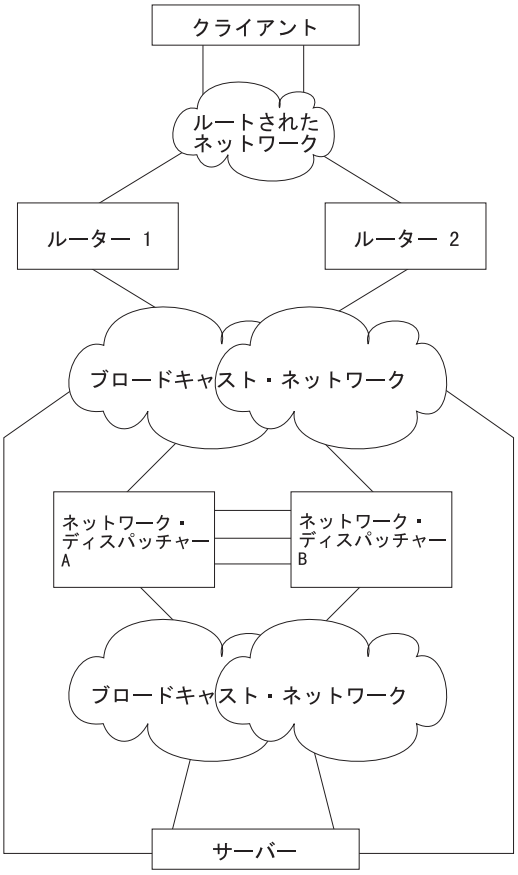


図 8. 高可用性ネットワーク・ディスパッチャー構成

2. ネットワーク・ディスパッチャー・マシンのインターフェースを構成する。この構成には、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が含まれます。ルーターの内部 IP アドレスは、ネットワーク・ディスパッチャーが使うので、set internal-ip-address コマンドを使って構成する必要があります。内部 IP アドレスは、ネットワーク・ディスパッチャーに構成されているクラスター・アドレスと一致してはいけません。 **set internal-ip-address** コマンドの詳細については、*プロトコルの構成と監視 解説書 第 1 巻* の「IP の構成および監視」の章を参照してください。
3. ネットワーク・ディスパッチャー・マシン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. `talk 6` で、**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・フィーチャーにアクセスする。
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。公示されるクラスター・アドレスを構成する場合、詳細については、123ページの『クラスター・アドレス公示でのネットワーク・ディスパッチャーの使用』を参照してくださ

い。ネットワーク・ディスパッチャーがクラスター・アドレスを公示しないことを選択する場合、公示されたサブネットの一部であり、ネットワーク・ディスパッチャーのルーターの位置にあるクラスター・アドレスを選択する必要があります。これは多くの場合サブネットで、このサブネットの上でネットワーク・ディスパッチャーが次ホップのルーターからクライアント・トラフィックを受け取ります。

注: クラスター IP アドレスは、ルーターの内部 IP アドレスと一致してはなりません。また、ルーターに定義されているどのインターフェース IP アドレスとも一致してはなりません。同じマシンでネットワーク・ディスパッチャーと TN3270 サーバーを実行しようとする場合、クラスター・アドレスは、ループバック・インターフェース上に定義される IP アドレスと一致する場合があります。詳しくは、119ページの『TN3270 でのネットワーク・ディスパッチャーの使用』を参照してください。

4. 対応するプロトコルにサービスする各サーバー・クラスターに対して、**add port** コマンドを使用して、TCP および UDP 宛先ポートを構成する。通常のポートの例は、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できます (つまり、1 つのサーバーは、同じクラスターの複数のポートの下で定義できます)。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は、1 つのサーバーが複数のクラスターに所属することもできます。
6. **add advisor** コマンドを使用して、アドバイザーを構成する。

   注:

   a. MVS アドバイザーの場合、どのクラスターにもポート番号値 (デフォルト = 10007) を定義してはなりません。このポート番号は、MVS アドバイザーが MVS システム内の WLM との通信するためにのみ使用します。

   b. TN3270 アドバイザーの場合は、2 つのポート値を入力します。クライアントとサーバー間の通信に使用するポート番号値 (デフォルト = 23) を、該当するクラスターに定義する必要があります。通信ポート値 (デフォルト = 10008) は、どのクラスターにも定義してはなりません。通信ポート値は、TN3270 アドバイザーが TN3270 サーバーからロード情報を収集するためにのみ使用します。
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し、**set manager** コマンドを使用して、アドバイザー入力を重みの計算に含むように、マネージャーの比率を設定する。

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。 データベースが正しく同期化されるのを保証するために、バックアップの実行プログラムを使用可能にする前に、1 次ネットワーク・ディスパッチャーの実行プログラムを使用可能にしておくことが必要です。

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 次ネットワーク・ディスパッチャーとバックアップ・ネットワーク・ディスパッチャー間のハートビートを実行するすべてのパスを構成する。パスは、発信元と宛先の IP アドレスで指定します。

   注: 1 つのインターフェースに障害が起きても、1 次マシンとバックアップ・マシン間のハートビート通信が損なわれないようにするために、1 次とバックアップのネットワーク・ディスパッチャー間には、2 つ以上のハートビート・パスを構成しておく必要があります。

   2 つのネットワーク・ディスパッチャー間に既存の LAN コネクションが 1 つしかない場合、2 番目のハートビートは、シンプル LAN コネクション (たとえば、2 つのイーサネット・ポート間で直接使用されるクロスオーバー・ケーブル)、またはポイントツーポイント・シリアル・コネクション (たとえば、非番号制 IP を使用する、ヌル・モデム・ケーブル上のバックツーバック PPP コネクション) で設定できます。
10. 完全なサービスを保証するために、**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到達できなければならないホスト 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になります。ネットワーク・ディスパッチャーのトラフィックが流れるインターフェースごとに、1 つ以上の到達可能アドレスを構成する必要があります。

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。これらのコマンドの詳細については、127ページの『第9章 ネットワーク・ディスパッチャー・フィーチャーの構成および監視』 を参照してください。

ネットワーク・ディスパッチャー用のサーバーの構成

ネットワーク・ディスパッチャーで使用するでサーバーは、次のように構成します。

1. ループバック装置に別名を付ける。

   TCP および UDP サーバーが機能するためには、ループバック装置 (通常は ***lo0*** と呼ばれる) をクラスター・アドレスに設定する (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、パケットをサーバー・マシンに転送する前に、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、サーバー・マシンはクラスター・アドレスあてのパケットを受け入れます。

   サーバーが自分の IP アドレスではなくクラスター・アドレスを使用してクライアントに応答するということは、重要なことです。このことは、TCP サーバーの場合は問題になりませんが、UDP サーバーの場合は、クラスター・アドレスあてに送信された要求に応答するときに自分の IP アドレスを使用するものが含まれています。サーバーが自分の IP アドレスを使用している場合、一部のクライアントは、それが予期した発信元 IP アドレスからのものではないために、サーバーの応答を廃棄してしまいます。要求からの宛先 IP アドレスをクライアントへの応答に使用する UDP サーバーのみを使用することが必要です。この場合、要求からの宛先 IP アドレスは、クラスター・アドレスです。

ネットワーク・ディスパッチャーの使用

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は、ループバック装置の別名をクラスター・アドレスに指定する必要があります。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、複数のクラスター・アドレスにサービスするようにサーバー・マシンを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・アドレスとして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・アドレスとして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・アドレスとして設定する必要があります。高可用性を使用している場合、高可用性引き継ぎ機構を正しく機能させるためには、MVS システム内の RouteD を使用可能にしなければなりません。

注: この章にリストされているコマンドは、以下のオペレーティング・システムおよびレベルでテスト済みです。すなわち、AIX 4.2.1 と 4.3、HP-UX 10.2.0、Linux、OS/2 Warp Connect バージョン 3.0、OS/2 Warp バージョン 4.0、Solaris 2.6 (Sun OS 5.6)、Windows NT 3.51 と 4.0、および OS/390 です。

ループバック装置の設定または別名指定には、表10 に示すように、ご使用のオペレーティング・システムのコマンドを使用してください。

表 10. ディスパッチャーのループバック装置の別名指定用のコマンド

システム	コマンド
AIX	**ifconfig lo0 alias** *cluster_address* **netmask** *netmask*
HP-UX	**ifconfig lo0** *cluster_address*
Linux	**ifconfig lo:1** *cluster_address* **netmask** *netmask* **up**
OS/2	**ifconfig lo** *cluster_address*
Solaris	**ifconfig lo0:1** *cluster_address* **127.0.0.1 up**

表 10. ディスパッチャーのループバック装置の別名指定用のコマンド (続き)

システム	コマンド
Windows NT	a. 「**スタート**」をクリックして、「**設定**」をクリックします。 b. 「**コントロール・パネル**」をクリックし、「**ネットワーク**」をダブルクリックします。 c. まだ行っていない場合は、MS ループバック・アダプター・ドライバーを追加します。 1) 「ネットワーク」ウィンドウで、「**アダプター**」をクリックします。 2) 「**MS ループバック・アダプター**」を選択して、「**OK**」をクリックします。 3) 指示されたら、インストール CD またはディスクを挿入します。 4) 「ネットワーク」ウィンドウで、「**プロトコル**」をクリックします。 5) 「**TCP/IP プロトコル**」を選択し、「**プロパティー**」をクリックします。 6) 「**MS ループバック・アダプター**」を選択して、「**OK**」をクリックします。 d. ループバック・アドレスをクラスター・アドレスとして設定します。デフォルトのサブネット・マスク (255.0.0.0) を受け入れ、ゲートウェイ・アドレスは入力しないでください。 **注:** 「ネットワークの設定」をいったん終了し、再びこの画面に入らないと、「TCP/IP 構成」の下に「MS ループバック・ドライバー」が表示されないことがあります。

OS/390	OS/390 システム上でのループバック別名の設定
	• IP パラメーター・メンバー (ファイル) で、管理者は Home アドレス・リスト内にエントリーを作成する必要があります。たとえば、次のように入力します。
	`HOME`
	`;Address Link`
	`192.168.252.11 tr0`
	`192.168.100.100 ltr1`
	`192.168.252.12 loopback`
	• ループバックに複数のアドレスを定義できます。
	• デフォルトでは 127.0.0.1 が構成されます。

2. 余分なルートがないかチェックする。

   一部のオペレーティング・システムでは、デフォルトのルートが作成されており、削除することが必要になる場合があります。

   a. Windows NT 上に余分なルートがないか検査するには、**route print** コマンドを使用します

   b. すべての UNIX® システムおよび OS/2® 上に余分なルートがないかどうかを検査するには、**netstat -nr** コマンドを使用します

   c. Windows NT の例: route print コマンドを入力すると、次のようなテーブルが表示されます。 (この例は、デフォルトのネットマスク 255.0.0.0. を使用して、クラスター 9.67.133.158 への余分なルートを検出し、除去する場合を示しています。)

```
Active Routes:
      Network Address          Netmask  Gateway Address        Interface  Metric
              0.0.0.0          0.0.0.0      9.67.128.1      9.67.133.67     1
              9.0.0.0        255.0.0.0     9.67.133.158     9.67.133.158     1
           9.67.128.0    255.255.248.0      9.67.133.67      9.67.133.67     1
          9.67.133.67  255.255.255.255        127.0.0.1        127.0.0.1     1
         9.67.133.158  255.255.255.255        127.0.0.1        127.0.0.1     1
       9.255.255.255  255.255.255.255      9.67.133.67      9.67.133.67     1
           127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1     1
           224.0.0.0        224.0.0.0     9.67.133.158     9.67.133.158     1
           224.0.0.0        224.0.0.0      9.67.133.67      9.67.133.67     1
     255.255.255.255  255.255.255.255      9.67.133.67      9.67.133.67     1
```

d. ″Gateway アドレス″ 列でクラスター・アドレスを見つけます。余分なルートがある場合、そのクラスター・アドレスは 2 度表示されます。この例では、クラスター・アドレス (9.67.133.158) が 2 行目と 8 行目に表示されています。

e. クラスター・アドレスが表示されている各行で、ネットワーク・アドレスを見つけます。これらのルートのうちの一方は必要なものであり、他方の余分なルートを削除することが必要です。削除すべき余分なルートは、ネットワーク・アドレスがクラスター・アドレスの第 1 桁で始まっており、その後に 3 つのゼロが続いているものです。この例では、余分なルートは 2 行目のもので、そのネットワーク・アドレスは 9.0.0.0 になっています。

```
9.0.0.0        255.0.0.0     9.67.133.158     9.67.133.158     1
```

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11 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 11. 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** *cluster_address 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:** a. 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。 b. Windows NT の場合、サーバーをリブートするたびに、余分のルートを削除する必要があります。 c. サーバーをリブートするたびに余分のルートを手作業で削除しなくても済むようにするには、各サーバーのリブート後に余分のルートを自動的に削除するサービスを、Windows NT Resource Kit を使用して作成し、インストールすることができます。

TN3270 でのネットワーク・ディスパッチャーの使用

ネットワーク・ディスパッチャーは、大規模な 3270 環境に TN3270E サーバー・サポートを提供するために TN3270E サーバー機能を稼働している 2210、2212、ネットワーク・ユーティリティー、または 2216 のクラスターで使用することができます。 TN3270 アドバイザーを使用すると、ネットワーク・ディスパッチャーは各 TN3270E サーバーからの負荷統計をリアルタイムで収集し、負荷を TN3270E サーバー間に可能な限り最適に配分することができます。ネットワーク・ディスパッチャー・ルーターの外部の TN3270E サーバーに加えて、クラスター内の TN3270E サーバーの中の 1 台を内部にする、つまりネットワーク・ディスパッチャーと同じルーター内で稼働することができます。

構成の要点

外部 TN3270E サーバー (つまり、TN3270E サーバーが、ネットワーク・ディスパッチャーと同じルーターで稼働していない) の構成は、独立型の TN3270E サーバーの設定と本質的に同じです。事実、TN3270E サーバーは、クライアントからのトラフィックが別のマシンを経由して転送されたかどうかを認知しません。ただし、ネットワーク・ディスパッチャー用に外部 TN3270E サーバーを設定する際には、いくつかの点に注意する必要があります。

- TN3270E サーバーを設定する際には、TN3270E サーバーの IP アドレスも、サーバー・マシン上でインターフェース・アドレスとして構成する必要があります。クライアントは、TN3270E サーバーの IP アドレスにパケットを送信し、サーバー・マシンは、そのパケットを受け入れて、ローカル機能 (この場合は、TN3270E サーバー機能) に送達します。 TN3270E サーバーの前にネットワーク・ディスパッチャーがある場合、クライアントは、ネットワーク・ディスパッチャーのクラスター IP アドレスにパケットを送信し、ネットワーク・ディスパッチャーは、パケットを変更せずにサーバーに転送します。したがって、パケットは、クラスター IP アドレスと等しい宛先 IP アドレスを持つサーバー・マシンに到着します。したがって、各サーバー内の TN3270 サーバー IP アドレスは、クラスター IP アドレスと等しく設定する必要があり、クラスター IP アドレスは、各サーバー・マシン上でインターフェース・アドレス (IP が使用可能な任意のインターフェース) としても定義する必要があります。そのため、パケットはサーバー・マシンによって受け入れられ、TN3270E サーバー機能にローカルに送達されます。
- TN3270E サーバー上で使用されているルーティング・プロトコル (たとえば、OSPF または RIP) の中に、クラスター・アドレスを公示するものが含まれていないことを確認する必要があります。クライアント・ネットワークに関する限り、ネットワーク・ディスパッチャー・ルーターはクラスター・アドレスを 『独占』 している必要があります。
- クライアントからネットワーク・ディスパッチャーへのトラフィックが、ネットワーク・ディスパッチャーからサーバーへのトラフィックと同じ LAN 上を流れる場合、クラスター・アドレスについて ARP にサーバーが応答しないようにする必要があります。すなわち、サーバーのインターフェース上では、クラスター・アドレスをこの LAN に定義することはできません。クライアントのトラフィックをネットワークから受け取る LAN (単数または複数) 上の ARP に応答するのは、ネットワーク・ディスパッチャーだけであるようにすることが必要で

す。クラスター・アドレスは、別のインターフェース上のインターフェース・アドレスとして TN3270E サーバーに構成したり、TN3270E サーバーの内部 IP アドレスとして構成することもできます。

- 各 TN3270E サーバーは、固有のサーバー IP アドレスでネットワーク・ディスパッチャーに構成する必要があります。これは、ネットワーク・ディスパッチャーがサーバーを検出するのに使用するアドレスです。このアドレスは、TN3270E サーバー機能を実行するルーターのインターフェース・アドレスとしても構成する必要があります。固有のサーバー IP アドレスが、ネットワーク・ディスパッチャー・マシンにとってローカル側にあるサブネットの一部ではない場合、ネットワーク・ディスパッチャーは、ネットワーク・ディスパッチャー・マシンに定義されたスタティック・ルートを介して、またはサーバーの固有 IP アドレスを公示するルーティング・プロトコルを介して、サーバーを検出できなければなりません。
- 非活動期間がクラスターの stale-timeout を超えるときに、TN3270 コネクションが、早過ぎる時期にネットワーク・ディスパッチャー・コネクション・テーブルから削除されないようにするために、クラスターの stale-timeout より小さいタイムアウト値を指定して、TN3270E サーバーのキープアライブ・タイマーをタイミング・マーク・モードで構成する必要があります。 TN3270E サーバーは、クライアントにメッセージを送信し、応答を要求して、コネクションが古くならないようにします。

TN3270E サーバーがネットワーク・ディスパッチャーと同じルーター内にあるときは、次のことが適用できます。

- 内部 TN3270E サーバーに対して負荷が平衡化されたパケットは、クラスター・アドレスをパケットの宛先 IP アドレスとしているので、TN3270E サーバーの IP アドレスは、クラスター・アドレスとして構成する必要があります。
- TN3270E サーバーがネットワーク・ディスパッチャー・マシンの外部にある場合は、TN3270E サーバーの IP アドレスは、内部 IP アドレスまたはインターフェース・アドレスとしてルーターに定義して、パケットが TN3270E サーバー機能にローカル側で送達できるようにする必要があります。 TN3270E サーバーがネットワーク・ディスパッチャー・ルーターの内部にある場合は、TN3270E サーバーの IP アドレスは、内部 IP アドレスまたはインターフェース・アドレスとしてルーターに定義することはできません。 TN3270E サーバーの IP アドレス (つまり、クラスター・アドレス) が、内部 IP アドレスまたはインターフェース・アドレスとして定義されている場合、パケットは、ネットワーク・ディスパッチャーに到着するのではなく、ルーター内の TN3270E サーバー機能に直接進みます。
- 各 TN3270E サーバーは、固有のサーバー IP アドレスでネットワーク・ディスパッチャーに構成する必要があります。内部 TN3270E サーバーの場合、サーバー固有の IP アドレスを、ネットワーク・ディスパッチャー・マシンの内部 IP アドレスに等しく構成してください。
- V3.4 より前では、TN3270E サーバーは、ネットワーク・ディスパッチャーによる内部アクセスか、外部アクセスのどちらかにでも設定できましたが、内部と外部の両方にしたり、内部と外部を切り替えたりすることはできませんでした。その結果、両方のネットワーク・ディスパッチャー・ルーターに内部 TN3270E サーバーを置いて、ネットワーク・ディスパッチャー高可用性ソリューションを実

装すると、片方のルーターのネットワーク・ディスパッチャーが、もう一方のネットワーク・ディスパッチャー・ルーターにある TN3270E サーバーと負荷を平衡化できなくなります。

MRS V3.4 から、両方のネットワーク・ディスパッチャー・ルーターに内部 TN3270E サーバーを置いてネットワーク・ディスパッチャー高可用性ソリューションを実装すると、内部 TN3270E サーバーにどちらのネットワーク・ディスパッチャーからでもアクセスするように設定できます。両方のネットワーク・ディスパッチャー・ルーターにループバック装置を追加し、各ループバック・インターフェース上に TN3270E サーバーの IP アドレス (つまり、クラスター・アドレス) を定義するだけです。ネットワーク・ディスパッチャーがアクティブ状態である場合、ループバック・インターフェース上のクラスター・アドレスは使用不可になり、そのクラスター・アドレスを宛先とするパケットは、ネットワーク・ディスパッチャーに到着します。ネットワーク・ディスパッチャーがスタンドバイ状態である場合、ループバック・インターフェース上のクラスター・アドレスは使用可能になるので、そのクラスター・アドレスを宛先とするパケットは、ローカル側で TN3270E サーバーに送達されます。このように、内部 TN3270E サーバーは、高可用性設定で両方のネットワーク・ディスパッチャーによって使用することができます。

アクティブなネットワーク・ディスパッチャー・マシンだけが、クラスター・アドレスについて ARP に応答するマシンでなければなりません。クラスター・アドレスは、ループバック・インターフェース上の両方のネットワーク・ディスパッチャー・マシンで定義されるので、両方のネットワーク・ディスパッチャー・マシンでプロキシー ARP を使用不可にして、スタンドバイ・ネットワーク・ディスパッチャー・マシンが、クラスター・アドレスについて ARP に応答しないようにする必要があります。

また、アクティブなネットワーク・ディスパッチャー・マシンは、クライアント・ネットワークに関する限り、クラスター・アドレスも独占する必要があるので、スタンドバイ・ネットワーク・ディスパッチャー・マシン (クラスター・アドレスがループバック・インターフェース上で定義されている) は、クラスター・アドレスを公示できません。デフォルトでは、RIP は、ホスト・ルート (マスク 255.255.255.255 があるルート) を公示しませんが、ホスト・ルートの公示が使用可能である場合は、RIP ポリシーを定義して、クラスター・アドレスの公示を使用不可にする必要があります。

次の例は、RIP がクラスター IP アドレス (ここでは 10.0.0.1 であると想定されています) を公示しないようにするポリシーを示しています。 2 番目のポリシー・エントリーにより、RIP はその他のすべてのルートを公示できることに注意してください。

```
IP config> add route-policy
Route Policy Identifier [1-15 characters] []? rip-send
Use strictly linear policy? [No]: yes
IP config>change route-policy rip-send
rip-send IP Route Policy Configuration
IP Route Policy Config> add entry
Route Policy Index [1-65535] [0]? 1
IP Address [0.0.0.0]? 10.0.0.1
IP Mask [0.0.0.0]? 255.255.255.255
Address Match (Range/Exact) [Range]? exact
Policy type (Inclusive/Exclusive) [Inclusive]? exclusive
IP Route Policy Config> add entry
Route Policy Index [1-65535] [0]? 2
IP Address [0.0.0.0]?
```

```
IP Mask [0.0.0.0]?
Address Match (Range/Exact) [Range]?
Policy type (Inclusive/Exclusive) [Inclusive]?
IP Route Policy Config> list

IP Address      IP Mask           Match  Index  Type
-------------------------------------------------------
10.0.0.1        255.255.255.255   Exact  1      Exclude
0.0.0.0         0.0.0.0           Range  2      Include
IP Route Policy Config> exit
IP config>enable sending policy global rip-send
IP config>
```

OSPF の場合、AS 境界ルーティング、および直接ルートのインポートが使用可能であるか、OSPF がループバック・インターフェース上で使用可能であると、ループバック・インターフェース上で定義されるクラスター・アドレスが公示されるので、ユーザーは、クラスター・アドレスの公示を使用不可にするために OSPF ポリシーを定義する必要があります。

次の例は、OSPF がクラスター IP アドレス (ここでは 10.0.0.1 であると想定されています) をインポートしないようにするポリシーを示しています。 2 番目のポリシー・エントリーにより、OSPF はその他のすべての直接ルートをインポートできることに注意してください。

```
IP> add route-policy ospf-send
Use strictly linear policy? [No]: yes
IP config> change route-policy ospf-send
ospf-send IP Route Policy Configuration
IP Route Policy Config> add entry
Route Policy Index [1-65535] [0]? 1
IP Address [0.0.0.0]? 10.0.0.1
IP Mask [0.0.0.0]? 255.255.255.255
Address Match (Range/Exact) [Range]? exact
Policy type (Inclusive/Exclusive) [Inclusive]? exclusive
IP Route Policy Config> add entry
Route Policy Index [1-65535] [0]? 2
IP Address [0.0.0.0]?
IP Mask [0.0.0.0]?
Address Match (Range/Exact) [Range]?
Policy type (Inclusive/Exclusive) [Inclusive]?
IP Route Policy Config> add match-condition protocol direct
Route Policy Index [1-65535] [0]? 2
Route policy entry match condition updated or added
IP Route Policy Config> list

IP Address      IP Mask           Match  Index  Type
-------------------------------------------------------
10.0.0.1        255.255.255.255   Exact  1      Exclude
0.0.0.0         0.0.0.0           Range  2      Include
    Match Conditions:  Protocol: Direct
IP Route Policy Config> exit
IP config> exit
Config> protocol ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config> enable as
Use route policy? [No]: yes
Route Policy Identifier [1-15 characters] []? ospf-send
Always originate default route? [No]:
Originate default if BGP routes available? [No]:
OSPF Config>
```

明示的な LU とネットワーク・ディスパッチャー

ネットワーク・ディスパッチャー環境で明示的 LU を定義する場合は、特別な注意が必要です。暗黙的または明示的 LU へのセッション要求を、任意のサーバーに転送することができます。このことは、どのサーバーにセッションが転送されるのかは前もって分からないので、明示的 LU は各サーバーに定義しておく必要があることを意味しています。

クラスター・アドレス公示でのネットワーク・ディスパッチャーの使用

クラスター・アドレス公示を使用すると、ネットワーク・ディスパッチャー内に定義される各クラスター・アドレスが、ネットワーク・ディスパッチャー・マシン内で使用可能になっているルーティング・プロトコルによって公示されるかどうかを構成することができます。クラスター・アドレスが公示されない場合、ネットワーク・ディスパッチャー・マシンにとってローカル側である公示サブネットの一部であるクラスター・アドレスを選択する必要があります。公示されるように構成されるクラスター・アドレスは、ホスト・ルートとして公示され、公示されるサブネットの一部である必要はありません。クラスター・アドレスの公示は、次のシナリオで便利です。

- 同じコンテンツを提供する、地理的に分散した複数のサーバー・サイトがあり、クライアントを最も近いアクティブなサーバー・サイトに接続したい場合があります。クラスター・アドレス公示を使用してこれを実現するには、すべてのサーバー・サイトで同じクラスター・アドレスを構成し、それらのクラスター・アドレスをすべてのサイトから公示します。ネットワーク内のルーティング・プロトコルは、最も近いサーバー・サイトに各クライアント・コネクションを送信します。最も近いサイトがダウンしている場合、コネクションは次に最も近いサーバー・サイトに進みます。ネットワーク内の変更 (ルーターまたは通信リンクがダウンするか、元の状態に戻る)、またはサーバー・サイトの可用性の変更により、既存のクライアント・サーバー・コネクションの途中であっても、最も近いサーバー・サイトが変わる場合があることに注意してください。これは、HTTP のように存続期間が短いコネクションでは問題ではありませんが、Telnet や TN3270 のような存続期間が長いコネクションの場合は問題であると見なされます。
- クラスター・アドレス公示を使用すると、クラシカル IP ATM ネットワーク上でネットワーク・ディスパッチャーの高可用性を使用することができます。スタンドバイ・ネットワーク・ディスパッチャーがアクティブ・ネットワーク・ディスパッチャーから処理を引き継ぐ場合、すべてのインターフェース上で ARP を送信して、クラスター・アドレスを宛先とする今後のトラフィックが、新しい MAC アドレスに送信されるようにします。クラシカル IP ATM を使用する場合、ARP サーバーは更新されますが、ARP サーバーは、クライアントがキャッシュをリフレッシュすることを強制することはできません。クライアント・キャッシュが更新されるのは、クライアントに設定されたリフレッシュ・タイムアウトが満了した後です。これには数分かかる場合があります。 1 次ネットワーク・ディスパッチャーの ATM アドレスをキャッシュに入れていないクライアントからのコネクションは、ただちにバックアップ・ネットワーク・ディスパッチャーに到着しますが、引き継ぎの時点で存在していたコネクションは失われます。そのコネクションが再確立されるのは、そのクライアントのクライアント・リフレッシュ・タイマーが切れて、クライアントのキャッシュが更新された後です。ATM サブネットの一部ではないクラスター・アドレスをルーターに定義し、そ

れらのクラスター・アドレスを公示すると、ルーティング・プロトコルによって、クラスター・アドレスを宛先とするトラフィックが、適切なネットワーク・ディスパッチャーにルート指定されます。 1 次ネットワーク・ディスパッチャーは、スタンドバイ状態に入ると、クラスター・アドレスの公示を停止し、バックアップ・ネットワーク・ディスパッチャーは、アクティブになると、クラスター・アドレスの公示を開始します。

ネットワーク・ディスパッチャー・マシン内のルーティング・プロトコルは、クラスター・アドレスを公示する前に、正しく構成しておく必要があります。

- RIP の場合、ホスト・ルートの送信を使用可能にする必要があります。
- OSPF の場合、AS 境界ルーティングを使用可能にし、直接ルートとサブネット・ルートの両方をインポートする必要があります。
- BGP の場合、元のポリシー内のアドレスの範囲に、公示されるクラスター・アドレスが含まれていることを確認し、classless-bgp を使用可能にする必要があります。

スケーラブル高可用性キャッシュ (SHAC) でのネットワーク・ディスパッチャーの使用

Web サーバー・キャッシュのグループと共にネットワーク・ディスパッチャーを使用すると、スケーラブル高可用性キャッシュを作成することができます。スケーラブル高可用性キャッシュ (SHAC) は、1 台または 2 台のネットワーク・ディスパッチャー・マシン (2 番目のマシンは、最初のマシンのバックアップとして使用されます)、複数の Web サーバー・キャッシュ・マシン、および 1 台以上のバックエンド・サーバーで構成されます。 125ページの図9 は、SHAC の設定例を示しています。ネットワーク・ディスパッチャー・マシンは、クライアント・トラフィックの負荷をキャッシュ・マシンと平衡化し、キャッシュ・マシンは、キャッシュからのファイルを扱うか、またはファイルがキャッシュに入っていない場合は、バックエンド・サーバーからファイルを取得します。

ネットワーク・ディスパッチャー・マシンでは、クラスターとポートを構成する必要があります。ポートのモードは、外部のスケーラブルなキャッシュ配列の負荷を平衡化することを指定するために、*extcache* に設定する必要があります。 128ページの『Add』の **add port** コマンドを参照してください。ポートでは、キャッシュ・マシンはサーバーとして構成されます。他のサーバーと同様に、ネットワーク・ディスパッチャー・マシンで構成される固有なサーバー IP アドレスには、キャッシュのインターフェース IP アドレスが使用されます。 SHAC にとっては、アドバイザーと管理プログラムが重要になります。外部キャッシュがあるポート (つまり、ポート・モードが extcache である) では、ネットワーク・ディスパッチャー・マシンで HTTP アドバイザーを使用可能にする必要があります。キャッシュが操作可能かどうかは、アドバイザーの照会で判断します。マネージャーを使用可能にする必要があり、マネージャーの比率が、重みの計算にアドバイザー入力を含むように設定されなければなりません (つまり、アドバイザーのパーセントを 0 より大きい値に設定します)。

ネットワーク・ディスパッチャー・マシンのクラスタ / ポートで、キャッシュをサーバーとして構成する場合、キャッシュ・マシン上のネットワーク・ディスパッチャー機能にも同じクラスターとポートを構成する必要があります。キャッシュ・マ

シンに定義されるポートは、mode cache に設定される必要があり、バックエンド・サーバーは、これらのポートでサーバーとして定義されます。また、バックエンド・サーバーの負荷と可用性を決定できるように、HTTP アドバイザーは、キャッシュ・マシンでも実行される必要があります。

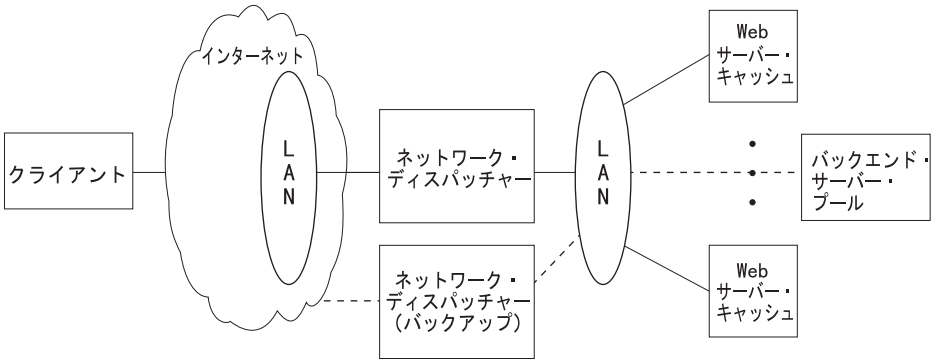


図 9. LAN に接続されたサーバー

第9章 ネットワーク・ディスパッチャー・フィーチャーの構成および監視

この章では、ネットワーク・ディスパッチャー・フィーチャーの構成コマンドおよび操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コマンド』
- 147ページの『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』
- 147ページの『ネットワーク・ディスパッチャー監視コマンド』
- 156ページの『ネットワーク・ディスパッチャーの動的再構成サポート』

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12 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 12. 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
? (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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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、サーバー、および到達可能アドレスを構成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を構成することができ、またハートビートに使用する IP アドレスも構成できます。

構文:

add advisor . . .
backup . . .
cluster . . .
heartbeat . . .
port . . .
reach . . .
server . . .

Advisor *name port# interval timeout comm-port*

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の報告が古いと見なされる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。追加しようとするアドバイザーのタイプと対応するアドバイザー番号を入力します。

表 13. アドバイザー名とポート番号

アドバイザー番号	アドバイザー名	デフォルト・ポート番号
0	FTP	21
1	HTTP	80
2	MVS	10007
3	TN3270	23
4	SMTP	25
5	NNTP	119
6	POP3	110
7	TELNET	23
8	SSL	443

有効値: 0 ～ 8

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: 1 ～ 65535

デフォルト値: 表13 を参照

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: 1 ～ 65535

デフォルト値: 5

timeout

アドバイザーの報告が古いと見なされる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場合、マネージャーは使用する必要がある報告を無視することになります。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、アドバイザーの報告がタイムアウトにならないことを意味しています。

comm-port

TN3270 アドバイザーが TN3270 サーバーと通信するのに使用するポート番号を指定します。このパラメーターは、TN3270 アドバイザーの入力にのみ使用します。 TN3270 サーバー構成で設定されるアドバイザー・ポート番号と一致する必要があります。

有効値: 1 〜 65535

デフォルト値:

- TN3270 デフォルト値:10008

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。不可平衡の決定に使用するサーバーのウェイトを設定するときにマネージャーがアドバイザーの入力を考慮するよう、管理プログラムの比率も設定しておきます。また、アドバイザーが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 の構成および監視を参照してください。

例 1:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL) [1]? 1
Port number [80]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
```

例 2:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL) [1]? 3
Port number [23]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
Communication Port number [10008]?
```

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。その場合には、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、自動的に活動ネットワーク・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 talk 5 で **switchover** コマンドを使用しないと、再びそれを活動状態にすることはできません。 155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 Stale-timer Advertise-cluster-address Advertise-route-cost*

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。公示されるクラスター・アドレスを構成する場合、詳細については、123ページの『クラスター・アドレス公示でのネットワーク・ディスパッチャーの使用』を参照してください。クラスター・アドレスが公示されるように構成されていない場合、ネットワーク・ディスパッチャー・マシンにとってローカル側である公示サブネットの一部であるクラスター・アドレスを選択する必

要があります。これは多くの場合サブネットで、このサブネットの上でネットワーク・ディスパッチャーが次ホップのルーターからクライアント・トラフィックを受け取ります。

注: クラスター IP アドレスは、ルーターの内部 IP アドレスと一致してはなりません。また、ルーターに定義されているどのインターフェース IP アドレスとも一致してはなりません。同じマシンでネットワーク・ディスパッチャーと TN3270 サーバーを実行しようとする場合、クラスター・アドレスは、ループバック・インターフェース上に定義される IP アドレスと一致する場合があります。詳しくは、119ページの『TN3270 でのネットワーク・ディスパッチャーの使用』を参照してください。

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* または *Stale-timer* 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

Stale-timer

コネクションが非活動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

Advertise-cluster-address

クラスター・アドレスが公示されるかどうかを指定します。

有効値: yes または no

デフォルト値: No

Advertise-route-cost

公示されるルートのコストを指定します。この質問が尋ねられるのは、**advertise cluster address** に対する応答が *yes* の場合のみです。

有効値: 0 ～ 4294967295

デフォルト値 : 0

例:

```
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.12
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Advertise cluster address [No]? y
Advertise route cost [0]? 20
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.12
Fintimeout has been set to 30 for cluster 113.3.1.12
Staletimer has been set to 1500 for cluster 113.3.1.12
NDR Config>
```

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。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。

注: 1 つのインターフェースに障害が起きても、1 次マシンとバックアップ・マシン間のハートビート通信が損なわれないようにするために、1 次とバックアップのネットワーク・ディスパッチャー間には、2 つ以上のハートビート・パスを構成しておく必要があります。

2 つのネットワーク・ディスパッチャー間に既存の LAN コネクションが 1 つしかない場合、2 番目のハートビートは、シンプル LAN コネクション (2 つのイーサネット・ポート間で直接使用されるクロスオーバー・ケーブル)、またはポイントツーポイント・シリアル・コネクション (非番号制 IP を使用する、ヌル・モデム・ケーブル上のバックツーバック PPP コネクション) で設定できます。

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ピア・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# port-type 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 : 1 〜 65535

デフォルト値: 80

port-type
このポートで負荷平衡を取ることができる IP トラフィックのタイプを指定します。サポートされるタイプは、次のとおりです。

- 1 = TCP
- 2 = UDP
- 3 = 両方

有効値: 1、2、3

デフォルト値: 3

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分配す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

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、 外部のスケーラブル・キャッシュ配列に送る (extcache) 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 : 0, 1, 2, 4,、ただし

- 0 = none
- 1 = sticky
- 2 = pftp
- 4 = extcache

デフォルト値 : 0

例:

```
Config>feature ndr
NDR>add cluster 1.2.3.4 4000 30 1500
NDR>add port
Cluster address [0.0.0.0]? 1.2.3.4
Port number [80]? 80
Port type [3]?
Maximum weight [20]?
Port mode [0=none, 1=sticky, 2=pftp, 4=extcache ]? 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 : 1 〜 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 の値

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14 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 14. パラメーター構成の制限

パラメーター	制限
Advisors	2210 につき 8
Clusters	2210につき 32
Heartbeats	2210につき 8
Ports	クラスターにつき 8
Reachs	2210につき 8
Servers	構成されたポートに 32、構成されたすべてのクラスターにある各ポート番号に 128
Unique server IP addresses	2210 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。使用不可にしようとするアドバイザーのタイプと対応するアドバイザー番号を入力します。

詳細については、128ページの表13を参照してください。

有効値: 0 ～ 8

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: 1 ～ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

例:

```
disable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL) [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・フィーチャーは使用不可になります。

例:

```
disable executor
Executor is now 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、稼働している場合)。

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、任意選択のコンポーネントです。ただし、ユーザーがマネージャーを使用しない場合、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いてラウンドロビン・スケジューリング方式で負荷の平衡を図ります。

例:

```
disable manager
Manager is now 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稼働を停止します。

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#*

ネットワーク・ディスパッチャーに対してアドバイザーを使用可能にします。

name アドバイザーのタイプを指定します。使用可能にしようとするアドバイザーのタイプと対応するアドバイザー番号を入力します。

詳細については、128ページの表13を参照してください。

有効値: 0 〜 8

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: 1 〜 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

例:

```
enable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp=6=pop3,7=telnet,8=SSL) [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。不可平衡の決定に使用するサーバーのウェイトを設定するときにマネージャーがアドバイザーの入力を考慮するよう、管理プログラムの比率も設定しておきます。また、アドバイザーが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、*プロトコルの構成と監視 解説書 第 1 巻* の「IP の構成および監視」の章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
Executor is now 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
Manager interval was set to 2.
Manager proportions were set to  50   50   0   0
Manager refresh cycle was set to 2
Manager sensitivity was set to 5.
Manager smoothing factor was set to 1.50.
```

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、142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
advisor
backup
cluster
manager
port
server

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     CommPort
        http    80      5               0               Enabled
        MVS     10007   15              0               Enabled
        TN3270  23      5               0               Enabled   10008

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  Advertise/Cost
       131.2.25.91     4000            30              1500         Yes      / 20

Ports:
  Cluster-Addr    Port#   Weight  Port-Mode  Port-Type
  131.2.25.91     23      20 %    none       TCP
  131.2.25.91     80      20 %    none       Both

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
```

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。

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。

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。

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。

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。除去しようとするアドバイザーのタイプと対応するアドバイザー番号を入力します。

詳細については、128ページの表13を参照してください。

有効値: 0 〜 8

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: 1 ～ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

例:

```
remove advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL) [0]?
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稼働を停止します。

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

ターゲット・ネットワーク・ディスパッチャーの 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 : 1 〜 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

例:

```
remove port
WARNING: Deleting a port will make any server
associated with it also be deleted.   [0.0.0.0]? 7.82.142.15
Port number [0]? 80
Cluster address [0.0.0.0]? 20.21.22.15
```

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 : 1 〜 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

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 comm-port*

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。設定しようとするアドバイザーのタイプと対応するアドバイザー番号を入力します。

詳細については、128ページの表13を参照してください。

有効値: 0 ～ 8

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: 1 ～ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

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場合、マネージャーは使用する必要がある報告を無視することになります。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。

comm-port

TN3270 アドバイザーが TN3270 サーバーと通信するのに使用するポート番号を指定します。このパラメーターは、TN3270 アドバイザーの入力にのみ使用します。

有効値: 1 〜 65535

デフォルト値:

- TN3270 デフォルト値:10008

例:

```
set advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp=6=pop3,7=telnet,8=SSL) [0]?
Port number [0]? 21
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 20
```

cluster *address FIN-count FIN-timeout 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 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* または *Stale-timer* 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

Stale-timer

コネクションが非活動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
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が、マネージャーによって更新され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 に等しくなければなりません。ファクターには、次のものがありあす。

active 実行プログラムによって追跡される各 TCP/IP サーバー上の活動状態のコネクションの数

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プロトコル・アドバイザーからの入力

有効値: 0 ～ 100

デフォルト値 : 0

system

MVS WLM システム監視ツールによって提供される MVS システム・アドバイザーからの入力

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の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、要求の分配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 の間の 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# port-type max-weight port-mode*

特定のクラスターとポート番号の port-type、max-weight、および port-mode 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 : 1 ～ 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

port-type

このポートで負荷平衡を取ることができる IP トラフィックのタイプを指定します。

有効値:

- 1 = TCP
- 2 = UDP
- 3 = 両方

デフォルト値: 3

max-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分配す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

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)、パッシブ ftp を使用する (pftp)、外部のスケーラブル・キャッシュ配列に送る、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) の中から選択して指定します。

有効値:

- 0 = none
- 1 = sticky
- 2 = pftp
- 4 = extcache

デフォルト値 : 0 (none)

例:

```
set port
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]? 23
Port type (tcp=1, udp=2, both=3) [0]?
Max. weight (0-100) [20]? 30
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1, pftp=2 extcache=4) []?
```

server *cluster-address port# server-address weight state*
クラスター内の特定のサーバーの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 : 1 〜 65535

デフォルト値: なし。ユーザーがポート番号を入力する必要があります。

server-address
サーバーの IP アドレスを指定します。

有効値: 任意の有効なサーバー・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 の値

例:

```
set server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]?
Server address [0.0.0.0]?
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・ディスパッチャーは、SNMP を使用して監視することもできます。詳細については、*プロトコルの構成と監視 解説書 第 1 巻* の 『SNMP 管理』 の項を参照してください。

ネットワーク・ディスパッチャー監視コマンド

表15 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 15. 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
? (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。 xxxi 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。

表 15. ネットワーク・ディスパッチャー監視コマンド (続き)

コマンド	機能
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、強制的に活動ネットワーク・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。 xxxiページの『下位レベル操作環境の終了』 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

現在使用可能になっているネットワーク・ディスパッチャー・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    |    21  |         5 |   ACTIVE |
|  Http   |    80  | unlimited |   ACTIVE |
|  MVS    | 10007  | unlimited |   ACTIVE |
|  TN3270 |    23  | unlimited |   ACTIVE |
-----------------------------------------
```

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   |  PORT MODE  |  PORT TYPE  |
|------------------------------------------------------|
|     23   |         30     |    none     |     TCP     |
|     80   |         20     |    none     |     both    |
 ------------------------------------------------------
```

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 mode....................... NONE
Port type....................... TCP
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 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
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 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
```

表示される情報については、154 ページを参照してください。

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、そ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、そ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。アドバイザーのタイプと対応するアドバイザー番号を入力します。アドバイザー・タイプについては、128 ページの表13を参照してください。

port# ポート番号です。

例:

```
report advisor
0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet,8=SSL
Advisor name [0]? 1
Port number [0]? 80

-------------------------------
|      ADVISOR:     http      |
|      PORT:          80      |
-------------------------------
| 131.2.25.93      |       0  |
| 131.2.25.94      |      16  |
-------------------------------
```

サーバー・アドレスごとに表示されている値は、次のものを表します。

≥0 サーバーの負荷

-1 アドバイザーはサーバーとコンタクトできませんでした。

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  |
-----------------------------------
```

報告される情報は、次のとおりです。

Status サーバー・アドレスの状況を表示します。

Quiesce サーバーが静止しました。

Active サーバーが静止していません。

```
-------------------------------------------------------------------------------
|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.
```

報告される情報は、次のとおりです。

Weight このサーバーの全体的な重み計算

Now サーバーに割り当てられた直前の重み

New サーバーに割り当てられた最新の重み

Active % 全体的なサーバーの重み計算用のアクティブ・コネクションの比率。このパラメーターの値は、**set manager proportions** コマンドを使用して設定されます。 144 ページを参照。

Wt 全体的な重み計算に使用される重み

Connect このサーバーのアクティブ・コネクション数

New % 全体的なサーバーの重み計算用の新規コネクションの比率。このパラメーターの値は、**set manager proportions** コマンドを使用して設定されます。 144 ページを参照。

Wt 全体的な重み計算に使用される重み

Connect
このサーバーの新規コネクション数

Port % 全体的なサーバーの重み計算用のアドバイザーの比率。このパラメーターの値は、**set manager proportions** コマンドを使用して設定されます。 144 ページを参照。

Wt 全体的な重み計算に使用される重み

Load このサーバーについて、アドバイザーによって報告されるサーバーの負荷

System % 全体的なサーバーの重み計算用のシステム・モニターの比率。このパラメーターの値は、**set manager proportions** コマンドを使用して設定されます。 144 ページを参照。

Wt 全体的な重み計算に使用される重み

Load システム・モニターによって報告されるサーバー負荷

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 / ports / servers

advisor *name port#*
特定のアドバイザーの状態を入手します。

name アドバイザーのタイプを指定します。アドバイザーのタイプと対応するアドバイザー番号を入力します。アドバイザー・タイプについては、128ページの表13を参照してください。

port# ポート番号です。

例:

```
status advisor
0=ftp, 1=http, 2=MVS 3=TN3270, 4=SMTP, 5=NNTP, 6=POP3, 7=TELNET, 8=SSL
Advisor name [0]?
Port number [0]? 21

Advisor ftp on port 21 status:
==============================
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
Advertise cluster address....... Yes
Advertise route cost............ 20

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
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 TCP Count: 0 UDP Count: 0  Active:
0 FIN 0 Complete 0 Status: up Saved Weight: -1  Address: 131.2.25.94 Weight:
20 Count: 0 TCP Count: 0 UDP Count: 0  Active: 0 FIN 0 Complete 0 Status:
up Saved Weight: -1
PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port type....................... BOTH
Port mode....................... NONE
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 TCP Count: 0 UDP Count: 0  Active:
0 FIN 0 Complete 0 Status: up Saved Weight: -1  Address: 131.2.25.94 Weight:
20 Count: 0 TCP Count: 0 UDP Count: 0  Active: 0 FIN 0 Complete 0 Status:
up Saved Weight: -1
```

表示されるフィールドの定義については、154 ページを参照してください。

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
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 *cluster-address port#*

特定のポートの状態を入手します。ただし、

cluster-address
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 mode....................... NONE
Port type....................... BOTH
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 TCP Count: 10000 UDP count 2345
Active: 3431 FIN 3780 Complete 3431  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890  Active: 2980 FIN 2390 Status: up
Saved Weight: -1
```

報告されるサーバー情報は、次のとおりです。

Address サーバー IP アドレス

Weight このサーバーに現在割り当てられている重み

Count TCP コネクションと UDP パケットの累積数

TCP Count TCP コネクションの累積数

UDP Count UDP パケットの累積数

Active アクティブ TCP コネクション数

FIN TCP コネクションが FIN 状態である

Complete 完了した TCP コネクション (FIN の後に ACK が表示される)

Status 構成されたサーバー状態:

active	サーバーがアクティブです。
down	サーバーがダウンしています。
quiesced	サーバーが静止しています。
not responding	サーバーがアドバイザーに応答しません。

Saved weight サーバーがダウンとマーク付けされる前のサーバーの重み

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 mode....................... NONE
Port type....................... TCP
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 TCP Count: 100 UDP Count: 40
Active: 50 FIN 45 Complete 50  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 250 TCP Count: 100 UDP Count: 40
Active: 60 FIN 54 Complete 50  Status: up Saved Weight: -1

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
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 TCP Count: 10000 UDP Count: 2345
Active: 3431 FIN 3780 Complete 3431  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890  TCP Count: 10000 UDP Count: 2345
Active: 2980 FIN 2390 Complete 3431  Status: up Saved Weight: -1
```

Switchover

switchover コマンドは、切り替え方式が「手動」の場合、スタンドバイ・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、強制的に活動ネットワーク・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
```

ネットワーク・ディスパッチャーの動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

CONFIG (Talk 6) **delete interface** コマンドは、NDR には適用されません。ネットワーク・ディスパッチャーは 1 つのフィーチャーであり、インターフェース上に構成されません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、NDR には適用されません。ネットワーク・ディスパッチャーは 1 つのフィーチャーであり、インターフェース上に構成されません。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、NDR には適用されません。ネットワーク・ディスパッチャーは 1 つのフィーチャーであり、インターフェース上に構成されません。

CONFIG (Talk 6) 即時変更コマンド

NDR では、装置の操作状態を即時に変更する次の CONFIG コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、これらの変更は保管され、保存されます。

コマンド
CONFIG, feature ndr, add advisor
CONFIG, feature ndr, add backup
CONFIG, feature ndr, add cluster
CONFIG, feature ndr, add heartbeat
CONFIG, feature ndr, add port
CONFIG, feature ndr, add reach
CONFIG, feature ndr, add server
CONFIG, feature ndr, disable advisor
CONFIG, feature ndr, disable backup
CONFIG, feature ndr, disable executor **注:** 実行プログラムが使用不可である場合、実行時コード構造からすべてのクラスター、ポート、およびサーバーを除去しますが、*SRAM からは除去されません。*
CONFIG, feature ndr, disable manager
CONFIG, feature ndr, enable advisor
CONFIG, feature ndr, enable backup
CONFIG, feature ndr, enable executor
CONFIG, feature ndr, enable manager
CONFIG, feature ndr, remove advisor
CONFIG, feature ndr, remove backup
CONFIG, feature ndr, remove cluster **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とサーバーが、実行時コード構造と SRAM から除去されます。
CONFIG, feature ndr, remove heartbeat
CONFIG, feature ndr, remove port
CONFIG, feature ndr, remove reach
CONFIG, feature ndr, remove server
CONFIG, feature ndr, set advisor
CONFIG, feature ndr, set cluster
CONFIG, feature ndr, set manager
CONFIG, feature ndr, set port
CONFIG, feature ndr, set server

動的再構成不能コマンド

NDR 構成パラメーターはすべて、動的に変更することができます。

第10章 コード化サブシステムの構成と監視

コード化サブシステム (ES) では、データの圧縮と暗号化の機能が 1 つのグループにまとめられています。インターフェースとプロトコルは、ES によりコード化ソフトウェア装置にアクセスできるようになります。圧縮や暗号化のためにリンクがアクティブになると、ES も自動的にアクティブになります。ソフトウェア装置は、圧縮と暗号化を行うオペレーション・ソフトウェアで構成されています。ルーターのプロセッサーで圧縮と暗号化のアルゴリズムが稼働します。ソフトウェア装置を使用するのに、デフォルト構成を変更する必要はありません。

注: PPP およびフレーム・リレー上での圧縮セッションの構成方法については、167ページの『第11章 データ圧縮の構成と監視』を参照してください。PPP およびフレーム・リレー上の暗号化セッションの構成方法については、211ページの『第14章 暗号化プロトコルの使用および構成』を参照してください。IPSec セッションの構成法方法については、329ページの『第19章 IP セキュリティーの構成および監視』 を参照してください。

ES アクティビティーを監視するには、監視 (talk 5) プロンプトで **feature es** を入力します。

ES 構成パラメーターを使うと、ES ソフトウェア装置が使用するメモリーの量を制限できます。デフォルト構成を使うと、ES が必要とするメモリーを確保できます。メモリーの使用量を制限するには、構成プロセス (Talk 6) の **feature es**にある **set** コマンドを使います。

本章には、以下の節が含まれています。

コード化サブシステムの構成

ES 構成パラメーターを使うと、ソフトウェア・コード化装置を同時に使用する圧縮および暗号化のセッションの数を制限できます。ソフトウェア・コード化装置は、本質的には圧縮と暗号化のライブラリーの集合体で、ルーターのプロセッサー上で実行されます。セッションは、特定のインターフェースを通した全二重接続で、このインターフェースは、圧縮と暗号化ができるように構成しておきます

一般的に、データの暗号化操作は、プロセッサーに作業が集中します。ソフトウェアのコード化セッションの数を制限することで、データのコード化によるルーターのパフォーマンスへの影響はある程度制限できます。たとえば、圧縮用としてルーターに 20 のダイヤルイン・インターフェースを構成したときに、同時に 10 以上のインターフェースを圧縮するとルーターのパフォーマンスに悪影響を与えるとします。この場合、最大圧縮セッション数は 10 に設定します。これで、20 のインターフェースのうち 10 のインターフェースが圧縮に使われます。

ソフトウェア・コード化装置が必要とするメモリー量もセッション数を制限する理由です。1 回のソフトウェア圧縮セッションで必要とするルーターのメモリーは約

30 KB、暗号化では約 2 KB が必要です。ES があまりにも多くのメモリーを使ってしまうと、ほかの機能がメモリーの制約を受けて、ルーターのパフォーマンスに悪影響を与えます。詳しくは、170ページの『考慮事項』を参照してください。

ES セッションの最小数と最大数を設定するには、*unlimited* または *default* を選択するか、数値を指定します。*unlimited* と *default* の意味は同じで、ルーターは、暗号化と圧縮のためにアクティブ化されたすべてのセッションをメモリーがなくなるまでサポートします。

注: ES 構成パラメーター (talk 6) は、どれも動的には構成できません。変更したパラメーター値をアクティブにするには、ルーターをリスタートするか再ロードします。

ES 監視コマンドを使うには、構成プロセス (talk 6) の `Config>` プロンプトで **feature es** を入力します。 `ES Config>` プロンプトが現れます。表16は、コマンドのリストです。

表 16. ES 監視コマンド

コマンド	アクション
? (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。 xxxiページの『ヘルプの入手』 を参照してください。
List	圧縮と暗号化のセッションの現在の設定値を表示します。
Set	すべてのインターフェースで利用可能な暗号化と圧縮のセッション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。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

List

list コマンドは、圧縮と暗号化のセッションの現在の設定値を表示するときに使用します。

構文:

list

例:

```
ES Config> list
Data Compression and Encryption System Configuration
----------------------------------------------------

Parameters used for host-based encoding:
  Compression sessions:
    Reserved at initial bootup:           0
    Maximum allowed:                      unlimited
  Encryption sessions:
    Reserved at initial bootup:           0
    Maximum allowed:                      unlimited
```

Set

set コマンドは、データの暗号化と圧縮のセッションの最大数を設定するときに使用します。

構文:

set

sw minimum compression-sessions *n, unlimited, or default*

sw maximum compression-sessions *n, unlimited, or default*

sw minimum encryption-systems *n, unlimited, or default*

sw maximum encryption-systems *n, unlimited, or default*

注: sw はソフトウェアの省略語です。

software minimum compression-sessions *n, unlimited, or default*
インターフェースで使用できる圧縮セッションの最小数を設定します。ルーターは、この数のセッションを常に使えるように確保します。

デフォルト値 : 0

有効値 : 0 to *unlimited*; alternatively, *default*

software maximum compression-sessions *n, unlimited, or default*
インターフェースで使用できる圧縮セッションの最大数を設定します。アクティブ化したセッション数がこの数に達すると、これ以上のセッションをアクティブにすることはできません。

デフォルト値 : 0

有効値 : 0 to *unlimited*; alternatively, *default*

software minimum encryption-sessions *n, unlimited, or default*
インターフェースで使用できる暗号化セッションの最小数を設定します。ルーターは、この数のセッションを常に使えるように確保します。

デフォルト値 : 0

有効値 : 0 to *unlimited*; alternatively, *default*

software maximum encryption-sessions *n, unlimited, or default*
インターフェースで使用できる暗号化セッションの最大数を設定します。アクティブ化したセッション数がこの数に達すると、これ以上のセッションをアクティブにすることはできません。

デフォルト値 : 0

有効値 : 0 to *unlimited*; alternatively, *default*

コード化サブシステムの監視

ES 構成コマンドを使うには、監視プロセスの + プロンプトで、 **feature es** を入力します。 ES Monitor> プロンプトが現れます。表17 は、利用できるコマンドのリストです。

表 17. ES 監視コマンド

コマンド	アクション
? (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。 xxxiページの『ヘルプの入手』 を参照してください。
List	ES ポート、回路、装置、構成、ステータス、まとめなどをリストにして表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

List

list コマンドは、ES に関する情報をリストにして表示します。ポート、装置、ステータスなどを含む **list** コマンドの出力例を **list summary** コマンドで参照できます。

構文:

list ports / circuits / devices / config / status / summary

ports **list ports** コマンドは、コード化システムの潜在的なクライアントが作成したコード化ポートのリストを表示します。ポートは、コード化システムと ES を使えるように構成されたクライアントのあいだのリンクを確立します。たとえば、PPP インターフェース Net 1 に圧縮または暗号化を構成すると、このインターフェースに 1 つのポートが関連付けられます。 QLen フィールドは、そうしたポートに関連付けられたすべての回路について、圧縮および暗号化で未処理のすべてのリクエストをまとめて表示します。特定のインターフェースに構成された PPP などのクライアントは、特定のデータ・バッファーをコード化のために指定すると、ES にリクエストを送ります。

Status フィールドは、ポートに待ち行列がないときは *Idle*、リクエストが処理中のときは *Busy*、リクエストがポートで待ち行列にあるときは *Waiting* を表示します。

circuits

list circuits コマンドは、コード化システムのクライアントが定義した回路を表示します。各回路は、全二重の接続です。ある終了点で暗号化または圧縮されたデータは、もう一方の終了点で暗号を解除または解凍されます。

デフォルトでは、アクティブな回路だけが表示されるようになっています。アクティブと非アクティブの両方の回路を表示するには、**list circuits all** コマンドを使います。

みつかった回路については、**list ports** コマンドと同様に、ポートとユーザーが表示されます。さらに、2 行の情報があり、アウトバウンドの回路については Tx 行、インバウンドの回路については Rx 行が表示されます。回路 ID は、クライアントが提供する任意の番号なので、作成されたそれぞれの回路に結合します。フレーム・リレー回路の場合、この番号は、関連付けられたフレーム・リレー・データ・リンク回路 (DLCI) の ID と同じになります。ポイントツーポイントのリンクでは 1 つの回路が作られ、この回路は常に *1* の数字で識別できます。

さらに、次の項目が表示されます。

Dev この番号は、ストリームを処理中のコード化装置を示します。ソフトウェアが CPU をアクティブ化してコード化を行う場合は 1、圧縮 / 暗号化アダプターがコード化を行う場合は 2 となります。

Cmpr このフィールドには、ストリームに対してアクティブとなっている圧縮または解凍のアルゴリズムを表示します。 *LZC* のときは、STAC-LZC 圧縮が使われ、*MPPC* のときは、Microsoft® PPC が使われています。ストリームがステートレス・モードで処理しているときは、アルゴリズムの名前にアスタリスク (*) がつきます。ステートレス・モードでは、データ・パケットの履歴は、パケットの処理が終わるとなくなります。これに対し、連続モードでは、パケット処理の履歴を維持して、次のパケットの処理に利用します。たとえば、連続圧縮では、エンコーダーが前回のパケットの情報をキャッシュに維持し、次のパケットの処理について効率化をはかります。

Encr このフィールドには、使用中の暗号化または暗号解除のアルゴリズムを表示します。*DES* は標準の DES、*3DES* はトリプル DES、*RC4* は、RSA の RC4 アルゴリズムが使われていることを示します。ストリームがステートレス・モードで処理しているときは、名前にアスタリスク (*) がつきます。これは、RC4 のときは重要ですが、DES/3DES ではあまり意味がありません。表示されるのは、使用されている基本的な暗号化アルゴリズムの名称であって、クライアントが使用するカプセル化のフォーマットの名称ではないことに注意してください。たとえば、PPP は 2 つのカプセル化方式をサポートします。DES で暗号化をする DESE (RFC 1969) と RC4 を使う MPPE (Microsoft 非標準) です。

QLen このパラメーターは、ストリームの待ち行列にいて、コード化や解凍作業を待っている未処理のパケット数を表示します。この数字は、処理のために ES に実際に渡されたパケットの数であることに注意してください。クライアントのなかには、自己の待ち行列を保持しておいて、こうした私用待ち行列からコード化システムにパケットを少しずつ送るものがあります。

Status

ストリームの状況を即座に示します。すべてのストリームが待ち状態になっていて、busy 状態のものがないこともまれではありませ

ん。busy 状態を見るということは、処理サイクルのなかのごく短時間の待ち行列活動を捕えることです。次のような状態があります。

Idle 対象ストリームに待ち行列のパケットはない。

Busy システムが対象ストリームのパケットを処理中 (つまり、待ち行列の先頭にあったアイテムがコード化エンジンに進んでいるところ)。

Waiting
リクエストは保留中だが、対象ストリームで処理中のものはない。

devices
list devices コマンドは、システムが保有する使用可能なコード化装置をリストにして示します。コード化装置とは、通常は圧縮 / コード化アダプターを指します。アクセラレーター・ハードウェアがないときはソフトウェアを仮想装置として実装しますが、このリストには、これが *Host Software* 装置として表示されます。このコマンドには **list devices** と **list device n** という 2 つの形態があります。 1 つ目の形態は、システムが認識するすべての装置をまとめて簡単なリストにして表示します。2 つ目は、装置番号を n とすると、特定の装置 n の詳細リストを表示します。装置 1 は、ホスト・ソフトウェアを示し、これは仮想コード化装置です。装置 2 は、圧縮 / 暗号化アダプターです。番号 n の代わりにアスタリスク (*) を使うと、両方の装置のリストが表示されます。

config **list config** コマンドは、現在の構成パラメーターを表示します。このパラメーターは、ルーターがリスタートまたは再ロードされるときに、不揮発性メモリーから読み込まれます。ここで表示される情報は、構成 (Talk 6) の **list config** コマンドで表示される情報と同じです。

status **list status** コマンドは、暗号化システムのステータスを表示します。内容は、総合ステータス・フラグと各種システム統計です。これは、**list status** コマンドで表示されるフィールドの説明です。

Last Error
コード化システムのクライアントに戻された最後のエラー・コードです。これはデバッグを意味するもので、保守要員が使用します。

Internal Condition flags
このフィールドには、以下のリストに示すような特定の内部の状態を表示します。

Ready システムは、アップ状態で操作可能です。これは通常の状態です。

Not Working
コード化システムは、内部エラーにより作動不能です。

No Devices Available
使用可能なコード化装置がないことを示します。この状態は、ハードウェア系のエンコーダーがなく、内部のソフトウェアを使ってコード化すると発生します。

Out of Memory
システムがメモリーの割り当てに失敗したことを意味しま

す。この状態は、ルーターの RAM が少なく、コード化システムが悪影響を受けていることを示します。

Number of Ports

このフィールドには、ES 内に自分でポートを確立したクライアントの数を示します。ポートの定義については、**list ports** コマンドを参照してください。

Number of Circuits

回路の定義については、**list circuits** コマンドを参照してください。

Global Request pool size

割り当てられたリクエスト・バッファーと空きリクエスト・バッファーの数。コード化するパケット 1 つにつきおおよそ 1 つのリクエスト・バッファーが使われます。空バッファーの数が割り当てられたバッファーの数よりも少ないときは、コード化処理の最中です。

Total # of Requests processed

この数値は、コード化エンジンが処理したバッファーの合計数を示します。この数値は、ルーターが最後にリスタートまたは再ロードされてから、システムの全クライアントが圧縮または暗号化したパケットの合計数におおよそ一致します。

summary

このコマンドは、システム概要を表示します。 **list status**、 **list devices**、 **list ports** の各コマンドの出力を組み合わせた複合コマンドです。

例:

```
list summary

Encoding System Status
----------------------

Last Error:                             14 (Stream not active)

Internal Condition flags:               0x00000001   -->
                                         Ready

Number of Ports:                        2

Global Request pool size:               Alloc: 32  Free: 32
Total # of Requests processed:          7059


 Encoding System Devices
 Encoding System Devices

Device Type                      Slot/Port  Status
------ ------------------------  ---------  ----------
     1 Host Software                 0/0     Ready
     0 Null Device                   0/0     Ready


                      Encoding System Ports
                      ---------------------

                                +--Encoder State---+   +--Decoder State---+
Port  User                      QLen  Status           QLen  Status
----  ------------------------  ----  --------------   ----  --------------
   1  Net 2   (PPP/0)              0  Idle                0  Idle
   2  Net 3   (PPP/1)              0  Idle                0  Idle
```

コード化サブシステムの動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

コード化サブシステムは、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、コード化サブシステムには適用されません。 ES 構成パラメーターにより、ブート時に ES に割り振られるメモリーで、インターフェースに関連付けられていないメモリーの量が決定します。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、コード化サブシステムには適用されません。 ES 構成パラメーターにより、ブート時に ES に割り振られるメモリーで、インターフェースに関連付けられていないメモリーの量が決定します。

動的再構成不能コマンド

コード化サブシステムは、構成パラメーターの動的な変更をサポートしません。

第11章 データ圧縮の構成と監視

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』
- 172ページの『PPP リンク上でのデータ圧縮の構成と監視』
- 175ページの『フレーム・リレー・リンクのデータ圧縮の構成と監視』

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 リンクで使用することを目的としています。

装置上のデータ圧縮は、PPP インターフェースおよびフレーム・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と、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 によって提供される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 をモデルにしています)、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、速度が一定のリンク上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ピア・アプリケーションにデータを転送する前に圧縮する、あるいは 2 つのノード間でビット列の受け渡しだけを行っているデータ・リンク・レイヤーで装置が圧縮する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含まれます。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優れた方法かもしれませんが、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は圧縮を行っていないからです。

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』 情報とは、現在利用可能なデータに基づいて導出することができ、再作成が可能な情報のことを言います。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コード・シーケンスで置き換えます。圧縮機能と解凍機能でこれらのコード・シーケンス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、圧縮する情報に基づく) 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、***履歴*** とも呼ばれます。この章の残りの部分では履歴とデータ・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、履歴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 つの終了点間で受け渡されるデータ・ストリームに作用するものであ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、コネクションの終了点は、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履歴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、履歴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、通常は全体的な圧縮効率が上がります。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、通常、各パケットは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高率で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履歴は、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、または配列変更を検知できます。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が失われたのを検出し、相互に再同期できるようになっています (たとえば、伝送エラー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。エラーを検出すると、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、圧縮機能自体が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、170ページの図10 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転送されます)。

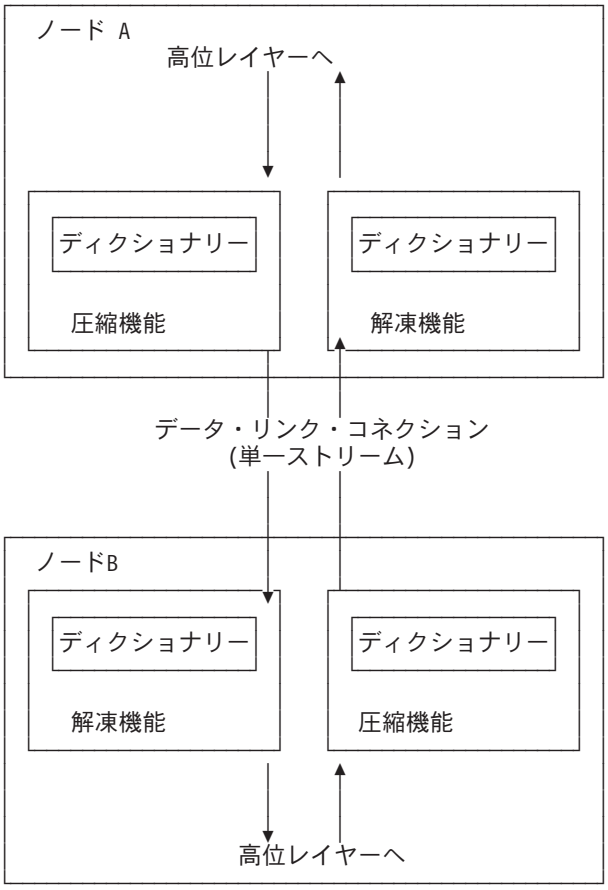


図 10. データ・ディクショナリーを使用した双方向データ圧縮の例

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、より具体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 リンク上で複数の履歴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ていません。

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が使用されているので (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 kbps (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、数百 kbps に限定する必要があると考えられます。 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。これを使用すると、実際に圧縮を実行す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ができます。活動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。圧縮および解凍履歴は、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、圧縮履歴に約 16 KB、解凍履歴に約 8 KB 必要です。これらの履歴は、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 (圧縮履歴は、相手側ルーターの対応する解凍履歴と同期される) ので、この問題は一層大きくなります。 PPP リンクの場合、これは圧縮履歴が 1 つと解凍履歴が 1 つを意味しています (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、このような履歴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、一定数の圧縮履歴と解凍履歴を作成します。これらは常に組みにして、***圧縮セッション*** として割り振られます (セッションは、1 つの圧縮履歴と 1 つの解凍履歴を単に結合したものです)。技術的には、圧縮と解凍は独立した機能ですが、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、個々の履歴ではなく、セッションを対象に行われます。圧縮と解凍に要するメモリーの量は、圧縮アルゴリズムによって異なるので、最悪のケースを考慮して、セッションは約 30 KB にしてあります。コード化サブシステム・フィーチャーの構成には、圧縮セッションのプールがあります。詳しくは、159ページの『第10章 コード化サブシステムの構成と監視』を参照してください。

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、必ず割り振られたセッションのプールのなかから 1 つのセッションを確保することで始めます。利用可能なセッションがない場合には、そのコネクションでは圧縮は行われません。ルーターは、後でセッション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。

割り振られる圧縮セッションの数は、構成可能なパラメーターです。割り振られるセッション数の設定値は、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ほとんどありません。実際には、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拡張されることさえあります。

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は、主として FTP ファイル・アーカイブ・サイトとしてセットアップ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

考慮が必要な最後のファクターは、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することもできます。特に最新モデムの多くは、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では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、実際には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構成と監視

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、相手側で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合意することも必要です。

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、使用する圧縮アルゴリズムとプロトコル特有のオプションが含まれます。

2. **set ccp algorithms** コマンドを使用して、交渉できる圧縮アルゴリズムを選択する。
3. **set ccp options** コマンドを使用して、各圧縮アルゴリズム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18 は、利用可能なコマンドをリストし、図11 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、*ソフトウェア使用者の手引き* の ‘ポイント・ポイント構成コマンド’ の項を参照してください。

表 18. 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	圧縮アルゴリズムの優先リストを指定します。
list ccp	圧縮構成を表示します。

```
Config>net 6  1
PPP 6 Config>enable ccp
PPP 6 Config>set ccp alg  2
Enter a prioritized list of compression algorithms (first is preferred),
all on one single line.
Choices (can be abbreviated) are:
STAC-LZS MPPC
Compressor list [STAC-LZS]? stac mppc
PPP 6 Config>set ccp options
STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext) [3]?
STAC: # histories [1]?
PPP 6 Config>li ccp

CCP Options
-----------
Data Compression enabled
Algorithm list: STAC-LZS MPPC
STAC histories : 1
STAC check_mode : SEQ

MPPE Options
------------
MPPE disabled
Optional encryption
Key generation : STATEFUL
```

図 11. 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、リンクのアルゴリズム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 algorithms stac mppc** を入力した場合と同じです)。

   複数のアルゴリズムを設定する場合、アルゴリズム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。

set ccp algorithms 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。

MPPE を使用可能にし、CCP を使用可能にすると、MPPC が圧縮アルゴリズムになります。

PPP リンク上のデータ圧縮の監視

圧縮の監視は、他の PPP コンポーネントの監視と同様です。 *ソフトウェア使用者の手引き* の ‘インターフェース監視プロセスへのアクセス’ の章で、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19 は、圧縮関連のコマンドをリストしています。 図12 は、PPP インターフェースにリストされる圧縮の例です。

表 19. 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
MPPE:         Not negotiated

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 12. PPP インターフェースの圧縮の監視

フレーム・リレー・リンクのデータ圧縮の構成と監視

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ごとに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 つの圧縮セッションを使用します。また、インターフェース自体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・リンクのデータ圧縮の構成

FR リンク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新規の PVC ごとに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。

176ページの表20 は、フレーム・リレー・リンク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、176ページの図13 は、フレーム・リレー・リンクの構成例を示しています。詳細については、*ソフトウェア使用者の手引き* の“フレーム・リレー構成コマンド”の項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 circuits (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 13. フレーム・リレー・リンクの圧縮の構成例

表 20. 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 20. 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: 孤立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 が利用可能な圧縮セッションの数が減ります。

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、下の例に示すように、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、インターフェースの圧縮を変更することができます。

フレーム・リレー・インターフェース上で圧縮を変更した例

```
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 [Y]?
The number of currently defined circuits is 5
Change all of these circuits to perform compression?
```

フレーム・リレー・リンク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。 ソフトウェア*使用者の手引き*の“フレーム・リレー監視コマンド” の章で、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21 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・インターフェースの圧縮のリスト例です。

表 21. 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12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プロセスです。 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、MSCHAP、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増します。 PAP、MSCHAP、CHAP、および SPAP の構成についての追加情報は、*ソフトウェア使用者の手引き* の'PPP 認証プロトコル' の項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。ローカル認証またはリモート認証を実行するように AAA を構成できます。

次のタイプの機能のセキュリティー・プロトコルを構成できます。

- 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 構成とは別に構成し、別に保管します。サーバー・プロファイルは、構成時に付けた名前を使用します。

どの環境でも、会計はローカルに行うことはできず、Radius または TACACS+ のいずれか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+ を使用する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プロセス。認証は、アクセスのために名前とパスワードを使用します。

許可 ユーザーのアクセスが許可されるサービスを決めるプロセス。

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プロセス。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・プロトコルを持つことができ、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、*ソフトウェア使用者の手引き* の ポイント・ポイント構成コマンド の項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+、TACACS

許可方式
Local、RADIUS、TACACS+

会計方式
RADIUS、TACACS+

表 22. 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
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

ログインの使用

AAA ログイン構成の場合、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:

リモート認証サーバーが応答しない場合、login-of-last-resort が使用可能になっているときに、ローカル・ログイン・ユーザー ID およびパスワードを使用することが可能です。これにより、リモート認証がタイムアウトになっても、シングル・ローカル・ログインを試行することができます。また、tech-support-bypass が使用可能である場合、tech support id および password をログインに使用することができ、この ID とパスワードは、認証サーバーに要求を送信しません。

リモート認証を使用する際に、特権レベルを指定することが重要です。ログイン・ユーザーは、正しいユーザー ID とパスワードを入力できますが、特権が指定されていないと、ユーザーはコンソールにアクセスできません。 3 つの特権レベルを設定できます。つまり、管理者特権、オペレーター特権、および監視特権です。RADIUS の場合、SERVICE-TYPE 属性番号 6 を使用するか、ベンダーの属性番号 216 を追加してください。個々の RADIUS 属性の詳細については、547ページの『付録. リモート AAA 属性』を参照してください。

リモート認証を構成する場合、許可は別のリモート許可プロトコル (Radius または TACACS+) に設定し、会計は Radius または TACACS+ を使用するように設定することも可能です。

- 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、許可もリモートに設定され、会計もリモートに設定されます。
- 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、許可プロトコルがローカルに設定されている場合にのみ、自動的に許可プロトコルを同じに設定し、会計プロトコルは無視します。
- 許可プロトコルをリモートに設定すると、認証プロトコルがローカルに設定されている場合にのみ、自動的に認証プロトコルを同じに設定し、会計プロトコルは無視します。
- 会計プロトコルをリモートに設定すると、認証プロトコルがローカルに設定されている場合にのみ、自動的に認証プロトコルを同じに設定し、許可がローカルに設定されている場合にのみ、自動的に許可プロトコルを同じに設定します。
- 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。
- 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 23. 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	ローカルの場合はリモート、その他の場合は無視	無視
AUTHOR をリモートに設定	ローカルの場合はリモート、その他の場合は無視	リモート	無視
ACCOUNTING をリモートに設定	ローカルの場合はリモート、その他の場合は無視	ローカルの場合はリモート、その他の場合は無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可

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します。トンネル認証をローカルまたはリモートに設定した場合は、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。

会計用のトンネル構成は、IPSec トンネルにも適用されます。トンネルの認証と許可は、IPSec トンネルには適用されません。 AAA を使用して IPSec トンネルの認証も許可も行うことはできません。

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 / 許可方式

Local、RADIUS

会計方式

RADIUS、TACACS Plus

表 24. 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

表 24. トンネル・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	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

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、パスワードを検査することができます。

注: 以下の規則は、PPP ユーザーのログインにだけが対象です。コンソール・ログインには適用されません。

- 長さが最小文字数である。必要な文字数を設定します。
- 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。
- 所定の日数の経過後に変更された。パスワードの変更の間隔の日数を設定します。
- 特定の回数のログイン失敗後にロック。失敗の回数を設定します。

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拒否します。

SecurID サポート

2210 は、Security Dynamics ACE/サーバーで SecurID を使用するダイヤルイン・クライアントを認証することができます。このサポートは、ACE/サーバー上で

TACACS、TACACS+、または RADIUS を使用して、クライアントを認証します。このダイヤルイン・クライアントの構成は、2210 の他のダイヤルイン・クライアントと同様に行います。

ダイヤルイン・クライアントは通常のようにログオンしますが、パスワードとして SecurID パスコードを使用します。 SecurID パスコードは、4 〜 n 桁の PIN 番号とその後の SecurID トークン・カードからの番号で構成されます。 (PIN の最大桁数は、サーバーによって異なります。) ユーザー ID とパスワードは、次のようになります。

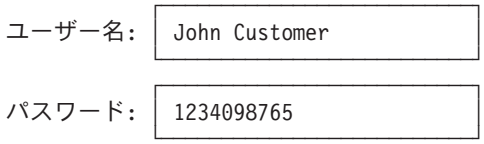


図 14. SecurID ユーザー名とパスコード

ACE/サーバーは、ログオンを認証するときに、クライアントに対して次のトークンを入力するように要求することがあります。次のトークンとは、トークン・カードの次のトークンです。次のトークンの最大桁数は、クライアントが使用している SecurID トークン・カードによって異なります。クライアントはパスワードの入力を求められたときに、`passcode*token` の形式で、パスコードと次のトークンを入力することができます。たとえば、次のように入力します。

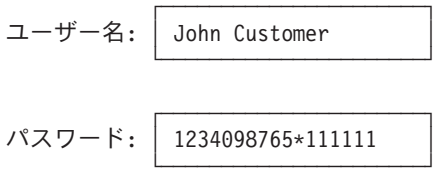


図 15. SecurID パスコードと次のトークン

注: サーバーがクライアントに次のトークンを入力するように要求した場合、クライアントは、以下のようにしなければなりません。

1. PIN を入力する。
2. カードからの新規のトークンを待ち、そのトークンを入力する。
3. * の後に、カードからの次のトークンを入力する。

ACE/サーバーの管理者は、サーバーが次のトークンまたは新規の PIN を要求する条件を構成します。

ダイヤルイン・クライアントは、次のトークンを入力する必要がある場合に、認証システムから警報を受け取れるようにするためには、SPAP を使用する必要があります。クライアントが SPAP を使用せず、ログオンに成功しなかった場合、`passcode*token` 形式を使用して、新規パスワードの入力を試みることが必要です。それでも成功しない場合は、クライアントと ACE/サーバーとの間に別の問題がある可能性があります。

SecurID の制約

以下のような制限があります。

- Security Dynamics Inc. (SDI) および DES 暗号化はサポートされません。
- SecurID 『New PIN』 機能はサポートされません。
- TACACS は 『New PIN』 または 『Next-Token』 機能をサポートしません。クライアントは、ログインするときに次のトークンを指定することはできますが、サーバーはそれを使用しません。
- コールバック用に構成されたクライアントはサポートされません。
- TACACS または TACACS+ で CHAP を使用する場合、CHAP 再チャレンジ間隔を 0 に設定してください。
- RADIUS 認証および SecurID を使用する場合は、CHAP を使用しないでください。
- クライアントは、TACACS+ および SPAP を使用すると最良の結果が得られます。
- マルチリンクを使用して SecurID 認証を行う Windows 3.1 DIALs クライアントはサポートされません。
- SecurID 認証を使用する場合は、最新のクライアント・ソフトウェア (たとえば、Windows 95 または OS/2) を使用することを強くお勧めします。

第13章 認証の構成

この章では、認証の構成コマンドおよびオペレーショナル・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』
- 209ページの『認証 (AAA) 動的再構成サポート』

認証構成プロンプトへのアクセス

AAA 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25 は、AAA 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 25. 認証構成コマンド

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。
Disable	各種の AAA オプションを使用不可にします。
Enable	各種の AAA オプションを使用可能にします。
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。
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	トンネル用の AAA を構成します。
User-profiles	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。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Disable

disable コマンドは、選択された会計オプションを使用不可にするのに使用します。

構文:

disable accounting
ipsec-accounting
login-last-resort
tech-support-bypass

unauthent-accounting

accounting
AAA 会計を使用不可にすることを指定します。

ipsec-accounting
IPSec 会計を使用不可にすることを指定します。

login-last-resort
login last resort を使用不可にすることを指定します。

tech-support-bypass
tech support bypass を使用不可にすることを指定します。

unauthent-accounting
unauthent 会計を使用不可にすることを指定します。 PPP 認証を使用可能にしてユーザーを認証することなくアクティブになった PPP セッションは、考慮されません。開始レコードと停止レコードは送信されません。

Enable

enable コマンドは、選択された会計オプションを使用可能にするのに使用します。

構文:

enable accounting
ipsec-accounting
login-last-resort
tech-support-bypass
unauthent-accounting

accounting
AAA 会計を使用可能にすることを指定します。

ipsec-accounting
IPSec 会計を使用可能にすることを指定します。

login-last-resort
login last resort を使用可能にすることを指定します。リモート認証サーバーに認証情報を送信中にタイムアウトになった場合、ローカル側で認証されたユーザーがログインできるようにする単一のプロンプトが表示されます。

tech-support-bypass
tech support bypass を使用可能にすることを指定します。

unauthent-accounting
unauthent 会計を使用可能にすることを指定します。

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
all

authentication

authorization

config

options

List コマンドの出力例

次の例は、サポートされている list コマンド・オプションの通常の出力例を示しています。

```
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>


AAA Config> list options
Login Last Resort  : disabled
Tech Support Bypass: disabled
IPSEC Accounting   : enabled

INBYTES              enabled
OUTBYTES             enabled
INPKTS               enabled
OUTPKTS              enabled
```

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26 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 26. 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27 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 27. 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

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

省略時値: なし

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

省略時値: なし

lockout
ロック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 / 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。

195ページの表28 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 28. 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29 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 29. 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。

accounting-level

記録する会計情報のレベルを指定します。上位レベルでは、それより下位レベルにリストされているすべての情報を記録します。

範囲: 0 ～ 10

デフォルト値: 0

>0 以下の情報を記録します。

- INBYTES_AH
- OUTBYTES_AH
- INBYTES_ESP
- OUTBYTES_ESP

>1 以下の情報を記録します。

- INPKTS_AH
- OUTPKTS_AH
- INPKTS_ESP
- OUTPKTS_ESP

>2 以下の情報を記録します。

- INBYTES_BAD
- OUTBYTES_BAD
- INPKTS_BAD
- OUTPKTS_BAD

>3 以下の情報を記録します。

- INPKTS_BAD_AH
- OUTPKTS_BAD_AH
- INPKTS_BAD_ESP
- OUTPKTS_BAD_ESP

>4 以下の情報を記録します。

- INPKTS_BAD_AH_RPLY
- INPKTS_BAD_ESP_RPLY

accounting-port

RADIUS サーバーの会計ポートを指定します。

範囲: 1 ～ 10000

デフォルト値: 1646

authentication-port

RADIUS サーバーの認証ポートを指定します。

範囲: 1 ～ 1000

デフォルト値: 1645

author-authent

認証時に許可属性を転送するかどうかを指定します。

有効値: yes、no

デフォルト値: yes

account-for-packets

会計停止後にパケット数を送信するかどうかを指定します。

有効値: yes、no

デフォルト値: yes

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

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 進値

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。

options
会計オプションを入力できるようにします。

bytes 会計をバイト・レベルで実行することを指定します。

incoming
着信バイトの会計を実行することを指定します。

enable
指定されたオプションの会計を使用可能にします。

disable
指定されたオプションの会計を使用不可にします。

outgoing
発信バイトの会計を実行することを指定します。

enable
指定されたオプションの会計を使用可能にします。

disable
指定されたオプションの会計を使用不可にします。

packets
会計をパケット・レベルで実行することを指定します。

incoming
着信パケットの会計を実行することを指定します。

enable
指定されたオプションの会計を使用可能にします。

disable
指定されたオプションの会計を使用不可にします。

outgoing
発信パケットの会計を実行することを指定します。

enable
指定されたオプションの会計を使用可能にします。

disable
指定されたオプションの会計を使用不可にします。

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。

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。

203ページの表30 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 30. 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 31. ユーザー・プロファイル構成コマンド

コマンド	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。 xxxi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。
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。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Add

user profiles add コマンドは、リモート・ルーターのユーザー・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たり、IP ネットワークを通したルーターへのトンネル・ピア間アクセスを指定するのに使用します。

構文:

add ppp-user

tunnel

ppp-user

リモート・ルーターのユーザー・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。最大 500 のユーザーを追加できます。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 DIALS クライアントの PPP ユーザーを追加します。

コマンド構文およびオプションについては、*ソフトウェア使用者の手引き*の “CONFIG プロセス (CONFIG - Talk 6) およびコマンド” の章の Add を参照してください。

例:

```
Config> add ppp-user
Enter name:  [ ]? pppusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No]
Number of days before account expiry[0-1000] [0]? 10
Number of grace logins allowed after an expiry[0-100] [0]? 5
IP address: [0.0.0.0]? 1.1.1.1
Set ECP encryption key for this user? (Yes, No): [No] no
Disable user ? (Yes, No): [No]

     PPP user name: pppusr01
   User IP address: 1.1.1.1
      Virtual Conn: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
   Account expires: Sun 17Feb2036 06:28:16
  Account duration: 10 days  00.00.00
   Password Expiry: <unlimited>

User 'pppusr01' has been added
```

例:

```
Config> add ppp-user
Enter name:  [ ]? tunusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No] yes
Enter hostname to use when connection to this peer: []? host01
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

                    PPP user name: tunusr01
                         Endpoint: 1.1.1.1
                         Hostname: host01

User 'tunusr01' has been added
```

tunnel IP ネットワークを通したルーターへのトンネル・ピア間アクセスを指定します。これにより、ピアはルーターへのトンネル PPP セッションを開始することが許可されます。

コマンド構文およびオプションについては、*ソフトウェア使用者の手引き* の “CONFIG プロセスの構成” の章の Add の項を参照してください。

例:

```
Config> add tunnel
Enter name:  []? tunnel02
Enter hostname to use when connecting to this peer: []? host02
Set shared secret? (Yes, No): [No]? yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 2.2.2.22

       Tunnel name: tunnel02
          Endpoint: 2.2.2.22
```

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 allotted
-----------------  -------------------
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*

認証 (AAA) 動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

AAA は、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

AAA は、GWCON (Talk 5) **activate interface** コマンドをサポートしません。

GWCON (Talk 5) Reset Interface

AAA は、GWCON (Talk 5) **reset interface** コマンドをサポートしません。

CONFIG (Talk 6) 即時変更コマンド

AAA では、装置の操作状態を即時に変更する次の CONFIG コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、これらの変更は保管され、保存されます。

コマンド
CONFIG, add ppp-user
CONFIG, feature authentication, enable login-last-resort
CONFIG, feature authentication, disable login-last-resort **注:** 次回のログイン・シーケンスに有効です。
CONFIG, feature authentication, enable tech-support-bypass
CONFIG, feature authentication, disable tech-support-bypass **注:** 次回のログイン・シーケンスに有効です。
CONFIG, feature authentication, enable unauthent-accounting
CONFIG, feature authentication, disable unauthent-accounting

動的再構成不能コマンド

次の表は、動的に変更できない AAA 構成コマンドを記述しています。これらのコマンドを活動化するには、装置を再ロードまたはリスタートする必要があります。

コマンド
CONFIG, feature authentication, server add
CONFIG, feature authentication, server change
CONFIG, feature authentication, server delete
CONFIG, feature authentication, enable ipsec-accounting
CONFIG, feature authentication, disable ipsec-accounting
CONFIG, feature authentication, ppp set
CONFIG, feature authentication, tunnel set
CONFIG, feature authentication, login set
CONFIG, feature authentication, set accounting options

CONFIG, feature authentication, password-rules enable
CONFIG, feature authentication, password-rules disable

第14章 暗号化プロトコルの使用および構成

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。

2210 は、以下をサポートしています。

- PPP インターフェース上の Microsoft ポイント・ポイント暗号化 (MPPE) 用の 40 および 128 ビット・キーを備えた RC4 暗号化アルゴリズム
- RCF 1968 および 1969 に記述されている PPP 暗号制御プロトコルをサポートする 56 ビット・キーを備えた暗号化ブロック・チェーン方式のデータ暗号化規格 (DES-CBC) アルゴリズム
- フレーム・リレーの暗号化用の 40 ビット・キーを使用する、商業データ・マスキング・ファシリティー (CDMF)。このサポートは専有です。
- フレーム・リレーは、トリプル DES と 128 ビット・キーも使います。

暗号化制御プロトコルを使用した PPP の暗号化

暗号化制御プロトコル (ECP) 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 リンク上で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 ECP 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。コマンド構文およびオプションについては、*ソフトウェア使用者の手引き*の “CONFIG プロセスの構成”の章の **Add** コマンド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、**enable ecp** コマンドを使用して設定します (*ソフトウェア使用者の手引き* の talk 6 `PPP Config>` **enable** コマンドの項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。
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方法については、 *ソフトウェア使用者の手引き* の `PPP Config>` **disable ecp** コマンドの項を参照してください。
- リモート・ユーザーの暗号化キーおよびパスワードを変更する方法については、*ソフトウェア使用者の手引き* の `Config>` **change ppp-user** コマンドの項を参照してください。
- 暗号化の状況をリストする方法については、 *ソフトウェア使用者の手引き* の `PPP Config>` **list ecp** コマンドの項を参照してください。
- 装置の名前を設定する方法については、 *ソフトウェア使用者の手引き* の `PPP Config>` **set name** コマンドの項を参照してください。

PPP の ECP 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、監視する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、`PPP n>` プロンプトが現れます。*n* はネットワーク番号を表します。**network** コマンドの使用方法については、 *ソフトウェア使用者の手引き*の 『ポイントツーポイント・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。

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、最新の暗号化のネゴシエーション、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。(*ソフトウェア使用者の手引き* の **list control ecp** コマンドの項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。 (*ソフトウェア使用者の手引き* の **list ecp** コマンドの項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。 (*ソフトウェア使用者の手引き* の **list edp** コマンドの項を参照してください。)

Microsoft ポイント・ポイント暗号化 (MPPE)

Microsoft ポイント・ポイント暗号化 (MPPE) は、Microsoft ダイヤルアップ・ネットワーキング (DUN) クライアントと呼ばれる、リモート側で接続されている Windows ワークステーションが、それ自体と 2210 の間で PPP リンクを介して転送するデータを暗号化する手段を提供します。 MPPE は、ルーターからルーターへ PPP リンクを介して転送されるデータを暗号化するのにも使用できます。 MPPE は常に両方向で交渉されます。

MPPE は、シークレット・キー・アルゴリズムを使用して暗号化を行います。シークレット・キー・アルゴリズムは、暗号化と暗号化解除に同じキーを使用します。このキーはユーザーによって構成されませんが、送信側と受信側のワークステーション間での MPPE の交渉のプロセスで生成されます。 MPPE を使用するには、認証プロトコルの Microsoft チャレンジ / ハンドシェーク認証プロトコル (MS-CHAP) を構成する必要があります。

PPP インターフェースを MS-CHAP で認証する場合、ルーターは 『Microsoft モード』 に入り、圧縮が使用可能の場合は MPPC のみを交渉し、暗号化が使用可能の場合は MPPE のみを交渉します。 『Microsoft モード』 では、ルーターは圧縮アルゴリズムの優先順位リストを無視し、ECP ネゴシエーションを使用不可にします。

MPPE の構成

MPPE を構成するには、各インターフェースごとに以下のステップを実行することが必要です。

1. MS-CHAP を構成する。 MS-CHAP の使用および構成に関する情報は、*ソフトウェア使用者の手引き* の 『Microsoft PPP CHAP 認証 (MS-CHAP)』 および 『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。
2. ルーターとルーターの間の接続を構成している場合は、**set name** コマンドを使用して、ローカル PPP インターフェースの名前を設定する (*ソフトウェア使用者の手引き* の `PPP Config>` **set name** コマンドの項を参照してください)。
3. データ圧縮が必要な場合は、`PPP Config>` プロンプトで talk 6 **enable ccp** コマンドを使用して、MPPC を使用可能にする。 MPPE は、データ圧縮を必要としません。
4. MPPE を使用可能にする。 `PPP Config>` プロンプトで **enable mppe** コマンドを使用します (*ソフトウェア使用者の手引き* の `PPP Config>` **enable** コマンドの項を参照してください)。
5. ルーターをリストートして、構成を活動化する。

MPPE を使用不可にしたり、MPPE オプションをリストすることもできます。

- MPPE を使用不可にするには、`PPP Config>` プロンプトで talk 6 **disable mppe** コマンドを使用します。
- 構成された MPPE オプションをリストするには、`PPP Config>` プロンプトで talk 6 **list ccp** コマンドを使用します。

MPPE の監視

212ページの『PPP の ECP 暗号化の監視』の説明に従って、`PPP>` プロンプトを立ち上げます。 MPPE データ統計を見るには **list mppe** コマンドを使用し、MPPE 状況を見るには **list control ccp** コマンドを使用します。これらのコマンドの出力の例は、*ソフトウェア使用者の手引き* 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および監視』 の章に示されています。

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、暗号化が使用可能にされている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。*ソフトウェア使用者の手引き*に記載されているフレーム・リレー構成コマンド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。*ソフトウェア使用者の手引き*に記載されているフレーム・リレー構成コマンド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。暗号化キーを入力するためには PVC を構成する必要があるので、暗号化は孤立回線に対してはサポートされません。

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。

- インターフェースの暗号化を使用不可にする場合は、 *ソフトウェア使用者の手引き*のフレーム・リレー構成 **disable encryption** コマンドの項を参照してください。
- PVC の暗号化の設定を変更する場合は、*ソフトウェア使用者の手引き*の フレーム・リレー構成**change permanent-virtual-circuit** 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場合は、*ソフトウェア使用者の手引き*の フレーム・リレー構成 **list all**、**list lmi**、および **list permanent-virtual-circuit** コマンドの項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*> プロンプトが出されます。

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。 *ソフトウェア使用者の手引き* に記載されている フレーム・リレー監視の **list** コマンドを参照してください。

第15章 サービス品質 (QoS) の構成および監視

この章では、装置内の 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オペレーショナル・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。

サービス品質 (QoS) の概説

この QoS フィーチャーは、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。このフィーチャー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。

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コールにも適用されます。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、そのコールは、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・コネクションとして再試行されます (VCC が解放された理由は、解放時の原因コード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・コネクションがピーク・セル速度が原因でリジェクトされた場合、そのコールは、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、コールは 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、コールは 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 コールと、LE クライアントが発信するデータ・ダイレクト VCC コールの両方に適用されます。着信コールの場合、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。着信コールに 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。

受信したコールのトラフィック・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、そのコールは解放されます。着信コールに SCR が指定されている場合、そのコールは 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。発信コールの場合、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内の整数値 (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信コール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・コネクションになります。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 コールの 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内の整数値 (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 コールの 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、コールは 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 ～ 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 のコールの「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)

予約帯域幅のコールの 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 のコールに使用される 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・コールが使用されます。指定された QoS クラスは、ATM 性能パラメーターの目標値を定義します。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) の相互運用が目的

LEC は、上記のすべての QoS クラスのコール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 が原因でコール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、呼び出し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、インターオペラビリティー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コールがリジェクトされたときに、コーラーがより低速の 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『ベストエフォート』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、その後にフィーチャー番号 (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 32. サービス品質 (QoS) 構成コマンドの要約

コマンド	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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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 33. 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
? (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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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、221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、218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、217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内の整数値 (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、220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、217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内の整数値 (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、219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、218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 ～ 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、217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 or 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 のコールの「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、220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 34. 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
? (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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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、218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、217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内の整数値 (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、217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内の整数値 (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、219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、218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 ～ 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、217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、その後にフィーチャー番号 (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 35. サービス品質 (QoS) 監視コマンドの要約

コマンド	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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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 36. LE クライアント QoS 監視コマンドの要約

コマンド	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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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、216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。
- 216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-EFFORT 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 制御メッセージで宛先 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+
```

QOS 動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

サービス品質 (QOS) は、CONFIG (Talk 6) **delete interface** コマンドをサポートします。ただし、次の考慮事項があります。

QOS は、特定の LEC または ATM インターフェース用に構成されます。 QOS の変更が有効になるのは、コマンドがその特定のインターフェースに対して発行されるときです。

GWCON (Talk 5) Activate Interface

サービス品質 (QOS) は、GWCON (Talk 5) **activate interface** コマンドをサポートします。ただし、次の考慮事項があります。

QOS は、特定の LEC または ATM インターフェース用に構成されます。 QOS の変更が有効になるのは、コマンドがその特定のインターフェースに対して発行されるときです。

サービス品質 (QOS) インターフェース固有コマンドはすべて、GWCON (Talk 5) **activate interface** コマンドによってサポートされます。

GWCON (Talk 5) Reset Interface

サービス品質 (QOS) は、GWCON (Talk 5) **reset interface** コマンドをサポートします。ただし、次の考慮事項があります。

QOS は、特定の LEC または ATM インターフェース用に構成されます。 QOS の変更が有効になるのは、コマンドがその特定のインターフェースに対して発行されるときです。

サービス品質 (QOS) インターフェース固有コマンドはすべて、GWCON (Talk 5) **reset interface** コマンドによってサポートされます。

GWCON (Talk 5) 一時変更コマンド

サービス品質 (QOS) は、装置の操作状態を一時的に変更する次の GWCON コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、常にこれらの変更は失われます。

Talk 5 における QOS の変更はすべて、QOS が構成されているインターフェースに対してコマンドが発行されるときに、即時に変更が有効になります。

第16章 ポリシー・フィーチャーの使用

この章では、ポリシー・フィーチャーがルーターの他のソフトウェア・コンポーネントと対話して、QoS やセキュリティー、あるいはその両方について決定がなされる方法を説明します。さらに、ポリシー・フィーチャーに関連する概念と構成コマンドについても説明します。ポリシー・フィーチャーは、LDAP ディレクトリー・サーバーをポリシー情報の中央リポジトリーとして使用できるようにします。LDAP 機能の概念と LDAP を使用するための構成ステップについてもこの章で説明します。以下の節では、そうした概念のほか、ルーターがポリシーを実行する方法を説明し、その例も示します。

- 『ポリシーの概要』
- 245ページの『LDAP とポリシー・データベースのインターラクション』
- 249ページの『規則の作成』
- 250ページの『構成の例』

ポリシーの概要

ポリシー・フィーチャーは、ネットワーク内の IPv4 トラフィックの管理を容易にします。ポリシーは、ごく簡単なフィルター規則 (drop や pass) のほか、複雑なセキュリティーや QoS シナリオにも使用できます。複数のポリシーを組み合わせて、ルーターによるネットワーク内の IPv4 トラフィックの処理方法を決定します。

ポリシーの決定と実行

この種のルーター・グループに設定されるポリシーの内容は、ポリシーの決定基礎とポリシーの実行方法です。この 2 つの概念は、ポリシー決定ポイント (PDP)、およびポリシー実行ポイント (PEP) と呼ばれています。

ポリシー・データベースは、ルーターのメモリーに常駐し、これはローカル構成からロードされる 1 組のポリシーと LDAP から読み込まれるポリシーで構成されています。ポリシー・データベースは、以下の条件で作成されます。

- 装置の再ロードまたはリスタート
- **reset database** 監視コマンド
- 自動リフレッシュ
- SNMP 設定要求

ポリシー・データベースは PDP として機能し、1 組のポリシーで構成されていて、これにより、ポリシー・フィーチャーに関連したコンポーネントがパケットを処理する方法を決定します。ポリシーにより決定がくだされると (時刻情報、IP パケット情報、識別などのプロトコル特定の情報などにもとづいて決定する)、その決定は実行コンポーネント (PEP) に渡されてアクションが実行されます。 238ページの図16 は、そうしたコンポーネントの関係を示しています。

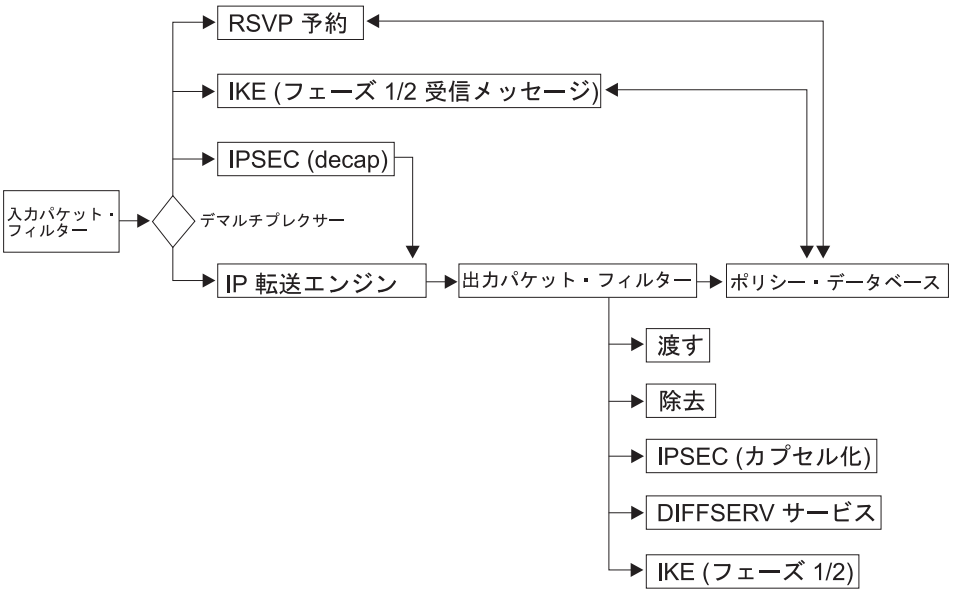


図 16. IP パケットのフローとポリシー・データベース

ポリシーの決定とパケット・フロー

あらゆるアクションを実行する前に、まずはじめに IP パケット が入力パケット・フィルターを渡さなければなりません。入力パケット・フィルターに規則がある場合は、パケットでアクションが取られていることがあります。パケットを除外するフィルターとの一致があったばあい、または入力パケット・フィルターに一致がない場合は、パケットは除去されます。

パケットが入力パケット・フィルターを渡すと、これはデマルチプレクス・フィルターに行き、パケットの向け先がローカルかどうかをチェックします。ローカルの場合は、パケットのタイプに応じて、その他のモジュールに渡されます。モジュールには、IPSec、IKE、RSVP、その他があります。パケットの向け先がローカルの IPSec、IKE、または RSVP の場合は、これらのモジュールがポリシー・データベースに照会を行ってアクションを決めます。

パケットの向け先がローカルではない場合、パケットは転送エンジンに渡され、ルーティングが決定されます。ルーティングの決定により、パケットが除去されなければ (ポリシー基準のルーティングでパケットが除去されることがあります)、パケットは出力パケット・フィルターに行きます。出力パケットにフィルター規則がある場合は、パケットのアドレスが変換されて (NAT)、パケットが渡されたり、除去されたりします。フィルター規則がない場合は、パケットは渡されます。フィルター規則があり、一致がなかった場合は、パケットは除去されます。パケットが出力パケット・フィルターを渡した場合は、IP エンジンがポリシー・データベースに照会を行い、パケットに対する今後のアクションを決定します。

注: 入出力パケット・フィルターをインターフェースで使用可能にした場合で、ポリシー・データベースで管理するパケットがこれらのインターフェースを通過すると考えられる場合は、ポリシー・データベースに紹介を実施する前にパケットが除去されないようにするため、入出力のパケット・フィルターには、これらのパケットを含むフィルター規則が必要になります。1 つの提案として、

パケット・フィルターを使わずに、ポリシー・データベースですべての pass/drop 規則を構成する方法が考えられます。

IP ポリシーの照会

IP 転送エンジンがポリシー・データベースに照会を実施すると、以下のような組み合わせの決定がなされます。

- 一致なし : パケットを渡す
- 一致あり : パケットを除去する
- 一致あり : パケットを渡す
- 一致あり : パケットを IPSec マニュアル・トンネル x で保護する
- 一致あり : パケットを IKE が交渉した IPSec トンネル x で保護する
- 一致あり : ISAKMP のフェーズ 1 および 2 について交渉を開始して、パケットを除去する
- 一致あり : DiffServ QoS x を実施して、パケットを IPSec に保護する

IPSec ポリシーの照会

IPSec は、パケットを受け取ると、まずはじめにパケットのカプセルを外し、次に、パケットが正しい IPSec トンネルに届いているかどうかを確認します (適合確認と呼ばれています)。これは、ポリシー・データベースへの照会で実施します。ポリシー・データベースは、この照会に対して、次のような決定を送り返してきます。

- 適合確認済み : パケットを転送する
- 適合確認できず : パケットを除去する

IKE ポリシーの決定

IKE は、ポリシー・データベースに照会し、表37に示すような *Phase 1* の IP ポリシー決定内容を送り返してもらえます。

表 37. IKE Phase 1 の照会と返却された決定

照会のタイプ	決定内容
Message 1 (メイン・モード)	一致なし、パケット除去
Message 1 (メイン・モード)	一致あり、Phase 1 ポリシー x と交渉
Message 5 (メイン・モード)	一致なし、ピアとの交渉を中止、パケット除去
Message 5 (メイン・モード)	一致なし、ピアとの交渉を中止、パケット除去
Message 5 (メイン・モード)	一致あり、ポリシー x が一致、Phase 1 終了
Message 5 (メイン・モード)	一致あり、ポリシー y が一致、現在の Phase 1 を中止して、新たなポリシーで Phase 1 を開始
Message 1 (アグレッシブ・モード)	一致なし、パケット除去
Message 1 (アグレッシブ・モード)	一致あり、ポリシー x が一致

IKE は、ポリシー・データベースに照会し、表38に示すような *Phase 2* の IP ポリシー決定内容を送り返してもらえます。

表 38. IKE Phase 2 の照会と返却された決定

照会のタイプ	決定内容
Message 2 (応答側)	一致なし、パケット除去
Message 2 (応答側)	一致あり、ポリシー x と交渉

RSVP ポリシーの決定

パケットが RSVP 制御メッセージの場合は、RSVP がポリシー・データベースに照会を行い、予約を受けるか拒否するかを決定します。受け入れた場合は、RSVP がポリシーにしたがって予約属性の制限を決定します。ポリシー・データベースのポリシーは、予約期間、割り当てる帯域幅の量、および保証最低遅延幅を制御できます。

ポリシー・オブジェクト

ポリシーにはプロファイルがあり、これには決定の基準となるパケットの属性、パケットの属性がプロファイルの属性と一致したときの実施すべきアクション、および決定やアクション実施の有効期限が含まれています。これらの項目につては、以下の節で詳細に説明します。

ポリシーの構成部分は、固有な名称をもったオブジェクトになっています。ポリシー・オブジェクトは、お互いに参照しあったり、複数のポリシー・オブジェクトが関連項目のグループとなって、1 つのポリシーを構成することがあります。構成情報を分割して固有のオブジェクトを個別に作ると、これらを複数のポリシー定義に再利用できるので、時間が節約でき、メンテナンスが簡単になります。各ポリシー・オブジェクトの詳細については、以下の節で説明します。

ポリシー

ポリシー・オブジェクトは、チェック条件とチェックが一致したときに実行するアクションを示します。ポリシーは、有効期限とプロファイルについて、名称つきの参照項目を作ります。ポリシーを有効にするには、こうした参照項目が必要になります。さらに、ポリシーは、IPSec 手入力トンネル・オブジェクト、IPSec アクション、ISAKMP アクション、RSVP アクション、および DiffServ アクションの中から、1 つまたは 2 つの条件について、名称のついた参照項目を作る必要があります。有効な組み合わせは以下のとおりです。

- IPSec 手入力トンネル
- IPSec アクションでパケットを除去
- IPSec アクションでパケットを渡す (セキュリティーなし)
- IPSec アクションでパケットを保護、ISAKMP アクション
- DiffServ アクション (除去)
- IPSec 手入力トンネルおよび DiffServ アクション (渡す)
- IPSec アクションでパケットを保護、ISAKMP アクション、DiffServ アクション (渡す)
- RSVP アクション
- RSVP アクションおよび DiffServ アクション (渡す)

注: これらの組み合わせでは、IPSec 手動トンネルは、IPSec アクションとして同じポリシー定義には存在できず (IKE 交渉の IPSec トンネル)、RSVP アクションは、どの IPSec トンネルとも関連付けてはなりません。パケットを保護する IPSec アクションがポリシーと関連付けた場合は、ISAKMP アクションもそのポリシーと関連付ける必要があります。

ポリシーには、それぞれ関連付けられた優先順位番号があります (優先順位番号の数字が大きいほど優先度は高くなります)。優先順位は、他のポリシーに対する優先権を決めます。通常、この設定が必要になるのは、2 つ以上のポリシー・プロファイルが相互に対立するときだけです。優先度は、より具体的なプロファイルを有するポリシーのほうが高くなります。たとえば、1 つのポリシーには、サブネット A からサブネット B へのトラフィックを IPSec (DES) で保護するように指定し、もう 1 つのポリシーには、ポイント a′ (サブネット A のある特定のホスト) からサブネット B へのトラフィックを IPSec (3DES) で保護するように指定したとします。A から B のポリシーよりも、さらに具体的なポリシー (a′ から B) のほうが優先度は高くなります。

当初の優先順位の数値の間隔を 5 以上にして、あとでポリシーを追加しても、対立しないようにしておく方法があります。それぞれのポリシーには、使用可能な属性があり、ポリシーをポリシー・データベースにロードしたときに、そのポリシーを使用可能にするかどうかを決めます。ポリシー・データベースを検索して、あるポリシーが一致がしたあと、そのポリシーが使用不可になった場合は、指定内容が近い次のポリシーが実行されます。

check-consistency 監視コマンドを使用すると、単一のポリシー内、または定義されているすべてのポリシー間の両方で、整合性と競合の検査を開始することができます。このコマンドは、問題を解決するのではなく、正しいアクションを取れるように問題を識別するものです。このコマンドの詳細については、301ページの『ポリシー監視コマンド』を参照してください。

プロファイル

プロファイルは、ポリシーを選択するために使用する情報を決定します。プロファイルには、発信元アドレスと宛先アドレスに関する情報、プロトコル情報、そして発信元と宛先のポート情報があります。

注: IPSec/ISAKMP のポリシーを定義するときは、セキュリティーを提供するそれぞれのゲートウェイには、セキュリティー・アソシエーションを定義付けるためのポリシーが必要になります。それぞれのゲートウェイのプロファイルは、発信元と宛先、および宛先と発信元を関連付ける必要があります。IPSec のポリシーに対するプロファイルには、トラフィックをトンネルにカプセル化するための発信元アドレスを指定し、宛先アドレスはトンネルのリモート側になる必要があります。

また、プロファイルは、type-of-service (TOS) バイト、入り口と出口の IP アドレスにしたがって選択ができます。デフォルトでは、パケットの送受信に使われる入力インターフェースや出力インターフェースがどれであっても、パケットはほかのセレクターと一致します。場合によっては、パケットを受信するインターフェースと送信するインターフェースを正確に指定する柔軟性が必要になることがあります。その場合は、インターフェース・ペア・オブジェクトを追加し、そのインターフェース・ペア・オブジェクトにプロファイルを使ってグループ名を関連付けます。インターフェース・ペア・オブジェクトは、グループと同じ名前を付けてグループに割り当てます。これにより、(IPaddrX で受信し、任意のインターフェースから送信するすべてのパケット、あるいは 任意のインターフェースで受信し、IPaddrX から

送信されるすべてのパケット) のような組み合わせを指定することができます。このやり方は、共通インターフェースに汎用除去規則を定義したときにはとくに便利です。

インターフェース・ペア: 入力インターフェースと出力インターフェースを識別します。この選択をしたときにこのインターフェースに IP アドレスを指定します。255.255.255.255 の値は、任意のインターフェースを指します。

プロファイルを使って IPSec/ISAKMP ポリシーを選択するときは、フェーズ 1 でローカル ID を送信するように指定するオプションと、フェーズ 1 のネゴシエーションで受け入れ可能なリモート ID のリストを出すオプションがあります。デフォルトでは、IPSec/IKE のトラフィックにはローカル ID がローカル・トンネル終了点で、リモート ID リストは *Any* です。オプションで、完全限定ドメイン名 (FQDN)、ユーザー FQDN、キー ID を指定できます。すべての ISAKMP フェーズ 1 ネゴシエーションは、公開認証かプリシェアード・キーで認証がとれているので、通常はこれで充分です。しかし、宛先アドレスに対してワイルドカードのポリシーを使うリモート・アクセスなどでは、ネットワーク資源にアクセスを許すためのリモート・アクセス・ユーザーのリストを指定したほうが賢明です。

こうしたユーザーは、通常の ISAKMP 認証方式によってやはり認証が必要ですが、ポリシー・データベースは、リモート・ピアから送られたローカル ID をポリシー・プロファイルのリモート・ユーザー・グループに指定された ID との一致を確認するので、認証工程をさらに追加できます。公共の認証局 (CA) が一般公衆に対して認証を管理する場合は、以上のことが必要になります。そして、ネットワーク管理者としては、アクセスのためにこうした特定のユーザー・グループが必要になります (たとえば、会社の従業員)。リモート・ユーザー・グループは、同じグループに属するユーザーのリストで構成されています。これらのユーザーは、1 つ以上の *USER* を追加して入力します。ユーザーのグループは、同様にお互いにグループ名を作っています。このグループは、オプションでプロファイルと関連付けることができます。

有効期限

有効期限は、有効な年、月、曜日、時刻などでポリシーの寿命を指定します。これにより、ネットワーク管理者は、ポリシーの有効期間を柔軟に決めることができます。たとえば、“常時”または“今年の 1 月、2 月、3 月の月曜日から金曜日までの 9 AM から 5 PM まで”のように指定できます。ポリシー・データベース内のポリシーが無効になると、次に具体的なポリシーが実行されます。そこで、月曜日から金曜日の 9 AM から 5 PM のサブネット A からサブネット B へのすべてのトラフィックを保護し、サブネット A からサブネット B へのその他のすべてのトラフィックを除去するようにポリシーに指定できます。この場合、最初のポリシーの優先度を高くします (**add policy** 監視コマンドを入力すると指定されます)。

DiffServ アクション

DiffServ アクションは、ポリシーに DiffServ アクションを指定したときに、そのポリシーに一致したパケットについて、提供するサービスの種類を示します。パケットを除去するように DiffServ アクションを構成することもできます。 DiffServ アクションを利用して、パケットを適当なサービスの種類にマッピングすることもできます。帯域幅を出力帯域幅の割合で割り当てたり、kbps を使った絶対値で構成することもできます。帯域幅の割り当てには、assured (AF)/best effort queue または

premium (EF) queue を指定します。この待ち行列に関する詳細情報および構成方法については、365ページの『第20章 ディファレンシエーテッド・サービス・フィーチャーの使用』 と 375ページの『第21章 ディファレンシエーテッド・サービス・フィーチャーの構成および監視』 を参照してください。

また、DiffServ アクションは、DS コード・ポイント (TOS バイト) が出口のインターフェースに送られる前に、EF および AF トラフィックに対して DS コード・ポイントのマーク方法を指定します。 EF および AF トラフィックは計量され、非準拠トラフィックはポリシングされます。非準拠 EF トラフィックは除去されます。非準拠 AF トラフィックの DS バイトは、任意選択により、Three Color Marker (TCM) 方式を使用して再度マーク付けされます。パケットのマーク付け、計量、およびポリシングにより、DiffServ が使用可能になったネットワーク内のコア・ルーターは、DS コード・ポイントに基づいてパケットを分類し、非準拠トラフィックを最初に除去することによって輻輳を制御します。これにより、DiffServ が使用可能になったネットワークでは、優先トラフィックのスループットが上昇し、遅延が減少します。

RSVP アクション

RSVP アクションは、RSVP の予約があり、予約要求がポリシーのプロファイルと一致したときに、RSVP のフローを許可するか拒否するかを指定します。予約を許可する場合は、RSVP アクションに、許可された予約期間、許可された帯域幅、そしてオプションで DiffServ アクションの参照項目を記述します。 DiffServ アクションの参照項目があると、パケットがルーターから送信される前の TOS バイトのマーク方法を RSVP が決定できます。このことは、パケットが RSVP のネットワークから DiffServ のネットワークへ渡るときは便利です。 RSVP は、QoS を RSVP 境界まで提供し、TOS バイトを適切にマークするので、DiffServ ネットワークは正しい帯域幅を適用することができます。

IPSec アクション

IPSec アクションは、除去する、渡す、保護するなどのアクションを指定します。除去するアクションの場合は、このポリシーに一致するすべてのパケットは除去されます。渡すアクションでセキュリティーがないときは、すべてのパケットはそのまま渡されます。セキュリティーありで渡すアクションのときは、すべてのパケットは、このアクションが指定するセキュリティー・アソシエーション (SA) で保護されます。IPSec アクションには、IPSec トンネルと IKE SA のトンネル終了点の IP アドレスも含まれています。

SA の属性は、IPSec アクションが参照する IPSec プロポーザルによって決定されます。 IPSec アクションは、複数の IPSec プロポーザルを指定することができ、これは送信されて、指定された順序でチェックされます。IPSec アクションに複数のプロポーザルがあると、受け入れられるすべてのセキュリティーの組み合わせを含めることができるので、VPN ゲートウェイのあいだで構成の不一致が起こる数を少なくできます。

IPSec プロポーザル

IPSec プロポーザルには、フェーズ 2 の ISAKMP ネゴシエーションのあいだに、ESP または AH、(あるいはその両方) が提案したりチェックするトランスフォームに関する情報が含まれています。完全な転送秘密を必要とする場合は (Diffie Hellman の再計算)、IPSec プロポーザルが使用する DH グループを識別します。

IPSec プロポーザルが参照するトランスフォームの送信やチェックは、指定された順序で実行されます。リストの最初の ESP または AH のトランスフォームは、使用がもっとも適したものでなければなりません。リストに 1 つ以上のトランスフォームがあるときは、それぞれをピアにあるトランスフォームのリストと突き合わせて一致したものを探します。ピアのリストに一致する構成済みのトランスフォームが 1 つもない場合は、ネゴシエーションの失敗となります。 IPSec プロポーザルは、AH と ESP のトランスフォームを組み合わせてリストに表示できますが、有効な組み合わせは以下のとおりです。

- AH だけのリスト (トンネルまたは転送モード)
- ESP だけのリスト (トンネルまたは転送モード)
- AH (転送モード) のリストと ESP (トンネル・モード) のリスト

IPSec トランスフォーム

IPSec トランスフォームの属性は、IPSec の暗号化と認証のパラメーターに関する情報があり、さらにキーをリフレッシュする頻度を指定します。トランスフォームは、AH (認証のみ) または ESP (暗号化、認証、その両方) のどちらかですが、トンネル・モードまたは転送モードのどちらかの操作を選択して構成できます。

ISAKMP アクション

ISAKMP アクションは、フェーズ 1 のキー管理情報を指定します。フェーズ 1 のネゴシエーションをメイン・モード (アイデンティティーを保護する) で開始するかアグレッシブ・モードで開始するかを指定します。また、フェーズ 1 のセキュリティー・アソシエーションを装置の始動時にするか、オンデマンドでするかを指定します。 ISAKMP アクションは、1 つ以上の ISAKMP プロポーザルを参照する必要があります。最初の参照項目が、もっとも許容できる ISAKMP プロポーザルでなければなりません。

ISAKMP プロポーザル

ISAKMP プロポーザルは、フェーズ 1 のセキュリティー・アソシエーションについて、暗号化および認証の属性を指定します。また、キーの作成に使用する Diffie Hellman グループとフェーズ 1 のセキュリティー・アソシエーションの期間を指定します。 ISAKMP プロポーザルで認証方式を選択します。プリシェアード・キーまたは証明モードのどちらかです。

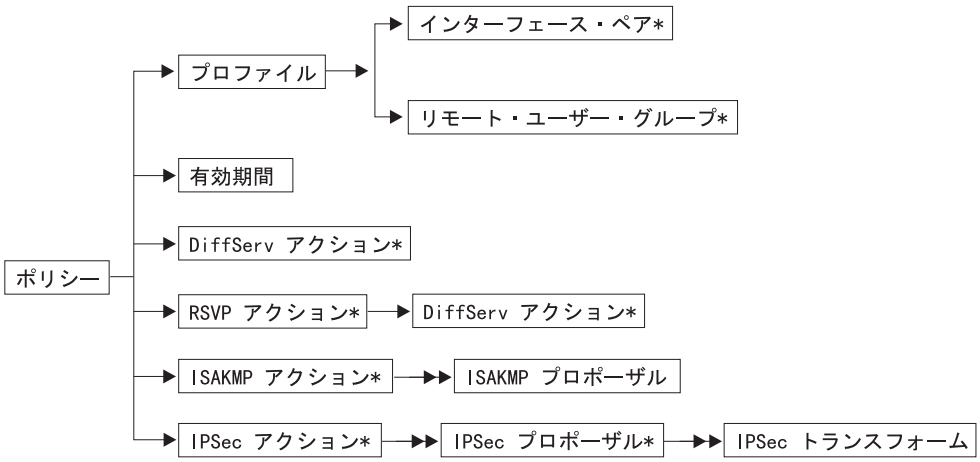
ユーザー

ISAKMP のネゴシエーションに認証方式としてプリシェアード・キーを使う場合、ISAKMP を使うすべてのポリシーについて、USER を構成しなければなりません。USER の構成は、ISAKMP ピアで使用するプリシェアード・キーを識別します。ユーザーのオブジェクトには、IP アドレス、FQDN、ユーザーの FQDN またはキー ID、ユーザーが希望する認証方式など、リモートの ISAKMP ピアを識別するための情報が含まれています。プリシェアード・キーまたは証明モードを選択できます。プリシェアード・キーを選択した場合は、プリシェアード・キーを ASCII と 16 進法のどちらで入力するか、そしてキーの値を指定します。USER は、同一のグループ名を割り当てて、まとめてグループにすることができます。このグループは、オプションでポリシーのプロファイルと関連付けて、フェーズ 1 でさらに厳格なポリシーのルックアップを実行できます。

IPSec 手入力トンネル

IPSec 手入力トンネルは、暗号化および認証のパラメーターの静的構成です。トンネルのネゴシエーションは実施されないので、両方のピアの構成はまったく同じでなければなりません。構成の一部として、実際にキーを入力し、トンネルの両側で一致しなければなりません。このモードではネゴシエーションがないので、キーのリフレッシュはありません。IPSec 手入力トンネルについての詳細は、311ページの『第18章 IP セキュリティーの使用』の IPSec フィーチャー機能に関する説明を参照してください。

図17は、ポリシーの構成オブジェクトの関係を示しています。



注:

1. → は参照項目が 1 つ
2. →▶ は参照項目が 2 つ
3. * は参照項目がオプション
4. ISAKMP/IPSec のセキュリティー・ポリシーでは、トラフィック・プロファイルがトラフィック・フローを保護トンネルに定義します。

図 17. ポリシーの構成オブジェクトの関係

LDAP とポリシー・データベースのインターラクション

この種のルーターでは、Lightweight Directory Access Protocol (LDAP) サーバーをポリシー情報のリポジトリー (ポリシー・データベース) として使用できます。 LDAP は、ディレクトリー・サーバーを検索、変更するプロトコルです。 LDAP は、X.500 標準の軽量バージョンです。ルーターは、ディレクトリー・サーバー内で情報を検索する機能をサポートしています (変更はできない)。対象装置のディレクトリー・サーバーにあるポリシー情報をルーターのポリシー検索エージェントが取り出します。LDAP のバージョン 2 または 3 で運転する LDAP サーバーであれば、ルーター内に実装に対応します。構成をローカルに保存する通常の方法に比べて、ディレクトリー・サーバーにポリシー情報を保存すると、1 つの場所で変更ができ、その変更内容を拡張ネットワークにあるすべての装置に適用できることが大きな長所です。これには、公衆境界を通り越した装置のほか、管理ドメインの装置も含まれます。

たとえば、ディレクトリーに IPSec トランスフォームの定義があったとします。会社のポリシーの暗号化を DES から 3DES に変更しようとすると、通常は各ネット

ワークの境界でそれぞれの装置の構成を変更しなければなりません。ディレクトリーを使ってポリシーを作成すると、1 つの IPSec トランスフォームを変更するだけですみます。ネットワークにあるポリシーを使用可能にしたすべての装置は、データベースの再構築が必要になります。もう 1 つの例として、“GoldService” という名前の DiffServ アクションを変更して、帯域幅を 40% から 45% に増加したいとします。LDAP サーバーとポリシーのインフラストラクチャーによって、このように構成をよりよい形に変更し、構成の不一致を少なくすることができます。

ネットワーク管理者の場合は、毎日特定の時刻に、データベースを自動的にリフレッシュする機能が使えます。このオプションを選択するには、ポリシー・フィーチャーの **set refresh** コマンドを入力します。リフレッシュを使用可能または使用不可に指定できます。使用可能にした場合は、データベースをリフレッシュする時刻を指定します。自動的に変更する場合は、このオプションは便利です。たとえば、新しいポリシーを追加して、アメリカのマーケティング部と日本の開発部をインターネットで接続するとします。セキュリティー・ゲートウェイは、SG1 と SG2 だとします。この情報を単純にディレクトリーに入力し、SG1 と SG2 の自動リフレッシュを使用可能にしておけば、真夜中にこの変更を自動的に拾います。

LDAP サーバーからポリシー情報を正常に読み取った後、装置の持続記憶域にこの情報を入れることができます。これを行った後、キャッシュに入れた情報を常に読み取ることを選択できるので、LDAP サーバーを問い合わせるのに必要な時間がなくなります。また、リフレッシュが要求されるときに LDAP サーバーが利用できない場合、キャッシュに入れられたコピーをポリシー検索エンジンに読み取らせることもできます。詳細については、301ページの『ポリシー監視コマンド』の **cache-ldap-plcys** および **flush-cache** 監視コマンド、ならびに 295ページの『LDAP ポリシー・サーバーの構成コマンド』の **enable ldap** 構成コマンドを参照してください。

LDAP ポリシー検索エンジンを使って、ポリシー・データベースを構築するあいだに使用するセキュリティー・レベルを指定することができます。このセキュリティー・オプションは、ポリシー・フィーチャーの **set default** コマンドで定義します。以下のオプションがあります。

- 検索中にすべてのトラフィックを渡す (デフォルト)。
- LDAP ポリシー検索要求および検索結果を除いて ほかのすべてのトラフィックを除去する。
- LDAP ポリシー検索要求および IPSec が保護する検索結果を除いて ほかのすべてのトラフィックを除去する。

場合によっては、最初の 2 つのうちのどちらかのオプションで充分です。しかし、LDAP トラフィックが公共インフラストラクチャーを通過する場合は、3 つ目のオプションを選択して、情報の保護と認証を行うべきです。この場合、フェーズ 1 と 2 の認証および暗号化のオプションを選択します。トンネルの終了点の IP アドレスも入力します (1 次および 2 次の LDAP サーバー)。このブートストラップ IKE/IPSec トンネルは、LDAP トラフィックが送られる前にネゴシエーションが行われます。このフィーチャーにより、247ページの図18に示された構成を確立できます。

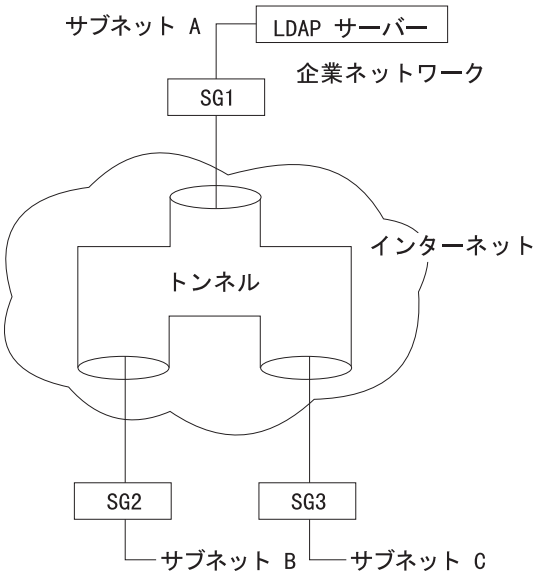


図 18. インターネットのトラフィックの保護

この図は、企業ネットワークのサブネット A にある LDAP サーバーを示しています。 SG1、SG2、および SG3 が LDAP サーバーからポリシーを取り出しています。 SG2 と SG3 のポリシーは、インターネットを通して検索され、IPSec により保護されます。

ポリシー・データベースがディレクトリーからポリシーを正しく取り出すために必要な構成情報は以下のとおりです。

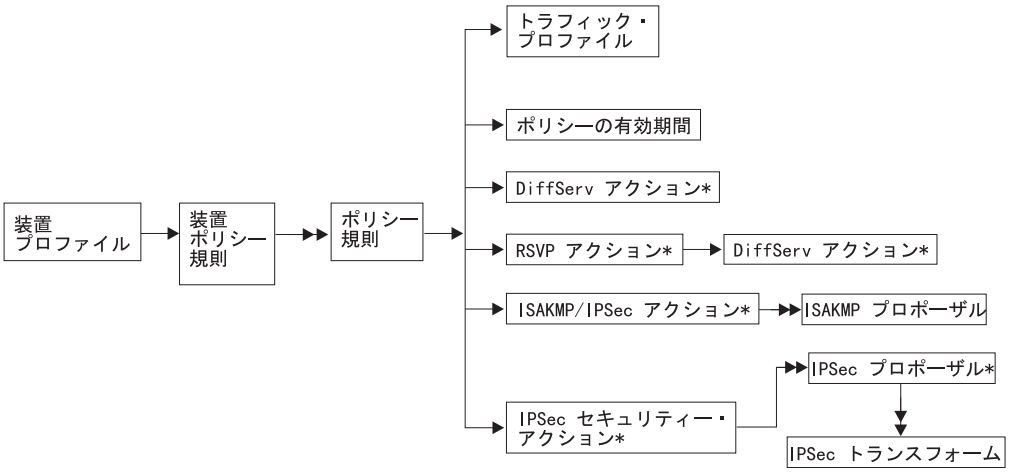
- 1 次サーバーの IP アドレス (バックアップの 2 次サーバーを構成してもよい)
- サーバーが対象とするポート番号 (注: SSL と TLS はサポートされていません)
- 必要であれば、ユーザー名とパスワード情報
- このルーターまたはルーターのクラスに対する DeviceProfile オブジェクトの基本的な識別名
- デフォルト・ポリシーの情報

この構成情報を入力すると、次にポリシー・データベースをリフレッシュするときに、ディレクトリー・サーバーに対しポリシー情報の問い合わせを試みます。ポリシー・データベースがあると、ローカルで構成したポリシーと LDAP サーバーから読み取った規則を組み合わせることができます。対立する 2 つの規則があり、ともに優先順位が同じときは、ローカル構成から読み取った規則の優先権がディレクトリー・サーバーから読み取った規則の優先権よりも上になります。

ポリシーのスキーマ

LDAP のスキーマは、ディレクトリー内の入力項目の内容を決定するクラスや属性の定義に関する規則と情報です。通常、LDAP スキーマは、SNMP MIB と同じような ASN1 構文で書かれています。この種のルーターがサポートするポリシー・スキーマは、IETF 内で実施される標準前の作業でできています。IETF の IPSec およびポリシー作業グループ、そして DMTF のポリシー作業グループが実施する標準トラック作業をベースにしています。ポリシー・スキーマは、ルーターのポリシー・フィーチャー内に構成された既存オブジェクトにごく一致します。ポリシー・スキー

マの定義ファイルと LDAP サーバーの構成ファイルは、次の URL にアクセスすると、みつかります。URL: **http://www.networking.ibm.com/support** 必要なルーター製品を選択してから、*Downloads* リンクを選んでください。図19は、ポリシー・スキーマの全体構造を示しています。



注:

1. →は参照項目が 1 つ
2. →→ は参照項目が 2 つ
3. * は参照項目がオプション
4. ISAKMP/IPSec のセキュリティー・ポリシーでは、トラフィック・プロファイルがトラフィック・フローを保護トンネルに定義します。

図 19. ポリシー・スキーマの構造

DeviceProfile と DevicePolicyRules は、ポリシー・スキーマの 2 つの重要なオブジェクトです。この 2 つで、ポリシー検索エージェントは、装置に必要なポリシーを探し出します。DeviceProfile は、装置の管理 IP アドレスと必須の DevicePolicyRules 参照項目に関する情報を含んでいます。装置をまとめて 1 つの DeviceProfile としたり、ネットワーク内の各装置にそれぞれ DeviceProfile を作ることもできます。どちらにするかは、同じ規則の組み合わせを取り出す装置がネットワークに 1 つ以上あるかどうかで決まります。セキュリティー・ゲートウェイの場合では、各ゲートウェイにそれぞれのトンネル・終了点があるので、こういうケースはありません。QoS のみの装置では、1 つのグループのすべての装置が同じポリシーの組み合わせを読み取ることが考えられます。

DevicePolicyRules オブジェクトは、装置に取り出された DeviceProfile 内の数値にもとづいて取り出されます。DevicePolicyRules オブジェクトが取り出されると、装置の PolicyRules リストが取り出されます。オブジェクトが見つからなかったり、オブジェクトの整合性検査でエラーが検出されると、検索は中止し、エラーを識別して ELS (PLCY メッセージ) が表示されます。エラーが発生すると、ネットワーク管理者は、以下の中から 1 つを構成して処理します。

- ローカルで読み取ったすべてのポリシーを削除し、除去に復帰するかすべての規則を渡す
- ローカルで読み取ったすべてのポリシーを維持する。このオプションは、ポリシー・フィーチャーの **set default** コマンドで指定します。

どちらの場合も、構成した再試行の間隔で再び検索が試みられます。1 次のプライマリー・サーバーと接続できなかった場合は、5 回の試みをしたあとに 2 次のサーバーが試みられます。2 次のサーバーに到達できないときは、 5 回の試みをしたあとに 1 次サーバーを再び試みます。再試行の間隔は、ポリシー・フィーチャーの **set ldap retry-interval** コマンドで設定します。ネットワークの待ち時間が原因で検索が失敗した場合は、検索のタイムアウトがデフォルトで 3 秒になっていますので、ポリシー・フィーチャーの **set ldap search-timeout** コマンドを使ってこれを変更できます。

規則の作成

ネットワークが自分の希望通りに動作するにように、ポリシーを構成できます。ルーターは、ポリシー情報を 1 組の規則として解釈し、トラフィックのフローと比較します。過去には、トラフィックのパターンごとにインバウンドとアウトバウンドのパケット・フィルターを手動で定義してこれに対応していたはずです。ポリシー・データベースでは、ポリシーを 1 つだけ構成すればよいので、こうした操作は必要ありません。

ほとんどの作業は、ポリシー・データベースが構築されるたびに内部で実行されます。場合によっては、ルーターはポリシーを直接 1 つの規則に解釈します。ISAKMP/IPSec の場合は、ポリシーを 5 つの規則に解釈します。5 つの規則は、トラフィックの方向 (インとアウト) と IKE のネゴシエーションでフェーズ 1 とフェーズ 2 のあいだに起こる制御フローのために必要になります。ポリシーと規則の関係は、以下のようになります。

1 つの DiffServ ポリシー → 1 つの DiffServ 規則

1 つの RSVP ポリシー → 1 つの RSVP 規則

1 つの ISAKMP/IPSec ポリシー → 5 つの ISAKMP/IPSec 規則

例: サブネット A からサブネット B へのトラフィックを保護する。トンネルの終了点は SGa と SGb。

1. フェーズ 1 インバウンド (Profile = SGb to SGa, Proto UDP, Src Port 500, Dst Port 500): 装置が ISAKMP 応答側として機能するときは、リモートの ISAKMP ピアから着信するフェーズ 1 のネゴシエーションをフィルター処理するために、この規則が必要になります。
2. フェーズ 2 アウトバウンド (Profile = SGa to SGb, Proto UDP, Src Port 500, Dst Port 500): トラフィックが ISAKMP フェース 1 ネゴシエーションを開始する場合は、必要となるフェーズ 1 情報をフィルター処理するために、この規則が必要になります。 この場合、装置は ISAKMP イニシエーターとして機能します。
3. フェーズ 2 インバウンド (Profile = SGb to SGa, Proto UDP, Src Port 500, Dst Port 500): リモートの ISAKMP ピアから着信するフェーズ 2 トラフィックをフィルター処理するために、この規則が必要になります。このトラフィックは、フェーズ 2 のリフレッシュまたは初期ネゴシエーションをリモー

ト・ピアが開始した結果です。アウトバウンド・トラフィック (規則 5) は、必要なときは常にネゴシエーションを開始するので、フェーズ 2 のアウトバンド規則は必要ありません。

4. 保護トンネルへのトラフィック (Profile = Subnet A to Subnet B): この規則は、未保護のトラフィックを保護トンネルに置くために必要な規則です。セキュリティー・アソシエーションがまだネゴシエーションされていない場合は、フェーズ 1 の規則が集められて、IKE がフェーズ 1 と 2 を開始します。SA が確立されると、この規則に一致するパケットは、カプセル化と転送のために、IPSec に渡されます。
5. 保護トンネルからのトラフィック (Profile = Subnet B to Subnet A): この規則は、保護トンネルで着信するはずのパケットが実際に保護トンネルで着信したことを確認するための規則です。パケットが IPSec でカプセルを外したのではなく、この規則が適用されると、パケットは除去されます。この規則は、ネットワークに不正に入り込んだトラフィックを処理します。

1 つの IPSec 手入力トンネル → 2 つの IPSec 規則

例: サブネット A からサブネット B へのトラフィックを保護する。トンネルの終了点は SGa と SGb。

1. 保護トンネルへのトラフィック (Profile = Subnet A to Subnet B): この規則は、未保護のトラフィックを保護トンネルに置くために必要な規則です。これは静的に構成されたトンネルなので常に使用でき、この規則に一致するパケットは、直接 IPSec に渡されて、カプセル化と転送が行われます。
2. 保護トンネルからのトラフィック (Profile = Subnet B to Subnet A): この規則は、保護トンネルで着信するはずのパケットが実際に保護トンネルで着信したことを確認するための規則です。パケットが IPSec でカプセルを外したのではなく、この規則が適用されると、パケットは除去されます。この規則は、ネットワークに不正に入り込んだトラフィックを処理します。

これらの規則は、ポリシー・フィーチャーの **list rule** 監視コマンドを使用して表示することができます。

構成の例

以下の例は、ポリシー・フィーチャーを使って、ネットワークのルーターを構成する方法を示しています。まずはじめに、以下のようにポリシー・フィーチャーにアクセスします。

```
* talk 6
Config>feature policy
IP Network Policy configuration
```

IPSec/ISAKMP ポリシーと QoS

ポリシー情報の入力方法は 2 つあります。1 つは、ポリシー・オブジェクトを個別を定義して、グループにまとめる方法です。この方法を使うには、はじめに IPSec トランスフォームを定義し、次に IPSec プロポーザルを定義します（これは IPSec トランスフォームを参照します)。次に、IPSec アクションを定義し (これは IPSec

プロポーザルを参照します)、これを続けてポリシーの定義を完成します。 図20 を参考にして、この方法はポリシー・オブジェクトの右側から始めて、左側に進みます。

2 つめの方法は、このほうが簡単な方法ですが、まずはじめに高水準のポリシー・オプションを定義します。次に、プロンプトに答えながら、個別のポリシー・オブジェクトの定義を入力していきます。構成例は、図20の図にしたがって、図の数値を使っています。この例では、左から右方向に進み、 **add policy** コマンドで始まります。

以前に定義したオブジェクトが必要条件に合うときは、新しいオブジェクトを作らないでこれを再利用できます。たとえば、以前のポリシーで allTheTime の有効期間を構成していればこれを再利用できます。次の手順は全プロセスを示していますが、定義済みのポリシー情報を再利用する方法については示されていません。定義済み情報の利用方法については、260ページの『IPSec/ISAKMP だけのポリシー』を参照してください。

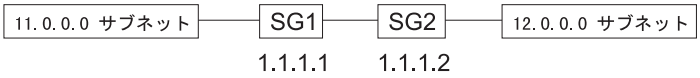


図 20. IPSec/ISAKMP と QoS の構成

以下に示すポリシーの構成方法は SG1 の例です。ポリシーのステートメントは以下のとおりです。

トンネル終了点が SG1 と SG2 のサブネット 11 からサブネット 12 のトラフィックを保護し、DiffServ GoldService を使ってこのトンネル内のトラフィックに QoS を提供します。

1. ポリシーの追加。

```
Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? examplePolicySecure11to12
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]? 10
```

2. 構成されたプロファイルがないので、新しいものを定義します。

```
List of Profiles:
        0: New Profile

Enter number of the profile for this policy [0]?
```

3. 新しいプロファイルの定義: この場合、サブネット 11 からサブネット 12 のトラフィックが対象となります。

```
Enter a Name (1-29 characters) for this Profile []? trafficFrom11NetTo12Net
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 11.0.0.0
Enter IPV4 Source Mask [255.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 12.0.0.0
Enter IPV4 Destination Mask [255.0.0.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
```

```
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:


Here is the Profile you specified...


Profile Name    = trafficFrom11NetTo12Net
        sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
        dAddr:Mask=       12.0.0.0 : 255.0.0.0       dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
Is this correct? [Yes]:
```

4. プロファイルの定義が完成したら、ポリシー構成メニューに戻ります。

```
List of Profiles:
        0: New Profile
        1: trafficFrom11NetTo12Net

Enter number of the profile for this policy [1]? 1
```

5. 有効期間が定義されていないので、新しいものを定義します。

```
List of Validity Periods:
        0: New Validity Period

Enter number of the validity period for this policy [0]?
```

6. 有効期間の構成に関する質問: この例では、有効期間は 1999 年各月の月曜日から金曜日の 9 AM から 5 PM です。

```
Enter a Name (1-29 characters) for this Policy Valid Profile []?
             MonToFri-9am:5pm-1999
Enter the lifetime of this policy. Please input the
information in the following format:
              yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]? 19990101000000:19991231000000
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]? mon tue wed thu fri
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]? 00:00:00
Enter the ending time (hh:mm:ss)
 [00:00:00]? 17:00:00

Here is the Policy Validity Profile you specified...

Validity Name   = MonToFri-9am:5pm-1999
        Duration  = 19990101000000 : 19991231000000
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 09:00:00 : 17:00:00
Is this correct? [Yes]:
```

7. 有効期間の定義が完成したら、ポリシー構成メニューに戻ります。

```
List of Validity Periods:
        0: New Validity Period
        1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]? 1
Should this policy enforce an IPSEC action? [No]: yes
```

8. トンネルの終了点はいつも異なるので、常に新しい IPSec アクションを定義する必要があるのでしょうか。同一の 2 つのゲートウェイのあいだに複数のトンネルがある場合、そしてトンネルの終了点が未知となるワイルドカードのリモート・アクセス構成は例外です。

```
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
```

9. IPSec アクションのメニュー

```
Enter a Name (1-29 characters) for this IPsec Action []? secure11NetTo12Net
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]? 2
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [11.0.0.5]? 1.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 1.1.1.2
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
```

10. 定義された IPSec プロポーザルがないので、新しいものを定義します。 IPSec プロポーザルを一度定義すれば、複数の IPSec アクションでこれを再利用できます。

```
List of IPSEC Proposals:
        0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
```

11. IPSec プロポーザルの構成

```
Enter a Name (1-29 characters) for this IPsec Proposal []? genP2Proposal
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: yes
```

12. 構成された ESP トランスフォームがないので、新しいものを定義します。 ESP トランスフォームを一度定義すれば、どの IPSec プロポーザルにもこれを再利用できます。

```
List of ESP Transforms:
        0: New Transform

Enter the Number of the ESP transform [0]? 0
```

13. IPSec トランスフォームの構成

```
Enter a Name (1-29 characters) for this IPsec Transform []? esp3DESwSHA
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

Select the Protocol ID (1-2) [1]? 2
List of Encapsulation Modes:
     1)  Tunnel
     2)  Transport

Select the Encapsulation Mode(1-2) [1]? 1
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]? 2
List of ESP Cipher Algorithms:
     1)  ESP DES
     2)  ESP 3DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? 2
Security Association Lifesize, in kilobytes (1024-65535) [50000]?
Security Association Lifetime, in seconds (120-65535) [3600]?

Here is the IPSec transform you specified...

Transform Name  = esp3DESwSHA
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES
Is this correct? [Yes]:
```

14. IPSec プロポーザル・メニューに戻ります。

```
List of ESP Transforms:
        0: New Transform
        1: esp3DESwSHA

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [Yes]: no

Here is the IPSec proposal you specified...

Name  = genP2Proposal
        Pfs   = N
        ESP Transforms:
                esp3DESwSHA
Is this correct? [Yes]:
```

15. IPSec アクションのメニューに戻ります。

```
List of IPSEC Proposals:
        0: New Proposal
        1: genP2Proposal

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPSec Action you specified...

IPSECAction Name = secure11NetTo12Net
        Tunnel Start:End         =       1.1.1.1 : 1.1.1.2
        Tunnel In Tunnel         =            No
        Min Percent of SA Life   =            75
        Refresh Threshold        =            85 %
```

```
        Autostart               =             No
        DF Bit                  =           COPY
        Replay Prevention       =       Disabled
        IPSEC Proposals:
                genP2Proposal
Is this correct? [Yes]:
```

16. ポリシー・メニューに戻ります。

```
IPSEC Actions:
        0: New IPSEC Action
        1: secure11NetTo12Net

Enter the Number of the IPSEC Action [1]? 1
```

17. 保護 IPSec アクションのタイプを指定したので、フェーズ 1 のネゴシエーションのために ISAKMP アクションを確認します。定義されたものはないので、新しいものを入力します。 多くの場合、すべてのセキュリティー・ポリシーについて 1 つの ISAKMP アクションとプロポーザルがあれば充分です。

```
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
```

18. ISAKMP アクションの構成

```
Enter a Name (1-29 characters) for this ISAKMP Action []? genPhase1Action

List of ISAKMP Exchange Modes:
     1)  Main
     2)  Aggressive

Enter Exchange Mode (1-2) [1]?
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

ISAKMP Connection Lifesize, in kilobytes (100-65535) [5000]?
ISAKMP Connection Lifetime, in seconds (120-65535) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]: no
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
```

19. 構成された ISAKMP プロポーザルがないので、新しいものを作ります。

```
List of ISAKMP Proposals:
        0: New Proposal
```

20. ISAKMP プロポーザルの構成

```
Enter the Number of the ISAKMP Proposal [0]?
Enter a Name (1-29 characters) for this ISAKMP Proposal []? genP1Proposal

List of Authentication Methods:
     1)  Pre-Shared Key
     2)  RSA SIG

Select the authentication method (1-2) [1]? 2

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
     1)  DES
     2)  3DES

Select the Cipher Algorithm (1-2) [1]? 2
Security Association Lifesize, in kilobytes (100-65535) [1000]?
Security Association Lifetime, in seconds (120-65535) [15000]?
```

```
List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?


Here is the ISAKMP Proposal you specified...

Name = genP1Proposal
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB
Is this correct? [Yes]:
```

21. ISAKMP アクションの構成に戻ります。

```
List of ISAKMP Proposals:
        0: New Proposal
        1: genP1Proposal

Enter the Number of the ISAKMP Proposal [1]?
Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

ISAKMP Name     = genPhase1Action
        Mode                    =            Main
        Min Percent of SA Life  =              75
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =              No
        ISAKMP Proposals:
                genP1Proposal
Is this correct? [Yes]:
```

22. ポリシーの構成に戻ります。

```
ISAKMP Actions:
        0: New ISAKMP Action
        1: genPhase1Action

Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]: yes
```

23. DiffServ GoldService アクションを定義します。

```
DiffServ Actions:
        0: New DiffServ Action

Enter the Number of the DiffServ Action [0]?
```

24. DiffServ アクションの構成

    DiffServ アクションが、assured queue に対するものである場合:

```
Enter a Name (1-29 characters) for this DiffServ Action [AF11]? GoldService
Enter the permission level for packets matching this DiffServ
Action (1. Permit, 2. Deny) [2]? 1
List of DiffServ Queues:
   1) Premium
   2) Assured/BE
Enter the Queue Number(1-2) for outgoing packets matching
this DiffServ Action [2]?
How do you want to specify the bandwidth allocated to this service?
Enter absolute kbps(1) or percentage of output bandwidth(2) [2]?
Enter the percentage of output bandwidth allocated to this service [10]? 20

List of Assured Forwarding Class:
  1) AF11 Class DS Byte
  2) AF21 Class DS Byte
```

```
  3) AF31 Class DS BYte
  4) AF41 Class DS Byte
  5) New Class DS Byte

Enter the AF Class (1-5) for outgoing packets matching
this DiffServ Action [5]? 1

List of Policing Type in AF Class:
  1) Single Rate Color Blind TCM
  2) Single Rate Color Aware TCM
  3) Two Rate Color Blind TCM
  4) Two Rate Color Aware TCM
  5) None
Enter the AF Class (1-5) Policing for outgoing packets matching
this DiffServ Action [5]? 1

Single Rate TCM:
Committed Info Rate (CIR in bytes/sec) [0]? 25000
Committed Burst Size (CBS in bytes) [4000]?
Excess Burst Size (EBS in bytes) [4000]?

Here is the DiffServ Action you specified...

DiffServ Name   = GoldService                    Type =Permit

        DS mask:modify=xFC:x20
        Queue:BwShare  =Assured    : 20 %
        TCM:Class = SR,CB:AF11
        CIR = 25000 bytes/sec;   CBS = 4000 bytes
        EBS = 4000 bytes

Is this correct? [Yes]:
```

DiffServ アクションが、premium queue に対するものである場合:

```
Name (1-29 characters) for this DiffServ Action []? ExpService
Enter the permission level for packets matching this DiffServ
Action (1. Permit, 2. Deny) [2]? 1
List of DiffServ Queues:
   1) Premium
   2) Assured/BE
Enter the Queue Number(1-2) for outgoing packets matching
this DiffServ Action [2]? 1
How do you want to specify the bandwidth allocated to this service?
Enter absolute kbps(1) or percentage of output bandwidth(2) [2]?
Enter the percentage of output bandwidth allocated to this service [10]? 19

Transmitted DS-byte mask [0]? fc
Transmitted DS-byte modify value [0]? b8

List of EF Policing Config Type
   1) Default
   2) Custom

Enter the Parameter Type [1]? 2
Enter the Token Rate (in bytes/sec) [0]? 25000
Enter the Token Bucket Size (in bytes) [0]? 4000


Here is the DiffServ Action you specified...


DiffServ Name   = ExpService                    Type =Permit
        DS mask:modify =xFC:xB8
        Queue:BwShare  =Premium    : 19 %
        Token Rate:    = 25000 bytes/sec
        Token Bucket:  = 4000 bytes
Is this correct? [Yes]:
```

25. ポリシーの構成に戻ります。

```
DiffServ Actions:
        0: New DiffServ Action
        1: GoldService
```

```
Enter the Number of the DiffServ Action [1]? 1
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name     = examplePolicySecure11to12
        State:Priority =Enabled    : 10
        Profile        =trafficFrom10NetTo12Net
        Valid Period   =MonToFri-9am:5pm-1999
        IPSEC Action   =secure11NetTo12Net
        ISAKMP Action  =genPhase1Action
        DiffServ Action=GoldService
Is this correct? [Yes]:
```

26. DiffServ や IPSec が使用可能になっていない場合は、ポリシーを実行する前に警告がでます。DiffServ または IPSec、あるいはその両方を使用可能にします (DiffServ フィーチャーまたは IPSec フィーチャー)。

```
You must enable and configure DiffServ in feature DS before
QOS can be ensured for this policy
```

27. このプロセスの最後のステップは、リモートの ISAKMP ピアについて、USER プロファイルの定義を追加することです。ISAKMP のネゴシエーションで、公開認証によりピアの認証ができるときは、このステップは必要ありません。しかし、前回の例では、認証方式としてプリシェアード・キーを選択しました。そこで、ユーザーを確認するため、プリシェアード・キーを入力して、これをピアに使ってもらいます。

```
Policy config>add user
Choose from the following ways to identify a user:
        1: IP Address
        2: Fully Qualified Domain Name
        3: User Fully Qualified Domain Name
        4: Key ID (Any string)
Enter your choice(1-4) [1]?
Enter the IP Address that distinguishes this user
 [0.0.0.0]? 1.1.1.2
Group to include this user in []? peers
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (10 characters) in ascii:

Here is the User Information you specified...

Name      = 1.1.1.2
Type      = IPV4 Addr
        Group     =peers
        Auth Mode =Pre-Shared Key
        Key(Ascii)=exampleKey
Is this correct? [Yes]:
```

28. これでポリシーの構成ステップは完了です。DiffServ、IPSec、その他のネットワークまたは IP 構成を構成するときは、IPSec トンネルの機能が有効になる前にこれらを構成してください。以下の list コマンドの例は、上記で完成した構成を示しています。これらの変更を有効にするには、装置を再ロードするか、ポリシー・フィーチャーの **reset database** 監視コマンドを入力します。

```
Policy config>list all

Configured Policies....

Policy Name     = examplePolicySecure11to12
        State:Priority =Enabled    : 10
        Profile        =trafficFrom11NetTo12Net
        Valid Period   =MonToFri-9am:5pm-1999
        IPSEC Action   =secure11NetTo12Net
        ISAKMP Action  =genPhase1Action
```

```
        DiffServ Action=GoldService
--More--

Configured Profiles....

Profile Name    = trafficFrom11NetTo12Net
        sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
        dAddr:Mask=       12.0.0.0 : 255.0.0.0       dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
--More--

Configured Validity Periods

Validity Name   = MonToFri-9am:5pm-1999
        Duration  = 19990101000000 : 19991231000000
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 09:00:00 : 17:00:00
--More--

Configured DiffServ Actions....

DiffServ Name   = GoldService                    Type =Permit

 DS mask:modify=xFC:x20
 Queue:BwShare  =Assured    : 20 %
 TCM:Class = SR, CB, AF11
 CIR = 25000 bytes/sec;   CBS = 4000 bytes
 EBS = 4000 bytes
--More--

Configured IPSEC Actions....

IPSECAction Name = secure11NetTo12Net
        Tunnel Start:End         =        1.1.1.1 : 1.1.1.2
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =             75
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                genP2Proposal
--More--

Configured IPSEC Proposals....

Name  = genP2Proposal
        Pfs   = N
        ESP Transforms:
                esp3DESwSHA
--More--

Configured IPSEC Transforms....

Transform Name  = esp3DESwSHA
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES
--More--

Configured ISAKMP Actions....

ISAKMP Name     = genPhase1Action
        Mode                     =            Main
        Min Percent of SA Life   =              75
        Conn LifeSize:LifeTime   =            5000 : 30000
        Autostart                =              No
        ISAKMP Proposals:
                genP1Proposal
--More--

Configured ISAKMP Proposals....
Name = genP1Proposal
```

```
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB
--More--

Configured Policy Users....
Name      = 1.1.1.2
Type      = IPV4 Addr
        Group     =peers
        Auth Mode =Pre-Shared Key
        Key(Ascii)=exampleKey
--More--

Configured Manual IPSEC Tunnels....

                            IPv4 Tunnels
-------------------------------------------------------------------------------

  ID         Name        Local IPv4 Addr  Rem IPv4 Addr    Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
```

IPSec/ISAKMP だけのポリシー

次の構成手順の例は、図21 にしたがって、図の数値を使用し、左から右方式で、作成済みの情報を使って前回の手順例を構築する方法を示しています。

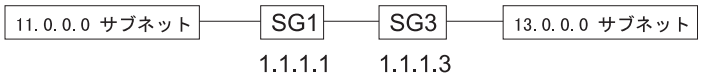


図 21. IPSec の構成と作成済みの定義の再利用

以下に示すポリシーの構成方法は SG1 の例です。この例のポリシーのステートメントは以下のとおりです。

トンネル終了点が SG1 と SG3 のサブネット 11 からサブネット 13 のトラフィックを保護し (TCP トラフィックのみ)、QoS を提供しません。

1. ポリシーの追加。

```
Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? examplePolicySecure11to13
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]? 10
List of Profiles:
        0: New Profile
        1: trafficFrom10NetTo12Net

Enter number of the profile for this policy [1]? 0
Enter a Name (1-29 characters) for this Profile []? trafficFrom11NetTo13Net
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 11.0.0.0
Enter IPV4 Source Mask [255.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 13.0.0.0
Enter IPV4 Destination Mask [255.0.0.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range
```

```
Select the protocol to filter on (1-4) [3]? 1
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:

Here is the Profile you specified...

Profile Name    = trafficFrom11NetTo13Net
        sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
        dAddr:Mask=       13.0.0.0 : 255.0.0.0       dPort=    0 : 65535
        proto     =              6 : 6
        TOS       =            x00 : x00
        Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: trafficFrom10NetTo12Net
        2: trafficFrom11NetTo13Net

Enter number of the profile for this policy [1]? 2
```

2. 有効期間を再利用する。

```
List of Validity Periods:
        0: New Validity Period
        1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]?
Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
        0: New IPSEC Action
        1: secure11NetTo12Net

Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? secure11To13
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
 [11.0.0.5]? 1.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 1.1.1.3
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
```

```
system initialization(Y-N)? [No]:
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.
```

3. 定義済みの構成の IPSec プロポーザルを再利用する。

```
List of IPSEC Proposals:
        0: New Proposal
        1: genP2Proposal

Enter the Number of the IPSEC Proposal [1]?
Are there any more Proposal definitions for this IPSEC Action? [No]:


Here is the IPSec Action you specified...


IPSECAction Name = secure11To13
        Tunnel Start:End         =        1.1.1.1 : 1.1.1.3
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =             75
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                genP2Proposal
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: secure11NetTo12Net
        2: secure11To13

Enter the Number of the IPSEC Action [1]? 2
```

4. 定義済みの構成の ISAKMP アクションを再利用する。

```
ISAKMP Actions:
        0: New ISAKMP Action
        1: genPhase1Action

Enter the Number of the ISAKMP Action [1]?
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name     = examplePolicySecure11to13
        State:Priority =Enabled    : 10
        Profile        =trafficFrom11NetTo13Net
        Valid Period   =MonToFri-9am:5pm-1999
        IPSEC Action   =secure11To13
        ISAKMP Action  =genPhase1Action
Is this correct? [Yes]:
```

すべての公共トラフィックを除去する (フィルター規則)

このポリシーの例では、IPSec を通して保護されていないすべてのトラフィックを除去する公共インターフェースについて、簡単な除去規則の構成方法を示しています。この規則は、ごく一般的な規則で、構成されたあらゆるすべての規則のなかで優先順位を**もっとも低くすべき**です。

1. ポリシーの追加

```
Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? dropAllPublicTraffic
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
        0: New Profile
        1: trafficFrom10NetTo12Net
        2: trafficFrom11NetTo13Net

Enter number of the profile for this policy [1]? 0
```

2. 公共のインターフェース (1.1.1.1) に出入りするすべてのトラフィックを含むような新しいプロファイルを定義します。

```
Enter a Name (1-29 characters) for this Profile []? allPublicTraffic
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]?
Enter IPV4 Source Mask [0.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]?
Enter IPV4 Destination Mask [0.0.0.0]?

Protocol IDs:
     1)  TCP
     2)  UDP
     3)  All Protocols
     4)  Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
```

3. 発信元または宛先 (あるいはその両方) の情報がワイルドカードになっているので、このトラフィックが出入りすると思われるインターフェースを指定します。

```
The Source and/or Destination Address information you specified
includes all addresses.  You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy.  The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]: yes
Interface Pair Groups:
0: New Ifc Pair
Number of Ifc Pair Group [1]? 0
```

4. 公共インターフェースから出ていくトラフィックについて、インターフェース・ペアを追加します。

```
Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
 [255.255.255.255]?
Egress Interface IP Address (255.255.255.255 = any egress)
 [255.255.255.255]? 1.1.1.1
Interface Pair Groups:
0: New Ifc Pair
1) Group Name: inOutPublic
  In:Out=255.255.255.255 : 1.1.1.1

Number of Ifc Pair Group [1]? 0
```

5. 公共インターフェースから入ってくるトラフィックについて、もう 1 つのインターフェース・ペアを追加します。前回のインターフェース・ペアと同じ名前にして、同じグループに割り当てます。

```
Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
 [255.255.255.255]? 1.1.1.1
Egress Interface IP Address (255.255.255.255 = any egress)
 [255.255.255.255]?
Interface Pair Groups:
0: New Ifc Pair
1) Group Name: inOutPublic
  In:Out=255.255.255.255 : 1.1.1.1
  In:Out=        1.1.1.1 : 255.255.255.255

Number of Ifc Pair Group [1]?

Here is the Profile you specified...

Profile Name    = allPublicTraffic
sAddr:Mask=        0.0.0.0 : 0.0.0.0         sPort=    0 : 65535
dAddr:Mask=        0.0.0.0 : 0.0.0.0         dPort=    0 : 65535
proto     =              0 : 255
TOS       =            x00 : x00
Remote Grp=All Users
1.  In:Out=255.255.255.255 : 1.1.1.1
2.  In:Out=        1.1.1.1 : 255.255.255.255
Is this correct? [Yes]:
List of Profiles:
0: New Profile
1: trafficFrom10NetTo12Net
2: trafficFrom11NetTo13Net
3: allPublicTraffic

Enter number of the profile for this policy [1]? 3
```

6. 新しい有効期間を all the time に指定して作成します。

```
List of Validity Periods:
0: New Validity Period
1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]? 0
Enter a Name (1-29 characters) for this Policy Valid Profile []? allTheTime
Enter the lifetime of this policy. Please input the
information in the following format:
yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]?
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]?

Here is the Policy Validity Profile you specified...

Validity Name   = allTheTime
Duration  = Forever
Months    = ALL
Days      = ALL
```

```
Hours     = All Day
Is this correct? [Yes]:
List of Validity Periods:
0: New Validity Period
1: MonToFri-9am:5pm-1999
2: allTheTime

Enter number of the validity period for this policy [1]? 2
Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
0: New IPSEC Action
1: secure11NetTo12Net
2: secure11To13
```

7. すべてのトラフィックを除去するための新しい IPSec アクションを追加します (フィルター・アクション)。

```
Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? dropTraffic
List of IPsec Security Action types:
     1)  Block (block connection)
     2)  Permit

Select the Security Action type (1-2) [2]? 1

Here is the IPSec Action you specified...

IPSECAction Name = dropTraffic
Action   = Drop
Is this correct? [Yes]:
IPSEC Actions:
0: New IPSEC Action
1: secure11NetTo12Net
2: secure11To13
3: dropTraffic

Enter the Number of the IPSEC Action [1]? 3
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name     = dropAllPublicTraffic
State:Priority =Enabled    : 5
Profile        =allPublicTraffic
Valid Period   =allTheTime
IPSEC Action   =dropTraffic
Is this correct? [Yes]:
```

LDAP ポリシー検索エンジンを構成して使用可能にする

この例は、LDAP ポリシー検索エンジンの構成方法と、使用可能にする方法を示しています。この例では、2 つの LDAP ディレクトリーがあり (1 次と 2 次)、それぞれの IP アドレスは、11.0.0.2 と 13.0.0.1 です。両者とも TCP ポート 389 を対象として、装置は LDAP サーバーを cn=router、パスワードを myPassWord としてバインドするものとします。ルーターのポリシーに対するディレクトリー・ツリーの基本入力は、cn=RouterDeviceProfile,o=ibm,c=us です。

注: 現在、1 次と 2 次の LDAP サーバーは、ともに同じポートを対象にして、ルーターに対しては同じ認証を使用します。両方のディレクトリー・サーバーについて、ルーターの DeviceProfile は同一です。

この例では、デフォルトのポリシーの設定方法を示し、IPSec を通して LDAP 通信

を保護する方法も示します。この例では、ISAKMP の認証にプリシェアード・キーを使い、フェーズ 1 とフェーズ 2 の認証と暗号化には SHA と 3DES を使います。LDAP のポリシーを検索する装置のトンネルの開始点は 1.1.1.4、トンネルの終了点は、11.0.0.1 の LDAP サーバーが 1.1.1.1、13.0.0.1 の LDAP サーバーが 1.1.1.3 です。

1. LDAP ポリシー検索エンジンを構成、使用可能にし、結果を表示します。

```
Policy config>set ldap primary-server 11.0.0.1
Policy config>set ldap secondary-server 13.0.0.1
Policy config>set ldap port 389
Policy config>set ldap bind-name cn=router
Policy config>set ldap bind-pw myPassWord
Policy config>set ldap anonymous-bind no
Policy config>set ldap policy-base cn=RouterDeviceProfile,o=ibm,c=us
Policy config>enable ldap policy-search
Policy config>list ldap
LDAP CONFIGURATION information:

Primary Server Address:               11.0.0.1
Secondary Server Address:             13.0.0.1


Search timeout value:                 3 sec(s)
Retry interval on search failures:    1 min(s)
Server TCP port number:               389
Server Version number:                2


Bind Information:
Bind Anonymously:                     No
  Device Distinguished Name:          cn=router
  Device Password:                    myPassWord


Base DN for this device's policies:   cn=RouterDeviceProfile,o=ibm,c=us


Search policies from LDAP Directory:  Enabled
```

2. デフォルト・ポリシーを設定します。

```
Policy config>set default-policy
List of default policy rules:
  1)  Accept and Forward all IP Traffic
  2)  Permit LDAP traffic, drop all other IP Traffic
  3)  Permit and Secure LDAP traffic, drop all other IP Traffic

Select the default policy rule to use during policy refresh periods [1]? 3
List of default error handling procedures:
  1)  Reset Policy Database to Default Rule
  2)  Flush any rules read from LDAP, load local rules

Select the error handling behavior for when loading Policy Database  [1]?

Please enter the set of Security Information for encrypting and
authenticating the LDAP traffic generated by the device when
retrieving policy information from the LDAP Server

Enter phase 1 ISAKMP negotiation parameters:

List of Diffie Hellman Groups:
     1)  Diffie Hellman Group 1
     2)  Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?
```

```
List of Hashing Algorithms:
     1)  MD5
     2)  SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
     1)  DES
     2)  3DES

Select the Cipher Algorithm (1-2) [1]? 2
Authentication: (1)Pre-shared Key or (2)Certificate(RSA Sig) [2]? 1
Enter the Pre-Shared Key []? test

Enter phase 2 IPSEC negotiation parameters:
List of IPsec Authentication Algorithms:
     0)  None
     1)  HMAC-MD5
     2)  HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [1]? 2
List of ESP Cipher Algorithms:
     1)  ESP DES
     2)  ESP 3DES
     3)  ESP CDMF
     4)  ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? 2
Tunnel Start IPV4 Address (Primary LDAP Server)
 [0.0.0.0]? 1.1.1.4
Tunnel End Point IPV4 Address (Primary LDAP Server)
 [0.0.0.0]? 1.1.1.1
Tunnel Start IPV4 Address (Secondary LDAP Server)
 [1.1.1.4]?
Tunnel End Point IPV4 Address (Secondary LDAP Server)
 [1.1.1.1]? 1.1.1.3
Policy config>list default-policy

Default Policy Rule:                  Drop All IP Traffic except secure LDAP
Default error handling procedure:     Reset Policy Database to Default Rule

Phase 1 ISAKMP negotiation parameters:
Diffie Hellman Group ID:              1
Hashing Algorithm:                    SHA
ISAKMP Cipher Algorithm:              ESP 3DES CBC
Per-shared key value:                 test

Phase 2 IPSEC negotiation parameters:
IPsec ESP Authentication Algorithm:   HMAC SHA
ESP Cipher Algorithm:                 3DES
Local Tunnel Addr (Primary Server):   1.1.1.4
Remote Tunnel Addr (Primary Server):  1.1.1.1
Local Tunnel Addr (Secondary Server): 1.1.1.4
Remote Tunnel Addr (Secondary Server): 1.1.1.3
```

ここで、ポリシー・フィーチャーを使って、ネットワークのルーターを管理する準備ができました。プロファイル、プロポーザル、トランスフォーム、アクションなど、ポリシーに必要なパラメーターを構成するコマンドについては、 275ページの『ポリシー構成コマンド』、295ページの『LDAP ポリシー・サーバーの構成コマンド』、および 301ページの『ポリシー監視コマンド』を参照してください。

ポリシーのクィック構成例

ポリシー・フィーチャーで使用可能な **qconfig** コマンドを使用すると、4 つのシナリオのいずれかに基づいてポリシーを速やかに追加することができます。簡単な質問がいくつか尋ねられます。その応答に基づいて、ポリシー・オブジェクトが生成されます。 **qconfig** コマンドは、事前定義されたポリシー・テンプレートを利用して、構成の質問を最小限にします。 **qconfig** を使用してポリシー・オブジェクトを変更することはできません。このコマンドは、ポリシーを速やかに追加する手段にすぎません。このコマンドの詳細については、275ページの『ポリシー構成コマンド』を参照してください。

次の例は、この章のこれ以前の部分で説明された IPSec/ISAKMP 例を複写したものです。基本的に、目的は、SG1 および SG2 を使用して 11.0.0.0 サブネットから 12.0.0.0 サブネットまでのトラフィックを保護し、認証することです。さらに、これらのセキュリティー・ゲートウェイを使用して保護されるトラフィックにも、QoS が提供されます。この例では、QoS は AF11 であり、強力なセキュリティーが選択されています。

```
Policy config>qconfig
Enter a Name (1-29 characters) for this Policy [policyQC_1]?
Please choose from one of the following Scenarios:

1: Branch Office Scenario
2: Remote Access User Scenario (IPSEC and L2TP)
3: Drop Traffic not matched on Untrusted Interface
4: Custom
Selection [1]?
Local Subnet (Base Address) [0.0.0.0]? 11.0.0.0
Local Subnet (Net Mask) [255.0.0.0]?
Local Tunnel Endpoint [11.0.0.5]? 1.1.1.1
Remote Subnet (Base Address) [0.0.0.0]? 12.0.0.0
Remote Subnet (Net Mask) [255.0.0.0]?
Remote Tunnel Endpoint [0.0.0.0]? 1.1.1.2
Configure Ports and Protocols? [No]:
1: Strong Security, 2: Very Strong Security, 3: Help [1]?
Authenticate Peer using 1:Pre-shared Key or 2:Certificate(RSA Signatures) [2]? 1
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (4 characters) in ascii:
Select from the following DiffServ Actions:
        0: Best Effort (No DiffServ)
        1: EF
        2: AF11
        3: AF21
        4: AF31
        5: AF41
        6: GoldService

Enter Selection [0]? 2
Configure advanced options? [No]:


Here is the information you entered...

Policy Name:  policyQC_1 (Branch Office Scenario)
Local Information:
------------------
            Subnet:  11.0.0.0/255.0.0.0
   Tunnel Endpoint:  1.1.1.1
        Port Range:  00000-65535

Remote Information:
-------------------
            Subnet:  12.0.0.0/255.0.0.0
   Tunnel Endpoint:  1.1.1.2
        Port Range:  00000-65535

Other Information:
------------------
          Protocol:  000-255
          Priority:  10
          Security:  Strong Security
        Encap Mode:  Tunnel
         Auth Mode:  Pre-Shared Key
   Validity Period:  allTheTime
   DiffServ Action:  AF11
Continue? [Yes]:
```

```
----------------------------------------
Based on the input to these simple questions, the QCONFIG mechanism generated the following objects:
1.

   Policy config>list policy by-name policyQC_1

   Policy Name     = policyQC_1
           State:Priority =Enabled    : 10
           Profile        =policyQC_1
           Valid Period   =allTheTime
           IPSEC Action   =policyQC_1
           ISAKMP Action  =generalPhase1Action
           DiffServ Action=AF11
2.

   Policy config>list ipsec-action by-name policyQC_1
   IPSECAction Name = policyQC_1
           Tunnel Start:End         =        1.1.1.1 : 1.1.1.2
           Tunnel In Tunnel         =             No
           Min Percent of SA Life   =              1
           Refresh Threshold        =             85 %
           Autostart                =             No
           DF Bit                   =           COPY
           Replay Prevention        =       Disabled
           IPSEC Proposals:
                   strongP2EspProp
                   strongP2EspAhProp
                   veryStrongP2EspProp
                   veryStrongP2EspAhProp
3.

   Policy config>list profile by-name policyQC_1

   Profile Name    = policyQC_1
           sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
           dAddr:Mask=       12.0.0.0 : 255.0.0.0       dPort=    0 : 65535
           proto     =              0 : 255
           TOS       =            x00 : x00
           Remote Grp=All Users
4.

   Policy config>list user by-name
   List of Users:
     num: User Info                          :Group Name
        1: 1.1.1.2                           :IKE-Peers
   Enter the number of user [1]?
   Name      = 1.1.1.2
   Type      = IPV4 Addr
           Group     =IKE-Peers
           Auth Mode =Pre-Shared Key
```

事前定義されたポリシー・オブジェクト

次のポリシー・オブジェクトが、ユーザー用に事前定義されています。これらのオブジェクトは、最も一般的な構成を表し、多くのポリシー構成に使用するためのものです。これらの事前定義されたポリシー・オブジェクト定義を、**qconfig** コマンドと共に使用すると、簡単にポリシーをネットワーク構成に追加することができます。事前定義されたテンプレートを変更することも、削除することもできません。オブジェクトを変更したい場合、新しい名前を指定した **copy** コマンドを使用して、オブジェクトをコピーする必要があります。コピーした後、そのコピーを変更することができます。新しいリリース、または PTF バージョンのコードにアップグレードするときに、テンプレートを変更していなかった場合、ポリシー・フィーチ

ャーの **refresh-templates** 構成コマンドを使用して、最新のテンプレートを取得する必要があります。それ以外の場合は、元の定義が引き続き使用されます。

ポリシー・フィーチャーについて、次の事前定義されたオブジェクトが存在します。

有効期間

次の有効期間オブジェクトが事前定義されます。

```
Validity Name   = allTheTime
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day

Validity Name   = allTheTimeMonThruFri
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = All Day

Validity Name   = 9to5MonThruFri
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 09:00:00 : 17:00:00

Validity Name   = 5to9MonThruFri
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 17:00:00 : 09:00:00
```

DiffServ アクション

次の DiffServ アクション・オブジェクトが事前定義されます。

```
DiffServ Name   = EF                              Type =Permit
        DS mask:modify =xFC:xB8
        Queue:BwShare  =Premium    : 19 %
        Token Rate:    = 0 bytes/sec
        Token Bucket:  = 0 bytes

DiffServ Name   = AF11                             Type =Permit
        DS mask:modify =xFC:x28
        Queue:BwShare  =Assured    : 15 %
        No Policing Selected

DiffServ Name   = AF21                             Type =Permit
        DS mask:modify =xFC:x48
        Queue:BwShare  =Assured    : 10 %
        No Policing Selected

DiffServ Name   = AF31                             Type =Permit
        DS mask:modify =xFC:x68
        Queue:BwShare  =Assured    : 10 %
        No Policing Selected

DiffServ Name   = AF41                             Type =Permit
        DS mask:modify =xFC:x88
        Queue:BwShare  =Assured    : 5 %
```

IPSec アクション

次の IPSec アクション・オブジェクトが事前定義されます。

```
IPSECAction Name = ipsecDropTraffic
        Action   = Drop

IPSECAction Name = ipsecPassTrafficClear
        Action   = Clear
```

IKE フェーズ 2 用の IPSec プロポーザル

次の IKE フェーズ 2 用の IPSec プロポーザル・オブジェクトが事前定義されます。

```
Name  = strongP2EspProp
        Pfs   = N
        ESP Transforms:
                espTunnelMD5andDES
                espTunnelSHAandDES

Name  = strongP2EspAhProp
        Pfs   = N
        AH Transforms:
                ahTunnelMD5
                ahTunnelSHA
        ESP Transforms:
                espTunnelDES

Name  = veryStrongP2EspProp
        Pfs   = N
        ESP Transforms:
                espTunnelSHAand3DES
                espTunnelMD5and3DES

Name  = veryStrongP2EspAhProp
        Pfs   = N
        AH Transforms:
                ahTunnelSHA
                ahTunnelMD5
        ESP Transforms:
                espTunnel3DES

Name  = veryStrongP2EspPropPFS
        Pfs   = Y     DHGrp= 1
        ESP Transforms:
                espTunnelSHAand3DES
                espTunnelMD5and3DES

Name  = strongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportMD5andDES
                espTransportSHAandDES

Name  = strongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportMD5
                ahTransportSHA
        ESP Transforms:
                espTransportDES

Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = strongP2EspAhPropXport
        Pfs   = N
```

```
        AH Transforms:
                ahTransportMD5
                ahTransportSHA
        ESP Transforms:
                espTransportDES

Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
                espTransport3DES

Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
                espTransport3DES

Name  = veryStrongP2EspPropPFSXport
        Pfs   = Y     DHGrp= 1
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropPFSXport
        Pfs   = Y     DHGrp= 1
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
                espTransport3DES
```

IPSec トランスフォーム

次の IPSec トランスフォーム・オブジェクトが事前定義されます。

```
Transform Name  = ahTransportMD5
        Type =AH    Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =None

Transform Name  = ahTransportSHA
        Type =AH    Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =None

Transform Name  = ahTunnelMD5
        Type =AH    Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =None

Transform Name  = ahTunnelSHA
        Type =AH    Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =None
```

```
Transform Name  = espTunnelMD5andDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =DES

Transform Name  = espTunnelSHAandDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES

Transform Name  = espTunnelMD5and3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =3DES

Transform Name  = espTunnelSHAand3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES

Transform Name  = espTunnelDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =DES

Transform Name  = espTunnel3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =3DES

Transform Name  = espTransportMD5andDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =DES

Transform Name  = espTransportSHAandDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES

Transform Name  = espTransportMD5and3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =3DES

Transform Name  = espTransportSHAand3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES

Transform Name  = espTransportDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =DES

Transform Name  = espTransport3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =3DES
```

ISAKMP アクション

次の ISAKMP アクション・オブジェクトが事前定義されます。

```
ISAKMP Name     = generalPhase1Action
        Mode                    =            Main
        Min Percent of SA Life  =               1
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =              No
        ISAKMP Proposals:
                veryStrongP1PropRSACert
                strongP1PropRSACert
                veryStrongP1PropSharedKey
                strongP1PropSharedKey
```

ISAKMP プロポーザル

次の ISAKMP プロポーザル・オブジェクトが事前定義されます。

```
                        Name = strongP1PropSharedKey
                                AuthMethod = Pre-Shared Key
                                LifeSize   = 1000
                                LifeTime   = 15000
                                DHGroupID  = 1
                                Hash Algo  = MD5
                                Encr Algo  = DES CBC

                        Name = strongP1PropRSACert
                                AuthMethod = Certificate (RSA SIG)
                                LifeSize   = 1000
                                LifeTime   = 15000
                                DHGroupID  = 1
                                Hash Algo  = MD5
                                Encr Algo  = DES CBC

                        Name = veryStrongP1PropSharedKey
                                AuthMethod = Pre-Shared Key
                                LifeSize   = 1000
                                LifeTime   = 15000
                                DHGroupID  = 1
                                Hash Algo  = SHA
                                Encr Algo  = 3DES CB

                        Name = veryStrongP1PropRSACert
                                AuthMethod = Certificate (RSA SIG)
                                LifeSize   = 1000
                                LifeTime   = 15000
                                DHGroupID  = 1
                                Hash Algo  = SHA
                                Encr Algo  = 3DES CB
```

第17章 ポリシー・フィーチャーの構成と監視

この章では、ポリシー機能に備えられている LDAP コマンドとポリシー・コマンドについて説明します。これらのコマンドは、ネットワーク内にあるルーター装置の構成と操作で必要となります。この章には、以下の節があります。

ポリシー構成プロンプトへのアクセス

ポリシー構成コマンドの入力は、以下のようにします。

1. OPCON (*) プロンプトで **talk 6** を入力します。
2. `Config>` プロンプトで **feature policy** を入力します。

`Policy config>` プロンプトが現れます。これで、ポリシー構成コマンドを入力できます。

ポリシー構成コマンド

これらのコマンドを使って、ポリシーに含まれる情報を構成できます。 表39 は、ポリシー構成コマンドの要約です。この節ではこれらのコマンドを詳細に説明します。これらのコマンドは、`Policy config>` プロンプトで入力します。コマンドとオプションをまとめて 1 行に入力するか、コマンドだけを入力して、プロンプトに答えることもできます。コマンドにオプションを付ける代わりに、疑問符 (?) を付けると、コマンド・オプションのリストが表示されます。

表 39. ポリシー構成コマンド

コマンド	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。xxxiページの『ヘルプの入手』 を参照してください。
Add	ポリシーの作成に必要な情報を追加します。
Change	ポリシーの情報を変更します。
Copy	ポリシーの情報をほかのポリシーにコピーします。
Delete	ポリシーの情報を削除します。
Disable	ポリシーを使用不可にします。
Enable	ポリシーを使用可能にします。
List	ポリシーの情報を表示します。
Qconfig	事前定義されたテンプレートに基づいて、ポリシーを追加できるようにします。
refresh-templates	特定のプラットフォームで実行されるコードのバージョンについて、最新のテンプレートをインストールまたは除去できるようにします。これにより、各種のソフトウェア・リリースと PTF レベル間の変更が簡単になり、その変更の決定が単純化されます。

表 39. ポリシー構成コマンド (続き)

コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、ポリシーに情報を追加します。

構文: add
- diffserv-action
- interface-pair
- ipsec-action
- ipsec-manual-tunn
- ipsec-proposal
- ipsec-transform
- isakmp-action
- isakmp-proposal
- policy
- profile
- rsvp-action
- user
- validity-period

diffserv-action

DiffServ アクションの選択情報を入力するようにプロンプトが出ます。詳細については、365ページの『第20章 ディファレンシエーテッド・サービス・フィーチャーの使用』と 375ページの『第21章 ディファレンシエーテッド・サービス・フィーチャーの構成および監視』を参照してください。

name ポリシーの DiffServ アクションに対する固有の名前

permission level

DiffServ アクションに一致するパケットをルーターが転送するかどうかを指定します。

1 許可する

2 拒否する

デフォルト値: 2

queue number

DiffServ アクションに一致する発信パケットを置く待ち行列

1 プレミアム (EF)

2 保証 (AF)/ベストエフォート

デフォルト値: 2

bwshare type

共用帯域幅の割り当てタイプ

1 絶対値 (kbps)

2 パーセント値 (全出力帯域幅に対する割合)

デフォルト値: 2

bwshare
サービスに割り当てられた帯域幅 (kbps または全出力帯域幅に対する割合)。

保証転送 (Assured Forwarding)

Assured forwarding class
この DiffServ アクションに一致する発信パケットに、保証転送クラスを指定します。

1 AF1 クラス DS バイト

2 AF2 クラス DS バイト

3 AF3 クラス DS バイト

4 AF4 クラス DS バイト

5 新規クラス

Assured forwarding policing type
この DiffServ アクションに一致する発信パケットに、AF ポリシングのタイプを指定します。

1 Single-rate, color-blind TCM

2 Single-rate, color-aware TCM

3 Two-rate, color-blind TCM

4 Two-rate, color-aware TCM

5 なし

Single-Rate TCM Parameters

Committed information rate (CIR)
認定情報速度を指定します。

Committed burst size (CBS)
認定バースト・サイズを指定します。

Excess burst size (EBS)
過剰バースト・サイズを指定します。

注:

1. 毎秒の IP パケット・バイト数単位で CIR を指定します。これには、IP ヘッダーが含まれますが、リンク固有のヘッダーは含まれません。
2. CBS と EBS をバイト数で指定します。これらの値は、その内の 1 つ以上がゼロより大きくなるように構成する必要があります。CBS または EBS の値がゼロより大きい場合、ストリーム内の可能な限り最大の IP パケットのサイズより大きいか、それに等しくなるようにお勧めします。

Two-Rate TCM Parameters

Committed information rate (CIR)
認定情報速度を指定します。

Committed burst size (CBS)
認定バースト・サイズを指定します。

Peak information rate (PIR)
ピーク情報速度を指定します。

Peak burst size (PBS)
ピーク・バースト・サイズを指定します。

注:

1. 毎秒の IP パケット・バイト数単位で CIR および PIR を指定します。これには、IP ヘッダーが含まれますが、リンク固有のヘッダーは含まれません。 PIR 値は、CIR に等しいか、それより大きくなければなりません。
2. CBS と PBS をバイト数で指定します。どちらも、ゼロより大きく、かつストリーム内で可能な限り最大の IP パケットのサイズより大きいか、それに等しい値でなければなりません。

早期転送 (Expedited Forwarding)

transmitted ds-byte mask
早期転送の場合に送信された ds バイトに使用するマスク。この値は、パケットを送信したときに、パケットの DS バイトのどのビットを変更するかを決めます。このバイトに 0 のビットがあると、そのビットは変更してはいけないことを示します。

デフォルト値: 00 (ビット変更禁止)

transmitted ds-byte modify value
この装置によって転送されるパケットに適用される、早期転送の場合の IP DS (TOS) バイトのマーク付け。マークに 0 があると、そのビットを変更してはいけないことを示します。1 は、そのビットがマーク・バイトのビット値でマークされることを示します。次のように操作します。newTOSByte = (Mask^ & receivedTOSByte) | (Mask&Mark)。^ ^ ∧ は、ビット系の補数です (Mask:Mark)。

例:

```
11111101:00000001
```

この例では、受信した 0x07 の値は、0x03 の値で送信されます。

デフォルト値: X'00' (ビット変更禁止)

EF policing type
早期転送のポリシング構成タイプを指定します。

1 デフォルト構成

token rate および token bucket size パラメーターは、帯域幅パラメーター構成から計算されます。

2 カスタム構成

Token Rate:
トークン補充速度

Token Bucket Size:
トークンのバケット・サイズ

注:

1. 毎秒の IP パケット・バイト数単位でトークン速度を指定します。これには、IP ヘッダーが含まれますが、リンク固有のヘッダーは含まれません。
2. トークンのバケット・サイズをバイト数で指定します。この値は、ゼロより大きく、かつストリーム内の最大 IP パケットのサイズより大きいか、それに等しくなければなりません。

interface-pair
インターフェース・ペアは、特定のインターフェースやインターフェースの集合体をプロファイルに関連付けます。デフォルトでは、プロファイル・オブジェクトは、ポリシーが任意のインターフェースに適用されることを制限しません。そうした制約が必要なときは、インターフェース・ペアを追加します。インターフェース・ペアは、トラフィックが発着するインターフェースの IP アドレスを指定します。

次の例は、同じ名前のインターフェース・ペアが 2 つあり、このトラフィックは、任意のインターフェースに着信して公共のインターフェースから発信したり、その逆になったりします。

```
1) Group Name: inOutPublic
        In:Out=255.255.255.255 : 1.1.1.1
        In:Out=1.1.1.1 : 255.255.255.255
```

Name インターフェース・ペアの名前

Ingress interface
入力インターフェースの IPv4 アドレス

デフォルト値: 255.255.255.255 (any)

Egress interface
出力インターフェースの IPv4 アドレス

デフォルト値: 255.255.255.255 (any)

IPSec-action
フェーズ 2 のトンネルの設定情報を入力するようにプロンプトが出ます。

Name IPSec アクションの名前

Action type
パケットがこのアクションを含むポリシー・プロファイルに一致すると、パケットにはこのアクションが適用されます。

1 ブロックする (ブロック接続)

2 許可する (このアクションに一致するパケットを許可する)。IPSec のプロポーザルがない場合はパケットを渡す。IPSec プロポーザルがあるときは、パケットに IPSec セキュリティー処理を行う。

デフォルト値: 2

次のオプションは、「アクションのタイプにしたがって渡す」を指定したときに使用できます。

Traffic flow type
トラフィック・フローのタイプです (トンネルを保護、またはクリア)。

1 消去

2 保護トンネル

デフォルト値: 2

次のオプションは、トラフィック・フローを「保護する」に指定したときに利用できます。

Tunnel start point
トンネルの開始点の IPv4 アドレス

Tunnel end point
トンネルの終了点の IPv4 アドレス。(リモート・アクセスは 0.0.0.0)

デフォルト値: 0.0.0.0

Tunnel-in-tunnel
このトンネルで保護したトラフィックをこの装置に構成した別のポリシーでさらに保護するかどうかを指定します。

有効なオプション: Yes または No

デフォルト値: No

Percentage of SA lifesize/lifetime to accept
SA lifesize/lifetime の最小値 (パーセント値)。この数値以下の SA lifesize/lifetime は受け入れません。

デフォルト値: 75

SA refresh threshold
SA を自動的にリフレッシュする SA の lifetime および lifesize のパーセント値

デフォルト値: 85

DF-Bit-Setting
オリジナルのパケットから Don't Fragment ビットをコピーするかどうかを決め、トンネル・モードで実行するときに IPSec パケットの外側ヘッダーに設定するか消去するかを決めます。

1 コピー

2 設定

3 消去

デフォルト値: 1

Replay-Prevention
受け取った IPSec パケットについて、IPSec が再生防止を実行するかどうかを指定します。このモードでは、連続番号が有効で、これを 1 回以上は受け付けないことを IPSec が保証します。

1 使用可能

2 使用不可

デフォルト値: 2

Negotiate SA Automatically
システムを初期化したときに、フェーズ 2 の SA を自動的にネゴシエーションするかどうかを指定します。

Yes または No

デフォルト値: No

IPSec proposal
フェーズ 2 で送信またはチェックする IPSec プロポーザルの名前 (最大 5 つのプロポーザルを指定できます)。指定する順序によって、優先順位が決まります。はじめに指定したほうが優先順位が高くなります。

IPSec-manual-tunn
フェーズ 2 のトンネルを手動設定する情報を入力するようにプロンプトが出ます。

Tunnel name
IPSec 手動トンネルの名前

Tunnel lifetime
トンネルの存続時間 (分数)

デフォルト値: 46080

Encapsulation mode
使用するカプセル化モード

tunn トンネル・モード

trans 転送モード

デフォルト値: tunn

Policy 使用するトンネル・ポリシーのタイプ

AH 認証ヘッダー

ESP カプセル化セキュリティーのペイロード

AH-ESP
アウトバウンドのパケットについて、認証の前に暗号化を実行することを指定します。

ESP-AH
アウトバウンドのパケットについて、暗号化の前に認証を実行することを指定します。

デフォルト値: AH-ESP

Local IP address
発信元の IPv4 アドレス

デフォルト値: 11.0.0.5

Local encryption SPI
発信元のセキュリティー・パラメーターのインデックス値

デフォルト値: 256

Local encryption algorithm
発信元の暗号化アルゴリズム

Null 暗号化しない。

CDMF 商業用のデータ・マスキング機能

DES-CBC
データ暗号化規格と暗号化ブロック連鎖

3DES データ暗号化規格

デフォルト値: DES-CBC

Local encryption key
16 文字のキー

Padding
ローカル暗号への埋め込みの追加

デフォルト値: 0

Local ESP authentication
ローカルの認証を使用するかどうかを指定します。

Yes または No

デフォルト値: Yes

Remote IP address
宛先 IPv4 アドレス

デフォルト値: 0.0.0.0

Remote encryption SPI
宛先セキュリティー・パラメーターのインデックス値

デフォルト値: 256

Remote encryption algorithm
宛先の暗号化アルゴリズム

Null 暗号化しない。

CDMF 商業用のデータ・マスキング機能

DES-CBC
データ暗号化規格と暗号化ブロック連鎖

3DES データ暗号化規格

デフォルト値: DES-CBC

Remote encryption key
16 文字のキー

Verify remote encryption padding.
リモート暗号の埋め込みを検証するかどうかを指定します。

Yes または No

デフォルト値: No

Remote ESP authentication
リモートの ESP 認証を使用するかどうかを指定します。

Yes または No

デフォルト値: Yes

DF bit
Don't Fragment ビットの処理方法を指定します。

Copy DF ビットをコピーします。

Set DF ビットをオンにします。

Clear DF ビットをオフにします。

デフォルト値: COPY

Enable tunnel
トンネルが作られたときに、トンネルを使用可能にするかどうかを指定します。

Yes または No

デフォルト値: Yes

IPSec-proposal
IPSec プロポーザルの作成情報を入力するようにプロンプトが出ます。

IPSec proposal name
IPSec プロポーザルの名前

Perfect forward secrecy
以前に妥協したキーを使って現在のキーを決定することを禁止するために、IKE を使用するかどうかを指定します。

Yes または No

デフォルト値: No

Diffie Hellman のグループ ID
Diffie Hellman グループのタイプ

1 Diffie Hellman グループ 1

2 Diffie Hellman グループ 2

デフォルト値: 1

AH transform
このプロポーザルに対する AH トランスフォームの名前 (最大 5

つのトランスフォームを指定できます)。指定する順序によって、優先順位が決まります。はじめに指定したほうが優先順位が高くなります。

ESP transform
このプロポーザルに対する ESP トランスフォームの名前 (最大 5 つのプロポーザルを指定できます)。指定する順序によって、優先順位が決まります。はじめに指定したほうが優先順位が高くなります。

IPSec-transform
IPSec トランスフォームに関する情報を入力するようにプロンプトが出ます。

IPSec transform name
IPSec トランスフォームの名前

Protocol ID
使用するセキュリティー・プロトコル

1 IPSec-AH

2 IPSec-ESP

デフォルト値: 1

AH Authentication Algorithm
使用する AH 確認アルゴリズム

1 HMAC-MD5

2 HMAC-SHA

デフォルト値: 1

Encapsulation mode
使用するカプセル化モード

1 Tunnel

2 転送

デフォルト値: 1

ESP Authentication Algorithm
使用する ESP 確認アルゴリズム

0 なし

1 HMAC-MD5

2 HMAC-SHA

デフォルト値: 2

ESP cipher algorithm
使用する ESP 暗号アルゴリズム

1 ESP DES

2 ESP 3DES

3 ESP CDMF

4 ESP なし (暗号化なし)

デフォルト値: 1

SA lifesize
このプロポーザルに対する SA のライフ・サイズ (kb)

デフォルト値: 50000

SA lifetime
このプロポーザルに対する SA のライフタイム (秒)

デフォルト値: 3600

ISAKMP-Action
使用する ISAKMP アクションに関する情報を入力するプロンプトが出されます。

Name ISAKMP アクションの名前

Exchange mode
フェーズ 1 ネゴシエーションの交換モードのタイプ

1 メイン

2 アグレッシブ

デフォルト値: 1

Percentage of Minimum SA lifesize/lifetime
SA lifesize/lifetime の最小値 (パーセント値)。この数値以下の SA lifesize/lifetime は受け入れません。

デフォルト値: 75

ISAKMP connection lifesize
フェーズ 1 接続のライフ・サイズ (kb)。フェーズ 1 接続の期限が終わると、次にフェーズ 2 SA がリフレッシュするときは、フェーズ 2 が開始する前に、フェーズ 1 による完全なネゴシエーションが必要になります。

デフォルト値: 5000

ISAKMP connection lifetime
フェーズ 1 接続のライフタイム (秒)。フェーズ 1 接続の期限が終わると、次にフェーズ 2 がリフレッシュするときは、フェーズ 1 が完全に開始します。

デフォルト値: 5000

Negotiate SA automatically
システムを初期化したときに、SA を自動的にネゴシエーションするかどうかを指定します。

Yes または No

デフォルト値: No

ISAKMP proposal
フェーズ 2 のクィック・モードのときに、送信およびチェックする ISAKMP プロポーザル (最大 5 つのプロポーザルを指定できます)。指定する順序によって、優先順位が決まります。はじめに指定したほうが優先順位が高くなります。

ISAKMP-Proposal
ISAKMP ネゴシエーションで使用する ISAKMP プロポーザルに関する情報を入力するようにプロンプトが出ます。

ISAKMP proposal name
ISAKMP プロポーザルの名前

Authentication method
ISAKMP フェーズのネゴシエーションで使用する認証のタイプ

1 プリシェアード・キー

2 RSA SIG (証明モード)

デフォルト値: 1

Hash algorithm
フェーズ 1 のネゴシエーションで使用するハッシュ・アルゴリズムのタイプ

1 MD5

2 SHA

デフォルト値: 1

Cipher algorithm
フェーズ 1 のネゴシエーションで使用するハッシュ・アルゴリズムのタイプ

1 DES

2 3DES

デフォルト値: 1

Diffie Hellman のグループ ID
フェーズ 1 のネゴシエーションで使用する Diffie Hellman グループのタイプ

1 Diffie Hellman グループ 1

2 Diffie Hellman グループ 2

デフォルト値: 1

SA lifesize
このプロポーザルに対する SA のライフ・サイズ (kb)

デフォルト値: 50000

SA lifetime
このプロポーザルに対する SA のライフタイム (秒)

デフォルト値: 5000

Policy ポリシーの構成情報を入力するようにプロンプトが出ます。プロファイル名 (必須)、RSVP 名 (オプション)、DiffServ 名 (オプション)、IPSec 名 (オプション)、ISAKMP 名 (オプション)、有効期間プロファイル (オプション) などがあります。ポリシーを有効にするには、DiffServ、IPSec、ISAKMP、または RSVP のいずれかを指定します。

デフォルト値: 常に有効

Name ポリシー構成の名前

Priority
他のポリシーに対するこのポリシーの優先順位 (数字が大きいほど、優先順位が高い)。1 つのパケットに複数のポリシーがあるときに、対立を避けるときにこれを使います。

デフォルト値: 5

Profile
このポリシーで使う構成済みのデータ・トラフィック・プロファイルの名前。

Validity period
このポリシーで使う構成済みの有効期間の名前

IPSec action
このポリシーが IPSec アクションを実行する場合は、このポリシーに使う構成済みの IPSec アクションの名前。保護 IPSec アクションを指定するときは、 ISAKMP アクションも指定します。

ISAKMP action
このポリシーに使用する構成済みの ISAKMP アクションの名前。ISAKMP アクションを指定するときは、IPSec アクションも指定します。

Diffserv action
このポリシーに DiffServ アクションをマッピングする場合は、構成済みの DiffServ アクションの名前

RSVP action
このポリシーで実行する RSVP アクションの名前

Profile
アクションを実行するポリシーのプロファイルについて、1 組のセレクターを定義するための情報 (条件) を入力するようにプロンプトが出ます。

name ポリシー・プロファイルの名前

ipv4-src-address-format
IPv4 発信元アドレスのフォーマット (範囲、ネットマスク、単一アドレス)

ipv4-src-address
IPv4 発信元アドレス (アドレス形式が *range* のときはロー・アドレス)

デフォルト値: 0.0.0.0

ipv4-src-mask
IPv4 発信元マスク (アドレス形式が *range* のときはハイ・アドレス)

デフォルト値: 255.0.0.0

ipv4-dest-address-format
IPv4 宛先アドレスのフォーマット (範囲、ネットマスク、単一アドレス)

ipv4-dest-address
IPv4 宛先アドレス (アドレス形式が *range* のときはロー・アドレス)

デフォルト値: 0.0.0.0

ipv4-dest-mask
IPv4 宛先アドレス (アドレス形式が *range* のときはハイ・アドレス)

デフォルト値: 255.0.0.0

protocol-id
フィルター処理するプロトコル ID

1 TCP

2 UDP

3 すべてのプロトコル

4 範囲を指定する

デフォルト値: 3

src-port-start
発信元ポート番号範囲の最初のポート番号

デフォルト値: 0

src-port-end
発信元ポート番号範囲の最後のポート番号

デフォルト値: 65535

dest-port-start
宛先ポート番号範囲の最初のポート番号

デフォルト値: 0

dest-port-end
宛先ポート番号範囲の最後のポート番号

デフォルト値: 65535

src-id-type
リモートに送られる発信元 ID のタイプ。この値は、ISAKMP フェーズ 1 ネゴシエーションに必要な ISAKMP 情報を含むポリシーを確認するのに使用します。 ISAKMP パケットの識別ペイロードにある情報と比較します。この情報は、リモート・ピアが IP アドレス以外の値を使って装置を識別するときに必要になります。

1 ローカルのトンネル終了点

2 ホストが完全限定のドメイン名

3 ユーザーが完全限定のドメイン名

4 キー ID

any-user-access
プロファイルの定義に一致するユーザーは誰でもアクセスが許可されます。 No を指定すると、このプロファイルに対するリモート・ユーザー・グループの名前を入力するようにプロンプトが出ます。この属性は、ある特定のポリシーにリモート・アクセス・ピアがアクセスすることを制限するときに使用します。

Yes または No

デフォルト値: Yes

Received DS byte mask
着信パケットの DS (TOS) バイトに使用する 8 ビットのマスク

デフォルト値: 0

Received DS byte match
着信 DS (TOS) バイトの ANDing 結果と受信 DS バイト・マスク値を比較するための 8 ビットのパターン

デフォルト値: 0

Interface pairs
このポリシーが特定のインターフェースへのトラフィック・フローを制限するときは、これがインターフェース・ペア・グループの名前となります。

RSVP-Action
使用する RSVP アクションに関する情報を入力するようにプロンプトが出ます。

Name RSVP アクションの名前

Permission
このアクションに一致する RSVP セッションの許可レベルを指定します。

1 許可する

2 拒否する

デフォルト値: 2

Max token rate
各フローに対して RSVP が割り当てる最大帯域幅 (kbps)

デフォルト値: 100

Max duration
フローが存続できる最長時間 (秒) (0 は永遠を意味する)

デフォルト値: 600

RSVP-to-DS

このアクションに一致する RSVP のフローを構成済みの DiffServ アクションにマップするかどうかを指定します。RSVP は、DiffServ アクションの情報を利用して、DiffServ が使用可能になっている次の上流の装置について、TOS バイトをマークします。これは、RSVP が使用可能なネットワークから DiffServ が使用可能なネットワークにパケットが送信されるようなネットワークで使用します。

Yes または No

デフォルト値: No

User リモート IKE ピアのユーザー・プロファイル定義についての情報を入力するように求めるプロンプトが出されます。この情報には、ピアがフェーズ 1 ネゴシエーション中に自らの身元を明らかにする方法、このピアに使用する認証方式、および認証機構がプリシェアード・キーである場合は、使用するキー値が含まれます。プリシェアード・キーを使用する場合、そのプリシェアード・キーを ID タイプと名前に対応させるために、ユーザーを定義する**必要があります**。このコマンドは、フェーズ 1 ネゴシエーションで特定ユーザーに使用されるキーを設定します。このキーは、起動側にはメッセージ 1 と 5 で使用され、応答側にはメッセージ 2 と 6 で使用されます。

Identification

ユーザーの識別。メイン・モード認証の場合、ユーザー識別タイプは、IP アドレスである**必要があります**。アグレッシブ・モード認証の場合、識別タイプは、その他のタイプのいずれかでなければなりません。この理由は、メイン・モードでは、メッセージ 5 と 6 まで ID が交換されず、これはプリシェアード・キーには遅過ぎるので、ルックアップ機構だけが、IKE ピアの IP アドレスを使用して行なわれるからです。アグレッシブ・モードでは、ID はメッセージ 1 と 2 で交換されるので、プリシェアード・キーのルックアップは、ID タイプと対応する値によって行うことができます。

1 IP アドレス

2 完全修飾ドメイン名

3 ユーザー完全修飾ドメイン名

4 キー ID (任意のストリング)

デフォルト値: 1

Group このユーザーが入るグループの名前

省略時値: なし

Authentication

ピアで使用する認証方式

1 プリシェアード・キー

1 ASCII フォーマットのキー

有効値: 2 ～ 128 文字の偶数

2 16 進形式のキー

有効値: 2 ～ 256 桁の 16 進数字の偶数

2 公開認証

デフォルト値: 1

VALIDITY-PERIOD

ポリシーが有効な期間、そしてポリシー・プロファイルを作成する期間について、情報を入力するようにプロンプトが出ます。

Name 有効期間のプロファイルの名前

yyyymmddhhmmss:yyyymmddhhmmss

この有効期間プロファイルを含むポリシーが有効な期間

例:

```
19980101000000:19981231000000
```

Months

この有効期間プロファイルを含むポリシーが有効な月。月を自由な順序で並べることができます。月の名称は 3 文字で表し (jan、dec など)、月と月の間にはスペースを空けます。一年のすべての月を指定するときは `all` を指定します。

Days この有効期間プロファイルを含むポリシーが有効な曜日。曜日を自由な順序で並べられます。曜日の名称は 3 文字で表し (mon、fri など)、曜日と曜日の間にはスペースを空けます。一週間のすべての曜日を指定するときは `all` を入力します。

Starting time

有効な期間プロファイルを含むポリシーが有効な時刻。時刻は、hh:mm:ss の形式で指定するか、一日中有効にするときは * を指定します。

デフォルト値: *

Ending time

有効な期間プロファイルを含むポリシーが無効となる時刻。時刻は、hh:mm:ss の形式で指定します。

デフォルト値: なし

Change

change コマンドは、ポリシー・オブジェクトの情報を変更するときに使用します。使用可能なオブジェクトについては、**add** コマンドの説明を参照してください。

Copy

copy コマンドは、あるポリシー・オブジェクトの情報を他のポリシー・オブジェクトにコピーします。使用可能なオブジェクトについては、**add** コマンドの説明を参照してください。 (インターフェース・ペア、手動トンネル、およびユーザー・オプションで **copy** コマンドは使えません。)

Delete

delete コマンドは、ポリシー・オブジェクトの情報を削除します。使用可能なオブジェクトについては、**add** コマンドの説明を参照してください。

Disable

disable コマンドは、ポリシーの構成を使用不可にします。

構文: disable policy

Policy 使用不可にするポリシーの構成名を入力するようにプロンプトが出ます。

Enable

enable コマンドは、ポリシーの構成を使用可能にします。

構文: enable policy

Policy 使用可能にするポリシーの構成名を入力するプロンプトがでます。

List

list コマンドは、ポリシーの構成情報の一部またはすべてを表示します。

構文: list all
default-policy
ldap
refresh

All ポリシーの構成情報をすべて表示します。

Default-policy
デフォルト・ポリシーの名前を表示します。

LDAP 定義された LDAP 構成の名前を表示します。

Refresh
ポリシーのリフレッシュ・ステータス (使用可能、または使用不可)、およびリフレッシュ間隔を表示します。

Qconfig

qconfig コマンドは、ネットワーク装置用のセキュリティー・ポリシーをすばやく作成するのに使用します。短いリストから構成シナリオを選択した後、このコマンドは、ユーザーの選択に基づいて、短い一連の簡単な質問を表示します。その後、シナリオに関連した事前定義テンプレート (互換性のあるポリシー・オプションの完全なセット) を使用して、ポリシー全体を作成します。これにより、ポリシーの詳細を指定する必要がなくなり、ポリシーの構成に必要な時間と間違いを行う可能性が減少します。

このコマンドは、カスタム・シナリオを除くすべてのシナリオに、セキュリティー・レベルを指定するように求めるプロンプトを出します。

構文: qconfig *policy-name*
scenario

policy-name

ポリシーに割り当てられる名前 (最大 29 文字) を指定します。

デフォルト値: システムによって生成された固有な名前

scenario

ポリシーを作成するシナリオを指定します。

省略時値: なし

1 支社のシナリオ

これを選択すると、ローカル・サブネットを保護する 2 つのセキュリティー・ゲートウェイ間の確実な接続用のポリシー・オプションを指定できます。

以下のオプションがあります。

ローカル IP サブネット

ローカル IP トンネル終了点

リモート IP サブネット

リモート IP IP トンネル終了点

ポートとプロトコル

セキュリティー・レベル

1: 強力なセキュリティー。セキュリティー、パフォーマンス、および柔軟性が必要な場合にこのオプションを選択します。SHA と MD5 確認アルゴリズムおよび DES と 3DES 暗号化アルゴリズムの組み合わせを含む一連のプロポーザル (PFS なし) をネゴシエーションします。パフォーマンスを損なわないようにするために、強力なプロポーザルが最初にネゴシエーションされ、その後でさらに強いプロポーザルがネゴシエーションされます。

2: 非常に強力なセキュリティー。最高レベルのセキュリティーが必要な場合に、このオプションを選択します。 SHA と MD5 確認アルゴリズムおよび 3DES 暗号化アルゴリズムの組み合わせを含む一連の小規模なプロポーザル (PFS、Grp 1 あり) をネゴシエートします。

認証方式

1: プリシェアード・キー - ASCII キー

2: 証明 (RSA 署名) - ローカル ID

DiffServe アクション

0: Best Effort (No DiffServ)

1: EF

2: AF11

3: AF21

4: AF31

5: AF41

ローカル側で構成されたその他の任意の DiffServ アクションも、このリストに表示されます。

有効期間

1. 1: allTheTime
2. 2: allTheTimeMonThruFri
3. 3: 9to5MonThruFri
4. 4: 5to9MonThruFri

ローカル側で構成されたその他の任意の有効期間も、このリストに表示されます。

ポリシーの優先順位

2 リモート・アクセス・ユーザーのシナリオ (IPSec および L2TP)

これを選択すると、セキュリティー・ゲートウェイとリモート・アクセス・ユーザー間の確実な接続用のポリシー・オプションを指定することができます。このシナリオでは、リモート・アクセス・クライアントが、トランスポート・モードで IPSec の上で L2TP を実行する機能を備えていることを前提としています。

L2TP は、リモート・アクセス・クライアントの公衆 IP アドレスとセキュリティー・ゲートウェイの公衆 IP アドレスとの間にポイント・ポイント接続を設定します。 UDP は、トランスポート・レイヤー接続を提供し、発信元ポートと宛先ポートは 1701 です。 L2TP が、セキュリティー・ゲートウェイ機能を実行するルーター上で fixed-udp-source-port 用に構成されることが重要です。 IPSec は、これらのポートとプロトコル上の L2TP 接続に対する保護を提供します。

構成シナリオが完了した後、プリシェアード・キーを使用して認証される任意の人物に対して、ポリシー・フィーチャーにユーザーを追加する必要があります。証明認証の場合、ルーター上で PKI パラメーターを構成し、適切な証明がロードされることを確認する必要があります。

以下のオプションがあります。

保護インターフェースの IP アドレス

通常、これは、ローカル IP トンネル終了点と同じ値です。パケットが保護された状態で送信され、保護された状態で到着するインターフェースの IP アドレスを表します。

セキュリティー・レベル

1: 強力なセキュリティー

2: 非常に強力なセキュリティー

DiffServe アクション

0: Best Effort (No DiffServ)

1: EF

2: AF11

3: AF21

4: AF31

5: AF41

ローカル側で構成されたその他の任意の DiffServ アクションも、このリストに表示されます。

有効期間

1. 1: allTheTime
2. 2: allTheTimeMonThruFri
3. 3: 9to5MonThruFri
4. 4: 5to9MonThruFri

ローカル側で構成されたその他の任意の有効期間も、このリストに表示されます。

ポリシーの優先順位

3 非トラステッド・インターフェース上で一致しないトラフィックの除去。このシナリオは、装置がファイアウォールの役目を果たす構成に必要です。多くのネットワーク構成では、ファイアウォールが、セキュリティー・ゲートウェイの前にあり、除去規則は必要ありません。除去規則が必要である場合は、このシナリオを選択してください。

以下のオプションがあります。

非トラステッド・インターフェースの IP アドレス

これは、不必要なパケットが除去されるインターフェースの IP アドレスです。通常、公衆ネットワークまたは非トラステッド・ネットワークとの接続の IP アドレスです。

4 **カスタム・シナリオ**

これを選択すると、**qconfig** を使用してポリシーを定義する際に、最大の柔軟性が得られます。カプセル化モード (Tunnel または Transport) を選択するように求めるプロンプトが出されます。トンネル・モードを選択すると、支社のシナリオと同じ質問が表示されます。トランスポート・モードを選択する場合、支社のシナリオの質問が表示されますが、ローカル・サブネットとリモート・サブネットを扱う質問を除きます。これらの質問は適用されません。

LDAP ポリシー・サーバーの構成コマンド

LDAP ポリシー構成コマンドを使うと、LDAP サーバーのオプションを指定して、ポリシー情報を取り出すことができます。表40 は、ポリシー構成コマンドの要約です。この節ではこれらのコマンドを詳細に説明します。これらのコマンドは、`Policy config>` プロンプトで入力します。コマンドとオプションをまとめて 1 行に入力するか、コマンドだけを入力して、プロンプトに答えることもできます。コマンドにオプションを付ける代わりに、疑問符 (?) を付けると、コマンド・オプションのリストが表示されます。

表 40. LDAP 構成コマンド

コマンド	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。xxxiページの『ヘルプの入手』 を参照してください。
Disable ldap	LDAP 構成オプションを使用不可にします。

LDAP 構成コマンド (Talk 6)

表 40. LDAP 構成コマンド (続き)

コマンド	機能
Enable ldap	LDAP 構成オプションを使用可能にします。
Set ldap	LDAP 構成オプションを指定します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Disable LDAP

disable ldap コマンドは、ディレクトリー内の LDAP ポリシー検索機能を使用不可にするか、キャッシュに入ったポリシーが LDAP サーバーから持続記憶域に読み込まれないようにするのに使用します。

構文: disable ldap cached-search

policy-search

cached-search

LDAP が、キャッシュに入ったポリシーをサーバーから持続記憶域に読み取らないようにします。

policy-search

LDAP のディレクトリー内ポリシー検索機能を使用不可にします。

Enable LDAP

enable ldap コマンドは、ディレクトリー内の LDAP ポリシー検索機能を使用可能にするか、キャッシュに入ったポリシーが LDAP サーバーから持続記憶域に読み込まれるようにするのに使用します。

構文: enable ldap cached-search

policy-search

cached-search

LDAP がディレクトリー内のポリシー検索機能を実行できるようにするか、キャッシュに入ったポリシーが LDAP サーバーから持続記憶域に読み込まれるようにします。

ポリシー検索オプションが使用不可であるときに、このオプションを使用可能にすると、ポリシー検索エンジンは、ローカル・キャッシュからのポリシーだけを読み取ります。キャッシュ検索オプションとポリシー検索オプションの両方を使用可能にすると、ポリシー検索エンジンは、まず LDAP サーバーから読み取ろうとします。これが失敗すると、キャッシュに入った LDAP ポリシー・オブジェクトを読み取ります。 LDAP ポリシーをキャッシュに入れる方法については、301ページの『ポリシー監視コマンド』の **cache-ldap-polcys** コマンドを参照してください。

policy-search

ディレクトリー内の LDAP ポリシー検索機能を使用可能にします。

Set Default-Policy

set default-policy コマンドは、ポリシー・データベースのリフレッシュ中に使用するポリシー・オプションを指定します。このコマンドは、エラー処理のオプションと LDAP ポリシー・サーバーへのアクセスに必要なデフォルトのセキュリティーを設定します。

構文: set default-policy

default-error-handling

default-security

default-error-handling

ポリシー・データベースのリフレッシュ中に使用するエラー処理のオプションを指定します。

注: デフォルトのエラー処理設定では、エラーが起きたときの装置の対応を決め、ポリシー・データベースを再度作成します。エラーが起きたときの装置の対応方法について、オプションを選択できます。以下のオプションがあります。

1. ポリシー・データベースをデフォルトのセキュリティーにリセットする。
2. LDAP から読み取った規則を洗い流し、ローカル規則とデフォルトのセキュリティーをロードする。

これらの設定値は、ポリシー・データベースを組み立てるようなエラーがあったときにだけ有効となります。どちらのオプションでも、エラーが起きたときは、除去するか渡すかのデフォルト・セキュリティーは継承します。 2 つ目のオプションを選択すると、トラフィックがローカルに定義されたポリシーに一致しない限り、トラフィックはすべて除去されるか、あるいは渡されます。ポリシー・データベースの組み立てが成功すると、このオプションは使用されません。

default-security

ポリシー・データベースのリフレッシュ中に使用するセキュリティー・オプションを指定します。

注: ポリシー・データベースの組み立てが成功すると、デフォルトの対応は「渡す」に定義されます。つまり、パケットがどのポリシー規則にも一致しないときは、そのまま渡されます。規則に一致しないパケットをすべて除去したいとき、あるいは特定のインターフェースに対してそうしたいときは、そのようにポリシーに定義します。

1 すべての IP トラフィックを受け入れて転送する。

2 LDAP トラフィックは許可するが、その他のすべての IP トラフィックは除去する。

このオプションを選択すると、LDAP トラフィックを送受信する装置のローカル IP アドレスを入力するようにプロンプトが出ます。

3 保護 LDAP トラフィックは許可するが、その他のすべての IP トラフィックは除去する。

このオプションを選択すると、次の情報を入力するようにプロンプトが出ます。

DHGroupId
ISAKMP フェーズ 1 ネゴシエーションのときに使用する Diffie-Hellman グループ ID

1 DH グループ 1

2 DH グループ 2

Phase1-Hash-Algorithm
フェーズ 1 のネゴシエーションで使用するハッシュ・アルゴリズム。ハッシュ・アルゴリズムは、フェーズ 1 メッセージの認証を行います。

1 MD5

2 SHA

Phase1-Cipher-Algorithm
フェーズ 1 のネゴシエーションで使用する暗号アルゴリズム。暗号アルゴリズムは、フェーズ 1 ネゴシエーションで暗号化を保護します。

1 DES

2 3DES

Phase1-Authentication-Method
リモート・ピアで使用する認証方式。リモート・ピアがネゴシエーションの相手として正しい装置かどうかを ISAKMP が判断する方法を指定します。

1 プリシェアード・キー

2 証明 (RSA SIG)

Pre-Shared-Key-Value
プリシェアード・キー・フェーズ 1 の認証方式を指定すると、ASCII でキーの値を入力するようにプロンプトが出ます。

Phase2-ESP-Authentication-Algorithm
ESP は、デフォルトのセキュリティーで許されている唯一の IPSec プロトコルです。 フェーズ 2 ISAKMP ネゴシエーションで使用する認証アルゴリズムを入力するようにプロンプトが出ます。

0 なし

1 HMAC-MD5

2 HMAC-SHA

Phase2-ESP-Cipher-Algorithm
ESP は、デフォルトのセキュリティーで許されている唯一の IPSec プロトコルです。フェーズ 2 ISAKMP ネゴシエーションで使用する暗号化アルゴリズムを入力するようにプロンプトが出ます。

1 ESP DES

2 ESP 3DES

3 ESP CDMF

4 ESP NULL

Primary-Tunnel-Start
装置と 1 次 LDAP サーバーを保護するセキュリティー・ゲートウェイの間での IKE と IPSec のトラフィックのために使用される装置の IP アドレス

Primary-Tunnel-End
IKE と IPSec のトラフィックに使用される 1 次 LDAP サーバーを保護するリモートのセキュリティー・ゲートウェイ上の IP アドレス

Secondary-Tunnel-Start
装置と 2 次 LDAP サーバーを保護するセキュリティー・ゲートウェイの間の IKE と IPSec トラフィックに使用される装置の IP アドレス

Secondary-Tunnel-End
IKE と IPSec トラフィックに使用される 2 次 LDAP サーバーを保護するリモートのセキュリティー・ゲートウェイ上の IP アドレス

Set LDAP

set ldap コマンドは、LDAP の操作パラメーターを構成するときに使用します。

構文: set ldap
- anonymous-bind
  - yes
  - no
- bind-name <*name*>
- bind-pw <*pw*>
- policy-base <*string*>
- primary <*ip-address*>
- secondary <*ip-address*>
- version <*value*>

anonymous-bind [Yes or No]
匿名で LDAP ディレクトリーにバインドするか、自分が指定したバインド名称とバインド・パスワードにバインドするかを指定します。

デフォルト値: Yes

bind-name <*name*>
ディレクトリーの検索を実行する前に、LDAP サーバーへのバインドについて、必要情報を入力するようにプロンプトが出ます。*name* パラメーター

は、ルーターが自分自身を識別するために使用する固有の名称を指定します。このパラメーターを入力しないと、バインドが匿名要求として発行されます。

bind-pw <*pw*>
ディレクトリーの検索を実行する前に、LDAP サーバーへのバインドについて、必要情報を入力するようにプロンプトが出ます。*pw* パラメーターは、固有の名前に関連付けられたパスワードです。このパラメーターを入力しないと、バインドが匿名要求として発行されます。

policy-base <*string*>
ルーターの SRAM と LDAP サーバーでポリシーの検索する範囲を定義するときに使用される文字列を入力するようにプロンプトが出ます。たとえば、このオプションを使うと、ルーター A、NHD、または IBM-US だけに適用するポリシーを戻すことができます。policy-base は、LDAP サーバーにある DeviceProfile オブジェクトの固有の名前です。

primary <*ip-address*>
ポリシーを取り出す LDAP サーバーの IPv4 アドレスを入力するようにプロンプトが出ます。

secondary <*ip-address*>
デフォルト・サーバーに到達できないときに使用するバックアップの LDAP サーバーの IPv4 アドレスを入力するようにプロンプトが出ます。

version <*value*>
LDAP サーバーがサポートする LDAP バージョン番号を入力するようにプロンプトが出ます。

デフォルト値: 2 (受け入れられるのは 2 または 3 だけ。)

Set Refresh

set refresh コマンドは、1 日に 1 回のポリシー・データベースの自動リフレッシュを使用可能または使用不可にします。使用可能にすると、ポリシー・データベースは、1 日に 1 回、指定された時刻に自動的にリフレッシュします。これにより、ポリシーが使用可能になっているネットワーク内のすべてのルーターは、LDAP ディレクトリーのなかで起きたポリシーの変更を自動的に取り入れることができます。このパラメーターをリセットするには、ポリシー・フィーチャーの Talk 5 **reset refresh** コマンドを使用します。

構文: set refresh

enabled

yes

no

<*time*>

enabled [yes または no]
自動リフレッシュを実行するかどうかを指定します。

<*time*> 使用可能に指定すると、リフレッシュをする時刻を指定します (24 時間制)。

ポリシー監視プロンプトへのアクセス

ポリシー・フィーチャーのポリシー・コンソールには、ポリシー・データベース内のポリシーを表示したり、それぞれのポリシーを使用可能にしたり、あるいは使用不可にする部分があります。ポリシー監視環境にアクセスするには、OPCON プロンプト (*) で **talk 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで以下のコマンドを入力します。

```
+ feature policy
Policy>
```

ポリシー監視コマンド

これらのコマンドを使うと、ポリシー・データベースに定義されたプロファイルを表示したり、それぞれのポリシーを使用可能にしたり、あるいは使用不可にできます。表41 は、ポリシー監視コマンドの要約です。この節ではこれらのコマンドを詳細に説明します。これらのコマンドは、Policy console プロンプトで入力します。コマンドとオプションをまとめて 1 行に入力するか、コマンドだけを入力して、プロンプトに答えることもできます。コマンドにオプションを付ける代わりに、疑問符 (?) を付けると、コマンド・オプションのリストが表示されます。

表 41. ポリシー監視コマンド

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。
Cache-ldap-plcys	LDAP サーバーからルーターの持続構成記憶域に読み取られた最新のポリシー情報のコピーを保管します。
Check-consistency	個々のポリシー内、および構成されたすべてのポリシー間で整合性を検査します。
Disable	ポリシー・データベースにロードされたポリシーを使用不可にします。
Enable	ポリシー・データベースにロードされたポリシーを使用可能にします。
Flush-cache	キャッシュに入ったポリシー情報を、ルーターの持続構成記憶域から消去します。
Reset	ポリシーに関連した基準をリフレッシュまたはリセットします。
Search	LDAP クライアントとサーバーの間のアクティビティーについて、テストやデバッグを行います。
Status	ポリシー・データベースに関する情報を表示します。
List	LDAP の構成および定義されたポリシーに関する情報を表示します。
Test	ポリシーに照会を行い、選択された規則を取り出します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Cache-LDAP-Plcys

cache-ldap-plcys コマンドは、LDAP サーバーからルーターの持続構成記憶域に読み取られた最新のポリシー情報のコピーを保管するのに使用します。これは、キャッシュに入った既存のすべてのポリシー情報を持続記憶域から除去します。

構文: cache-policy

注: 2212 および 2216 プラットフォーム上で、このコマンドを入力すると、Talk 6 **write** コマンドと同じように、ルーター構成全体も書き込みます。

Check-Consistency

check-consistency コマンドは、個々のポリシー内 (内部) で構成されたオプション間、および並行した定義のあるポリシー (外部) 間で、不整合がないかどうかを検査するのに使用します。これにより、矛盾を解決するための正しいアクションを取ることができます。

内部 の不整合とは、1 つのポリシー内のアクション・オブジェクト間に存在するものです。たとえば、DiffServ アクション・タイプ Deny のあるポリシーに、IPSec アクション・タイプ Permit もある場合です。*外部* の不整合とは、並行したプロファイルがある別々のポリシー間に存在するものです。たとえば、あるポリシーには、DiffServ アクション・タイプ Block があり、別のポリシーには IPSec アクション・タイプ Permit がある場合です。もう 1 つの例は、並行するポリシーが異なる IPSec アクション・タイプを指定する場合です。

構文: check-consistency

例:

ポリシーが次のように構成されていることを前提とします。

```
Policy Name: dsDown
Loaded from: Local
State: Enabled and Valid
Priority: 5
Hits: 0
Profile: DSUP
Validity: always
DiffServ: dsDown
RSVP: rsvpActUp
Policy Name: ManualTunnel
Loaded from: Local
State: Enabled and Valid
Priority: 5
Hits: 0
Profile: DSUP
Validity: always
Tunnel ID: 1
```

Policy Name: ike

Loaded from: Local

State: Enabled and Valid

Priority: 30

Hits: 0

Profile: DSUP

Validity: always

IPSec: ipsecUP

ISAKMP: generalPhase1Action

consistency-check コマンドの出力は、次のように表示されます。

```
Policy console>check-consistency
Checking for inconsistencies with a policy...
Rule dsDown contains two conflicting actions:
   RSVP Action is of type PERMIT
   DiffServ Action is of type BLOCK

Checking for inconsistencies among policies with overlapping profiles...
  Mismatching IPSec and DiffServ actions at Priority 181 between:
        Rule: ike.traffic     State: ENABLE  Prio: 5 IPSec Action: PERMIT
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK

   Two rules with IPSec actions:
        Rule: ike.traffic     State: ENABLE  Prio: 30 Action: PERMIT
        Rule: Man             State: ENABLE  Prio: 5 Action: PERMIT

   Two rules with IPSec actions:
        Rule: ike.inBoundTunnel State: ENABLE  Prio: 30 Action: PERMIT
        Rule: Man.inBoundTunnel State: ENABLE  Prio: 5 Action: PERMIT

   Two rules with IPSec actions:
        Rule: Man.inBoundTunnel State: ENABLE  Prio: 5 Action: PERMIT
        Rule: ike.inBoundTunnel State: ENABLE  Prio: 30 Action: PERMIT

   Two rules with IPSec actions:
        Rule: Man             State: ENABLE  Prio: 5 Action: PERMIT
        Rule: ike.traffic     State: ENABLE  Prio: 30 Action: PERMIT

  Mismatching IPSec and DiffServ actions at Priority 5 between:
        Rule: Man             State: ENABLE  Prio: 5 IPSec Action: PERMIT
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK

  Mismatching IPSec and DiffServ actions at Priority 5 between:
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK
        Rule: ike.traffic     State: ENABLE  Prio: 30 IPSec Action: PERMIT

  Mismatching IPSec and DiffServ actions at Priority 5 between:
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK
        Rule: Man             State: ENABLE  Prio: 5 IPSec Action: PERMIT
```

Disable

disable コマンドは、ポリシー・データベースに現在ロードされているポリシーを使用不可にします。使用不可にしたポリシーの基準に一致するデータ・パケットは、デフォルトの決定が適用されます。

構文: disable *policy-name*

Enable

enable コマンドは、ポリシー・データベースに現在ロードされているポリシーを使用可能にします。 使用可能にしたポリシーの基準に一致するデータ・パケットは、そのポリシーの構成内容にしたがって決定がなされます。

構文: enable *policy-name*

Flush-Cache

flush-cache コマンドは、LDAP サーバーからルーターの持続構成記憶域に読み取られたポリシー情報の、キャッシュに入った最新のコピーを消去するのに使用します。

構文: flush-cache

Reset

reset コマンドは、ポリシー関連の基準をリフレッシュ、またはリセットします。

構文: reset ldap-config
policy-database
refresh-time

ldap-config
LDAP の構成を (**set ldap** コマンドの指定にしたがって) 動的にメモリーにロードします。変更内容は、次の検索操作でアクティブになります。また、このコマンドは、ポリシー・データベースをリセットし、ポリシー・データベースのリフレッシュ時刻を無効にします。

policy-database
ポリシー・データベースをリフレッシュします。すべてのトンネル、フェーズ 1 およびフェーズ 2 の SA を停止し、RSVP と DiffServ データ構造をリセットし、ポリシー・データベースを洗い流します。次に、ポリシーを LDAP サーバーからロードし、オート・スタートを実行します。データベースが再構築される間は、LDAP サーバーとのパケットのやりとり以外は、ルーターからのパケットの出し入れは禁止されます。

refresh-time
毎日の決まった時刻にポリシー・データベースが自動的にリフレッシュする時刻を設定します。リフレッシュ時刻を使用不可にすると、ルーターをリブートするかリスタートするまでは、データベースはリフレッシュされません。

Search

search コマンドは、LDAP クライアントとサーバーの間で、アクティビティーのテストやデバッグをします。ディレクトリーに対して検索を行い、検索結果を talk 5 で表示できます。

構文: search *filter*
ipaddress

filter 検索操作のフィルター値を指定します。

ipaddress
サーバーの IP アドレスを指定します。

Status

status コマンドは、ポリシー・データベースに関する情報を表示します。

構文: status

status ポリシー・データベースの最新リフレッシュ結果、前回のリフレッシュからの経過時間、および次の予定リフレッシュ時刻を表示します。

例:

```
Policy>status
Status of Last Search:       Failed
Time since last refresh:     4 seconds
Next Policy Refresh not scheduled
```

List

list コマンドは、LDAP の構成およびポリシーに関する情報を表示します。

構文: list
- default-policy
- ldap
- policy
- refresh
- rule
- stats

default-policy
ポリシー・データベースのリフレッシュのときに使用するデフォルト・ポリシーを表示します。

ldap SRAM にある LDAP の構成を表示します。

policy

basic 論理ポリシー名ごとにポリシーのコンポーネントを表示します。ポリシーを 1 つだけ選択したり、すべてのポリシーを表示することもきます。ポリシーのコンポーネントの名前が、Talk 6 の構成で入力した通りの名前で表示されます。

complete
ポリシーのリストと同じですが、このリストにはそれぞれの論理ポリシーのパラメーター値がすべて表示されます。

generated
ポリシーのリストと同じですが、このリストにはそれぞれの論理ポリシーで作成された規則の名前がすべて表示されます。

refresh
ポリシーのリフレッシュ・ステータス (使用可能、または使用不可)、およびリフレッシュ間隔を表示します。

rule 以下のオプションにしたがって、作成された規則に関する情報を表示します。

basic 作成した規則をすべてリストにします。リストの中から規則を選択したり、すべての規則を表示できます。リストには、規則のコンポーネント名が表示されます。以下のコンポーネントがあります。

policy name

loaded from (LDAP or local)
state
priority
number of hits
profile
validity (以下のアクション・リストを続ける)
IPSec (and, or)
ISAKMP (and, or)
DiffServ (and, or)
RSVP

complete
規則と同じですが、このリストには各コンポーネントのパラメーターの名前がすべて表示されます。

stats ヒットされた規則とヒット数をリストにします。1 つの規則には複数のアクションがあり、すべてのアクションがヒットされるとは限りません。そこで、このオプションは、規則のなかでヒットされたアクションとそのヒット数を示します。

Test

test コマンドは、ポリシー・データベースの挙動を確認するときに使用します。このコマンドを使うと、1 組のセレクターを入力し、これがポリシー・エンジンに照会を行い、一致した規則を取り出します。 発信元と宛先のアドレス、発信元と宛先のポート、プロトコル ID、および TOS 値を入力するようにプロンプトが出ます。一致する規則があると、コマンドが規則名を回答します。 一致がないときは、*No match found* が示されます。

構文: test forwarder
ISAKMP
IPSec
RSVP

forwarder
IP 転送エンジンからデータベース照会をシミュレートし、そうした照会の結果として生まれるはずのポリシー決定を回答します。回答されるポリシーには、 DiffServ 情報、IKE フェーズ 1 情報、および IPSec 手動トンネル ID などがあります。

ISAKMP
フェーズ 1 ポリシー情報の IKE からデータベース照会をシミュレートし、そうした照会の結果として生まれるはずのポリシー決定を回答します。このオプションを使うときは、発信元および宛先のアドレスをトンネル・終了点の IP アドレスに設定し、プロトコルを 17 に、そして発信元と宛先のポートを 500 にします。

IPSec フェーズ 2 ポリシー情報の IKE からデータベース照会をシミュレートし、そうした照会の結果として生まれるはずのポリシー決定を回答します。このオプションを使うときは、発信元および宛先のアドレスをトンネル・終了点の IP アドレスに設定し、プロトコルを 17 に、そして発信元と宛先のポートを 500 にします。

RSVP RSVP からデータベース照会をシミュレートし、そうした照会の結果として生まれるはずの RSVP ポリシー決定を回答します。

ポリシー動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

ポリシー・フィーチャーは、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、ポリシー・フィーチャーには適用されません。ポリシー・フィーチャーの構成により、IP トラフィックに適用される規則と後続のアクションの集合が決まります。これは、個々のインターフェースとは無関係です。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、ポリシー・フィーチャーには適用されません。ポリシー・フィーチャーの構成により、IP トラフィックに適用される規則と後続のアクションの集合が決まります。これは、個々のインターフェースとは無関係です。

GWCON (Talk 5) 構成要素リセット・コマンド

ポリシー・フィーチャーは、次のポリシー・フィーチャー固有の GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature Policy, Reset, Database コマンド

説明: フィーチャー・ポリシーで構成されるポリシーはすべて、ローカル構成から読み取られます。LDAP 検索が使用可能になっている場合、この装置のポリシーは、LDAP サーバーから読み取られます。ポリシーによって使用される DIFFSERV アクション、IPSec および IKE ポリシー・オブジェクトなどの、基本ポリシー・オブジェクトに加えられたその他の変更もすべて、構成から再ロードされます。

すべてのポリシーが読み取られた後、これらのポリシーから生成される規則の集合から、ポリシー・データベースが作成されます。ポリシーが読み取られている間、**feature policy, set default-policy** コマンドを使用して、Talk 6 で構成されたデフォルト規則でデフォルトのデータベースが作成されます。

ネットワークの影響:

ポリシー・データベースが作成されている間、Talk 6 で構成されたデフォルト・ポリシーに基づいて、IPv4 ユニキャスト・トラフィックが転送されます。デフォルト・ポリシーは、すべてのトラフィックを渡すか、2210 との間の両方向の LDAP トラフィックを除くすべてのトラフィックを除去す

るか、または 2210 との間の、IPSec を使用して保護された LDAP トラフィックを除くすべてのトラフィックを除去します。

制限: なし。

次の表は、**GWCON, feature policy, reset, database** コマンドが起動されるときにアクティブになるポリシー・フィーチャーの構成変更を要約しています。

GWCON, feature policy, reset, database コマンドによって変更がアクティブになるコマンド
CONFIG, feature policy, add, policy
CONFIG, feature policy, delete, policy
CONFIG, feature policy, change, policy
CONFIG, feature policy, disable, policy
CONFIG, feature policy, enable, policy

GWCON, Feature Policy, Reset, LDAP コマンド

説明: ポリシー・フィーチャーの LDAP 構成パラメーターが、更新されます。

ネットワークの影響:

次回にポリシー・データベースが更新されると、サーバーを検索するかどうか、および検索する場合はどのパラメーターを使用するかを判別するのに、新しい LDAP 構成パラメーターが使用されます。

制限: なし。

次の表は、**GWCON, feature policy, reset, ldap** コマンドが起動されるときにアクティブになるポリシー・フィーチャーの構成変更を要約しています。

GWCON, feature policy, reset, ldap コマンドによって変更がアクティブになるコマンド
CONFIG, feature policy, set, ldap, anonymous-bind
CONFIG, feature policy, set, ldap, bind-name
CONFIG, feature policy, set, ldap, bind-pw
CONFIG, feature policy, set, ldap, policy-base
CONFIG, feature policy, set, ldap, port
CONFIG, feature policy, set, ldap, primary-server
CONFIG, feature policy, set, ldap, retry-interval
CONFIG, feature policy, set, ldap, search-timeout
CONFIG, feature policy, set, ldap, secondary-server
CONFIG, feature policy, set, ldap, version
CONFIG, feature policy, enable, ldap, cached-search
CONFIG, feature policy, enable, ldap, policy-search
CONFIG, feature policy, disable, ldap, cached-search
CONFIG, feature policy, disable, ldap, policy-search

GWCON, Feature Policy, Reset, Refresh

説明: ポリシー・データベースのリフレッシュ・パラメーターが再ロードされま

す。このリフレッシュ・パラメーターは、データベースが一日に 1 回自動的に更新されるどうか、および使用可能になる場合は、一日の内いつ更新されるかを決定します。

ネットワークの影響:

ポリシー・リフレッシュ・フィーチャーが使用可能になる場合、リフレッシュ構成で指定された時間イベントが発生すると、ポリシー・データベースが更新されます。これには、手動で **reset database** コマンドを実行するのと同じ効果があります。

制限: なし。

次の表は、**GWCON, feature policy, reset, refresh** コマンドが起動されるときにアクティブになるポリシー・フィーチャーの構成変更を要約しています。

GWCON, feature policy, reset, refresh コマンドによって変更がアクティブになるコマンド
CONFIG, feature policy, set, refresh

CONFIG (Talk 6) 即時変更コマンド

ポリシー・フィーチャーでは、装置の操作状態を即時に変更する次の CONFIG コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、これらの変更は保管され、保存されます。

コマンド
CONFIG, feature policy, set, default-policy **注:** 次回にポリシー・データベースが更新されるときに、デフォルト・ポリシーの設定値がリフレッシュ期間中に使用され、ポリシー・データベースの更新時に発生する可能性があるエラー状態を処理します。
CONFIG, feature policy, add, user
CONFIG, feature policy, change, user **注:** 装置をリスタートまたは再ロードしなくても、ユーザー用に定義されたプリシェアード・キーが、ただちに使用できます。このユーザーが、プロファイルのリモート・ユーザー・グループに関連したグループに含まれている場合、この関連付けを行う前に、ポリシー・データベースをリセットしておく必要があります。

第18章 IP セキュリティーの使用

この章では、IP セキュリティー・フィーチャーの使用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。

IP セキュリティーの概要

この節では、IPv4 と IPv6 の両者について、IP セキュリティー機能の概要を説明します。

保護トンネルの使用

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、保護すべき IP ルートごとに保護トンネルを構成できます。 IPSec 保護 トンネルは、両方向の論理接続です。リモート・ホスト、ルーター、およびファイアウォールに接続し、これを通してローカル・ルーターは保護 IP パケットを転送できます。保護トンネルは、発信元ホスト・アドレス、宛先ホスト・アドレス、ポート番号、トンネル ID などのパラメーターで識別できます。

IPv4 を使うと、ポリシー・データベースにトンネル・ポリシーを構成して、ネゴシエーションされたトンネルを定義したり、344ページの『ルーター A のトンネルの構成』に示されている Talk 6 **add tunnel** コマンドを使って、手動トンネルを作れます。IPv6 では、Talk 6 **add tunnel** コマンドを使います。

保護 IP トンネルを確立するには、特別の認証ヘッダーを添付する IP 認証ヘッダー (AH) 機能 (314ページの『IP 認証ヘッダー』参照)、およびデータを暗号化する IP カプセル化セキュリティー・ペイロード (ESP) 機能 (315ページの『IP カプセル化セキュリティー・ペイロード』参照) をポリシーに指定します。ポリシーは、パケットに次のセキュリティー対策のどちらを実施するかを決めます。

- AH アルゴリズムと AH 認証キー (必要に応じて 334ページの『アルゴリズムの構成』または 346ページの『アルゴリズムの構成』を参照してください)。
- ESP 暗号アルゴリズムと ESP 暗号キーおよび暗号解除キー (必要に応じて 334ページの『アルゴリズムの構成』または 346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) (316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。)

注: 送信側と受信側は、それぞれの保護トンネルについて、同一のオプションを選択しなければなりません。

IP セキュリティーの概念

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・フィーチャーを使用して保護できます。

RFC 2401 の定義によるセキュリティー: インターネット・プロトコルのセキュリティー・アーキテクチャーには、以下の機能があります。

認証 受信データと送信データが同じであること、また送信側と主張する相手が本当の送信側であることが分かっている。

保全性 データが変更されずに発信元から宛先に転送されることが保証される。

機密性 指定の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。

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。

注: 一部の国では、米国の輸出規制や暗号化パラメーターが表示されないなどの理由で、暗号化サポートが提供されない場合がありますが、ESP-NULL アルゴリズムは、どこでも利用可能です。 ESP-NULL アルゴリズムの定義については、315ページの『ESP 暗号化アルゴリズム』を参照してください。

IP セキュリティーの用語

IPv4 関連の IPSec を説明するためには、以下の用語が使用されています。

認証ヘッダー (AH)
パケットのヘッダー情報があるデータ域で、データの起点を証明し、データの保全性と再生を保護します。

証明 ASN.1 エンコード・データ項目 (ITU X.509 規格) で、エンド・エンティティーの ID を公開キーにバインドします。(ここでは、エンド・エンティティーは、ISAKMP ネゴシエーション・エンティティーを示します。) エンド・エンティティーは、認証要求を提出して、自己の ID と公開キーを認証局 (CA) に登録します。CA は、要求を検証して、サインをしたあと、エンティティーに発行します。ISAKMP は、フェーズ 1 処理のときに、公開キー認証を使って、最初のメッセージの交換を証明し、これによりルーターのあいだにマスター・シークレット (暗号キー) が設定されます。

認証局 (CA)
“signed” X.509 ディジタル認証を発行する信頼機関。ネットワークのユーザーは、ISAKMP を使ってユーザーの保護データを交換するときには、この認証を使わなければなりません。ISAKMP を使う相手と保護データを交換をするには、ルーターが CA を登録し、認証として X.509 ディジタル認証を取得する必要があります。

注: 定期的に CA を検査して、ISAKMP を使う相手の現行のリストを使用していることを確認する必要があります。詳細については、331ページの『公開キー・インフラストラクチャーの構成コマンド』の PKI Talk 6 **load**コマンドを参照してください。

ディジタル・シグニチャー
コード化されたユーザー ID を含むデータ項目。これは、X.509 ディジタル

認証の一部分となります。ユーザーは、お互いの認証のために、フェーズ 1 ネゴシエーションで認証を交換します。サインが必要な入力データ域で公開キー操作を実行するとシグニチャーが作成されます。

カプセル化セキュリティー・ペイロード (ESP)
データグラムのカプセル化と暗号化を行う IPSec 機能です。受信者以外は内容を判別できません。これにはデータの保全性と再生保護の機能があります。 ESP は、データの起点も認証します。動作モードには、オリジナルのデータグラムのペイロードだけを暗号化し、アドレス情報は認証のない相手にも見えるようにしておくトランスポート・モード、そして、ヘッダーなどを含むすべてのオリジナルのデータグラムを暗号化するトンネル・モードがあります。後者の場合は、重要なアドレスを秘密にしておくことができます。

インターネット・キー・エクスチェンジ (IKE)
ISAKMP と Oakley のプロトコルから派生したプロトコルです。インターネットで暗号キーを交換したり、通信相手を認証するのに使われます。

ISAKMP
インターネット・セキュリティー・アソシエーション・アンド・キー・マネージメント・プロトコルです。ISAKMP は、データ交換のあいだに、セキュリティーの関連付けを自動的に実行し、パケットの暗号キーを管理します。

管理情報ベース (MIB)
中央の信頼機関がルーターの運用に関する統計情報を要求し、この照会に対してルーターが送信するデータ・ブロックです。信頼機関は、ネットワークの問題を検出し、該当者に対策をとるように連絡をとります。

Oakley
ISAKMP が使用する暗号キー管理のプロトコルです。

Perfect Forward Secrecy (PFS)
フェーズ 2 のネゴシエーションです。新しい暗号キー情報があったときに獲得するデータ・セキュリティーのレベルです。ISAKMP は、通信者のあいだで公開 Diffie Hellman 値を交換してこれを実行します。このセキュリティー機能により、以前に妥協したキーをもとに今回の暗号キーを判別することを防止します。

フェーズ 1 ネゴシエーション
送信側と受信側のあいだの通信です。これにより ISAKMP セキュリティーの関連付けと暗号キーを確立し、フェーズ 2 ネゴシエーションで交換する ISAKMP メッセージを保護します。フェーズ 1 は、プロセッサーに作業が集中するので、実行頻度は少なく、日ごとや週ごとに行われます。

フェーズ 2 ネゴシエーション
送信側と受信側のあいだで行われる ISAKMP メッセージの交換です。この間に、セキュリティー・アソシエーションと暗号キーのネゴシエーションが行われて、ユーザーのデータ交換を保護します。このネゴシエーションは、2 ～ 3 分おきに常に行われており、ユーザーが介入しなくても、定期的に暗号キーをリフレッシュします。

プロキシー
別のネットワーク装置の代わりに機能するように割り当てられたルーターです。

公開キー・インフラストラクチャー (PKI)
ユーザーの ID をユーザーの公開キーにバインドし、バインドした公開キーをセキュリティーを確保しながら配布するために CA が使用しているフレームワークです。

クィック・モード
フェーズ 2 のネゴシエーションです。非 ISAKMP のセキュリティー・アソシエーションを示す用語です。

再生 データグラムを取り込むことです。データグラムの内容を判別する試み、またはデータグラムを繰り返し送信してサービス拒否の意志表示を装着することを意味します。

セキュリティー・アソシエーション (SA)
暗号アルゴリズム情報、キー情報、通信相手の識別情報など、データ・パケットに関する情報をまとめたデータ域です。

トランスフォーム
認証および暗号化の選択に関する構成情報に名前を付けた集合体です。

IP 認証ヘッダー

認証ヘッダー (AH) については、RFC 2402 IP 認証ヘッダーに説明があります。このヘッダーには、IP データグラムの認証データが含まれています。

ネゴシエーションされた IPSec を使う IPv4 では、データグラムに割り当てられたポリシーが暗号認証機能を実装しますが、これはインターネット・キー・エクスチェンジ (IKE) プロトコルと公開キーまたはプライベート・キーのペアに依存します。IPv4 手動トンネルと IPv6 では、送信側が使用する暗号機能は秘密の認証キーに依存します。どちらの場合も、データグラムの内容には暗号認証機能が適用されます。AH だけを指定したり、ESP とあわせて指定することもできます。詳しくは、315ページの『AH と ESP の使用』 を参照してください。

AH 確認アルゴリズム

AH トンネル・ポリシーを使用する保護トンネルには、次の認証アルゴリズムの 1 つを使用します。

- 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 AH アルゴリズムは、暗号ハッシュを使って (HMAC: ハッシュ・メッセージ認証コード)、キー入力メッセージ確認機能とオプションの再生防止機能を結合します。再生防止機能は、AH に含まれる連続番号を使い、以前に同じパッケージを受け取っていないことを確認します。 再生防止機能により、受信側をサービス拒否ハッキングから保護します。サービス拒否ハッキングは、同じパケットが繰り返し送信され、ルーターが同じパケットの処理に忙しくなり、正しいトラフィックの処理ができなくなることをいいます。 認証コードは、まずシークレット暗号キーとデータに適用され、次にシークレット・キーの出力と最初の操作の出力に適用されます。 315ページの図22には、HMAC-MD5 の運用例が示されています。

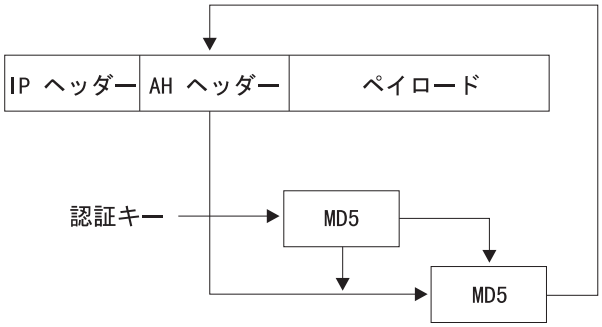


図 22. HMAC MD5 による認証メッセージの作成

IP カプセル化セキュリティー・ペイロード

IP カプセル化セキュリティー・ペイロード (ESP) については、RFC 2406 IP カプセル化セキュリティー・ペイロードに説明があります。ESP は、IP パケットの一部または全部を暗号化し、ユーザーに機密性、認証 (オプション)、および保全性を提供します。しかし、ESP-NULL アルゴリズムを選択すると、ESP が認証と保全性のチェックを行います。ESP だけを指定したり、AH とあわせて指定することもできます。詳しくは、『AH と ESP の使用』 を参照してください。

ESP 認証アルゴリズム

ESP の認証に使用可能なアルゴリズムは、314ページの『AH 確認アルゴリズム』で示した AH のアルゴリズムと同じです。

ESP 暗号化アルゴリズム

ESP 暗号化ポリシーを使用する保護トンネルは、以下の暗号化アルゴリズムの 1 つ、または ESP-NULL アルゴリズムを使います。

- 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、ESP-NULL を除いて、米国の輸出規制の対象になっています。お使いの 2210 で、これらのアルゴリズムの一部または全部を構成できない場合、これらのアルゴリズムの販売がご使用の国で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。

ESP-NULL アルゴリズムは、クリア・テキストのデータは暗号化しませんが、すべての国で利用できます。使用できる機能は、ESP の認証と保全性の確認だけで、暗号化はできません。ESP-NULL を使用するの場合は、ESP 認証アルゴリズムを***必ず***ご使用ください。

AH と ESP の使用

保護トンネルの認証および暗号化には、AH、ESP、AH-ESP、ESP-AH のうちの 1 つを使用できます。AH と ESP を組み合わせたいときは、次のようにします。

- AH-ESP のポリシーでは、アウトバウンドのパケットについて、認証の前に暗号化するように指定します。この場合、宛先ルーターでは、AH の認証機能がまず実行されてインバウンドのパケットをチェックし、その認証を通過したパケットだけが ESP に送られて暗号解除を受けます。

- ESP-AH のポリシーは、アウトバウンドについては、暗号化の前に認証を実行するように指定します。この場合、宛先ルーターでは、まず ESP 機能がインバウンドのパケットを暗号解読して、暗号解読に成功したパケットだけが AH に送られて認証を受けます。

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、接続によって運ばれるトラフィックにセキュリティー・サービスを提供するシンプレックスの“接続”です。セキュリティー・サービスは、AH または ESP を使って、SA に提供されますが、AH と ESP の両方は使いません。トラフィック・ストリームに AH と ESP の両方の保護を使用すると、トラフィック・ストリームを保護する SA が 2 つ (以上の) 作成されます。 2 つのホスト、または 2 つのセキュリティー・ゲートウェイを結ぶような典型的な両方向の通信を保護するには、2 つの SA が必要になります (各方向に 1 つずつ)。

トンネル・モードとトランスポート・モード

使用する動作モードにより (トンネル・モードまたはトランスポート・モード)、IPSec が IP パケットを処理する方法が決まります。デフォルトは、トンネル・モードで、ルーターがセキュリティー・ゲートウェイとして機能するときは、このモードが必要になります。ネットワークを通して、各パス上の単一セグメントのデータを保護します。トランスポート・モードは、ルーターがホストとして機能するときにだけ使用し、このモードでは、パスの全長についてデータを端から端まで保護します。

AH と動作モード

トンネル・モードでは、AH は IP パケットの前に置かれ、新しい 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 (内部ヘッダー) には、パケットの最終的な発信元と宛先のアドレスが入ります。新規 IP ヘッダー (外部ヘッダー) には、セキュリティー・ゲートウェイ (トンネルの終了点) 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。

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) 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、活動回数 [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。

317ページの図23は、AH が保護するデータグラムのフォーマットを示しています。

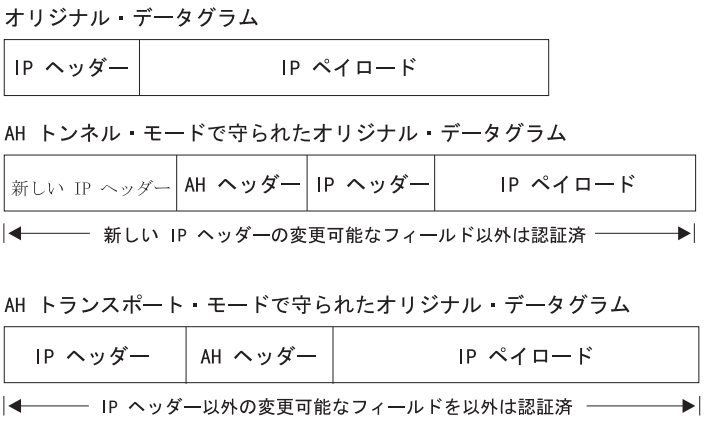


図 23. AH 保護によるデータグラムのフォーマット

ESP と動作モード

トンネル・モードでは、ペイロード・データには IP パケット全体が入れられ、新規の IP ヘッダーが作成されて ESP ヘッダーの前に置かれます。トンネル伝送されるパケットの IP ヘッダー (内部ヘッダー) には、パケットの最終的な発信元と宛先のアドレスが入り、新しい IP ヘッダー (外部ヘッダー) 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 パケットを暗号化します。ESP 認証が使用される場合は、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。

トランスポート・モードでは、ペイロード・データには、暗号化された高位レイヤー・プロトコル・データ (TCP または UDP データ) が入れられます。認証が使用される場合は、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。

図24は、ESP が保護するデータグラムのフォーマットを示しています。

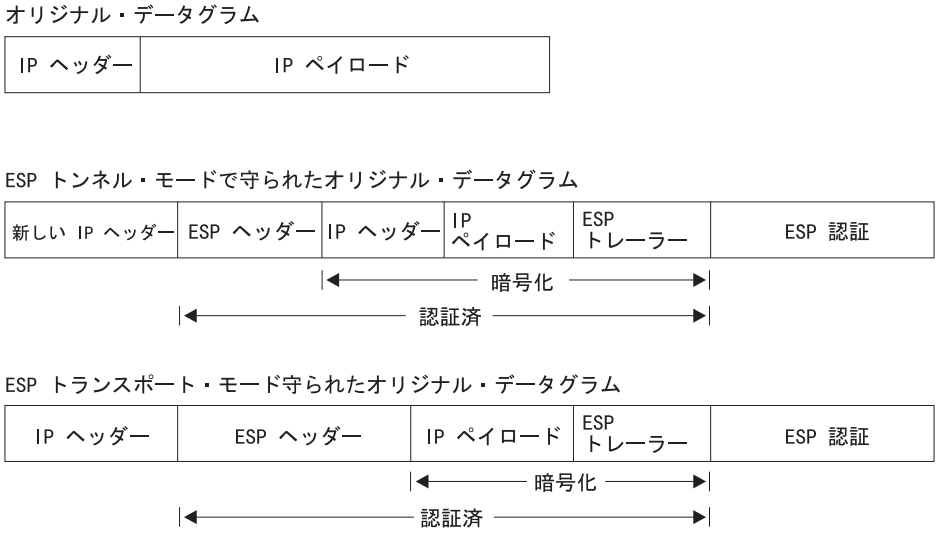
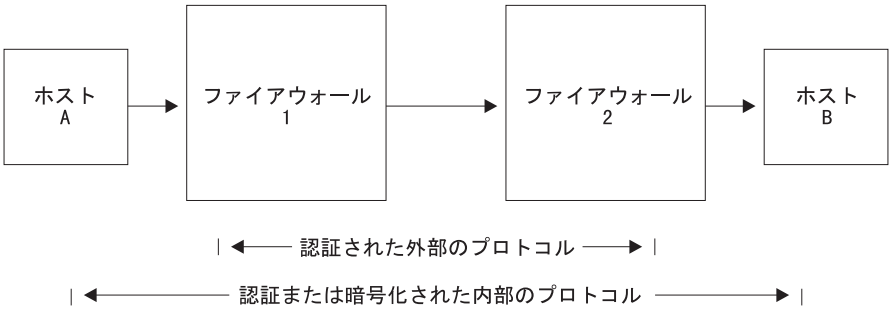


図 24. ESP 保護によるデータグラムのフォーマット

AH と ESP のネスティング

プロトコルをそのプロトコルの中にネスティングしたり、あるいは別のプロトコルにネスティングすることができます。 図25は、AH トンネル内で ESP 保護のデータグラムをネスティングしたときの効果を示しています。



ホスト A は ESP トランスポートを使う

IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証

ファイアウォール 1 は AH トンネルを使い、新しい IP ヘッダーを追加する

新しい IP ヘッダー	AH ヘッダー	IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証

ファイアウォール 2 は AH トンネル化データグラムを受信し、認証して、外部ヘッダーと AH ヘッダーを取り除く

IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証

図 25. AH トンネル内の ESP のネスティング

L2TP パケットを使った IP セキュリティーの使用

IPv4 では、IPSec を使って L2TP パケットを保護できます。UDP パケット内に L2TP フレームをカプセル化して L2TP トンネルを作ったあと、送信元と宛先のアドレスがトンネルの終了点を定義するような IP パケットの中に UDP パケットをカプセル化することができます。次に、IP パケットに AH、ESP、および ISAKMP のプロトコルを適用します。 図26は、IP カプセルの L2TP パケットが示されています。これには、インターネットの転送に必要な PPP とそのペイロード・プロトコルが含まれています。

IP ヘッダー	UDP ヘッダー	L2TP ヘッダー	PPP ヘッダー	PPP ペイロード

これらのフィールドは IP パケット・ペイロード

図 26. IPSec 保護の L2TP パケット

トンネル内トンネル・モード

セキュリティーを増すために、これまで説明したセキュリティーのほかに、トラフィック・ストリームのパケットを 2 回カプセル化して、1 つを IPSec から送信したあとに、2 つ目をもう 1 つの IPSec を通して送る方法があります (トンネル内トンネル)。

注: ルーター内で複数の暗号化をすることは (トンネル内トンネルを使い、両方のトンネルで暗号化をする方法)、米国の輸出規制により制約があります。厳格な輸出規制を受けたソフトウェア・ロードだけにサポートされています (128 ビット・キーおよびトリプル DES 付きの RC4 をサポートするソフトウェア・ロード)。

IPv4 では、ポリシー・データベース内の規則が最初のトンネルのカプセル化 (内部) についてパケットを指定します。次に、パケットを送信する前に、規則により、パケットは 2 つ目のトンネルに渡されて、2 回目のカプセル化 (外部) を行います。IPv6 では、パケット・フィルター・アクセス制御規則が最初のトンネルのカプセル化 (内部) をするパケットを識別し、パケットを送信する前に、2 つ目の規則がパケットを 2 つ目のトンネルに渡して、2 回目のカプセル化 (外部) を行います。

2 つの IPSec トンネルは、同じルーターから発生し、トンネルのリモート・エンドは、物理的に同じ位置にありますが、設備は異なります。最初のトンネルのリモート・エンドは、保護ゲートウェイまたはホストのどちらかですが、2 つ目のトンネルのリモート・エンドは、必ず保護ゲートウェイ・ルーターです。トンネルの宛先は異なるので、リモート IP アドレスも異なります。トンネル内トンネルに使用されるトンネルは、どちらもトンネル・モードに構成しますが、2 つ目のトンネルには埋め込みの追加はできません。

カプセル化を 2 回したあと、パケットは 2 つ目の (外部) ルーターを通して送信されます。トンネルの端で外部カプセルを取り除き、最初のトンネルのカプセル化で作られたヘッダー情報にしたがって、パケットは最初のトンネル (内部) に送信されます。このトンネルの終端で、最初のカプセルが除去され、パケットは最終的な宛先に転送されます。

パス MTU ディスカバリー

IPv4 と IPv6 の両方とも、2210 がセキュリティー・ゲートウェイとして働いている場合、IPSec はパス・マキシマム・トランスミッション・ディスカバリー (PMTU) をサポートします。PMTU ディスカバリーのサポートは、パケットを断片化できない場合に必要になります。IPv4 では、断片化不可 (DF) ビットがセットされている場合にパケットを断片化できません。IPv6では、パケットの断片化は、すぐ近くのルーターではできません。このような場合、パケットが保護トンネルの一端から他端までのパス内のリンク上に収まらない場合、『packet too big』 という ICMP エラー・メッセージがパケットの発信元に送られます。

ルーターはセキュリティー・ゲートウェイとして働いているので、このエラー・パケットは、パケットの本当の発信元ではなく、発信側ルーターに戻されます。受信側ルーターは、報告された MTU を本当の発信元に正しく戻す必要があります。発信元は、パケットが最終的な宛先に届くように、サイズを小さくします。 PMTU ディスカバリーのサポートについては、インターネット・プロトコルの RFC 2401: セキュリティー体系に記述されています。

IPv4 には、トンネル化パケットの外部ヘッダーに設定する DF ビットについて、以下のようなオプションがあります。

1. 内部ヘッダーからコピーする
2. 常に設定する
3. 常に消去する

これらのオプションは、保護トンネル内トンネル・モードを構成するときに使用できます。たとえば、ポリシー・フィーチャーの **add ipsec-manual-tunn** (IPv4)、または Talk 6 **add tunnel** (IPv6) コマンドがあります。 DF ビットは、選択オプションにしたがって処理されますが、以下の条件のときは異なります。

- トンネル MTU が最小 MTU に等しい。
- インバウンド・パケットのサイズが最小 MTU 以下である。
- カプセル化パケットのサイズが最小 MTU より大きい。

この場合、IPv4 では、構成に関係なくDF ビットは設定されず、保護パケットは、受信側へのパス上で必要に応じて断片化が可能です。IPv6 では、パケットはセキュリティー・ゲートウェイを出るときに、トンネルの PMTU に収まるように、必要に応じて断片化されます。着信パケットはすでに最小 MTU 以下であり、発信側ホストはサイズをそれ以上縮小できないので、この特別処置が必要になります。断片化が許されないと、このパケットは永久に最終的な宛先に到着しません。

ネットワーク・トポロジーや構成が変化すると、PMTU も変わるので、 PMTU 値は、経時処理で定期的に最大値をリセットする必要があります。経時処理のデフォルト値は、10 分ですが、Talk 6 **set path** コマンドで構成することができます。経時パラメーターを 0 にすると、PMTU の経時処理は無効になります。

IP セキュリティー・トンネルのあるネットワーク・ダイアグラム

321ページの図27のネットワークの例では、2 つの IPSec トンネルがルーター A (IPSec) とルーター B (IPSec と IPv4 のネットワーク・アドレス・トランスレーション) を接続しています。

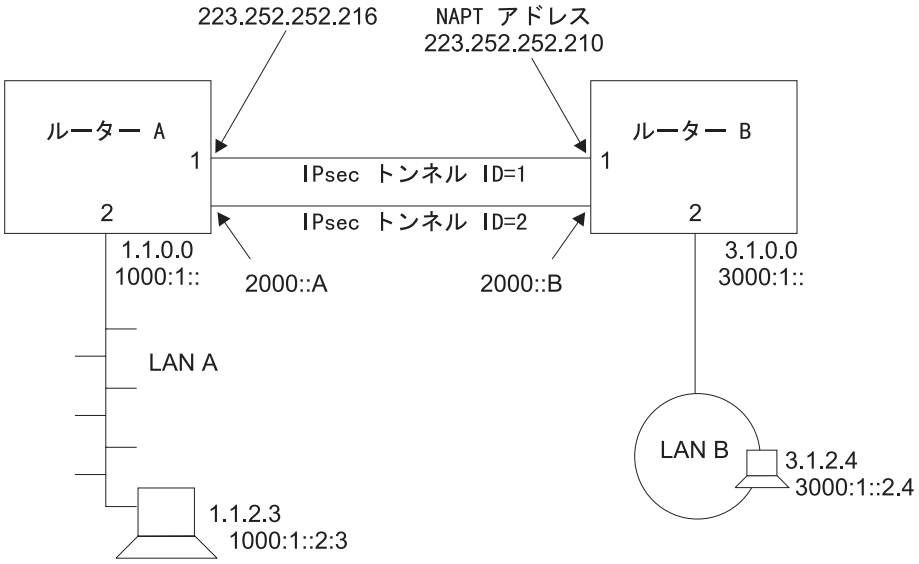


図 27. IPSec と NAT のあるネットワーク

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 IPv4 アドレス 223.252.252.216 からルーター B の IPv4 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。

このネットワークでも、IPSec トンネル ID 2 をもつ IPSec トンネルが、ルーター A の IPv6 アドレス 2000::A からルーター B の IPv6 アドレス 2000::B に構成されています。

IPv4 で、このネットワークを IKE 用に構成するには、329ページの『インターネット・キー・エクスチェンジの構成 (IPv4)』から始まるステップを実行します。手動 IPSec による IPv4 では、344ページの『手動トンネルの構成 (IPv4)』から始まるステップを実行します。IPv6 では、347ページの『手動トンネルの構成 (IPv6)』から始まるステップを実行します。

注: ネットワークで NAT を使用する計画がない場合でも、ルーター B の構成の説明を読むと、IPSec トンネルの各端のパラメーターの関係をよく理解できます。

インターネット・キー・エクスチェンジの使用

この節では、インターネット・キー・エクスチェンジ (IKE) を使って、IPSec セキュリティー・アソシエーション (SA) の定義と作成を自動化する方法を説明します。 IKE は、IETF がサポートする規格です (RFC 2409)。同一または異なるベンダーの IPSec を使用する製品に対し、セキュリティー要件の通信に関する標準手段を提供します。

IKE は、以下のセキュリティー要件を満足するためのフレームワークを提供します。

ネゴシエーション中のリモート・エンティティーの認証 (IKE ピア)

IKE は、プリシェアード・キーまたはディジタル認証を使って、通信相手のエンティティーにエンティティー自身を証明させることで、相手を識別します。

両方のピアで同一のキー資料を作成

IKE は、Diffie-Hellman の公開キーおよびプライベート・キーの機構を使い、公開キーのコンポーネントの交換と、各ピアによる同一キーを個別に作成します。

IPSec のセキュリティー・アソシエーションのネゴシエーションを保護する

IKE は、次の項で説明する 2 つのフェーズのプロセスを使って、セキュリティー・アソシエーションを作成し、IPSec トンネル のネゴシエーションを保護し、セキュリティー・アソシエーション のネゴシエーションと作成を行って、IPSec がユーザーのデータを守ります。

インターネット・キー・エクスチェンジ・フェーズ

IKE は、フェーズ 1 とフェーズ 2 の 2 つの異なるネゴシエーション交換を定義します。フェーズ 1 は、2 つの IKE ピアのあいだで保護トンネルを設定し、これはのちに IPSec トンネルのネゴシエーションの保護となります。 フェーズ 1 のあいだ、以下に示された順序で次のようなアクションが起こります。

1. フェーズ 1 セキュリティー・アソシエーションの特性についてネゴシエーションがあり、IKE のピアがこれに同意します。このほか、 *IKE の通信*を暗号化する暗号化アルゴリズム、使用するハッシュ・アルゴリズム、認証方式、キーを作成するときに使用される Diffie-Hellman グループなどの特別な機能があります。
2. IKE のピアにより、Diffie-Hellman キーが作成され、公開部分が交換されます。これらのキーを使って暗号キーを作成し、このキーが両方のフェーズ 1 ネゴシエーションを暗号化し、IPSec トンネルで使用するキーも作成されます。
3. IKE のピアは、サポートされている 2 つのモード、つまりプリシェアード・キー・モードまたはシグニチャー・モードのどちらかを使って認証されます。

   プリシェアード・キー・モードでは、両方の IKE ピアは、以前のオフライン・プロセスでキーを交換しているので、フェーズ 1 のときにこれを使ってピアを認証します。プリシェアード・キーは、ポリシー・フィーチャーの **add user** コマンドを使って構成します。

   シグニチャー・モードでは、サイン済みの X.509 ディジタル認証を使って、フェーズ 1 メッセージのペイロードの暗号化と暗号解読に使うキーを提供します。サインと検証を成功させるには、ピアの認証が必要です。シグニチャー・モードと X.509 ディジタル認証の使用方法については、324ページの『公開キー・インフラストラクチャーの使用』を参照してください。

フェーズ 1 ネゴシエーションは、次の 2 つの交換モードのどちらかになります。

- メイン・モードには、フェーズ 1 ネゴシエーションを実行するメッセージが 6 つあり、ネゴシエーションするピアのアイデンティティーを暗号化します。
- アグレッシブ・モードには、フェーズ 1 ネゴシエーションを実行するメッセージが 3 つあります。ピアは、最初の 2 つのメッセージで無保護のアイデンティティを交換します。

IP セキュリティー・トンネルのネゴシエーション

この項で説明する処理は、ポリシー・データベースの規則にある定義と一致する属性のパケットをルーターが送信準備するときに起こります。トンネルのネゴシエーションは 2 つのフェーズで起こります。フェーズ 1 では、送信元ルーターが通信を開始し、最初のメッセージとして 6 つのメッセージを交換します。 これによりフェーズ 2 のときに使用されるセキュリティー・オプションを確立します。これに受信側が答え、両者は、ISAKMP セキュリティー・アソシエーション (SA) 文字、そして認証と暗号化に使用するアルゴリズムについてネゴシエーションを実行し、それぞれのアイデンティティーを認証します。フェーズ 2 では、両者は合計 3 つのメッセージを交換して、SA および両者あいだで送受信する IP データグラムの保護に使用するキーについてネゴシエーションします。フェーズ 1 は、次のように進みます。

1. メッセージ 1: 認証方式 (ディジタル・シグニチャーなど)、認証アルゴリズム (HMAC-MD5など)、および使用する暗号化アルゴリズム (DES-CBCなど) などの通信活動の方法を送信側が提案します。
2. メッセージ 2: 受信側がサポートするセキュリティー・オプションがあれば、これを送信側に示します。
3. メッセージ 3: 送信側が Diffie Hellman 公開値と暗号キーが作成されるランダム値を送信します。
4. メッセージ 4: 受信側が自分の Diffie Hellman 公開値と暗号キーが作成されるランダム値を送信します。ここで、両者は、公開キーとプライベート・キー、およびISAKMP のメッセージ交換に使用するキー関連の情報を作成します。
5. メッセージ 5: 送信側は、ディジタル・シグニチャーを送信し、これには信頼できる認証局 (CA) が署名した X.509 ディジタル認証を含めることができます。送信側が有効な認証を発信しないときは、受信側は LDAP プロトコルを使って、信頼できる CA、保護 DNS サーバー、またはそれぞれの ID 値に以前使用した証明証をマップするような保護ローカル・キャッシュから証明をとるか、あるいは送信側に認証を要求しますが、最後の場合は送信側はすぐに認証を送信しなければいけません。
6. メッセージ 6: 受信側は、送信側のディジタル・シグニチャーを検証したあと、自分自身のアイデンティティーについて、同様の情報を送信側に送信します。

この時点で、両者は SA の文字に同意し、ISAKMP SA を処理するためのキーやキー関連の情報を獲得し、お互いを認証したことになります。ここで、両者は、フェーズ 2 に入り、非 ISAKMP SA とキーについてネゴシエーションを行い、これが両者のあいだで交換する IP データグラムを守るのに使われます。フェーズ 2 は、以下のように進みます。

1. メッセージ 1: 送信側は、AH または ESP のアルゴリズムの選択項目を送信し、非 ISAKMP SA を提案します。これには、その他のセキュリティー関連の情報を含むことがあります。
2. メッセージ 2: 受信側は、選択した提案項目を送信側に示し、セキュリティー関連の情報も含めます。
3. メッセージ 3: 送信側は、数項目のハッシュ記録を送信し、ネゴシエーションしたセキュリティー・プロトコルによる通信の準備ができたことを受信側に知らせます。受信側が情報を検証すると、リンクは完成し、両者は保護されたデータ・ストリームの交換を開始します。

公開キー・インフラストラクチャーの使用

この節では、公開キー・インフラストラクチャー (PKI) の使用方法を説明します。IKE は、PKI を通して公開キー・シグニチャー・モードをサポートして、IKE のエンティティーを認証します。この製品は、PKI サポートを必要としないプリシェアード・キー・モードをサポートしますが、このモードには本質的な短所があります。このモードで認証するためには、各ピアのプリシェアード・キーを使って、それぞれの IKE エンティティーを構成しなければなりません。このことは、IKE 機能のスケーラビリティーを大きく制限してしまいます。公開キーをベースにしたシグニチャーや公開暗号モードは、スケーラビリティーが改善されます。この製品では、IKE のエンティティーを認証するのに、シグニチャー・モードの IKE フェーズ 1 ネゴシエーションで、X.509 ディジタル認証を使用します。

ユーザー・ポリシー・プロファイルを構成するときに、ISAKMP ID フィールドに固有の数値を指定して、参加したいそれぞれの IKE エンティティーに、IKE ネゴシエーションでアイデンティティーを割り当てます。それぞれの IKE エンティティーは、ピアでアイデンティティーを認証します。

PKI は、公開キーの運用にむけて、定義と開発が行われています。 PKI では、主張するアイデンティティーに対し、X.509 ディジタル認証がエンティティーの公開キーをバインドします。IKE エンティティーは、 認証に含まれている公開キーを抽出できます。次に、公開キーを使って、IKE のネゴシエーションに参加しているピアのアイデンティティーを認証します。公開キーは、IKE のシグニチャー・モードで使われています。このモードでは、シグニチャーをする人は、プライベート・キーを使ってディジタル・シグニチャーにサインをします。受信側は、認証からサインする人の公開キーを抽出し、これを使ってサインを検証します。ディジタル認証機能を使うと、IKE のエンティティーが別の IKE のエンティティーのアイデンティティーをスケーラブルな形で認証できます。

PKI の構成

この製品では、ネゴシエーション中の両方の IKE エンティティーが同じ CA を使うことを前提としています。シグニチャーを使って IKE ネゴシエーションを開始する前に、ルーターについて PKI を構成する必要があります。ルーターのプライベート・キーとルーターの認証を作り、ルートの CA 認証をダウンロードしておきます。以下のステップでは、PKI の構成方法を説明します。

1. キーのペアを作成し、認証を要求する。

   公開キーを使うにはキー・ペアが必要になるので (シグニチャー・モードでは、プライベート・キーでサインを行い、公開キーで検証します)、ルーターのキー・ペアを作る必要があります。認証要求には、公開キーを作って CA に送り、これを X.509 ディジタル認証に置きます。次に、すべての潜在的な IKE ピアが CA 発行の認証からこの公開キーを抽出します。プライベート・キーは、ルーターのなかにあり、秘密になっていてルーターだけにしかわかりません。

   このバージョンでは、**certificate request** コマンドを発行できます。このコマンドを発行すると以下のことが起こります。

   a. キー・ペアを作成します。キーの長さは、512、768、1024 ビットの中から選択して指定します。作成したプライベート・キーは、キャッシュに置きます。

b. 認証要求に含める情報の内容を要求します (たとえば、IP アドレス形式によるルーター ID、ドメイン名、電子メールの名称)

c. 認証要求を作成します (PKCS#10 フォーマット)。これには作成した公開キーとその他の入力情報が含まれます。

d. ホスト・マシンへの TFTPs 認証要求

2. 認証の発行 (ルーターの外)

   CA が PKCS#10 の認証要求を受け取ります。CA は、要求を手動で確認し、認証を発行できます。認証には、ルーターの公開キーと要求者が入力した情報が含まれています。CA は、プライベート・キーを使って認証にサインをするので、サインする CA を信じる限り、このサインは信頼できるディジタル情報となります。これで認証を IKE のネゴシエーションに使う準備ができました。(この処理は、ルーター操作の範囲外なので、本書ではこれ以上詳しくは説明しません)。

3. ルーターの認証をダウンロード

   CA が認証を発行すると、PKI はこれをルーターにダウンロードできます。 CA による認証の発行方法によって、PKI は、ダウンロードで TFTP か LDAP を選択します。

   公開キーを操作するには、ルーターの認証に含まれているプライベート・キーや公開キーは、ディジタル・シグニチャーと一致しなければならないことに注意してください。 PKI が認証をルーターにダウンロードするとき、公開キーで作ったプライベート・キーは、ルーター・キーのキャッシュに置いておきます。ダウンロードした認証は、一致するプライベート・キーがなければ役に立ちません。つまり、認証要求を発行したときから認証がダウンロードされるまでは、ルーターのリスタートや再ロード、キャッシュの消去、新たな認証要求などを**してはなりません**。こうしたことを実行すると、キャッシュを実行するルーター内のプライベート・キーを壊してしまいます。

4. CA 認証のダウンロード

   IKE ピアの認証を検証するには、PKI はピアのルート CA 認証を獲得する必要があります。この製品は、単一レベルの CA 操作をサポートします。つまり、IKE エンティティーは、同じ CA に割り当てなければなりません。それぞれの IKE エンティティー (この場合は、それぞれのルーター) は、CA の認証をダウンロードし (TFPT または LDAP を使う)、ピアから受信した認証が正しいことを確認します。

5. 認証の保存と再ロード

   認証、一致するプライベート・キー、CA の認証などをルーターが獲得したら、IKE のネゴシエーションを開始できます。通常、認証は数カ月か数年のあいだ有効なので、認証とプライベート・キーを SRAM に保存しておけば、ルーターを再ロードしたり、リスタートするたびに認証要求をしたり、ダウンロードする必要がありません。今回のバージョンでは、**cert save** と **cert load** のコマンドがあり、これで認証とプライベート・キーを SRAM に保存したり、取り出したりできます。

   ルーターの認証やプライベート・キーは、ペアとして処理することに注意してください (たとえば、認証とプライベート・キーを SRAM へ保存したり、取り出すときは、いつも 2 つまとめて処理するようにします)。

TFTP および LDAP サーバーの情報を構成したり、リスト表示をするには、次の例のように、Talk 6 コマンドを使用してください。

例: サーバーを追加する (T6)

```
Config>f ipsec
IP Security feature user configuration
IPsec config>pki
PKI config>add server
Name ? (max 65 chars) []? test
Enter server IP Address []? 8.8.8.8
Transport type (Choices: TFTP/LDAP)  [TFTP]?
PKI config>
```

例: サーバーの構成をリストに表示する (T6)

```
PKI config>li server

1)  Name: SERVER1
    Type: TFTP
    IP addr: 8.8.8.8


2)  Name: TEST
    Type: TFTP
    IP addr: 8.8.8.8
```

例: ルート認証をリストに表示する (T6)

```
PKI config>li cert

Root CA  certificate:
       SRAM    Name:   R1
       Subject Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
  Default Root Cert:   No

       SRAM    Name:   R2
       Subject Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
  Default Root Cert:   Yes



Router   Certificate:
       SRAM    Name:   B1
       Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
       Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   No

       SRAM    Name:   B2
       Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
       Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   Yes

       SRAM    Name:   B3
       Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
       Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   No

       SRAM    Name:   YYY
       Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
       Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
```

```
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   No
```

例: 認証要求 (T5)

```
PKI Console>cert-req
Enter the following part for the subject name
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? IBM
   Organization Unit Name(Max 32 characters) []? NHD
   Common Name(Max 32 characters) []? router1
Key modulus size
 [512]?
Certificate subject-alt-name type:
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 12.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Memory transfer starting.
.Memory transfer completed - successfully.
Certificate request TFTP to remote host successfully.
Private Key Alias [ROUTER_KEY]? local
Generated private key LOCAL stored into cache
```

例: ルーター認証をリストに表示する (T5)

```
PKI Console>li cert
Router   certificate
      Serial Number:   909343811
       Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
       Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29

Root CA  certificate
      Serial Number:   914034740
       Subject Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
```

例: Cert Save (T5)

```
PKI Console>cert-save
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? yyy
Load as default router certificate at initialization?? [No]:
Private key YYY written into SRAM
Both Certificate and private key saved into SRAM successfully
PKI Console>
```

例: Cert Load (T5)

```
PKI Console>cert-load
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
Name []? yyy
Box certificate and private key saved into cache successfully
PKI Console>
```

手動 IP セキュリティーの使用 (IPv4)

2210, の IPv4 にある IP セキュリティー機能には、ポリシー・フィーチャーやその他の IPSec 関連のプロセスとあわせて、認証、保全性、信頼性、および非否認の特性があります。IPSec を手動で実装するには、ポリシー・データベースに IPSec オプションのサブセットを含むポリシーを予備構成し、手動トンネルのプロファイルと有効期間を定義します。データベースにすべての IPSec オプション (ポリシー) を予備構成すると、ポリシーが使用可能なルーターは、IPSec パケットの送信準備をするときに、ポリシーの内容にしたがって、宛先ルーターと動的にネゴシエーションを行って、IPSec オプションを確立することができます。手動トンネルの定義については、334ページの『手動 IP セキュリティーの構成 (IPv4)』を参照してください。ポリシーのオプションについては、237ページの『第16章 ポリシー・フィーチャーの使用』を参照してください。

手動 IP セキュリティーの使用 (IPv6)

2210 の IPv6 にある IP セキュリティー・フィーチャーには、認証、保全性、および機密性の特性があります。 手動トンネルの定義については、345ページの『手動 IP セキュリティーの構成 (IPv6)』を参照してください。

第19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、そして 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。 IPv4 については、237ページの『第16章 ポリシー・フィーチャーの使用』と 275ページの『第17章 ポリシー・フィーチャーの構成と監視』に、IP セキュリティー・ポリシーの構成と監視について追加説明があります。この章には、以下の節が含まれています。

- 『インターネット・キー・エクスチェンジの構成 (IPv4)』
- 330ページの『公開キー・インフラストラクチャーの構成 (IPv4)』
- 330ページの『認証の取得』
- 331ページの『公開キー・インフラストラクチャーの構成コマンド』
- 334ページの『手動 IP セキュリティーの構成 (IPv4)』
- 334ページの『IP セキュリティー構成環境へのアクセス』
- 335ページの『手動 IP セキュリティー構成コマンド』
- 344ページの『手動トンネルの構成 (IPv4)』
- 345ページの『手動 IP セキュリティーの構成 (IPv6)』
- 346ページの『IP セキュリティー構成環境へのアクセス』
- 346ページの『手動 IP セキュリティー構成コマンド』
- 347ページの『手動トンネルの構成 (IPv6)』
- 350ページの『手動 IP セキュリティーの監視 (IPv4)』
- 362ページの『手動 IP セキュリティーの監視 (IPv6)』
- 362ページの『IP セキュリティー動的再構成サポート』

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フィーチャーを使用することが必要です。詳細については、10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 トラフィック用の 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。

インターネット・キー・エクスチェンジの構成 (IPv4)

この節では、インターネット・キー・エクスチェンジ (IKE) の構成方法を説明します。

IPSec トンネルを確立する前に、以下のことをします。

1. トンネルを使用するパケットの属性と実行すべきアクションを構成する (ポリシー)。
2. 必要な暗号化および認証のオプションを構成する。

これらの作業については、237ページの『第16章 ポリシー・フィーチャーの使用』、 275ページの『第17章 ポリシー・フィーチャーの構成と監視』、および330ページの『公開キー・インフラストラクチャーの構成 (IPv4)』を参照してください。

公開キー・インフラストラクチャーの構成 (IPv4)

この節では、公開キー・インフラストラクチャー (PKI) の使用方法を説明します。

IPSec トンネルを確立する前に、以下のことをします。

1. 公開および秘密の暗号キーのペアを作り、信頼できる認証局 (CA) のディジタル認証を取得する。詳しくは、『認証の取得』を参照してください。
2. ルーターにポリシーを構成しますが、このルーターに使用する IPSec アルゴリズム、SA、その他のオプションを決める。詳しくは、323ページの『IP セキュリティー・トンネルのネゴシエーション』およびこの章の各節を参照してください。
3. IKE とポリシー・データベースを構成する。詳しくは、329ページの『インターネット・キー・エクスチェンジの構成 (IPv4)』、237ページの『第16章 ポリシー・フィーチャーの使用』、および 275ページの『第17章 ポリシー・フィーチャーの構成と監視』を参照してください。

認証の取得

IPSec トンネルを設定する前に、324ページの『公開キー・インフラストラクチャーの使用』で説明した信頼できる認証局を選択し、登録する必要があります。CA は、サイン入りの X.509 ディジタル認証を戻してきます。これにより、ネットワークの相手にこちらを確認してもらうことができます。認証には、コード化されたディジタル ID と公開および秘密の暗号キーのペアが含まれています。以下のことをしてください。

1. CA とサーバー・アドレスを見付ける。
2. 331ページの『公開キー・インフラストラクチャーの構成コマンド』に説明されている PKI Talk 6 **add ldapserver** または **add tftpserver** コマンドを使って、認証リポジトリー (保管庫) 検索オプションを構成する。
3. 353ページの『公開キー・インフラストラクチャー監視コマンド』に説明されている PKI Talk 5 **certificate request** を使って公開キーとプライベート・キーのペアを作る。これは、ルーター内またはリモートで実行できます。たとえば、バーチャル・プライベート・ネットワーク (VPN) の管理者であれば、キーのペアを暗号化して、ルーターに確実に転送できます。
4. 353ページの『公開キー・インフラストラクチャー監視コマンド』に説明されている PKI Talk 5 **certificate request** コマンドを使って、 CA に初期要求を提出します。要求は、PKCS#10 メッセージとして、電子メールか FTP で送ります。CA は、キーのペアを認証にバインドし、CA のプライベート・キーを使ってサインをします。そして、これを中央保管所 (LDAP または FTP) に保管するか、あるいは PKCS#7 メッセージで要求を請求した人のところに返却します。通常、認証は数カ月以上有効で、そのあとは更新します。認証は、ネットワークで信頼できる相手を識別できます。
5. 353ページの『公開キー・インフラストラクチャー監視コマンド』に説明のある PKI Talk 5 **certificate save** コマンドを使って、認証をルーターの SRAM に保存します。

注:

1. 『公開キー・インフラストラクチャーの構成コマンド』に説明のある PKI Talk 6 **list certificate** コマンドを使って、SRAM の認証記録リストを表示します。
2. SRAM の認証記録を削除するには、『公開キー・インフラストラクチャーの構成コマンド』に説明のある PKI Talk 6 **delete certificate** コマンドを使います。
3. 今後の IPSec ネゴシエーションで、認証要求の発信を省くには、353ページの『公開キー・インフラストラクチャー監視コマンド』に説明のある PKI Talk 5 **certificate load** コマンドを使って、受信した認証をキャッシュにロードします。

公開キー・インフラストラクチャーの構成コマンド

Add

PKI Talk 6 **add** コマンドは、認証保管サーバーとその位置を構成するときに使用します。

構文:

add server

server サーバーのための追加操作であることを指定します。

例 1: サーバーの追加

```
PKI config>add server
Name ? (max 65 chars) []? myldap
Enter server IP Address []? 8.8.8.9
Transport type (Choices: TFTP/LDAP)  [TFTP]? ldap
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
LDAP version [2]?
Bind to the server anonymously? [No]:
Enter your bind DN: []? c=us o=ibm
Enter your bind PW: []? testldap
```

Change

PKI Talk 6 **change** コマンドは、認証保管サーバーとその位置を変更するときに使用します。

構文:

change server

server サーバーのための追加操作であることを指定します。

例 1: サーバーの変更

```
PKI config>change server
Name []? myldap
Enter server IP Address []? 8.8.8.7
Server type will continue to be LDAP
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
```

```
LDAP version [2]?
Enter your bind DN: [c=us o=ibm]?
Enter your bind PW: [testldap]?
```

Delete

PKI Talk 6 **delete** コマンドは、ルーターの SRAM から認証記録やプライベート・キーを削除するとき、およびサーバーを削除するときに使用します。

構文:

delete certificate
private-key
server

certificate

1 つ以上の認証記録を削除することを指定します。

all すべての認証記録を削除することを指定します。

id 削除する認証の ID を指定します。

例 1: 認証の削除

```
PKI config>delete certificate
Cert Name []? test
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Box Certificate [TEST] deleted successfully
Corresponding private Key [TEST] deleted successfully
```

例 2: プライベート・キーの削除

```
PKI config>delete private-keys
Private Key Name []? test
Private Key [TEST] deleted successfully
Corresponding box certificate [TEST] deleted successfully
```

例 3: サーバー記録の削除

```
PKI config>delete server
Name []? myldap
Server MYLDAP deleted successfully
```

private-key

1 つ以上のプライベート・キー記録を削除する操作であることを指定します。

server サーバーを削除する操作であることを指定します。

List

PKI Talk 6 **list** コマンドは、ルーターの SRAM にある認証やキーの記録をリストにして表示したり、認証取り消しリスト (CRL--認証が取り消された、ISAKMP を使う通信者のリスト) を表示したりするのに使用します。現行の CRL を入手するには、PKI Talk 6 **load** コマンドを使用してください。

構文:

list certificates
crl
private-keys
servers

certificates
認証記録のリスト表示をする操作であることを指定します。

crl 認証取り消しリストのリスト表示をする操作であることを指定します。

private-keys
プライベート・キー記録のリスト表示をする操作であることを指定します。

servers
サーバー記録のリスト表示をする操作であることを指定します。

例: 認証のリスト

```
PKI config>list certificates

Root CA  certificate:
       SRAM    Name:   B
       Subject Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
          Validity:   1998/12/19 2:2:21 -- 2018/12/19 2:32:21
  Default Root Cert:   Yes



Router   Certificate:
       SRAM    Name:   W
      Subject  Name:   /c=US/o=ibm/ou=nhd/cn=testip
      Issuer   Name:   /c=US/o=ibm/ou=nhd
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1999/1/19 23:24:27 -- 2002/1/19 23:54:27
       Default Cert:   No
```

例: crl のリスト

```
PKI config>list crl
```

例: プライベート・キーのリスト

```
PKI config>list private-keys
Private Keys In SRAM:

1) Name W
```

例 : サーバー記録のリスト

```
PKI config>list servers
1)  Name: SERVER1
    Type: LDAP
    IP addr: 1.1.1.2
        LDAP search timeout (secs): 10
        LDAP retry interval (mins): 3
        LDAP server port number: 390
        LDAP version: 2
        Anonymous bind ?: y


2)  Name: TEST
    Type: TFTP
    IP addr: 8.8.8.8
```

Load

PKI Talk 6 **load** コマンドは、最新の認証取り消しリスト (CRL) を CA から取り出すのに使用します。このリストのコピーの有効性を確保するために、定期的に頻繁にこれを行う必要があります。認証時に、IPSec フィーチャーは、CRL の内容に基づいて認証の妥当性検査を行います。

構文:

load crl

手動 IP セキュリティーの構成 (IPv4)

この節では、IPv4 の 手動 IPSec で使用できる構成オプションを説明します。すべての IPSec 機能を IPv4 に適用できます。

IPSec 手動トンネルを構成するには、以下のステップを実行します。
1. IPSec トンネルを作成する。
2. IPSec をリセットする。
3. 手動トンネルのポリシーを構成する (プロファイル、有効期間、ポリシー)。
4. ポリシーをリセットする。

アルゴリズムの構成

表42に示されたアルゴリズムでトンネル・ポリシーを構成できます。

表 42. 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。

トンネル・ポリシーは、アウトバウンド・パケットでローカル・アルゴリズムを使い、インバウンド・パケットではリモート・アルゴリズムを使います。トンネルの近い側のルーターのローカル・アルゴリズムは、トンネルの遠い側にあるルーターのリモート・アルゴリズムと一致しなければなりません。リモート・アルゴリズムの値はオプションですが、デフォルトはローカル・アルゴリズムの値と同じになります。ESP 認証がオプションなので、ローカルの ESP 認証はオプションです。

暗号キーの構成

構成するローカル・アルゴリズムは、リモート・ホストのアルゴリズムと同じキーで構成します。335ページの『手動 IP セキュリティー構成コマンド』の **add tunnel** コマンドで、キーの説明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、OPCON プロンプト (*) で **t 6** を入力してから、`Config>` プロンプトで以下のコマンドを入力してください。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPV4-IPsec config>
```

手動 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。以下のコマンドは IPV4-IPsec config> プロンプトで入力します。

表 43. IP セキュリティー構成コマンドの要約

コマンド	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。 xxxi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、または定義済みのトンネルに関する情報をリストします。
Set	各種の IPSec 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。 xxxiページの『下位レベル操作環境の終了』 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。

構文:

add tunnel ...

tunnel-name

トンネルにラベルを付けるための任意指定パラメーター。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。

省略時値: なし

lifetime

トンネルが活動状態でいられる時間数 (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**必要** 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 アドレスです。

有効値: インターフェースに構成された、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: ルーターに構成された IP アドレスの 1 つ

local-spi

セキュリティー・アソシエーションとは、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 (インバウンドまたはアウトバウンド) 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インバウンド・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インバウンド・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: 255 よりも大きな 32 ビットの数値

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アウトバウンド・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。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。この暗号化アルゴリズムは、リモート側の暗号化アルゴリズムと一致していなければなりません。

ESP-NULL アルゴリズムは、ESP が暗号化を実行するのを防止します。このアルゴリズムは、すべての国で利用可能です。 ESP-NULL を選択した場合は、認証アルゴリズム HMAC-MD5 または HMAC-SHA-1 を選択して、認証を活動化しておく必要があります。

有効値: DES-CBC、CDMF、3DES、または ESP-NULL

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対応キーと一致していなければなりません。ESP-NULL 暗号化アルゴリズムを選択した場合は、このキーは構成しません。

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

アウトバウンド 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。

暗号化アルゴリズムが ESP-NULL の場合は、埋め込みは必要ありません。ESP-NULL アルゴリズムは元のパケット・サイズに 1 バイトを追加するからです。ローカル暗号化の埋め込みを構成した場合、その値は無視されます。

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)。暗号化アルゴリズムが ESP-NULL の場合、認証の指定は必須です。

有効値: Yes または No

デフォルト値: Yes

local-authentication-algorithm

アウトバウンド・パケットで使用される認証アルゴリズム。 ESP の場合、これは任意指定パラメーターで、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。使用す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た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: なし

remote-spi

セキュリティー・アソシエーションとは、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 (インバウンドまたはアウトバウンド) 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・ホストあてのアウトバウンド・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 トンネルのアウトバウンド・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: 255 よりも大きな 32 ビットの数値

デフォルト値: 256

remote-encryption-algorithm

リモート・ホストから受信するインバウンド・パケットで使用される暗号化解除アルゴリズム。これはローカル側の暗号化アルゴリズムと一致していなければなりません。

ESP-NULL アルゴリズムは、ESP が暗号化を実行するのを防止します。ESP-NULL を選択した場合は、認証アルゴリズム HMAC-MD5 または HMAC-SHA-1 を選択して、認証を活動化しておく必要があります。

有効値: DES-CBC、CDMF、3DES、または ESP-NULL

デフォルト値: ローカル側の暗号化アルゴリズムの値

remote-encryption-key
リモート側の 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。 ESP-NULL 暗号化アルゴリズムを選択した場合は、このキーは構成しません。

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、*verification-of-remote-encryption-padding* の値が Yes の場合にのみ必須であり、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
インバウンド・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
インバウンド・パケットに使用される認証アルゴリズム。 ESP の場合、これは任意指定パラメーターで、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。使用す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
リモート側の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 (リモート ESP 認証アルゴリズムが構成されている場合) 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非活動化しなければならないからです。この状態が起きた場合、手動で介入して、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、新規に作成することが必要になります。

また、再生防止が使用可能の場合、**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、シーケンス番号ミスマッチ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

DF-bit トンネル・モードの保護トンネルの外部ヘッダー内の断片化不可 (DF) ビットの扱いを指定します。パケットを断片化できないことを指定するために、IPv4 ヘッダー内にこのビットをセットすることができます。 DF ビット・パラメーターは、着信パケット内の DF ビットの扱い方を 2210 に知らせます。すなわち、内部ヘッダー内に見つかった DF ビットを外部ヘッダーにコピーするか、外部ヘッダーにビットをセットするか、あるいは外部ヘッダー内のビットをクリアするかどうかを指示します。

DF ビットがセットされており、パケットを断片化できない場合、IPSec はパス MTU (PMTU) ディスカバリー機能を使用します。詳細については、319ページの『パス MTU ディスカバリー』を参照してください。

有効値: コピー、セット、クリア

デフォルト値: コピー

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については、**add tunnel** コマンドの項を参照してください。

Delete Tunnel

Talk 6 **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 〜 65535

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 tunnel-name* **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 ～ 65535

デフォルト値: 1

tunnel-name
使用不可に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

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、個別に使用可能にされた IPSec トンネルは活動状態になりません。

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 tunnel-name* **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 ～ 65535

デフォルト値: 1

tunnel-name
使用可能に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

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 (活動および定義済みの両方) 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 (活動および定義済みの両方) が含まれます。活動トンネル (active tunnels) は、現在活動状態のトンネルです。定義済みトンネル (defined tunnels) は、定義されているが活動状態ではないトンネルです。IPv4 では、ルーターの SRAM で選択した認証もリストに表示されます。

構文:

list ...

all
status
tunnel
active *tunnel-id tunnel-name* all
defined *tunnel-id tunnel-name* all

例 1: すべての IPSec トンネルのリスト

```
IPsec config>list all

IPsec is ENABLED

IPsec Path MTU Aging Timer is 20 minutes

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      ******************
```

例 2: ESP ポリシーと ESP-NULL アルゴリズムを使用する IPSec トンネルのリスト

```
IPsec config>li tun 1000

Tunnel  Name             Mode   Policy   Life   Replay  Rcv  IPsec  State
ID                                              Prev    Win  Vers
------  ---------------  -----  ------  ------  ------  ---  -----  --------
1000    t1000            TUNN   ESP      46080    No    ---   V2    Enabled

Handling of DF bit in outer header:  COPY

Local Information:

      IP Address: 10.11.12.10
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:  1234    Encryption Algorithm: NULL
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: HMAC-MD5
Remote Information:

      IP Address: 10.11.12.11
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:  1234    Encryption Algorithm: NULL
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: HMAC-MD5
```

Set

set コマンドは、トンネル PMTU 値を制御するのに使用します。

構文:

set

path-mtu-age-timer

path-mtu-age-timer

2210 がトンネル PMTU 値を最大値への復元を実行するまでの時間を (分) 指定します。

デフォルト値: 10 (0 は使用不可を意味する)

手動トンネルの構成 (IPv4)

この節では、321ページの図27に示されたネットワークを使って、手動 IPv4 トンネルの構成方法を説明します。

ルーター A のトンネルの構成

次の例では、321ページの図27のネットワークで、IPv4 を使ってルーター A に IPSec 手動トンネルを構成する方法が示されています。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPV4-IPsec config>add tunnel
Adding tunnel 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]:
Copy, set, or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-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は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 B のトンネルの構成

ルーター A に構成した IPSec トンネル 1 と同じ IPSec 手動トンネルをルーター B の中にも構成します。ルーター B のこのトンネルの IP アドレスは、223.252.252.210 で、リモートの 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。

例: ESP を使った IP セキュリティー・トンネルの手動構成

トンネルがトンネル・モードにあり、トンネル・ポリシーが ESP である場合、DF ビットをセットするように求めるプロンプトが出ます。この例には、IPSec トンネルの構成のみを示します (パケット・フィルターの構成は示しません)。

```
IPV4-IPsec config>add tunnel
Adding tunnel 2
Tunnel Name (optional)? tunneltwo
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? [No]:
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0.0.0.0]?
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? [No]:
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>
```

例: ESP-Null を使った IP セキュリティー・トンネルの手動構成

認証が必要であることに注意してください。

```
IPV4-IPsec config>add tunnel
Adding tunnel 3
Tunnel Name (optional)? tunnel3
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]? 1234
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 10.11.12.11
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>
```

手動 IP セキュリティーの構成 (IPv6)

この節では、IPv6 の 手動 IPSec にある構成オプションを説明します。IPv6 には、すべての IPSec 機能が適用されます。IPv6 用の IPSec を構成する場合は、IPSec 構成の質問が次のように変更されるので注意してください。

- IPv6 アドレス形式でアドレスを入力します (たとえば、8:0:9:8::1)。
- DF ビットの設定についての問い合わせはありません。

IPSec 手動トンネルを構成するには、以下のステップを実行します。

1. IPSec トンネルを作成する。
2. IPSec をリセットする。

3. フィルター規則を構成する。
4. IPV6 をリセットする。

アルゴリズムの構成

表44のアルゴリズムを使って、トンネル・ポリシーを構成できます。

表 44. 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。

トンネル・ポリシーは、アウトバウンド・パケットでローカル・アルゴリズムを使い、インバウンド・パケットではリモート・アルゴリズムを使います。トンネルの近い側のルーターのローカル・アルゴリズムは、トンネルの遠い側にあるルーターのリモート・アルゴリズムと一致しなければなりません。リモート・アルゴリズムの値はオプションですが、デフォルトはローカル・アルゴリズムの値と同じになります。ESP 認証がオプションなので、ローカルの ESP 認証はオプションです。

暗号キーの構成

構成するアルゴリズムは、リモート・ホストのアルゴリズムと同じキーで構成します。335ページの『手動 IP セキュリティー構成コマンド』の **add tunnel** コマンドで、キーの説明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、OPCON プロンプト (*) で**t 6** を入力してから、`Config>` プロンプトで以下のコマンドを入力してください。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-IPsec config>
```

手動 IP セキュリティー構成コマンド

IPv6 で使用できる IP セキュリティーの構成コマンドについては、335ページの『手動 IP セキュリティー構成コマンド』を参照してください。IPv6 のコマンドは、とくに指定がない限り IPv4 と同じです。コマンドは、`IPV6-IPsec config>` プロンプトで入力します。

手動トンネルの構成 (IPv6)

この節を読むときには、321ページの図27のネットワーク例を参照してください。 IPSec トンネル 1 の終了点は、ルーター A のインターフェース 1 上にあります。 ルーター A は、IPsec 用に構成します。ルーター A を手動で構成するには、以下のステップを実行します。

1. IPSec トンネルを作成する。
2. IPSec トンネルの終了点であるルーター・インターフェース上に、1 つのアウトバウンド・パケット・フィルターを作成する。
3. パケット・フィルターのアクセス制御規則を作成する。
4. IPSec をリセットする。
5. IPv6 をリセットする。

ルーター A に IP セキュリティー・トンネルを作成する

次の例は、ルーター A に IPSec トンネル 1 を作る方法を示しています。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-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 [1000:1::1]? 2000::A
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]? 2000::B
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]:
IPV6-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は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 に IPSec トンネルを作成したあと、1 つの IP パケット・フィルターを設定する必要があります。下の例は、パケット・フィルター *out-router-A* の作成方法を示しています。 IPv6 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 IPv6 使用の章の IPv6 フィルターおよび アクセス制御の項を参照してください。

```
* talk 6
Config> Protocol IPv6
Internet protocol user configuration
IPv6 Config> set access-control on
IPv6 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
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config>
```

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。アウトバウンド・パケット・フィルター *out-router-A* に 2 つのアクセス制御規則を作ります。

アウトバウンド・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 トンネルに渡す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 トラフィックを渡すことを許可します。

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、パケットをネットワーク 1000:1:: からルーター B が取り付けられた宛先ネットワーク 3000:1:: に送ります。

```
IPv6 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]? 1000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 3000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
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 つのエンド間で保護パケットを渡すことを許可します。

```
Packet-filter 'out-router-A' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::A
Prefix Length [64]? 64
Internet destination [0::0]? 2000::B
Prefix Length [64]? 64
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可能です。

ルーター A の IP セキュリティーと IP をリセットする

ポリシーの構成ができたら、Talk 5 **reset ipsec** コマンドを使って、新しい IPSec 構成を SRAM に再ロードします。 **reset ipsec** コマンドは、IP の構成内容には影響しません。次に、Talk 5 **reset ipv6**コマンドを使って、ルーター内で IPv6 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。IPSec と IPv6 をリセットするか、ルーターをリスタートして、フィルター規則を再ロードします。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。詳しくは、 *プロトコルの構成*

*と監視 解説書第 2 巻*の 329ページの『第19章 IP セキュリティーの構成および監視』と**reset ipv6**コマンドを参照してください。

321ページの図27に示されているように、IPSec トンネル 2 には、ルーター B のインターフェース 1 に終了点があります。以下のステップにしたがって、ルーター B を手動で構成します。

1. IPSec トンネルを作成する。
2. IPSec トンネルの終了点であるルーター・インターフェース上に、1 つのアウトバウンド・フィルターを作成する。
3. パケット・フィルターのアクセス制御規則を作成する。
4. IPSec をリセットする。
5. IPv6 をリセットする。

ルーター B に IP セキュリティー・トンネルを作成する

ルーター B 内に、ルーター A に作成したのと同じ IPSec トンネル (IPsec トンネル 2) を作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 2000::B で、リモート IP アドレスは 2000::A 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 に指定されたパラメーターと一致し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 で実行したのと同様に、インターフェース 1 のアウトバウンド・パケット・フィルター (*out-router-B*) を構成します。インターフェース 1 は、IPSec トンネル 1 の終了点となるルーター B のインターフェースです。

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

*out-router-B*のアクセス制御規則を構成して、アウトバウンド・パケットをネットワーク 3000:1:: から IPSec に渡して、IPSec トンネル 2 で処理と転送を行います。このアクセス制御は、タイプ I および S です。

```
Packet-filter name [ ]? out-router-B
Packet-filter 'out-router-B' Config> add access
Enter type [E]? IS
Internet source [0::0]? 3000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 1000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
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 2 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]? 2000::B
Prefix Length [64]? 64
Internet destination [0::0]? 2000::A
Prefix Length [64]? 64
Packet-filter 'out-router-B' Config>
```

out-router-B に対して、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 2 あて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 IP セキュリティーと IPv6 をリセットする

IPSec 機能が活動し、フィルターをアクティブにする前に、IPSec と IPv6 をリセットする必要があります。talk 5 **reset IPSec** コマンドを使ってIPSec と IPv6 をリセットします。IPsec のリセットについては、348ページの『ルーター A の IP セキュリティーと IP をリセットする』を参照してください。IPSec をリセットしてから、talk 5 **reset IPv6**コマンドで IPv6 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。

例: ESP を使った IP セキュリティー・トンネルの構成

この例には、IPSec トンネルの構成のみを示します (パケット・フィルターの構成は示しません)。

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? (Yes or [No]):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? (Yes or [No]):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No][No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

例: ESP と ESP-NULL を使った IP セキュリティー・トンネルの手動構成

認証が必要であることに注意してください。

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP 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]:
IPV6-IPsec config>
```

手動 IP セキュリティーの監視 (IPv4)

この節では、手動 IPSec を IPv4 で構成する方法を説明します。インターネット・キー・エクスチェンジ環境にアクセスする方法と使用可能なコマンドを説明します。

インターネット・キー・エクスチェンジ環境へのアクセス

この節では、IPv4 でのインターネット・キー・プロトコル (IKE) の使用方法を説明します。

IP セキュリティー IKE 監視環境にアクセスするには、**+** プロンプトで、以下のコマンドを入力してください。

```
+ feature ipsec
IPSP>ike
IKE>
```

コマンド・キー・エクスチェンジ監視コマンド

この節では、IKE 監視コマンドについて説明します。

表 45. IKE 監視コマンドの要約

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。
Delete	特定のトンネルの ISAKMP フェーズ 1 SA、またはすべてのフェーズ SA を削除します。
List	特定のトンネルのフェーズ 1 SA、またはすべてのフェーズ SA に関する情報をリストにして表示します。
Stats	トンネルの統計情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Delete

IKE **delete** コマンドは、ある 1 つのトンネルのフェーズ 1 SA、またはすべてのフェーズ 1 の SA を動的に削除します。

構文:

delete tunnel
all

tunnel 特定のトンネルのフェーズ 1 SA を削除することを指定します。

all すべてのフェーズ 1 SA を削除することを指定します。

例: トンネルの削除

```
PKI config>delete tunnel
Peer address [10.0.0.3]?
```

List

IKE **list** コマンドは、特定のトンネルのフェーズ 1 SA、またはすべての SA に関する情報を表示します。

構文:

list tunnel
all

tunnel 特定のトンネルの SA に関する情報を表示するように指定します。

all すべての SA に関する情報を表示するように指定します。

例: すべての SA に関する情報を表示する

```
IKE>list all

Phase 1 ISAKMP Tunnels for IPv4:
-------------------------------------------------------------
 Peer Address    I/R  Mode  Auto    State         Auth
--------------  ---  ----  ----  ----------  ------------
       10.0.0.3   R   Aggr   N    QM_IDLE       pre-shared


IKE>list tunnel 10.0.0.3

                    Peer IKE address: 10.0.0.3
                   Local IKE address: 10.0.0.1
                                Role: Responder
                            Exchange: Aggr
                           Autostart: No
                        Oakley State: QM_IDLE
              Authentication Method: Pre-shared Key
               Encryption algorithm: des3
                      Hash function: md5
               Diffie-Hellman group: 1
                  Refresh threshold: 85
                    Lifetime (secs): 15000
```

Stats

IKE **stats** コマンドは、トンネルの統計を表示します。

構文:

stats tunnel

tunnel トンネルの SA に関する統計を表示します。

有効値: 構成されたトンネルの名前または ID

例: トンネルの SA 統計を表示する

```
IKE>stats

Peer address [10.0.0.3]?

    Peer IP address......:        10.0.0.3
    Active time (secs)...:             187

                                        In              Out
                                       ---              ---
    Octets..............:            1229             1248
    Packets.............:              14               16
    Drop pkts...........:               0                1
    Notifys.............:               6                0
    Deletes.............:               0                0
    Phase 2 Proposals...:              16               18
    Invalid Proposals...:               0
    Rejected Proposals..:               0                0
```

公開キー・インフラストラクチャー環境へのアクセス (IPv4)

この節では、IPv4 を使った公開キー・インフラストラクチャー (PKI) の使用方法を説明します。

IP セキュリティー PKI 監視環境にアクセスするには、**+**プロンプトで、以下のコマンドを入力してください。

```
+ feature ipsec
IPSP>pki
PKI>
```

公開キー・インフラストラクチャー監視コマンド

この節では、公開キー・インフラストラクチャー (PKI) の監視コマンドを説明します。

表 46. PKI 監視コマンドの要約

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。
Cert-load	認証をルーターの SRAM にロードします。
Cert-req	認証要求を CA に発信します。
Cert-save	今後の利用のため、認証をキャッシュに保存します。
List certificate	認証に関する情報を表示します。
List configured-servers	構成済みのサーバーに関する情報を表示します。
Load certificate	認証記録を SRAM からランタイム・キャッシュにロードします。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Cert-load

PKI **cert-load** コマンドは、認証とプライベート・キーの記録を SRAM からランタイム・キャッシュにロードします。

構文:

cert-load

例: 認証記録を SRAM からキャッシュにロードする

```
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
Name []? test
mystr=1.1.1.1
Box certificate and private key saved into cache successfully
```

Cert-req

PKI **cert-req** コマンドは、CA に認証を要求します。

構文:

cert-req

例: CA に認証を要求する

```
Enter the following part for the subject name
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? ibm
   Organization Unit Name(Max 32 characters) []? nhd
   Common Name(Max 32 characters) []?
Key modulus size (512|768|1024)
 [512]?
Certificate subject-alt-name type:
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 1.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
```

```
Enter tftp server IP Address []? test
Bad address, try again
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Certificate request TFTP to remote host successfully.
```

Cert-save

PKI **cert-save** コマンドは、認証とプライベート・キーの記録を SRAM に保存します。

構文:

cert-save

例: 認証記録を SRAM に保存する

```
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? test
Load as default router certificate at initialization? [No]:
Private key TEST written into SRAM
Both Certificate and private key saved into SRAM successfully
```

List Certificate

PKI **list certificate** コマンドは、X.509 ディジタル認証に関する情報を表示します。

構文:

list certificate

例: 認証情報を表示する

```
Router   certificate
      Serial Number:   914034877
      Subject  Name:   /c=US/o=ibm/ou=nhd/cn=testip
      Issuer   Name:   /c=US/o=ibm/ou=nhd
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1999/1/19 23:24:27 -- 2002/1/19 23:54:27
```

List Configured-servers

PKI **list configured-servers** コマンドは、構成したサーバーに関する情報を表示します。

構文:

list configured-servers

例: 構成したサーバーの情報を表示する

```
1)  Name: SERVER1
    Type: LDAP
    IP addr: 0.0.0.0
        LDAP search timeout (secs): 0
        LDAP retry interval (mins): 0
        LDAP server port number: 0
        LDAP version: 0
        LDAP version: 0
        Anonymous bind ?: y


2)  Name: TEST
    Type: TFTP
    IP addr: 9.9.9.9
```

```
3)  Name: TFTP
    Type: TFTP
    IP addr: 2.2.2.2
```

Load Certificate

PKI **load certificate** コマンドは、SRAM からランタイム・キャッシュに認証をロードします。

構文:

load certificate

例: 認証をキャッシュにロードする

```
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]?
Server info name []? test
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /tmp/test.cert

Attempting to load certificate file. Please wait ...
Router Certificate  loaded into run-time cache
```

IP セキュリティー監視環境へのアクセス (IPv4)

IPv4 IP セキュリティー監視環境へアクセスするには、OPCON プロンプト (*) で **t 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで、以下のコマンドを入力します。

```
+ feature ipsec
IPSP>ipv4
IPV4-IPsec>
```

IP セキュリティー監視コマンド (IPv4)

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。

表 47. IP セキュリティー監視コマンドの要約

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。
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。
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。

表 47. 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
Itp	IP セキュリティー・トンネル PING。 IPSec トンネルの遠端の通信者にコンタクトできるかどうかを判別します。
List	IP セキュリティーに関する総合情報、およびアクティブな定義済みのトンネルに関する総合情報を表示します。
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。
Set	パス MTU (PMTU) 経時タイマーを動的に設定します。
Stats	すべてのトンネルまたは活動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。 xxxiページの『下位レベル操作環境の終了』 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 ...

パラメーターについては、335ページの『手動 IP セキュリティー構成コマンド』の **add tunnel** コマンドの説明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 ～ 65535

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・プロトコルを動的に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 ～ 65535

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、個別に使用可能にされた IPSec トンネルは活動状態になりません。

注: IPSec を使用不可にしてルーターをリスタートすると、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 ～ 65535

デフォルト値: 1

all すべてのトンネル

Itp

itp コマンド (IPSec トンネル PING) は、IPSec トンネル上で特殊な IP パケットを作成し、送信するのに使用します。これは、トンネルの遠端にあるルーターが、パケットを戻すことによって応答できることを確認します。 **Enter** を押してコマンドを終了するまで、rate 引き数で指定された頻度で、パケットは繰り返し送信されます。**Enter** を押すと、itp は、送信したすべてのパケットの状況を印刷します。

注: itp コマンドは、トンネル・モードで動作しているトンネルに対してのみ作動します。もう一方のルーターは、IP 転送機能を備えている必要があり、使用可能になっていなければなりません。

構文:

itp tunnel-id
size
rate

tunnel-id
必須。特定のトンネルに割り当てられた 2 バイト整数値

size オプション。PING パケットのデータ・ペイロードのサイズ。この値は、itp によって作成された最小サイズより大きく、トンネルの MTU 値より小さい値でなければなりません。

rate オプション。PING データ・パケットが送信される頻度 (秒数)

デフォルト値: 1

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 (活動および定義済みの両方) 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 (活動および定義済みの両方) が含まれます。活動トンネル (active tunnels) は、現在活動状態のトンネルです。定義済みトンネル (defined tunnels) は、定義されているが活動状態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: すべての定義済みトンネルのリスト

```
IPV4-IPsec>LIST TUNNEL DEFINED
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

Defined Tunnels for IPv4:
------------------------------------------------------------------------------
   ID     Type    Local IP Addr   Remote IP Addr   Mode    State
 ------  ------  ---------------  ---------------  -----  --------
      3  ISAKMP       211.0.1.17        211.0.5.2  TUNN   Enabled
```

```
      4  ISAKMP       211.0.1.17        211.0.5.3  TUNN   Enabled
      5  ISAKMP       211.0.1.17        211.0.5.4  TUNN   Enabled


Defined Manual Tunnels for IPv6:
--------------------------------------------------------------------------------
IPV4-IPsec>
```

例: 1 つの定義済みトンネルのリスト

```
IPV4-IPsec>LIST TUNNEL DEFINED
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 1

Tunnel    Type     Mode   Policy    Life    Replay     State
  ID                                                                  Prev
------    ------  -----   ------   -----   -------     ---------     -----------
     1    ISAKMP   TUNN      ESP       0        No     Enabled


Tunnel Name: ---------------

Local (Outbound) Information:
      IP Address: 211.0.1.17
  Authentication:  SPI: ----------          Algorithm: --------
      Encryption:  SPI: 2305164930    Encryption Algorithm: DES-CBC
                                                Extra Pad:   0
                               ESP Authentication Algorithm: HMAC-MD5

Remote (Inbound) Information:
      IP Address: 211.0.5.3
  Authentication:  SPI: ----------          Algorithm: --------
      Encryption:  SPI: 2661613010    Encryption Algorithm: DES-CBC
                                             Verify Pad?:  No
                               ESP Authentication Algorithm: HMAC-MD5
IPV4-IPsec>
```

例 1: すべての活動トンネルのリスト

```
IPV4-IPsec>LIST TUNNEL ACTIVE
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

Tunnel Cache for IPv4:
--------------------------------------------------------------------------------
 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
----   -------------   --------------   ----   --------    ------------------
  1       211.0.1.17      211.0.5.214   TUNN        ESP                  none
  2       211.0.1.17      211.0.5.215   TUNN        ESP                  none
  3       211.0.1.17       211.0.5.41   TUNN        ESP                  none


Tunnel Cache for IPv6:
--------------------------------------------------------------------------------
IPV4-IPsec>
```

例: 1 つの活動トンネルのリスト

```
IPV4-IPsec>LIST TUNNEL ACTIVE 1
                              Tunnel ID: 1
                          Tunnel Name: ---------------
                                 Type: ISAKMP
                                 Mode: TUNN
                               Policy: ESP
                          Replay Prevention: No
                            Tunnel LifeTime: 0 secs
                          Tunnel Expiration: None
                                 PMTU: n/a
                              Tunnel State: Enabled
```

```
                              DF bit handling: COPY
                                  SA State: Working
                               SA LifeTime: 360 secs
                               SA LifeSize: 50000 KBytes
                              SA Threshold: 85 percent
Local (Outbound) Information:
        IP Address: 211.0.1.17
    Authentication:  SPI: ----------              Algorithm: --------
        Encryption:  SPI: 2861614221   Encryption Algorithm: DES-CBC
                                                  Extra Pad:   0
                                  ESP Authentication Algorithm: HMAC-MD5

Remote (Inbound) Information:
        IP Address: 211.0.5.41
    Authentication:  SPI: ----------              Algorithm: --------
        Encryption:  SPI: 2266666369   Encryption Algorithm: DES-CBC
                                                Verify Pad?:  No
                                  ESP Authentication Algorithm: HMAC-MD5
IPV4-IPsec>
```

2 これは IPv6 アドレスです。 IP バージョンが IPv4 の場合、DF ビットの扱い方 (COPY、SET、または CLEAR) を定義するメッセージが表示されます。

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アクティブにします。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 ～ 65535

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

Set

パス MTU (PMTU) 経時タイマーを動的に設定します。

構文:

set path

path このパラメーターは、2210 がトンネル MTU を最大値に戻すまでの経過時間 (分) を定義します。

デフォルト値: 10 (0 は使用不可を意味する)

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 〜 65535

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:

```
IPV6-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
```

手動 IP セキュリティーの監視 (IPv6)

この節では、手動 IPSec を IPv6 で構成する方法を説明します。IP セキュリティー環境にアクセスする方法と使用可能なコマンドを説明します。

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 プロンプト (*) で **t 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで、以下のコマンドを入力します。

```
+ feature ipsec
IPSP>ipv6
IPV6-IPsec>
```

IP セキュリティー監視コマンド (IPv6)

IPv6 の IP セキュリティー監視コマンドは、とくに指定がない限り IPv4 と同じです。コマンドについては、355ページの『IP セキュリティー監視コマンド (IPv4)』を参照してください。 IPV6-IPsec> プロンプトでコマンドを入力します。

IP セキュリティー動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

IP セキュリティー (IPSec) は、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、IPSec には適用されません。IPSec は、個々のインターフェースから独立しています。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、IPSec には適用されません。IPSec は、個々のインターフェースから独立しています。

GWCON (Talk 5) 構成要素リセット・コマンド

IPSec は、次の IPSec 固有の GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature IPSec, Ipv4, Reset IPSec コマンド

説明: IPSec が再初期化されます。

ネットワークの影響:

IPSec がリセットされると、すべてのトンネルが失われます。手動トンネルが、SRAM から再作成されます。ネゴシエーションされたトンネルは消えます。これにより、これらのトンネルを使用するトラフィックは、ただちに停止します。

制限: なし。

次の表は、**GWCON, feature IPSec, ipv4, reset IPSec** コマンドが起動されるときにアクティブになる、IP セキュリティー・フィーチャーの構成変更を要約しています。

GWCON, feature ipsec, ipv4, reset ipsec コマンドによって変更がアクティブになるコマンド
CONFIG, feature ipsec, ipv4, enable tunnel
CONFIG, feature ipsec, ipv4, disable tunnel
CONFIG, feature ipsec, ipv4, disable ipsec
CONFIG, feature ipsec, ipv4, add tunnel
CONFIG, feature ipsec, ipv4, delete tunnel
CONFIG, feature ipsec, ipv4, change tunnel

GWCON, Feature IPSec, Ipv4, Reset Tunnel コマンド

説明: 1 つのトンネルまたはすべてのトンネルが再初期化されます。

ネットワークの影響:

1 つのトンネルまたはすべてのトンネルが、リセットされます。手動トンネルが、SRAM から再作成されます。ネゴシエーションされたトンネルは消えます。これにより、これらのトンネルを使用するトラフィックは、ただちに停止します。

制限: なし。

次の表は、**GWCON, feature IPSec, ipv4, reset tunnel** コマンドが起動されるときにアクティブになる、IP セキュリティー・フィーチャーの構成変更を要約しています。

GWCON, feature ipsec, ipv4, reset tunnel コマンドによって変更がアクティブになるコマンド
CONFIG, feature ipsec, ipv4, add tunnel
CONFIG, feature ipsec, ipv4, delete tunnel
CONFIG, feature ipsec, ipv4, change tunnel
CONFIG, feature ipsec, ipv4, disable tunnel

GWCON (Talk 5) 一時変更コマンド

IPSec は、装置の操作状態を一時的に変更する次の GWCON コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、常にこれらの変更は失われます。

コマンド
GWCON, feature ipsec, ipv4, change tunnel **注:** トンネルのパラメーターをメモリー内で変更できます。
GWCON, feature ipsec, ipv4, disable tunnel **注:** 1 つのトンネルまたはすべてのトンネルを使用不可にすることができます。これらのトンネルのトラフィックは、停止します。
GWCON, feature ipsec, ipv4, disable IPSec pass **注:** IPSec が使用不可になり、トラフィックはセキュリティーなしに転送されます。
GWCON, feature ipsec, ipv4, disable IPSec stop **注:** IPSec が使用不可になり、トラフィックが廃棄されます。
GWCON, feature ipsec, ipv4, delete tunnel **注:** 1 つまたはすべてのトンネルを削除します。これらのトンネルのトラフィックは、除去されます。
GWCON, feature ipsec, ipv4, enable tunnel **注:** 1 つまたはすべてのトンネルを使用可能にします。これらのトンネルのトラフィックは、許可されます。
GWCON, feature ipsec, ipv4, enable IPSec **注:** IPSec を使用可能にします。IPSec はトラフィックを処理できます。
GWCON, feature ipsec, ipv4, set path-MTU-age-timer **注:** パス MTU 経時タイマーを変更します。

動的再構成不能コマンド

次の表は、動的に変更できない IP セキュリティー・フィーチャーの構成コマンドを記述しています。これらのコマンドを活動化するには、装置を再ロードまたはリスタートする必要があります。

コマンド
CONFIG, enable ipsec **注:** 装置が初期化された後、IPSec が初めて使用可能になる場合、装置を再ロードまたはリスタートする必要があります。

第20章 ディファレンシエーテッド・サービス・フィーチャーの使用

この章では、ディファレンシエーテッド・サービス (差別化サービス) (DiffServ) フィーチャーの使用方法を説明します。この機能を使うと、IP データ・パケットを割り当てるときにルーターで優先サービスを使えます。ルーターは、IP ヘッダーに含まれる情報をもとに、ポリシー・データベースの構成内容 (ポリシー・フィーチャーで作成) とパケットを突き合わせて、パケットを分類します。詳しくは、237ページの『第16章 ポリシー・フィーチャーの使用』を参照してください。その結果、特定のパケットに優先サービスが提供されます。本章には、以下の節が含まれています。

ディファレンシエーテッド・サービスの概要

IP ネットワークにインストールされた今日のほとんどの転送装置は、データ・パケットに対して、先入れ先だしをベースとした標準的なベストエフォート送達サービスを行っています。ほとんどのトラフィックは、この送達方式で充分ですが、特定のパケットについて高速で早期に送達する新しい方式が登場しています。

ディファレンシエーテッド・サービス (DiffServ) フィーチャーは、ルーターが IP パケットの転送を処理するときに、そのパケットにさまざまなレベルのサービスを提供します。 DiffServ は、システム資源 (バッファー) を確保して、一部のパケットに資源 (帯域幅) をリンクすることで、優先サービスを提供します。 DiffServ には分類機能があり、IP 発信元アドレスと宛先アドレスおよびポート番号の範囲、プロトコルの種類、着信 DS (TOS) バイトなど、IP ヘッダーのさまざまなフィールドを調べて、IP パケットに与えられたサービスの種類を判別します。この処理をスケーラブルに行うため、それぞれのフローが各ストリームにまとめられます。ストリームはエンティティーですが、このエンティティーを通して、DiffServ はバッファーと帯域幅へのアクセスを管理します。 図28 は、パケット・ストリームに対する DiffServ の処理を示しています。

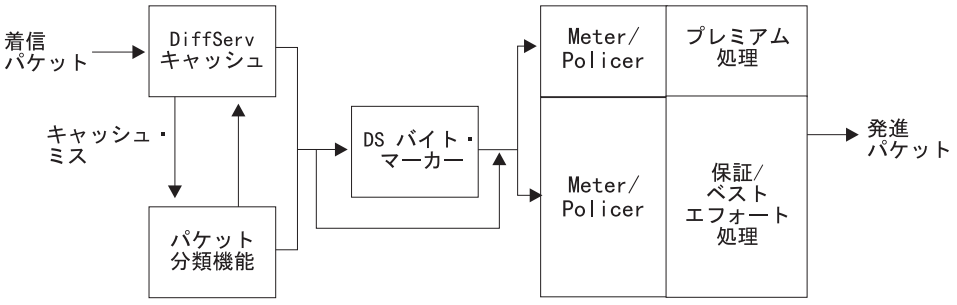


図 28. DiffServ データ・パケットのパス

DiffServ は、通常の最大努力型のサービスのほかに、以下のようなサービスがあります。

早期転送 (EF)

早期転送サービスは、DiffServ のプレミアム・サービスのことですが、ここではこの両方の呼び方を使います。このサービスでは、ある特定の伝送速度を保証し、保証転送サービスやベストエフォート・サービスよりも遅延比率が低くなります。過剰なトラフィックが発生した場合は、DiffServ はそうした過剰なトラフィックを除去します。プレミアムの待ち行列では、367ページの図29 の EF 待ち行列に示されているように、EF サービスが提供されます。

保証転送 (AF)

保証転送サービスは、DiffServ の保証サービスですが、ここではこの両方の呼び方 (保証転送と保証サービス) を使います。AF サービスでは、ある特定の伝送速度を保証しますが、遅延比率は保証されません。余分の資源があれば、DiffServ は過剰トラフィックを高速で転送します。

任意選択により、AF トラフィックは、ポリシー内の構成を使用して計量され、ポリシングが行なわれます。サポートされるポリシング・タイプは、single-rate と two-rate の Three Color Marker (TCM) です。 TCM により、着信トラフィックの特性に基づいて、パケットを分類または再マーク付けすることができます。 3 通りの分類、すなわち、緑、黄、および赤が提供されます。ポリシーは、カラー分類用のしきい値を指定する機能があります。AF/BE の待ち行列は、367ページの図29 に示されているように、AF サービスを提供します。

ベストエフォート (BE)

これは標準のベストエフォート・サービスです。サービス保証や遅延保証はありません。EF と AF のサービスについて資源を確保するときに、両者のバランスをとる必要があります。ベストエフォート・サービスのトラフィックが適度なサービスを受けられるようにするため、充分な資源を確保しておかなければなりません。 AF/BE の待ち行列は、367ページの図29 に示されているように、BE サービスを提供します。

ローカル・ルーターは、制御パケットを作って送信するので、ルーターが適切なサービスを提供できるように、充分な資源を残しておく必要があります。

エッジ・ルーターにおける DiffServ 計量、マーク付け、およびポリシングにより、DiffServ が使用可能になったネットワークにおけるコア・ルーターは、DS (TOS) コード・ポイントに基づいてパケットを分類し、非準拠トラフィックを除去するか、そのサービス・レベルを下げることによって輻輳を制御することができます。たとえば、コア・ルーターは、赤色のパケットをすべて廃棄し、黄色のパケットをベスト・エフォートとして転送し、除去可能性の低い緑色のパケットを転送することができます。これにより、DiffServ が使用可能になったネットワークでは、優先トラフィックのスループットが上昇し、遅延が減少します。

現在、DiffServ は PPP、Multilink PPP、および Frame Relay の各リンクに実装されていますが、RSVP サブシステムでも使用できます。 365ページの図28 は、ストリーム内のパケット処理の方法を示しています。ルーターにフローの中の最初のパケットが届くと (プレミアム・サービスを指定したパケットと仮定する)、DiffServ キャッシュにはサービスの種類が示されていないので、パケットは低速パスで処理されます。 DiffServ は、ポリシー・データベースを検索して、パケットの処理基準

(ポリシー) を取り出します。ポリシーに定義されたアクションは、DiffServ キャッシュに保存されています。同じフローの次のパケットがルーターに届くと、このフローの DiffServ キャッシュにすでに入力項目があることをルーターが見つけて、ポリシー定義のアクションが実行され、パケットは高速パスを通ります。そこで、このフローのこれ以降のパケットは、プレミアム・サービスを受けます。

図29 は、policer、バッファー管理、待ち行列、スケジューラーなど、異なるサービス・レベルの提供に必要な各基本コンポーネントの関係を示しています。

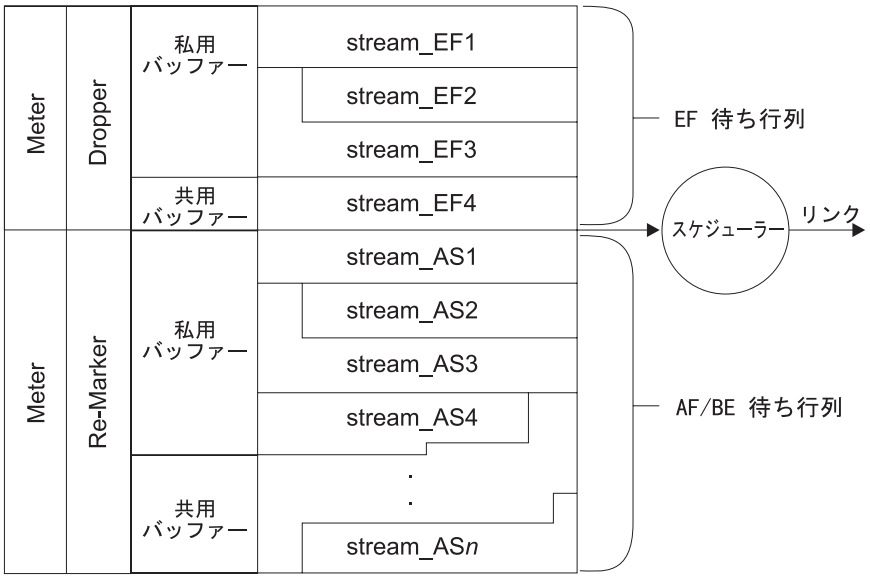


図 29. Policer、バッファー、待ち行列、およびスケジューラーの関係

早期転送サービス (EF) と保証転送サービス (AF) には、異なる特性がありますが、それぞれ、(1) 計量と policer、(2) バッファーと待ち行列管理、(3) スケジューラーといった、ルーターの 3 つの機能によりサポートされています。これらの機能には、通常の BE ルーター装置と比べて、優れたトラフィック制御機能があります。

ポリシー・フィーチャーを使って適当なポリシーを構成した後、DiffServ を実装するには、最初のステップとして、DiffServ の **enable ds** コマンドを使って DiffServ フィーチャーを有効にし、**set interface** コマンドを使ってインターフェースの出口を有効にします。

DiffServ オプションを構成して、ネットワーク資源を過剰使用やオーバー・ブックの状態にし、帯域幅やバッファーが実際よりも多くあるように見せかけるトラフィック・コンディショナーを構成することもできます。DiffServ は、オーバーブッキングをサポートしていません。

DiffServ のストリームがアイドルになると (ある程度の時間、ストリームに送られるパケットがなくなる状態)、システムが資源を取り戻してほかのストリームに利用します。ストリームが再びアクティブ化すると、資源はそのストリームに戻ります。オーバーブッキングのために資源がなくなった場合は、DiffServ が定期的に資源の再割り当てを試みます。

DiffServ コード・ポイントの概要

DiffServ は、RFC791 で定義されているように、IPv4 TOS オクテットの置換ヘッダーを提供します。これには、DiffServ (DS) フィールドと呼ばれる 1 バイトが入っています (図30 を参照)。 DS フィールドの高位 6 ビットは、DiffServ コード・ポイント (DSCP) として使用され、per-hop-behavior (PHB) を判別します。残りの 2 ビットは、将来の使用に備えて予約されます。次の例は、DS フィールドの形式を示しています。

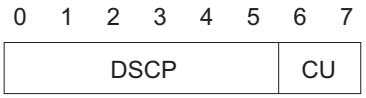


図30. IPv4 TOS オクテット・ヘッダーの DiffServ コード・ポイント形式

ここで、
DSCP = ディファレンシエーテッド・サービス・コード・ポイント
CU = 現在未使用

EF PHB の推奨コード・ポイントは 101110xx です。

図31 は、AF PHB の DS フィールドの形式を示しています。

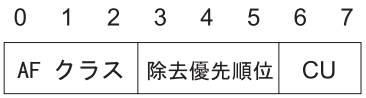


図31. AF PHB ヘッダーの DiffServ コード・ポイント形式

ここで、
AF クラス・タイプの 3 ビット
001 - AF11 クラス
010 - AF21 クラス
011 - AF31 クラス
100 - AF41 クラス
除去優先順位の 3 ビット
010 - 低い除去優先順位。TCM の緑色を意味します。
100 - 中程度の除去優先順位。TCM の黄色を意味します。
110 - 高い除去優先順位。TCM の赤色を意味します。
CU = 現在未使用

次のリストは、AF クラスと除去優先順位値を持つ推奨 AF コード・ポイント値です。

クラス 1	クラス 2	クラス 3	クラス 4
AF11 = 001010xx	AF21 = 010010xx	AF31 = 011010xx	AF41 = 100010xx
AF12 = 001100xx	AF22 = 010100xx	AF32 = 011100xx	AF42 = 100100xx
AF13 = 001110xx	AF23 = 010110xx	AF33 = 011110xx	AF43 = 100110xx

Meter と Policer の概要

計量とポリシングは、ポリシーで指定された EF と AF トラフィックに対して行なわれます。EF アルゴリズムは、トラフィックを計量し、指定されたしきい値を超えるパケットを除去します。AF アルゴリズムは、トラフィックを計量し、パケットに再度マーク付けしますが、除去しません。

早期転送 (EF)

EF トラフィックには、デフォルトのトークン・バケット・ベース policer があります。この policer は、パケットがポリシーの帯域幅パラメーター設定時に指定された速度を超えると、そのパケットを除去します。 policer のデフォルト動作を変更するには、Token Rate (TR) と Token Bucket Size (TBS) パラメーターを指定することができます。 meter は、パケットを送信できる十分な数のトークンがバケットに含まれているかどうかを判別します。トークンが使用可能な場合は、パケットが送信されます。使用可能でない場合は、policer がパケットを除去します。バケットは、Token Rate パラメーターで指定された速度でトークンを補充します。トークンの速度は、バイト / 秒単位で測定されます。つまり、これには、IP ヘッダーが含まれますが、リンク固有のヘッダーは含まれません。トークン速度は、IP ヘッダー圧縮およびレイヤー 2 データ暗号化と圧縮の前に測定されます。Token Bucket Size は、速度限界を超えた一時バーストをペナルティーなく処理するのに使用されます。

保証転送 (AF)

AF トラフィックには、3 つのポリシング・オプションがあります。すなわち、(1) single-rate Three Color Marker (srTCM)、(2) two-rate Three Color Marker (trTCM)、および (3) none (ポリシングなし) です。これらのポリシング・オプションは、AF1、AF2、AF3、および AF4 クラスに使用可能であり、ポリシーの設定時に指定されます。

srTCM は、2 つのバケットと 1 つの補充速度を使用して、トークン・バケット・アルゴリズムに基づいてトラフィック・ストリームを計量します。これは、3 つのトラフィック・パラメーターにしたがって、パケットに緑、黄、または赤のマークを付けます。3 つのトラフィック・パラメーターとは、(1) Committed Information Rate (CIR)、(2) Committed Burst Size (CBS)、および (3) Excess Burst Size (EBS) です。パケットが CBS を超えない場合は、緑にマーク付けされ、CBS を超えるが、EBS を超えない場合は黄色にマークされ、それ以外の場合は赤にマークされます。 CIR は、毎秒の IP パケットのバイト数単位で測定されます。つまり、これには、IP ヘッダーが含まれますが、リンク固有のヘッダーは含まれません。 CIR は、IP ヘッダー圧縮およびレイヤー 2 データ暗号化と圧縮の前に測定されます。CBS と EBS はバイト単位で測定されます。

meter は、color-blind または color-aware モードで動作します。 color-blind モードでは、DS コード・ポイントにおける除去優先順位ビットの設定にかかわらず、着信パケットは緑にマークされているものと想定されます。 CBS は、緑色のバケットのサイズを表し、EBS は、黄色のバケットのサイズを表します。まず、緑色のバケットを調べて、使用可能なトークンを探します。緑色のトークンが十分にある場合、パケットは緑色にマークされ、送信されます。緑色のトークンが十分ない場合、黄色のバケットが調べられます。黄色のトークンが十分にある場合、パケットは黄色にマークされ、送信されます。黄色のトークンが十分ない場合、パケットは赤色にマークされます。 color-aware モードでは、着信パケットの色がチェックさ

れ、対応するトークン・バケットが最初にチェックされます。トークンが使用可能な場合、パケットは受信済みとして送信されます。使用可能でない場合、除去優先順位値が適宜減少します。Color-aware モードは、入り口パケットがすでに分類され、事前に色がマークされている場合に便利です。

trTCM も、緑と黄色のバケットに別々の補充速度を提供する点を除いて、srTCM とほぼ同じトークン・バケット・アルゴリズムです。構成パラメーターは、(1) Committed Information Rate (CIR)、(2) Committed Burst Size (CBS)、(3) Peak Information Rate (PIR)、および (4) Peak Burst Size (PBS) です。CBS は、緑色のバケットのサイズを表し、PBS は、黄色のバケットのサイズを表します。このアルゴリズムは、srTCM の場合と同じですが、CIR 値が、緑のバケットの補充速度を決定し、PIR 値が、黄色のバケットの補充速度を決定する点を除きます。 trTCM が便利なのは、ピーク速度を認定情報速度とは別に実施する必要がある場合です。 PIR を超えるパケットは、赤 (除去可能性が最も高い) にマークされます。

バッファーと待ち行列管理の概要

トラフィックが EF 用であるか、または policer が許可した AF または BE トラフィックである場合、速度ベースのバッファー*管理* 機能がこのトラフィックを処理します。この機能は、DiffServ が使用可能な出力インターフェースについて、私用プールまたは共通の共用プールのどちらかからバッファーを割り当てます。 EF トラフィック用のバッファーは、私用プールからしか割り当てられません。

1 つのインターフェースで使える物理的バッファー・スペースの合計量を指定するには、Talk 6 **set receive-buffers** 構成コマンド (説明と構文については、ソフトウェア *使用者の手引き* を参照) を使用してください。プレミアム・サービスと保証サービスの待ち行列について、出口のバッファー・サイズを設定するには、DiffServ の Talk 6 **set interface** コマンドを使用します。これは DiffServ が管理するバッファー・スペースです。

DiffServ は、プレミアム・サービス (EF) の待ち行列と保証転送サービス (AF) の待ち行列の 2 つの異なるプールを管理します。バッファー・スペースを指定するときは、システムで実際に使用できるバッファー・スペースの量を反映してください。

バッファー管理は、インターフェースの私用プールにパケットに使用できるバッファーがあるかどうかを確認します。使用できるバッファーがある場合は、これを受け入れて、パケットを待ち行列に入れます。バッファーがないときは、共用プールのバッファー・スペースの割り当てを試み、これができればパケットを待ち行列に入れます。共用バッファー・スペースがない場合は、バッファー管理がパケットを除去します。

スケジューラーの概要

スケジューラー 機能は、定期的に待ち行列を調べ、待ち行列にあるパケットを待ち行列から取り出し、インターフェース・アダプターに送って送信します。このスケジューラーは、自己時計による公正キューイング (fair queuing) のスケジューラーで、これは加重公平キューイング (weighted fair queuing) 重量公正待ち行列化の変形です。スケジューラーのウェイトを構成して、スケジューラーが待ち行列を調べる頻度を指定できます。

ディファレンシエーテッド・サービスの用語

DiffServ では、次の用語を使用します。

Committed Information Rate (CIR)
このパラメーターは、ユーザーの AF トラフィック・ストリームが、過剰送信と見なされる前に動作できる最大速度を指定します。毎秒の IP パケットのバイト数単位で測定されます (IP ヘッダーは含まれますが、リンク固有のヘッダーは含まれません)。これは、AF ストリームの single-rate と two-rate TCM 機能の両方によって使用されます。

Committed Burst Size (CBS)
このパラメーターは、CIR を超える速度で、バーストで送信できる最大バイト数を (IP パケットのバイト数で) 指定します。CBS は、single-rate TCM と two-rate TCM 機能の両方で、認定トークン・バケットのサイズを制限します。

DiffServ キャッシュ
このキャッシュには、ルーターがサービスを提供した最後のアクティブな IP フローについて、トラフィックとサービスのプロファイルが含まれています。

Excess Burst Size (EBS)
このパラメーターは、CIR を超える速度で、CBS を超えてバーストで送信できる最大バイト数を (IP パケットのバイト数で) 指定します。このパラメーターは、single-rate TCM 機能によって使用され、過剰トークン・バケットのサイズを制限します。

フロー 発信元アドレスとそのポート、IP プロトコル、宛先アドレスとそのポートが同一の一連のパケットです。

Token Rate
このパラメーターは、ユーザーの EF トラフィック・ストリームが、過剰送信と見なされる前に動作できる最大速度を指定します。毎秒の IP パケットのバイト数単位で測定されます (IP ヘッダーは含まれますが、リンク固有のヘッダーは含まれません)。

Token Bucket Size
このパラメーターは、トークン速度を超える速度で、バーストで送信できる、EF トラフィック・ストリームの IP パケットの最大バイト数を測定します。

Peak Bucket Size (PBS)
このパラメーターは、two-rate TCM 機能によってのみ使用されます。 PIR を超える速度でバーストで送信できる最大バイト数を (IP パケットのバイト数で) 指定します。このパラメーターは、ピーク・トークン・バケットの最大サイズを制限します。

Peak Information Rate (PIR)
このパラメーターは、two-rate TCM 機能によってのみ使用されます。ユーザーが AF ストリーム・パケットを送信できるピーク速度 (IP ヘッダーを含むが、リンク固有のヘッダーは含まない、毎秒の IP パケットのバイト数) を表します。これを超えると、パケットの除去優先順位が、最高値に設定されます。

ストリーム
フローの集合体です。

バーチャル・インターフェース (VIF)
フレーム・リレーのリンクでは、それぞれの DLCI 接続はバーチャル・インターフェースとして扱われます。

ディファレンシエーテッド・サービスの構成

以下の手順では、選択したパケットに対し優先サービスを提供するための DiffServ の構成方法についてハイレベルな説明をします。まずはじめに、DiffServ フィーチャーにアクセスします。

1. * プロンプトで、**talk 6** を入力します。
2. Config> プロンプトで、**feature ds** を入力します。これで、DS config> プロンプトが表示され、構成ダイアログが開きます。

```
* talk 6
Config>feature ds
DS config>
```

3. ルーターで DiffServ フィーチャーを使用可能にします。

```
DS config>enable ds
DiffServ enabled
```

4. インターフェース・パラメーターを使用可能にして、設定します。

```
DS config>set interface
Enter Diffserv Interface number [0]? 2
Set Premium Queue Bandwidth (%) (1 - 99) [20]?
    Assured Queue Bandwidth (%) = 80
Configure Advanced setting (y/n)? [No]: no
Accept input (y/n)? [Yes]:
```

注: Configure Advanced の設定プロンプトで no を指定した場合は、プレミアム待ち行列と保証転送およびベストエフォートのキューのデフォルト・パラメーターが使用されます。

```
Configure Advanced setting (y/n)? [No]: yes
Set Premium Queue Weight (%) (20 - 99) [90]?
    Assured Queue Weight (%) = 10
EGRESS BufSize for Premium Queue (in bytes) (550 - 27500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?
EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?
```

この例では、回線帯域幅の 20%、スケジューラー・ウェイトの 90% が EF 待ち行列に与えられます。EF 待ち行列の出口バッファー・サイズは 5500 バイト (平均パケット・サイズ 550 バイトのパケットが 10 個分) で、そのうちの 95% が QoS ストリームに割り当て可能です。 AF/BE 待ち行列の出口バッファー・サイズは 27 500 バイト (平均パケット・サイズ 550 バイトのパケットが 50 個分) で、そのうちの 80% が QoS ストリームに割り当て可能です。

5. ルーターで DiffServ を使用可能にし、インターフェース・パラメーターの設定が終わったら、**Ctrl-P** を入力して、* プロンプトに戻ります。

DiffServ を有効にし、インターフェース・パラメーターを設定したあとは、装置をリスタートまたは再ロードして、DiffServ をアクティブにします。 DiffServ コマン

ドについて詳しくは、375ページの『第21章 ディファレンシエーテッド・サービス・フィーチャーの構成および監視』を参照してください。

第21章 ディファレンシエーテッド・サービス・フィーチャーの構成および監視

この章では、ディファレンシエーテッド・サービス (DiffServ) フィーチャーのコマンドを説明します。このフィーチャーにより、ルーターとインターフェースを構成して、選択されたデータ・パケットに優先サービスを提供します。本章には、以下の節が含まれています。

ディファレンシエーテッド・サービス構成プロンプトへのアクセス

DiffServ 構成コマンドは、以下のように入力します。

1. OPCON (*) プロンプトで、**talk 6** と入力する。
2. Config> プロンプトで、**feature ds** と入力する。

DS Config> プロンプトが現れます。これで、DiffServ 構成コマンドを入力できます。

ディファレンシエーテッド・サービス構成コマンド

これらのコマンドを使って、DiffServ オプションを構成すると、選択されたデータ・パケットに優先サービスを実行できます。表48 は、DiffServ 構成コマンドの要約です。この節ではこれらのコマンドを詳細に説明します。コマンドは、DS Config> プロンプトで入力します。コマンドとオプションをまとめて 1 行に入力するか、コマンドだけを入力して、プロンプトに答えることもできます。コマンドにオプションを付ける代わりに、疑問符 (?) を付けると、コマンド・オプションのリストが表示されます。

表 48. DiffServ 構成コマンド

コマンド	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。xxxiページの『ヘルプの入手』 を参照してください。
Delete	ルーターの SRAM から DiffServ 構成レコードを削除します。
Disable	ルーターまたは特定の出口インターフェースで DiffServ を無効にします。
Enable	ルーターまたは特定の出口インターフェースで DiffServ を有効にします。
List	ルーターの DiffServ システムとインターフェース関連の設定について、情報を表示します。
Set	ルーターの DiffServ 関連の設定を指定します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Delete

delete コマンドは、DiffServ システム構成レコードまたはインターフェース・レコードをルーターの SRAM から削除します。

構文: delete ds
interface

ds ルーターの DiffServ システム構成レコードを削除します。

例:

```
DS Config> delete ds
Diffserv system config record deleted
```

interface 削除するインターフェース番号を入力するようにプロンプトが出ます。

例:

```
DS Config> delete interface
Enter Diffserv Interface number to delete [0]? 3
Diffserv interface config record deleted
```

Disable

disable コマンドは、ルーターまたは特定の出口インターフェースで DiffServ 機能を無効にします。

構文: disable ds
interface

ds ルーターの DiffServ 機能を無効にします。

例:

```
DS Config> disable ds
DiffServe feature disabled
```

interface 無効にするインターフェース番号を入力するようプロンプトが出ます。

例:

```
DS Config> disable interface
Enter Interface number [0]? 2
DiffServe interface disabled
```

Enable

enable コマンドは、ルーターまたは特定の出口インターフェースで DiffServ 機能を有効にします。

構文: enable ds
interface

ds ルーターの DiffServ 機能を有効にします。

例:

```
DS Config> enable ds
DiffServe feature enabled
```

interface 有効にするインターフェース番号を入力するようプロンプトが出ます。

例:

```
DS Config> enable interface
Enter Interface number [0]? 2
DiffServe interface enabled
```

注: DiffServ を有効にできるのは、PPP および Frame Relay のリンクだけです。

List

list コマンドは、ルーターの DiffServ システムとインターフェース関連の設定に関する情報を表示します。

構文: list
- all
- ds
- interface

all ルーターの DiffServ とインターフェースの構成について情報を表示します。

ds ルーターの DiffServ の構成内容を表示します。

例:

```
DS Config> list ds

System Parameters:

        DiffServ:               ENABLED
        Packet_size:            550
        Min BE Alloc (%):       10
        Min CTL Alloc (%):      5
        Number_of_Q:            2
```

interface ルーター内のインターフェース、その DiffServ の有効または無効のステータス、各インターフェースと待ち行列のパラメーターを表示します。

例:

```
DS Config> list interface
-------------------------------------------------------------------------------
                          ---------- Premium -------   --------- Assured --------
Net If     Status  NumQ Bwdth  Wght  OutBuf  MaxQos Bwdth  Wght  OutBuf  MaxQos
Num                       (%)   (%) (bytes)     (%)   (%)   (%) (bytes)     (%)
-------------------------------------------------------------------------------
2   PPP   Enabled     2    20    90    5500      95    80    10   27500      80
3   PPP   Enabled     2    20    90    5500      95    80    10   55000      80
```

Set

set コマンドは、ルーターの DiffServ システムとインターフェース関連のパラメーターを設定するときに使用します。

構文: set
- be-alloc-min
- ctl-alloc-min
- interface
- pkt-size

DiffServ 構成コマンド (Talk 6)

be-alloc-min ベストエフォート・サービスに割り当てる出力バッファー・スペースの合計量に対する最小割合を指定します。

デフォルト値: 10

例:

```
DS Config> set be-alloc-min
Enter Minimum percent output BW allocated to BE service (10 - 50) [10]?
```

ctl-alloc-min ネットワーク制御サービスに割り当てる出力バッファー・スペースの合計量に対する最小割合を指定します。

デフォルト値: 5

例:

```
DS Config> set ctl-alloc-min
Enter Minimum percent output BW allocated to CTL service (5 - 20) [5]?
```

interface DiffServ のためにインターフェースを有効にし、インターフェース特定のパラメーターを入力するようにプロンプトが出ます。

Queue bandwidth
プレミアム待ち行列に使用する出力リンクの割合を指定します。残った割合は、保証待ち行列の値に使用されます。

デフォルト値: 20

Queue weight
スケジューラーがプレミアム待ち行列を監視する時間の割合を指定します。残った割合は、保証待ち行列の値に使用されます。待ち行列のウェイトは、デフォルトでは 90% になっていて、スケジューラーが EF トラフィックに迅速に対応できるようになっています。

デフォルト値: 90

Egress buffer size
プレミアム待ち行列と保証待ち行列で待ち行列を作れるデータ量 (バイト) を指定します。

このパラメーターは、プレミアム待ち行列に対して、プレミアム待ち行列におくことのできるデータ量 (バイト) を制御します。このパラメーターの数値が大き過ぎると、プレミアム・トラフィックで大きな待ち行列の遅延が起こります。たとえば、このパラメーターを 25 キロバイトにして、出力リンク速度を 1.5 Mbps (T1 スピード) とすると、133 msec (25 000 バイト * 8 ビット/バイト) /1 500 000 bps、または 0.133 sec (133 ミリ秒) の待ち行列遅延が起こる可能性があります。このパラメーター値が小さ過ぎると、小さなバーストをバッファーできなくなります。たとえば、このパラメーターを 2 kb に設定すると、1500 バイトのパケットで 2 パケットのバーストをバッファーするのには充分ではないことを意味します (バッファー・スペースに 3000 バイトが必要になります)。

この両極端に対する妥協策として、デフォルト設定は 5500 バイトになっており、これはデフォルトのパケット・サイズの 550 バイトの 10 倍です。

デフォルト値: 5500 (プレミアム待ち行列)

このパラメーターは、保証待ち行列に対して、保証待ち行列におくことのできるデータ量 (バイト) を制御します。このパラメーターもプレミアム待ち行列と同じような対応が必要ですが、保証待ち行列のトラフィックでは、遅延に対する条件が厳しくはありません。むしろ、保証待ち行列のトラフィックは、バースト性の高い TCP フローで構成されています。このため、複数のフローのバーストに対応するため、充分なバッファー・スペースを定義する必要があります。

デフォルトのサイズは、27 500 バイトであり、デフォルトのパケット・サイズである 550 の 50 倍です。

デフォルト値: 27500 (保証待ち行列)

Egress QoS allocation

すべての DiffServ ストリームが予約できる出口バッファーのサイズを指定します (パーセント)。 残った割合は、共用プールの最小値として使用されます。

デフォルト値: 95 (プレミアム待ち行列)

デフォルト値: 80 (保証待ち行列)

注:

1. Multilink PPP の場合、バンドル仮想インターフェース上で DiffServ を使用可能にしてください。バンドル・インターフェースの個々のリンク上で DiffServ を使用可能にすることはできません。
2. Frame Relay サブインターフェースの場合、ベース Frame Relay ネット上で DiffServ を使用可能にしてください。サブインターフェース上で DiffServ を使用可能にすることはできません。

例:

```
DS Config> set interface
Enter Diffserv Interface number [0]? 2

DiffServ Interface enabled

Set Premium Queue Bandwidth (%) (1 - 99) [20]?
    Assured Queue Bandwidth (%) = 80

Configure Advanced setting (y/n)? [No]: y

Set Premium Queue Weight (%) (20 - 99) [90]?
    Assured Queue Weight (%) = 10

EGRESS BufSize for Premium Queue (in bytes) (550 - 27500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?

EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?

        DiffServ Interface: ENABLED
PREMIUM Queue Bandwidth (%) =                          20
PREMIUM Queue Weight (%) =                             80
PREMIUM Queue EGRESS BufSize in bytes =              5500
PREMIUM Queue Max EGRESS QoS allocation (%) =          95
ASSURED/BE Queue Bandwidth (%) =                       80
ASSURED/BE Queue Weight (%) =                          20
```

```
ASSURED/BE Queue EGRESS BufSize in bytes =         27500
ASSURED/BE Queue Max EGRESS QoS allocation (%) =      80
Accept input (y/n)? [Yes]:
```

pkt-size トラフィック・フローの平均パケット・サイズを指定します (バイト数)。これにより、入り口と出口のインターフェースで使用できるバッファー・スペースをDiffServ が決めます。この数値が変わった場合は、ルーターをリスタートし、DiffServ の **set interface** コマンドの値を見直し、必要であれば変更します。

デフォルト値: 550

例:

```
DS Config> set pkt-size
Average packet size (64 - 64000) [550]?
```

ディファレンシエーテッド・サービス監視環境へのアクセス

この DiffServ フィーチャーのコンソール部は、DiffServ 関連の設定項目について表示や管理を行います。DiffServ 監視環境にアクセスするには、OPCON プロンプト (*) で、**talk 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで、以下のコマンドを入力します。

```
+ feature ds
DS Console>
```

ディファレンシエーテッド・サービス監視コマンド

以下のコマンドを使うと、DiffServ 関連の設定項目を表示します。 表49 は、DiffServ 監視コマンドの要約です。この節ではこれらのコマンドを詳細に説明します。コマンドは、DS Console プロンプトで入力します。コマンドとオプションをまとめて 1 行に入力するか、コマンドだけを入力して、プロンプトに答えることもできます。コマンドにオプションを付ける代わりに、疑問符 (?) を付けると、コマンド・オプションのリストが表示されます。

表 49. DiffServ 監視コマンド

コマンド	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。xxxiページの『ヘルプの入手』 を参照してください。
Clear	特定の入り口および出口のインターフェースのあいだのストリームについて、統計を消去します。
DScache	ルーターの DiffServ キャッシュにある情報を消去または表示します。
List	ルーターの DiffServ システムとインターフェース関連の設定について、情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Clear

clear コマンドは、特定の入り口および出口のインターフェースのあいだのストリームについて、統計を消去します。

構文: clear stream-stats

例:

```
DS Console> clear stream-stats
Incoming Network number : 0
Outgoing Network number : 2
Net 0->2 stream stats cleared at sysclock 85327 Second.
```

DScache

dscache コマンドは、ルーターの DiffServ キャッシュの情報を消去または表示します。

構文: dscache actions
clear
nexthop
order
stats

actions 特定の IP 発信元から特定の IP 宛先に送られたパケット、および DiffServ ストリーム ID がある場合はこの ID に送られたパケットに対してとられるアクションを表示します。

例:

```
DS Console> dscache actions
Source Address to list []?
Destination Address to list []?
Source          Destination     Pro ProtocolInf Net TosIn/Out Action StrmID
10.1.100.1      9.1.140.1         1 T:x08 C:x00   0 x00->x15  PASS   85
9.1.140.1       10.1.100.1        1 T:x00 C:x00   1 x00->x15  PASS   null
```

clear すべての DiffServ キャッシュを消去するように指定します。

nexthop ネクスト・ホップの IP アドレスを表示します。

例:

```
DS Console> dscache nexthop
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source          Destination     Pro ProtocolInf Net  Tos  NextHop
5.0.13.248      5.0.11.249       17  1031> 1031   0  x00  5.0.61.7      (PPP/1)
5.0.13.248      5.0.11.249       17  1032> 1032   0  x00  5.0.61.7      (PPP/1)
5.0.13.248      5.0.11.249       17  1033> 1033   0  x00  5.0.67.1      (PPP/1)
```

order パケットが到着した順序を表示します。

例:

```
DS Console> dscache order
Order Source          Destination     Pro ProtocolInf Net  Tos
   1  5.0.16.246      5.0.13.248        1 T:x03 C:x03   2  x00
   2  5.0.13.248      5.0.16.246       17  4000> 5678   0  x00
   3  5.0.16.246      5.0.13.244        1 T:x03 C:x03   1  x00
   4  5.0.13.248      5.0.15.243       17   123>  123   0  x00
```

stats 特定の IP 発信元から特定の IP 宛先に送られたパケットについて、統計を表示します。

例:

```
DS Console> dscache stats
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source          Destination     Pro ProtocolInf Net  Tos    RxPkts    RxBytes
5.0.13.248      5.0.11.249       17  1031> 1031   0  x00       432     444096
5.0.13.248      5.0.11.249       17  1032> 1032   0  x00       432     444096
5.0.13.248      5.0.11.249       17  1033> 1033   0  x00       437     459516
```

List

list コマンドは、ルーターの DiffServ システムとインターフェース関連の設定に関する情報を表示します。

構文: list　　interface

queue

stream

vifs

interface　ルーター内のインターフェース、その DiffServ の有効または無効のステータス、その入り口バッファーの位置、その他の情報を表示します。

Net　インターフェース番号を表示します。

Status
DiffServ ステータスを表示します。

KB/s　リンク速度を毎秒 kb で表示します。

VirtTime
スケジューラーが使用する仮想時刻を表示します (DiffServ ではないリンクは n/a、処理中のパケットがないときは 0 を示します)。

InMax　保証転送に構成された最大バッファー・サイズを表示します。

InCurr　入力ストリームに現在使用されているバッファー・スペースの量を表示します。バッファーには、処理中のパケットがあります。

InShar
この出口インターフェースで使用できる共用バッファー・スペースの量を表示します。

InMaxA
集合されたすべての QoS ストリームに割り当てることができる最大バッファー・スペース量を表示します。

InCurA
入力ストリームで使用できるバッファー・スペースの割り当て量を表示します。

NumI　入力ストリームの数を表示します。

NumO　出力ストリームの数を表示します。

例:

```
DS Console> list interface
DiffServ interfaces:
Net Status   KB/s  VirtTime InMax  InCurr InShar InMaxA InCurA NumI NumO
--- -------- ----- -------- ------ ------ ------ ------ ------ ---- ----
  0 Disabled  1250      n/a  55000    550  49775  44000   5225   22  n/a
  1 Disabled  1250      n/a  27500      0  27500  22000      0   20  n/a
  2 Enabled    256        0  27500      0  27500  22000      0   20    3
  3 Enabled    256        0  55000      0  55000  44000      0   20    3
  4 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  5 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  6 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  7 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  8 Disabled  2000      n/a  27500      0  27500  22000      0   20  n/a
  9 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
```

queue

DiffServ 出口待ち行列に割り当てられたウェイトと出口インターフェースのバッファー割り当てステータスを表示します。

Queued packets

待ち行列にあるパケットの現在数を表示します (待ち行列にパケットがないときは 0 を示します)。

Svc Tag

待ち行列が次にサービスを受ける仮想時刻を表示します。

Weight

待ち行列の構成済みスケジューラー・ウェイトを表示します。

out_max_alloc

DiffServ ストリームに割り当てることができる最大バッファー・スペースの量を表示します。

out_curr_alloc

現在割り当てられているバッファー・スペースの量を表示します。

out_max_buff

待ち行列の最大バッファー・スペースの量を表示します。

out_curr_buff

パケットが現在使用している割り当てバッファー・スペースの量を表示します。

out_share_buff

現在共用プールにあるバッファー・スペースの量を表示します。

例:

```
DS Console> list queue
OUT Network number : 1

Premium Queue:
        Queued packets: 0
        Svc Tag:        4294967295
        Weight: 90
        out_max_alloc:  5225 (Bytes)
        out_curr_alloc: 0 (Bytes)
        out_max_buff:   5500 (Bytes)
        out_curr_buff:  0 (Bytes)
        out_share_buff: 5500 (Bytes)


Assured Queue:
        Queued packets: 0
        Svc Tag:        4294967295
        Weight: 10
        out_max_alloc:  22000 (Bytes)
```

```
out_curr_alloc: 4125 (Bytes)
out_max_buff:   27500 (Bytes)
out_curr_buff:  0 (Bytes)
out_share_buff: 23375 (Bytes)
```

stream meter-mark

AF ストリームの計量とマーク付けについての情報を表示します。

Id ストリーム識別番号

t ストリーム・タイプ

- **D** DiffServ ストリーム
- **B** ベストエフォート・ストリーム
- **C** ネットワーク制御ストリーム
- **R** RSVP ストリーム

I/o q 出力インターフェース待ち行列タイプ

- **q1** プレミアム待ち行列
- **q2** 保証待ち行列とベストエフォート待ち行列

pkt snt
このストリームで送信されたパケットの合計数

buf drp
このストリームで、バッファー・スペース不足のために除去されたパケットの数

snt g 緑にマーク付けされた送信パケットの数

snt y 黄色にマーク付けされた送信パケットの数

snt r 赤にマーク付けされた送信パケットの数

g->y color-aware モードで、緑マークのパケットが黄色マークとして送信された数

g->r color-aware モードで、緑マークのパケットが赤マークとして送信された数

y->r color-aware モードで、黄マークのパケットが赤マークとして送信された数

例:

```
DS Console> list stream meter-mark 0 1
At interface 0, 4 in-streams; clock=25493 sec.
Streams from net 0 to net 1:
 Id   t I/o q  pkt snt  buf drp   mrk g    mrk y   mrk r   g->y    g->r    y->r
 ---- - -----  -------  -------  -------  ------  ------  ------  ------  ------
(af1)
 101  D   in     3615        0        0       0       0       0       0       0
         o-q2    3615        0     1223    1222    1770       0       0       0
```

stream packet-stats

ストリーム内のパケットについての情報を表示します。

Id ストリーム識別番号

t ストリーム・タイプ

- **D** DiffServ ストリーム

B ベストエフォート・ストリーム

C ネットワーク制御ストリーム

R RSVP ストリーム

I/o q 出力インターフェース待ち行列タイプ

q1 プレミアム待ち行列

q2 保証待ち行列とベストエフォート待ち行列

allo/cur(K)
このストリームによって割り当てられ、現在使用されている合計バッファー・スペース (キロバイト単位)

tot pkt
このストリームの伝送で受信したパケットの合計数

tot Kby
このストリームの伝送で受信したキロバイト数

pkt snt
このストリームで送信されたパケットの合計数

Kby snt
このストリームで送信されたキロバイト数の合計

ovr snt
共用バッファーを使って送信されたパケット数

buf drp
このストリームで、バッファー・スペース不足のために除去されたパケットの数

pol drop
プレミアム待ち行列で policer により除去されたパケットの数

例:

```
DS Console> list stream packet-stats 0 1
At interface 0, 4 in-streams; clock=25496 sec.
Streams from net 0 to net 1:
 Id   t I/o q  allo/cur(K)  tot pkt  tot Kby  pkt snt  Kby snt  ovr snt  buf drp pol drp
 ---- - -----  -----------  -------  -------  -------  -------  -------  ------- -------
(af1)
 101  D    in   6.3/   0.0     3615     3730     3615     3730        0        0
          o-q2   6.3/   0.0                      3615     3730        0        0       0

(ef)
 100  D    in   5.2/   0.0     2393     2469     2393     2469        0        0
          o-q1   5.2/   0.0                      2393     2469        0        0     132

(-)
 40   B    in   0.0/   0.0        0        0        0        0        0        0       0
          o-q2   2.8/   0.0                         0        0        0        0       0

(-)   C    in   0.0/   0.0        0        0        0        0        0        0
          o-q2   1.4/   0.0                         0        0        0        0       0
```

stream police-para
EF および AF ストリームに対して構成されたポリシング・パラメーターについての情報を表示します。

Id ストリーム識別番号

t ストリーム・タイプ

D DiffServ ストリーム

B ベストエフォート・ストリーム

C ネットワーク制御ストリーム

R RSVP ストリーム

I/o q 出力インターフェース待ち行列タイプ

q1 プレミアム待ち行列

q2 保証待ち行列とベストエフォート待ち行列

TR/CIR in B/s
構成済みトークン速度または認定情報速度 (バイト / 秒単位)

TBS/CBS in bytes
構成済みトークン・バケット・サイズまたは認定バースト・サイズ (バイト単位)

PIR in B/s
構成済みピーク情報速度 (バイト / 秒単位)

EBS/PBS in bytes
構成済み過剰バケット・サイズまたはピーク・バースト・サイズ (バイト単位)

pol typ
ポリシング・アクションのタイプ

None ポリシングなし

SRCB Single-rate、color blind TCM

SRCA Single-rate、color-aware TCM

TRCB Two-rate、color blind TCM

TRCA Two-rate、color-aware TCM

EF-DRP
デフォルト除去アクションのある EF policer

例:

```
DS Console> list stream police-para 0 1
At interface 0, 16 in-streams; clock=18429 sec.
Streams from net 0 to net 1:
 Id   t I/o q     TR/CIR    TBS/CBS    PIR      EBS/PBS  pol typ
                  in B/s   in bytes   in B/s   in bytes
 ---- - -----  ---------  ---------  -------  ---------  -------
(af1)
 101  D   in
         o-q2      25000       4000        0       4000  SRCB

(ef)
 100  D   in
         o-q1      48706       5225                      EF-DRP
```

vifs フレーム・リレー・バーチャル・インターフェースに関する情報を表示します。

例:

```
DS Console> list vifs 1

DiffServ virtual interface for dlci:  17
     Status: Inactive - no packets queued for transmission
     CIR: 64000 (bits/sec)
     Virtual Time: 0
     Service Tag:  0

DiffServ virtual interface for dlci:  16
     Status: Inactive - no packets queued for transmission
     CIR: 64000 (bits/sec)
     Virtual Time: 0
     Service Tag:  0
```

ディファレンシエーテッド・サービス動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

ディファレンシエーテッド・サービス (すなわち DiffServ または DS) は、CONFIG (Talk 6) **delete interface** コマンドをサポートします。ただし、次の考慮事項があります。

対応する DiffServ インターフェース SRAM レコードを削除します。この変更をアクティブにするには、装置をリブートする必要があります。

GWCON (Talk 5) Activate Interface

DiffServ は、GWCON (Talk 5) **activate interface** コマンドをサポートします。ただし、次の考慮事項があります。

DS 構成されたインターフェースがアクティブである場合、DS は通常の netup/netdown シーケンスを実行します。

GWCON (Talk 5) Reset Interface

DiffServ は、GWCON (Talk 5) **reset interface** コマンドをサポートします。ただし、次の考慮事項があります。

- DiffServ がインターフェース上で使用可能である場合、次の状態が発生します。**reset interface** が、このインターフェースとの間で作成されたすべてのストリームを消去します。また、DiffServ キャッシュも消去します。BRS が使用可能である場合、BRS がこのインターフェース上で DiffServ より優先されます。DiffServ インターフェース SRAM レコードにおける add/del/change について、変更をアクティブにするには、装置をリブートする必要があります。

動的再構成不能コマンド

次の表は、動的に変更できない DiffServ 構成コマンドを記述しています。これらのコマンドを活動化するには、装置を再ロードまたはリスタートする必要があります。

コマンド
CONFIG, feature DS, enable/disable/del ds
CONFIG, feature DS, enable/disable/del/set interface
CONFIG, feature DS, set be-alloc-min

CONFIG, feature DS, set ctl-alloc-min
CONFIG, feature DS, set pkt-size

第22章 Random Early Detection フィーチャーの使用

この章では、輻輳が発生した場合に、ネットワーク装置が構成済みの除去可能性に基づいて、ランダム着信パケットに除去のマークを付けてオーバーフローを避けるように、Random Early Detection (RED) フィーチャーを使用する方法について説明します。これは、送信ウィンドウ・サイズを縮小して輻輳指示に応答する良性トラフィック (たとえば、TCP) に便利です。 RED は、PPP、Multilink PPP、および Frame Relay の各リンクをサポートします。本章には、次の節が含まれています。

- 『Random Early Detection の使用』

Random Early Detection の使用

RED を使用すると、輻輳が発生した場合にオーバーフローを回避することができます。 RED は平均待ち行列長を計算し、それが指定された限界内であれば、構成可能な除去可能性に基づいて、着信パケットに除去のマークが付けられます。現行の待ち行列サイズではなく、*平均* の待ち行列長を使用すると、バースト性トラフィック待ち行列が、除去速度に影響を与えません。

RED パラメーターに次の値を指定していることを前提とします。

```
1 Weight factor: 4
2 Exponential Maximum Packet Drop Probability: 9
3 Minimum Threshold Value: 70
4 Maximum threshold Value: 100
5 Initial Average Queue Size: 60
```

1 この値は、現行の待ち行列が、平均の待ち行列長の計算に与える影響の程度を決定します。

このパラメーターの最小値 (1) は、ウェイトを下げることを指定し、無難な設定です。この値を指定すると、特定の時点の平均待ち行列長は、直前の平均待ち行列長に近い値であるので、待ち行列長が長いバースト性トラフィックが、新しい平均待ち行列長の計算に与える影響はほとんどありません。

このパラメーターの最大値 (8) は、ウェイトの増加を指定し、アグレッシブな設定です。この値を指定すると、平均待ち行列長は、現行の待ち行列長と等しいので、待ち行列長が長いバースト性トラフィックは、新しい平均待ち行列長の計算に大きな影響を与えます。

2 この値は、ピークの平均待ち行列長でパケットを除去する可能性です。

平均待ち行列長が一貫して最大しきい値に等しい場合、2^9 (512) パケットごとに 1 つのパケットに、除去のマークが付けられます。平均待ち行列長は、最小しきい値から最大しきい値まで増加するので、除去の可能性は線形に増加します。

3 この値は、パケットの除去可能性を計算し、それに応じてパケットにマークを付けるための最小待ち行列要件を指定します。

最大装置待ち行列値 (レイヤー 2 プロトコルによって決定される構成不能値) に対する割合として表示されます。たとえば、値を 40 パーセントに指定するときに、最大装置待ち行列値が 16 であると、最小しきい値は 6 (0.4*16) に設定されます。

4 この値は、パケットの除去可能性を計算し、それに応じてパケットにマークを付けるための最大待ち行列要件を指定します。

最大装置待ち行列値 (レイヤー 2 プロトコルによって決定される構成不能値) に対する割合として表示されます。たとえば、値を 100 パーセントに指定するときに、最大装置待ち行列値が 16 であると、最大しきい値は 16 (1.0*16) に設定されます。

5 この値は、パケットの除去可能性の計算に使用される初期設定値を指定します。

最大装置待ち行列値 (レイヤー 2 プロトコルによって決定される構成不能値) に対する割合として表示されます。平均待ち行列値がトラフィック自体によって設定される前に、バースト性トラフィックが、平均待ち行列長の計算でウェイトを増やさないようにします。(装置が初期化される時点で、待ち行列長はゼロであり、直前の平均待ち行列長は指定されていません。) 上記の例で示されているように、相対的に低い値を指定する必要があります。

RED を使用可能にし、インターフェース・パラメーターを設定した後、装置をリスタートまたは再ロードして、RED をアクティブにする必要があります。 RED コマンドの詳しい指定方法については、391ページの『第23章 Random Early Detection フィーチャーの構成および監視』を参照してください。

第23章 Random Early Detection フィーチャーの構成および監視

この章では、輻輳状態時にランダムにパケットを除去するようにインターフェースを構成するために、Random Early Detection (RED) フィーチャーによって提供される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。

- 『Random Early Detection 構成プロンプトへのアクセス』
- 『Random Early Detection 構成コマンド』
- 393ページの『Random Early Detection 監視環境へのアクセス』
- 394ページの『Random Early Detection 監視コマンド』

Random Early Detection 構成プロンプトへのアクセス

RED 構成コマンドを入力する場合には、次の手順を実行します。

1. OPCON (*) プロンプトで、**talk 6** と入力する。
2. `Config>` プロンプトで、**feature red** と入力する。

`RED Config>` プロンプトが現れます。これで、RED 構成コマンドを入力できます。

Random Early Detection 構成コマンド

以下のコマンドを使用すると、トラフィックの輻輳時にパケットを除去する方法を決定する RED オプションを構成することができます。これは、オーバーフローとグローバル再同期を防止することができます。 表50 は、RED 構成コマンドの要約です。この節ではこれらのコマンドを詳細に説明します。コマンドは `RED Config>` プロンプトで入力します。コマンドとオプションをまとめて 1 行に入力するか、コマンドだけを入力して、プロンプトに答えることもできます。コマンドにオプションを付ける代わりに、疑問符 (?) を付けると、コマンド・オプションのリストが表示されます。

表 50. Random Early Detection 構成コマンド

コマンド	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。xxxiページの『ヘルプの入手』 を参照してください。
Delete	RED 構成レコードまたはインターフェース・レコードを、ネットワーク装置の SRAM から削除します。
Disable	ネットワーク装置または特定の出口インターフェースで RED を使用不可にします。
Enable	ネットワーク装置または特定の出口インターフェースで RED を使用可能にします。
List	ネットワーク装置の RED 状況とインターフェース関連の設定について、情報を表示します。
Set	ネットワーク装置上の特定のインターフェースに RED 設定を指定します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Delete

delete コマンドは、インターフェースの RED 構成レコードを、ネットワーク装置の SRAM から削除するのに使用します。

構文: delete interface

interface 削除するインターフェース番号を入力するようにプロンプトが出ます。

例:

```
RED Config> delete interface
Enter RED Interface number to delete [0]? 3
RED interface config record deleted
```

Disable

disable コマンドは、ネットワーク装置に対して、または特定の出口インターフェース上で、RED を使用不可にするのに使用します。

構文: disable red
interface

red ネットワーク装置に対して RED を使用不可にします。

例:

```
RED Config> disable red
RED disabled
```

interface 特定の出口インターフェース上で RED を使用不可にします。

例:

```
RED Config> disable interface
Enter RED Interface number [0]? 2
RED interface disabled
```

Enable

enable コマンドは、ネットワーク装置に対して、または特定の出口インターフェース上で、RED を使用可能にするのに使用します。

構文: enable red
interface

red ネットワーク装置に対して RED を使用可能にします。

例:

```
RED Config> enable red
RED enabled
```

interface 特定の出口インターフェース上で RED を使用可能にします。

例:

```
RED Config> enable interface
Enter RED Interface number [0]? 2
RED interface enabled
```

注: RED を使用可能にできるのは、PPP、Multilink PPP、および Frame Relay のリンクだけです。

List

list コマンドは、ネットワーク装置の RED 状況とインターフェース関連の設定に関する情報を表示するのに使用します。

構文: list all

all ネットワーク装置の RED 状況を表示します。

例:

```
RED Config>list all

        RED Status: Enabled

-----------------------------------------------------
Status  Net If   qW   maxP   minT   maxT    initAvgQ
                              ------ %ofdevQ --------
-----------------------------------------------------
Enable  6   PPP  4    1/512  70     100     60


Abbreviation:

qW = Queue Weight
minT = Minimum Threshold, maxT = Maximum Threshold
maxP = Maximum Drop Probability: 1 drop in 512 pkts
%ofdevQ = A percentage of the Maximum Device Queue
```

Set

set コマンドは、ネットワーク装置上の特定のインターフェースに RED 設定を指定するのに使用します。

構文: set interface

interface *number*

RED オプションが設定されるインターフェースの番号を指定します。

デフォルト値: なし

例:

```
RED config>set interface
Enter RED Interface number [0]? [6]
RED Interface enabled
Exponential Maximum Packet Drop Probability (9 for 1/2e9) (5 - 10) [9]?
Advanced Setting (y/n)? [Yes]: yes

Maximum Device Queue = 5
Weight Factor (1 - 8) [4]?
Minimum Threshold value (% of the max device queue) (0 - 100) [70]?
Maximum Threshold value (% of the max device queue) (0 - 100) [100]?
Initial Average Queue Size (% of the max device queue) (0 - 100) [60]?
Accept input (y/n)? [Yes]: yes
```

Random Early Detection 監視環境へのアクセス

Random Early Detection フィーチャーのコンソール部を使用すると、RED 関連の設定を表示し、管理することができます。 RED 監視環境にアクセスするには、OPCON プロンプト (*) で **talk 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで以下のコマンドを入力します。

```
+ feature red
RED Console>
```

Random Early Detection 監視コマンド

以下のコマンドを使うと、RED 関連の設定項目を表示できます。 表51 は、RED 監視コマンドの要約です。この節ではこれらのコマンドを詳細に説明します。コマンドは、RED Console プロンプトで入力します。コマンドとオプションをまとめて 1 行に入力するか、コマンドだけを入力して、プロンプトに答えることもできます。コマンドにオプションを付ける代わりに、疑問符 (?) を付けると、コマンド・オプションのリストが表示されます。

表 51. RED 監視コマンド

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。
Clear	インターフェースの RED パラメーター設定をリセットします。
List	RED が使用可能になったネットワーク装置のインターフェース設定を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Clear

clear コマンドは、インターフェースの RED パラメーター設定をリセットするのに使用します。 **list** コマンドの説明の例が、**clear** コマンドの結果を示しています。

構文: clear *interface-number*

List

list コマンドは、RED が使用可能になったネットワーク装置のインターフェース設定に関する情報を表示するのに使用します。

構文: list *interface-number*

interface-number

ネットワーク装置内の指定インターフェースの RED 設定をリスト表示します。

例:

```
RED Console>list 6
-------------------------------------------------------------------------------
Status  If   maxQ   avgQ   minT   maxT  qW   maxP  pktCnt    pdpDepth  passCnt  drpCnt
                           (dvQ)  (dvQ)       (pkt) til drp     count     pkt      pkt
-------------------------------------------------------------------------------
Enable   6       5      3      3      5  4  1/512    1:3787        285     4283       1

Abbreviations:

maxQ = Maximum Queue Length, avgQ = Average Queue Size
```

```
minT = Minimum Threshold, maxT = Maximum Threshold
dvQ = Device Queue, qW = Queue Weight
maxP = Maximum Drop Probability: 1 drop in 512 pkts
pktCnt til drp = Packet Count before a drop occurs
pdpDepth = Probability Drop Depth: 1 drop in 2048 depth count

RED Console>clear 6

RED Console>list 6
-------------------------------------------------------------------------------------
Status  If   maxQ   avgQ   minT   maxT  qW   maxP  pktCnt    pdpDepth  passCnt  drpCnt
                           (dvQ)  (dvQ)      (pkt)  til drp     count     pkt     pkt
-------------------------------------------------------------------------------------
Enable   6      5      3      3      5   4  1/512   1:3530   0         0        0


Abbreviations:

maxQ = Maximum Queue Length, avgQ = Average Queue Size
minT = Minimum Threshold, maxT = Maximum Threshold
dvQ = Device Queue, qW = Queue Weight
maxP = Maximum Drop Probability: 1 drop in 512 pkts
pdkCnt til drp = Packet Count before a drop occurs
pdpDepth = Probability drop Depth: 1 drop in 2048 depth count
```

第24章 レイヤー 2 トンネルの使用 (L2TP、PPTP、L2F)

この章では、レイヤー 2 トンネル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。

レイヤー 2 トンネル (L2T) には、L2TP、L2F、PPTP のトンネル・プロトコルがあります。

レイヤー 2 トンネル・プロトコル (L2TP) は、UDP/IP のようなパケット方式データ・ネットワークを通して PPP をトンネル伝送するための IETF トラック規格です。L2TP はコネクション型です。

レイヤー 2 転送 (L2F) とポイントツーポイント・トンネル・プロトコル (PPTP) は、IP ネットワークを通して PPP をトンネル伝送するための IETF の非公式プロトコルです。

注: レイヤー 2 トンネルは、2210 型 1S4 と 1U4 ではサポートされていません。

L2TP の概説

L2TP は、多数の個別の自律プロトコル・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。

従来の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、登録された 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 アドレスを許容す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分担することができ、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、エンド・ユーザー、企業、およびインターネット・サービス提供者のいずれにとっても有益です。

L2TP では、既存のインターネット・インフラストラクチャーの IP 以外のプロトコル・アプリケーションへの現行投資も活用できることが保証されます。

図32 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・コンセントレーター (LAC) と L2TP ネットワーク・サーバー (LNS) の間に、任意の媒体タイプを使用することができます。この例では、必須のトンネル・モデルを使用しています。また、この章では、任意のトンネル・モデル構成についても説明します。

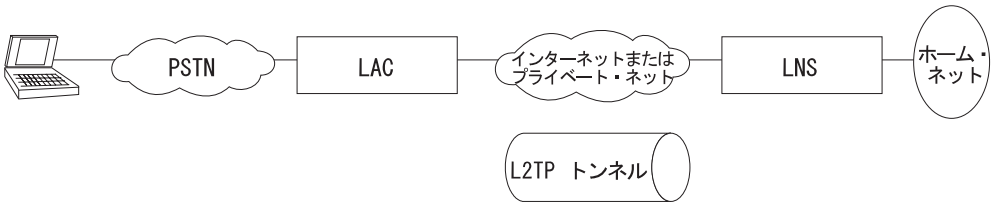


図 32. L2TP ネットワークの例

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・タイプと本文をコード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、インターオペラビリティーも可能になります。

L2TP アクセス集線装置 (LAC)
PPP 運用と L2TP プロトコルの両方を扱える、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を扱います。 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到着したコール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)
ユーザーに一時的なオンデマンド・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 の対によって定義されます。トンネルは、LAC と LNS 間で PPP データグラムを伝送します。 1 つのトンネルが多数のセ

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およびトンネル自体の確立、解放、保守を制御します。

サポートされるフィーチャー

L2TP は UDP/IP を介して稼働し、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
- 小規模ルーター (たとえば、認証ユーザーのプロファイルに基づいて単一静的ルートを確立するルーター) のトンネル伝送
- コールは、LAC から LNS へ (インバウンド)、LNS から LAC へ (アウトバウンド)、またはいずれかのピアによって (両方) 開始することができます。アウトバウンド・コールは、*固定* (常にアップ) またはデマンド・ベースの L2 トンネル伝送セッション。
- 1 つのトンネルでの複数のコール
- PAP、CHAP、および MS-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
- トンネル終了点認証
- 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) ルックアップ・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 ユーザー名ルックアップを使用したトンネル伝送
- SNMP を使用した L2TP トンネルの管理。 *プロトコルの構成と監視 解説書 第 1 巻* の 『SNMP 管理』 の項を参照してください。

注: Rhelm トンネル伝送では、*name@rhelm* 形式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 終了点として)
- **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設定。 L2TP は、データ・チャネルの順序制御も行います。
- ユーザーが UDP ポートに基づいて IP セキュリティー・フィルターを作成できるように L2TP UDP ポート (1701) を設定する機能
- L2TP ルーター・クライアント。 L2TP ルーター・クライアントは、『クライアント開始』 (自発的トンネル伝送とも呼ばれます) モデルです。この機能は、サービス提供者のトポロジーとは無関係に、保護された、トンネル伝送による、マル

チプロトコル・バーチャル私設ネットワーク (VPN) サービスを提供します。この機能により、クライアントと LAC を 1 つの物理ハードウェアに結集することができます。

- インバウンド・コールをリモート・ホスト名に照合して、該当するインターフェースに接続。 リモート・ホスト名が、ホスト名照合用に構成されたインターフェースのいずれにも一致しない場合、そのコールは、リモート・ホスト名照合を使用しないインバウンド・インターフェース上で終了します。

  注: 同じ LAC と LNS の対に対して複数のネット・マッピングを構成した場合、各マッピングにつき 1 つだけトンネルが存在することを確認してください。

- リモート・ホスト名照合を使用しないインバウンド・ネットの自動 IP、IPX、およびブリッジング構成。リモート・ホスト名照合を使用するアウトバウンド・ネットおよびインバウンド・ネットは、手動で構成する必要があります。

次のレイヤー 2 トンネル・プロトコルもサポートされています。

- L2F NAS およびゲートウェイ機能を両方ともサポート
- PPTP ルーター・クライアント、PAC (PPTP アクセス集線装置)、および PNS (PPTP ネットワーク・サーバー) をサポート

L2F は、L2TP をサポートしないネットワーク装置への接続で、相互運用可能なレイヤー 2 トンネル伝送を提供します。

PPTP は、L2TP をサポートしないネットワーク装置への接続で、相互運用可能なレイヤー 2 トンネル伝送を提供します。特に、PPTP は、Microsoft Windows 95 (DUN 1.2 以上)、Windows 98、および Windows NT から IBM のルーターへの VPN サービスに使用できます。

注: L2F と PPTP は、ともに レイヤー 2 トンネル機能に構成されています。

タイミングに関する考慮事項

ルーティング・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 の間の接続には、トンネル伝送のピア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。ピア間の待ち時間が PPP 状態遷移タイムアウト (通常は 3 秒) に達したり、それを超える状態が繰り返される場合は、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場合、接続全般が悪い状況になり、PPP 状態遷移を人為的に活動状態に維持しても、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、接続が非常に悪い状況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を大きく下回っている場合、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。

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 と交渉し、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 については特に重要です。 IBM LNS では、構成された MRU は、プロキシー LCP に許容される最大値です。 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、LAC からの他の LCP オプションは変更せずに、MRU を構成された MRU 値に等しくしようと試みます。

レイヤー 2 トンネルの構成

L2T 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、レイヤー 2 トンネル・フィーチャーにアクセスする。

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. 必要に応じて、L2TP、L2F、および PPTP を使用可能にする。

```
Layer-2-Tunneling config> enable L2TP

Layer-2-Tunneling config> enable L2F

Layer-2-Tunneling config> enable pptp
```

3. 必要な L2T ネットワークを追加する。 LAC、L2F NAS、または PPTP PAC に限定されるときは、L2T ネットワークを追加する必要はありません。同時にトンネル伝送するそれぞれの PPP 接続について、1 つの L2T ネットワークを定義します。

```
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
```

a. L2TP、L2F、または PPTP トンネルを構成する。

AAA ローカル・リストを使用して、L2TP トンネルを構成するには、次のように指定します。

```
Config> add tunnel-profile
Enter name:  []? lns.org
Tunneling Protocol? (PPTP, L2F, L2TP): L2TP
Enter local hostname: []? 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。 *フィーチャーの使用と構成* の 『認証、許可、および会計 (AAA) セキュリティーの使用』 を参照してください。

LNS を構成しているときに、トンネル認証が LAC と LNS の両者で無効になった場合は、トンネル・プロファイルを構成する必要はありません。

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:
Allow inbound access for user? (Yes, No):[Yes]
Will 'peter' be tunneled? (Yes, No): [No] Y
Tunneling Protocol (PPTP, L2F, L2TP): [L2TP] L2TP
Enter local hostname: []? 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>
```

b. インバウンド・トンネルのリモート・ホスト名照合を構成します (必要な場合)。

クライアント・ダイヤルインの場合は、通常はこのステップは不要です。接続に特定のネットワークを使うときに、このオプションを使用してください。

前の構成はネット 10 に対するものと想定します。

```
Config> net 10
     L2TP 10> set remote-hostname
     Remote Tunnel Hostname: [] ibm.com
```

注: リモート・ホスト名照合をオフにするには、次のコマンドを使用します。

```
Config> net 10
     L2TP 10> set any-remote-hostname
```

4. L2TP の発信コールを構成する。次の例は、IP アドレス 1.1.1.1 を持つ LAC および IP アドレス 1.1.1.2 を持つ LNS を示しています。 LNS は、LAC から 5552160 へのダイヤル・オンデマンド ISDN コールを発信するように構成されています。

LNS 構成:

```
Config> add tunnel-profile
     Enter name:  []? lac.org
     Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? lns.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]? 1.1.1.1

            Tunnel name: lac.org
               TunnType: L2TP
               Endpoint: 1.1.1.1
               Hostname: lns.org

     User 'lac.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction outbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lac.org
     L2TP 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN, V34)? [ISDN]
        Outbound calling address: 5552160
        Outbound calling subaddress:
     L2TP 10>
     L2TP 10> encapsulator
     PPP 10> set name vickie  a
     L2TP 10>
     L2TP 10> exit
     Config> add ppp-user larry  b
```

注:

a. LNS 装置が認証される場合は、認証名を設定します。この例には示されていない追加のプロンプトが出ます。詳細については、*ソフトウェア使用者の手引き* の “ポイント・ポイント・プロトコル・インターフェースの使用” の章にある 『PPP 認証の構成』を参照してください。

b. LNS で認証されるユーザーを追加します。この例には示されていない追加のプロンプトが出ます。コマンド構文およびオプションについては、*ソフトウェア使用者の手引き* の “CONFIG プロセス (CONFIG - Talk 6) およびコマンド” の章の Add を参照してください。

LAC 構成:

```
Config> add tunnel-profile
     Enter name:  []? lns.org
     Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? 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]? 1.1.1.2

            Tunnel name: lns.org
               TunnType: L2TP
               Endpoint: 1.1.1.1
```

```
                Hostname: lac.org

     User 'lns.org' has been added
     Config>
     Config> add dev dial-in  a
```

注: 物理的にコールするのに使用されます。

5. L2T ルーター・クライアントを構成する。次の例は、L2TP ルーター・クライアント機能を使用した L2TP ボックス・ボックス接続を示しています。この接続は単方向に設定され、ダイヤル・ベースです。

Client 構成:

```
Config> add tunnel-profile
     Enter name:  []? lns.org
     Tunnel Protocol? (PPTP, L2T, L2TP): [L2TP]
     Enter local hostname: []? client.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]? 1.1.1.1

            Tunnel name: lns.org
               TunnType: L2TP
               Endpoint: 1.1.1.1
               Hostname: client.org

     User 'lns.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction outbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lns.org
     L2TP 10> encapsulator
     PPP 10> set name donald   a
     PPP 10> exit
     L2TP 10> exit
     Config>
```

注: クライアント装置が認証される場合は、認証名を設定します。この例には示されていない追加のプロンプトが出ます。詳細については、*ソフトウェア使用者の手引き* の 『PPP 認証の構成』を参照してください。

.

LNS 構成:

```
Config> add tunnel-profile
     Enter name:  []? client.org
     Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? lns.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]? 1.1.1.2

            Tunnel name: client.org
               TunnType: L2TP
               Endpoint: 1.1.1.2
               Hostname: lns.org

     User 'client.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
```

```
L2TP 10> set connection-direction inbound
L2TP 10> set remote-hostname client.org
Config>
Config> add ppp-user donald b
Config>
```

注: b-- LNS で認証されるユーザーを追加します。この例には示されていない追加のプロンプトが出ます。詳細については、*ソフトウェア使用者の手引き* の 『**add** 構成コマンド』 の項を参照してください。

6. 必要であれば、**set** コマンド、および **enable** コマンドを使って、さまざまな L2T のフィーチャー・パラメーターを構成する。

```
Layer-2-Tunneling Config>set ?
Layer-2-Tunneling Config>enable ?
```

7. 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)。これは、インバウンドおよび *すべての*インバウンド・トンネル・ホスト名に設定します。

```
Layer-2-Tunneling Config>encapsulator
PPP-L2TP Config>
```

PPP の構成が完了したら、**exit** を押して、L2T 構成環境に戻ります。

第25章 レイヤー 2 トンネル・プロトコルの構成および監視

この章では、レイヤー 2 トンネル伝送 (L2T) の構成とオペレーショナル・コマンドについて説明します。L2T には、レイヤー 2 トンネル伝送プロトコル (L2TP)、レイヤー 2 転送プロトコル (L2F)、およびポイントツーポイント・トンネル伝送プロトコルが含まれます。本章には、以下の節が含まれています。

L2T インターフェース構成プロンプトへのアクセス

L2T インターフェース構成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 6** と入力する。
2. `Config>` プロンプトで **add dev layer-2-tunneling** と入力する (または、**add l2-nets** コマンドを使う)。 (410ページの『Add』を参照)。
3. `Config>` プロンプトで、**n** *interface#* と入力する。

```
Config> add device layer-2-tunneling
Enter the number of Layer-2-Tunneling interfaces [1]
Adding device as interface 8
Defaulting Data-link protocol to PPP
Config> n 8
Session configuration
L2T config:   8>
```

L2 トンネル伝送インターフェース構成コマンド

表52 は、L2T インターフェース構成コマンドの要約です。これらのコマンドは、`L2T Config n>` プロンプトで入力します (*n* はネットワーク番号です)。

表 52. L2 トンネル伝送インターフェース構成コマンド

コマンド	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。xxxiページの『ヘルプの入手』 を参照してください。
Disable	発信コールを使用不可にします。
Enable	発信コールを使用可能にします。
Encapsulator	L2T インターフェースの PPP パラメーターを構成します。**注:** encapsulator オプションは、インターフェースにリモートのホスト名が構成されていないと使用できません。
List	L2T インターフェースに関する情報を表示します。
Set	さまざまな L2T インターフェース・パラメーターを設定できます。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Disable

disable コマンドは、L2TP アクセス集線装置 (LAC) からのアウトバウンド・コールを無効にします。

構文:

disable outbound-calls-from-lac

outbound-calls-from-lac

LNS が LAC から L2TP トンネルを通してダイヤル・シグナルを開始することを防止します。

Enable

enable コマンドは、L2TP アクセス集線装置 (LAC) からのアウトバウンド・コールを有効にします。このコマンドは、L2TP と一緒に使ってください。

構文:

enable outbound-calls-from-lac

outbound-calls-from-lac

LNS が LAC から L2TP トンネルを通してダイヤル・シグナルを開始できるようにします。

例:

```
L2T 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN, V34)? [ISDN]
        Outbound calling address: 1234
        Outbound calling subaddress:
L2T 10>
```

Encapsulator

encapsulator コマンドは、L2T インターフェースの PPP パラメーターを構成するのに使用します。

構文:

encapsulator

このコマンドは、リモートのホスト名が構成されていないと使用できません。
`ppp-L2tp config>` プロンプトで使用できるコマンドについては、413ページの『Encapsulator』 を参照してください。

List

list コマンドは、さまざまな L2T インターフェース構成パラメーターの状態を表示します。

構文:

list

```
Layer-2-Tunneling Config>list
CONNECTION TYPE
---------- -----
  Connection Direction            INBOUND
  Remote Tunnel Hostname           *ANY*
```

Set

L2T インターフェースの操作パラメーターを構成するには、set コマンドを使用します。

構文:

set
- any-remote-hostname
- connection-direction
- idle
- remote-hostname

any-remote-hostname
このネット上のアウトバウンド・リモート・ホスト名をクリアし、インバウンド・リモート・ホスト名照合を使用不可にします。

connection-direction [inbound] or [outbound] or [both]
接続を開始できるのは、このネット上のピア (インバウンド)、ローカル装置 (アウトバウンド)、あるいはピアまたはローカル装置のいずれか (または両方) のどれであるかを指定します。「両方」を指定した場合は、アイドル・タイムを 0 に指定することはできません。

デフォルト値: インバウンド

idle-time *seconds*
L2 トンネル伝送がこのネット上のトンネル・セッションを切断する前に非活動状態になっている秒数を指定します。値 zero は、そのトンネルは固定であり、切断してはならないことを示します。

有効範囲: 0 ～ 1024

デフォルト値: 0

remote-hostname *hostname*
ピアのトンネル・ホスト名を指定します。

アウトバウンド・トンネルの場合、ホスト名が AAA サブシステムに構成されているトンネル・プロファイルを指定します。これは、ピアが自身を識別するために使用するトンネル・ホスト名になります。

インバウンド・トンネルの場合は、このホスト名で自身を識別できるトンネル・ピアだけがこのインターフェースに接続できます。

有効値: 1 ～ 64 桁の ASCII 文字から成る任意の名前

デフォルト値: *名前*

L2 トンネル伝送フィーチャー構成プロンプトへのアクセス

L2 トンネル伝送フィーチャー構成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 6** と入力する。
2. `Config>` プロンプトで、**feature layer-2-tunneling** と入力する。

L2 トンネル伝送フィーチャー構成コマンド

表53 は、L2 トンネル伝送フィーチャー構成コマンドの要約を示し、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。これらのコマンドは、`Layer-2-Tunneling Config>` プロンプトで入力します。

表 53. L2 トンネル伝送フィーチャー構成コマンド

コマンド	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。xxxiページの『ヘルプの入手』 を参照してください。
Add	L2 トンネル伝送ネットとピアを追加します。
Disable	L2 トンネル伝送機能を無効にします。
Enable	L2 トンネル伝送機能を有効にします。
Encapsulator	リモート・ホスト名で構成されていないすべての L2 トンネル・ネットについて、 PPP パラメーターを構成できるようにします。
List	L2 トンネル伝送構成に関する情報を表示します。
Set	バッファー、コール受信ウィンドウ、およびその他の L2 トンネル伝送パラメーターを設定できます。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、L2-Nets 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 終了点です。

構文:

add L2-nets

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。

L2-Nets を L2 トンネル伝送構成に追加します。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。

追加ネット数は、自動的に追加されるネットの数を指します。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 アドレスは、推奨されている運用方式です。 L2 ネットで番号制アドレスを使用する必要がある場合は、IP プロトコル構成環境で変更することができます (*プロトコルの構成と監視 解説書 第 1 巻* の 『IP の構成』 の章を参照してください)。

Disable

disable コマンドは、L2 トンネル伝送機能を使用不可にします。

構文:

disable
- fixed-ip-source-address
- fixed-udp-source-port
- force-chap-challenge
- hiding-for-pap-attributes
- L2f
- L2tp
- pptp
- proxy-auth
- proxy-lcp
- sequencing
- tunnel-auth

fixed-ip-source-address
ルーターが、指定された発信元アドレスを使用不可にします。

fixed-udp-source-port
固定 UDP ポートを使って消去します。このパラメーターを使用不可にした場合、ユーザーは LAC と LNS の間に IP アドレスによる IP セキュリティー・フィルターを構成することを強制されます。

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、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 の間のプロキシー PAP 情報の暗号化を使用不可にします。

L2f このルーター上の L2F を使用不可にします。

L2tp このルーター上の L2TP を使用不可にします。

pptp このルーター上の PPTP を使用不可にします。

proxy-auth
LAC からLNS へ PPP プロキシー認証を送信するのを使用不可にします。

proxy-lcp
LAC からLNS へ LCP 情報を送信するのを使用不可にします。

sequencing
データ・チャネルの順序制御を使用不可にします。

tunnel-auth
このルーターに共有の秘密に基づくトンネル・ピアの認証を使用不可にします。

Enable

enable コマンドは、L2 トンネル伝送機能を使用可能にします。

構文:

enable
- fixed-ip-source-address
- fixed-udp-source-port
- force-chap-challenge
- hiding-for-pap-attributes
- L2f
- L2tp
- pptp
- proxy-auth
- proxy-lcp
- sequencing
- tunnel-auth

fixed-ip-source-address
ルーターが、インバウンド宛先アドレスと等しい発信元アドレスを使用して応答します。

fixed-udp-source-port
このパラメーターを使用可能にすると、L2 に対して UDP ポートに基づく IP セキュリティー・フィルターを構成することが可能になり、L2 トラフィックの暗号化または認証を容易に行うことができます。 UDP ポートを 1701 で L2TP 用に設定します。

force-chap-challenge
LNS がプロキシー CHAP を受信する場合も、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 の間のプロキシー PAP 情報の暗号化を使用可能にします。

L2f このルーター上の L2F を使用可能にします。

L2tp このルーター上の L2TP を使用可能にします。

pptp このルーター上の PPTP を使用可能にします。

proxy-auth
LAC からLNS へ PPP プロキシー認証を送信するのを使用可能にします。

proxy-lcp
LAC からLNS へ LCP 情報を送信するのを使用可能にします。

sequencing
データ・チャネルの順序制御を使用可能にします。

tunnel-auth

このルーターに共有の秘密に基づくトンネル・ピアの認証を使用可能にします。

Encapsulator

encapsulator コマンドは、ppp-L2tp config> プロンプトにアクセスして、インバウンドおよび*あらゆる*リモート・ホスト名として構成されているすべてのレイヤー 2 トンネル伝送インターフェース向けに PPP パラメーターを構成します。

構文:

encapsulator

List

listコマンドは、さまざまな L2 トンネル伝送構成パラメーターの状態を表示します。

構文:

list

```
Layer-2-Tunneling Config>list
GENERAL ADMINISTRATION
------- --------------
  L2TP                                  = Enabled
  L2F                                   = Disabled
  PPTP                                  = Disabled
  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
  Local Hostname                        = Host6

DATA CHANNEL SETTINGS
---- ------- --------
  Force CHAP Challenge (extra security)= Disabled
  Hiding for PAP Attributes             = Disabled
  Hardware Error Polling Period (Sec)   = 120
  Sequencing                            = Enabled

MISCELLANEOUS
-------------
  SEND PROXY-LCP FROM LAC               = Enabled
  SEND PROXY-AUTH FROM LAC              = Enabled
  Fixed UDP Source Port (1701)          = Enabled
  Fixed Source IP Address               = Enabled
```

Set

L2 トンネル伝送の操作パラメーターを構成するには、set コマンドを使用します。

構文:

set

- buffers
- error-check-direction
- host-lookup-password
- local-hostname

max-calls

max-tunnels

transmit-retries

tunnel-rcv-window

buffers

要求された内部 L2 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分が利用可能になります。 L2T が活動状態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 (419ページの『Memory』を参照してください)。

有効範囲: 1 ～ 4000

デフォルト値: モデルにより異なる

モデル	デフォルト値
x2x、xSx、1Ux	30
x4x	100

error-check-period [seconds]

LAC のハードウェア・エラー・ポーリング期間を指定します。ポーリング期間は、WAN エラー通知メッセージとなって、LAC から LNS に送信されます。範囲は、60 ～ 65 000 秒です。

デフォルト値: 120 秒

host-lookup-password

RADIUS トンネルの許可のために、共用秘密を指定します。これは、サーバーに構成されている秘密と一致しなければなりません。

デフォルト値: なし。

local-hostname

ローカル・ルーターを識別するホスト名の文字列を指定します。これは、トンネル設定のメッセージの中で送信されます。

デフォルト値: IBM

max-calls

LAC または LNS として同時に活動状態にできる、すべてのトンネルを通るコールの最大数を指定します。

有効範囲: モデルにより異なる

モデル	範囲
x2x、xSx、1Ux	1 ～ 30
x4x	1 ～ 200

デフォルト値: モデルにより異なる

モデル	デフォルト値
x2x、xSx、1Ux	10
x4x	30

max-tunnels

LAC または LNS として同時に活動状態にできるトンネルの最大数を指定します。

有効範囲: モデルにより異なる

モデル	範囲
x2x、xSx、1Ux	1 ～ 30
x4x	1 ～ 200

デフォルト値 : モデルにより異なる

モデル	デフォルト値
x2x、xSx、1Ux	10
x4x	30

transmit-retries

セッションまたはトンネルが非活動状態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。

有効範囲: 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 L2TP 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。

有効範囲: 1 ～ 100

デフォルト値: 4

L2 トンネル伝送監視プロンプトへのアクセス

L2 トンネル伝送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。

L2 トンネル伝送監視コマンド

この節では、L2 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54は、L2 トンネル伝送監視コマンドの要約です。

表 54. L2 トンネル伝送監視コマンド

コマンド	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。xxxiページの『ヘルプの入手』 を参照してください。
Call	コール設定中の各コールに関する統計と情報を表示します。
Kill	トンネルを即時に終了します。

表 54. L2 トンネル伝送監視コマンド (続き)

コマンド	機能
Memory	現在の L2 トンネル伝送バッファー割り割り当てと使用状況を表示します。
Start	別のピアとのトンネル伝送を開始します。
Stop	トンネル伝送を停止し、各ピア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。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Call

call コマンドは、コール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 このコールで発生した一般的な伝送エラーを表示します。

例:

```
Layer-2-Tunneling Console> call errors
CallID | Serial # | ACK-timeout | Dropped pkts
 56744 |        1 |           0 |            0
```

CallID このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

ACK-timeout
ピアからタイムアウト通知を受信した回数

Dropped pkts
このコールで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、ピアによって紛失として通知されたパケットです。

physical-errors
コールで発生したデータ・エラーを表示します。

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 このコールに対応するローカル識別子

Serial #
このコールをログに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・エラーを含むパケットの数

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
配列エラーが発生した回数

time since updated
前回のエラーのポーリングからの経過時間

queue 各コール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 このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

Tx Win
ピア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 このコールで送信される次のパケット・シーケンス番号

Nr このコール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 各コール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 このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

Net # このコールに対応する装置番号。 LNS のコールの場合、これは L2 ネットです。 LAC のコールの場合、これは最初のコールを受信した PPP 装置です。

State 現在のコールの状態。有効なコールの状態は、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 コール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
ピア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
ピアのコール ID

TunnelID
このコールに対応するローカル・トンネル

statistics
各コール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 このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

Tx Pkts
このコールの送信されたパケット数

Tx Bytes
このコールの送信されたバイト数

Rx Pkts
このコールの受信されたパケット数

Rx Bytes
このコールの受信されたバイト数

RTT このコールの現行の算定一巡時間

ATO このコール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。トンネルの終了はピアに通知されません。

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*
終了させるトンネルを指定します。

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、別のピアとのトンネル伝送を開始するのに使用します。

構文:

start　　**tunnel** *hostname*

(ホスト名を入力するように求めるパラメーターはありません)

tunnel*hostname*
L2T 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、各トンネル内の各コールの状態を表示します。

errors トンネル上で発生したエラーを表示します。

例:

```
Layer-2-Tunneling Console> tunnel errors
Tunnel ID | Type |ACK-timeouts
 96785    | L2TP |    0
 43690    | PPTP |    2
 96785    | L2F  |    0
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用中のトンネル伝送プロトコルのタイプ

ACK-timeouts
ピアからタイムアウト通知を受信した回数

peer トンネルとそのトンネルに対応するピアを表示します。

例:

```
Layer-2-Tunneling Console> tunnel peer
Tunnel ID | Type | Peer ID | Peer Hostname
 96785    | L2TP |   89777 | peer1
 11264    | L2F  |   46538 | peer2
 34653    | L2F  |   11209 | peer3
 87511    | PPTP |   55377 | peer4
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用中のトンネル伝送プロトコルのタイプ

Peer ID
このトンネルに割り当てられたピアのトンネル識別子

Peer Hostname
ローカル・データベースに表示されるピアのホスト名

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
 76488    | L2F  |      4 |      4 |      5 |      6 |    0 |    0
 22209    | PPTP |      4 |      4 |      5 |      6 |    0 |    0
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用中のトンネル伝送プロトコルのタイプ

Rx Win
ローカルの受信ウィンドウを構成するパケットの最大数

Tx Win
ピア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
 17404    | PPTP |  0      | Established |   00:00:00     |       1 |  0
 96785    | L2TP |  0      | Established |   00:02:05     |       2 |  0
 38237    | L2F  |  0      | Established |   00:00:00     |       1 |  0
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用中のトンネル伝送プロトコルのタイプ

Peer ID
このトンネルに割り当てられたピアのトンネル識別子

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
ホストはピアからの応答を待っています。

Wait Ctrl Conn
ホストはピアからの接続標識を待っています。

Time since chg
前回の状態変更からの経過時間

 # Calls
このトンネル上の活動状態のコールの数

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:

L2 トンネル伝送監視コマンド (Talk 5)

```
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
 96366    | L2F  |   9344  |  34578   |   305   |  4300    |   10  | 31
 12344    | PPTP |    24   |   478    |   115   |  2745    |   10  | 31
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用中のトンネル伝送プロトコルのタイプ

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
 30000    | L2F  |  11.0.0.104     |  1058   |   1090
 45772    | PPTP |  11.4.4.027     |  1345   |   1020
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用中のトンネル伝送プロトコルのタイプ

Peer IP address
このトンネルのピアの IP アドレス

UDP Src
このトンネルの UDP 発信元ポート

UDP Dest
このトンネルの UDP 宛先ポート

L2 トンネル伝送の動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

レイヤー 2 トンネル伝送は、制限なしに、CONFIG (Talk 6) **delete interface** コマンドをサポートします。

GWCON (Talk 5) Activate Interface

レイヤー 2 トンネル伝送は、GWCON (Talk 5) **activate interface** コマンドをサポートします。ただし、次の考慮事項があります。

他の PPP インターフェース上では追加の制限はありません。

レイヤー 2 トンネル伝送の構成変更はすべて、次のものを除いて、自動的にアクティブになります。

GWCON (Talk 5) activate interface コマンドによって変更がアクティブにならないコマンド
CONFIG, net, enable ccp **注:** これが CCP が使用可能になった状態で最初の PPP ネットである場合、圧縮は使用可能になりません。
CONFIG, net, set lcp options (mru option) **注:** MRU 値は、リブート時にルーターに割り振られたバッファー・サイズよりも大きい値に設定されることはありません。

GWCON (Talk 5) Reset Interface

レイヤー 2 トンネル伝送は、GWCON (Talk 5) **reset interface** コマンドをサポートします。ただし、次の考慮事項があります。

他の PPP インターフェース上では追加の制限はありません。

レイヤー 2 トンネル伝送の構成変更はすべて、次のものを除いて、自動的にアクティブになります。

GWCON (Talk 5) reset interface コマンドによって変更がアクティブにならないコマンド
CONFIG, net, enable ccp **注:** これが CCP が使用可能になった状態で最初の PPP ネットである場合、圧縮は使用可能になりません。
CONFIG, net, set lcp options (mru option) **注:** MRU 値は、リブート時に PPP インターフェースに割り振られたバッファー・サイズよりも大きい値に設定されることはありません。

CONFIG (Talk 6) 即時変更コマンド

レイヤー 2 トンネル伝送では、装置の操作状態を即時に変更する次の CONFIG コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、これらの変更は保管され、保存されます。

コマンド
CONFIG, feature layer-2-tunneling, disable fixed-ip-source-address
CONFIG, feature layer-2-tunneling, disable fixed-udp-source-port
CONFIG, feature layer-2-tunneling, disable force-chap-challenge
CONFIG, feature layer-2-tunneling, disable hiding-for-pap-attributes
CONFIG, feature layer-2-tunneling, disable proxy-auth

CONFIG, feature layer-2-tunneling, disable proxy-lcp
CONFIG, feature layer-2-tunneling, disable sequencing
CONFIG, feature layer-2-tunneling, disable tunnel-auth
CONFIG, feature layer-2-tunneling, enable fixed-ip-source-address
CONFIG, feature layer-2-tunneling, enable fixed-udp-source-port
CONFIG, feature layer-2-tunneling, enable force-chap-challenge
CONFIG, feature layer-2-tunneling, enable hiding-for-pap-attributes
CONFIG, feature layer-2-tunneling, enable proxy-auth
CONFIG, feature layer-2-tunneling, enable proxy-lcp
CONFIG, feature layer-2-tunneling, enable sequencing
CONFIG, feature layer-2-tunneling, enable tunnel-auth
CONFIG, feature layer-2-tunneling, set error-check-period
CONFIG, feature layer-2-tunneling, set host-lookup-password
CONFIG, feature layer-2-tunneling, set local-hostname
CONFIG, feature layer-2-tunneling, set transmit-retries
CONFIG, feature layer-2-tunneling, set tunnel-rcv-window
CONFIG, add tunnel-profile

動的再構成不能コマンド

次の表は、動的に変更できないレイヤー 2 トンネル伝送構成コマンドを記述しています。これらのコマンドを活動化するには、装置を再ロードまたはリスタートする必要があります。

コマンド
CONFIG, feature layer-2-tunneling, enable l2f
CONFIG, feature layer-2-tunneling, enable l2tp
CONFIG, feature layer-2-tunneling, enable pptp
CONFIG, feature layer-2-tunneling, disable l2f
CONFIG, feature layer-2-tunneling, disable l2tp
CONFIG, feature layer-2-tunneling, disable pptp
CONFIG, feature layer-2-tunneling, set buffers
CONFIG, feature layer-2-tunneling, set max-calls
CONFIG, feature layer-2-tunneling, set max-tunnels

第26章 ネットワーク・アドレス変換機構の使用

ネットワーク・アドレス変換機構 (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機構 (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、また公衆ネットワーク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 公衆ネットワークのホストの有効なアドレスであり、公衆ネットワーク内で固有であることが必要です。公衆ネットワーク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 IP 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、公衆ネットワークには分かりません。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ネットワーク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 のこのフィーチャーは、私設アドレスが知られるのを防止するための一種のファイアウォールとしての役目を果たします。

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、終了点 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) 決定を下す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。

426ページの図33 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。

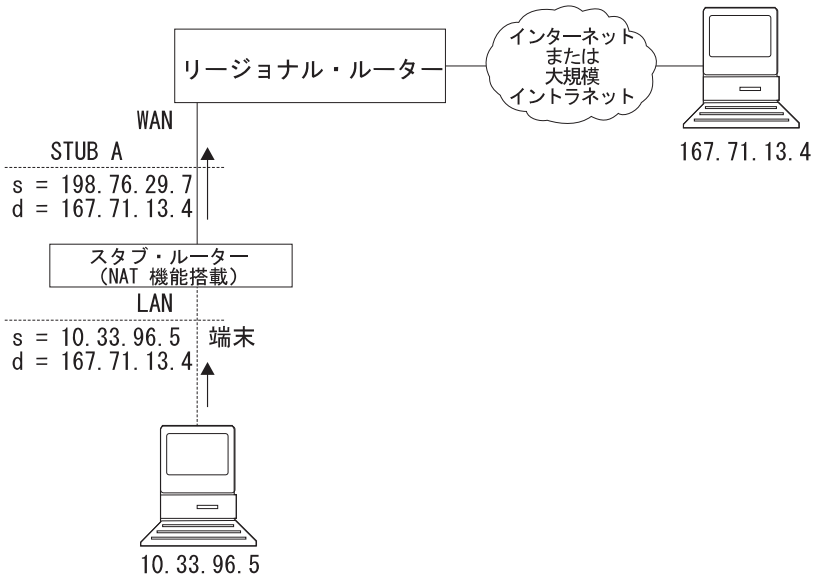


図 33. NAT を実行するネットワーク

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、私設 IP アドレスは *translate range* に割り当てます。

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、パケットがアウトバウンドされるときに、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。インバウンド・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、発信元私設アドレス 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 は公衆ネットワークから隠されるので、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・ポート変換機構

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・プールにつき 1 つの NAPT アドレスしか構成できません。

NAPT は、ごく簡単に 1 つの公開アドレス 指定するか、あるいは NAPT トラフィックが使用する動的アドレス・インターフェースを指定するだけで構成できます (動的アドレス・インターフェースは、公開アドレスを取り出すために PPP/IPCP を使用します)。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、公衆ネットワーク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インバウンド・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、事前割り当てされた私設ポートを組み込んだ 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 用に事前割り当てされた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 (事前割り当てアドレス 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 公衆アドレスと事前割り当てポート番号が、10.1.1.3 ポート 21 と 10.1.1.1 ポート 21 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、サーバーの事前割り当て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、公衆ネットワークに接続されているインターフェースに、1 つのインバウンド・パケット・フィルターと 1 つのアウトバウンド・パケット・フィルターを構成することが必要です。また、インバウンド・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、アウトバウンド・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ことも必要です。インバウンド・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インバウンド・パケットを NAT に渡します。アウトバウンド・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アウトバウンド・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、348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、429ページの図34 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、433ページの『第27章 ネットワーク・アドレス変換機構の構成および監視』を参照してください。

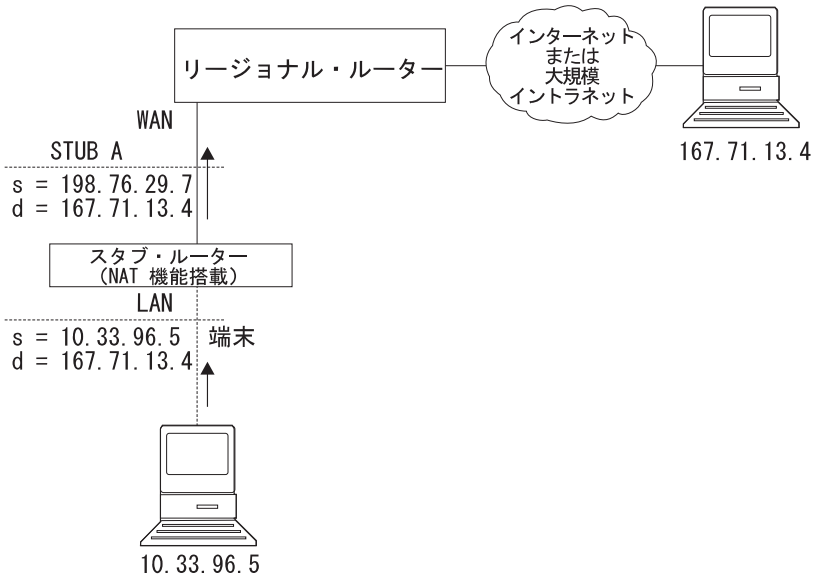


図 34. NAT を実行するネットワーク

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 No 198.76.29.7 255.255.255.0 6 pool1 198.76.29.7
   NAT config> reserve No 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、公衆ネットワーク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 サーバーの両方の役目を果たします。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 (公衆ネットワークに接続されているインターフェース) のインバウンド・パケット・フィルターとアウトバウンド・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インバウンド・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。インターネット発信元の 0.0.0.0 のアドレスとマスクは、公衆ネットワークからのすべての発信元アドレスを 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発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27章 ネットワーク・アドレス変換機構の構成および監視

この章では、ネットワーク・アドレス変換機構 (NAT) の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・アドレス変換機構の構成環境へのアクセス』
- 『ネットワーク・アドレス変換機構構成コマンド』
- 440ページの『ネットワーク・アドレス変換機構の監視環境へのアクセス』
- 440ページの『ネットワーク・アドレス変換機構監視コマンド』
- 442ページの『NAT 動的再構成サポート』

ネットワーク・アドレス変換機構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・アドレス変換機構構成コマンド

この節では、ネットワーク・アドレス変換機構 (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 55. NAT 構成コマンド

コマンド	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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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させて 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させて 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する時間を決めます。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、NAT の始動時のアソシエーションを確立します (これは、決して変更されることはありません)。

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、公衆ネットワーク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: 公衆ネットワークに固有の有効な IP アドレス公衆ネットワークは、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。さらに、公開アドレス・プールに動的 IP インターフェースを付加するのにも使用できます。

構文:

reserve *dynamic [interface][public-address][mask][number-in-group] name [napt-address]*

注: カッコ内の値は、例として示しています。

- Dynamic: この入力項目が公開アドレスのグループのためのものであるか、あるいは IPCP を使う PPP 接続の IP アドレスを取り出す動的アドレス・インターフェースのものなのかを指定します。有効値は *yes* または *no* です。デフォルト値は *no* です。ダイナミックが *yes* の場合は、インターフェースと名前を指定するだけですみます。

ダイナミックが *no* の場合は、インターフェースは指定しませんが、その他の数値はすべて指定します。

- Interface: 動的アドレス・インターフェースを IP 内の構成として指定します。任意の有効なインターフェース番号を指定できます。デフォルト値は 0 です。

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 個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。この場合、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: 公衆ネットワークに固有の有効な 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、IP 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 no 9.8.7.1 255.255.255.0 3  pool1 0.0.0.0
reserve no 9.8.7.6 255.255.255.0 12 pool1 9.8.7.9
reserve yes 2 dynamic_ip_pool
```

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 結合を保持する時間。結合とは、私設アドレスと公衆 IP アドレスの 1 つとの間の関係を保持することです。

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 結合を保持する時間。結合とは、私設アドレスと公衆 IP アドレスの 1 つとの間の関係を保持することです。

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ネットワーク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・アドレス変換機構の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、**+** プロンプトで以下の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・アドレス変換機構監視コマンド

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。以下のコマンドは NAT> プロンプトで入力します。

表 56. NAT 監視コマンド

コマンド	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。 xxxi ページの『ヘルプの入手』 を参照してください。

表 56. NAT 監視コマンド (続き)

コマンド	機能
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。 xxxiページの『下位レベル操作環境の終了』 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

NAT 動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

NAT は、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、NAT には適用されません。 NAT には、インターフェースに関連した SRAM レコードがありません。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、NAT には適用されません。 NAT には、インターフェースに関連した SRAM レコードがありません。

GWCON (Talk 5) 構成要素リセット・コマンド

NAT は、次の NAT 固有の GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature NAT, Reset NAT コマンド

説明: **Reset** は、すべての NAT タイマーを停止し、NAT 状態を使用不可に設定し、NAT が使用するすべてのメモリーを解放します。変換マッピング、パケット・フラグメント、および TCP セッション情報はすべて、消去されます。NAT の初期化ルーチンは、NAT の状態を構成レコードから読み取ります。NAT が使用可能になっている場合、公衆アドレスのプール、私設アドレスの範囲、マッピング・テーブル、フラグメント再組み立てテーブル、タイムアウト、およびタイマーはすべて、構成レコードから初期設定されます。この時点で、NAT は、IP パケット・フィルターによって NAT に提示されるパケットを受け入れる準備が再びできます。

ネットワークの影響:

NAT がすでに使用可能になっている場合、すべての TCP セッションはタイムアウトになり、アプリケーションに通知されます。 UDP とデータグラムのマッピングは失われ、これらのデータ・ストリーム上のパケットは除去されます。NAT が再初期化された後、UDP とその他のデータグラム・パケット・ストリームと同じように、TCP セッションも再確立することができます。

制限: IP が NAT にパケットを渡すために、IP パケット・フィルターは正しく構成する必要があります。

すべての NAT コマンドは、**GWCON, feature nat, reset nat** コマンドによってサポートされます。

CONFIG (Talk 6) 即時変更コマンド

NAT は、装置の操作状態を即時に変更する次の CONFIG コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、これらの変更は保管され、保存されます。

コマンド
CONFIG, feature nat, reset nat

第28章 LAN へのダイヤルイン・アクセス (DIAL) 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。 446 ページの図35 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。

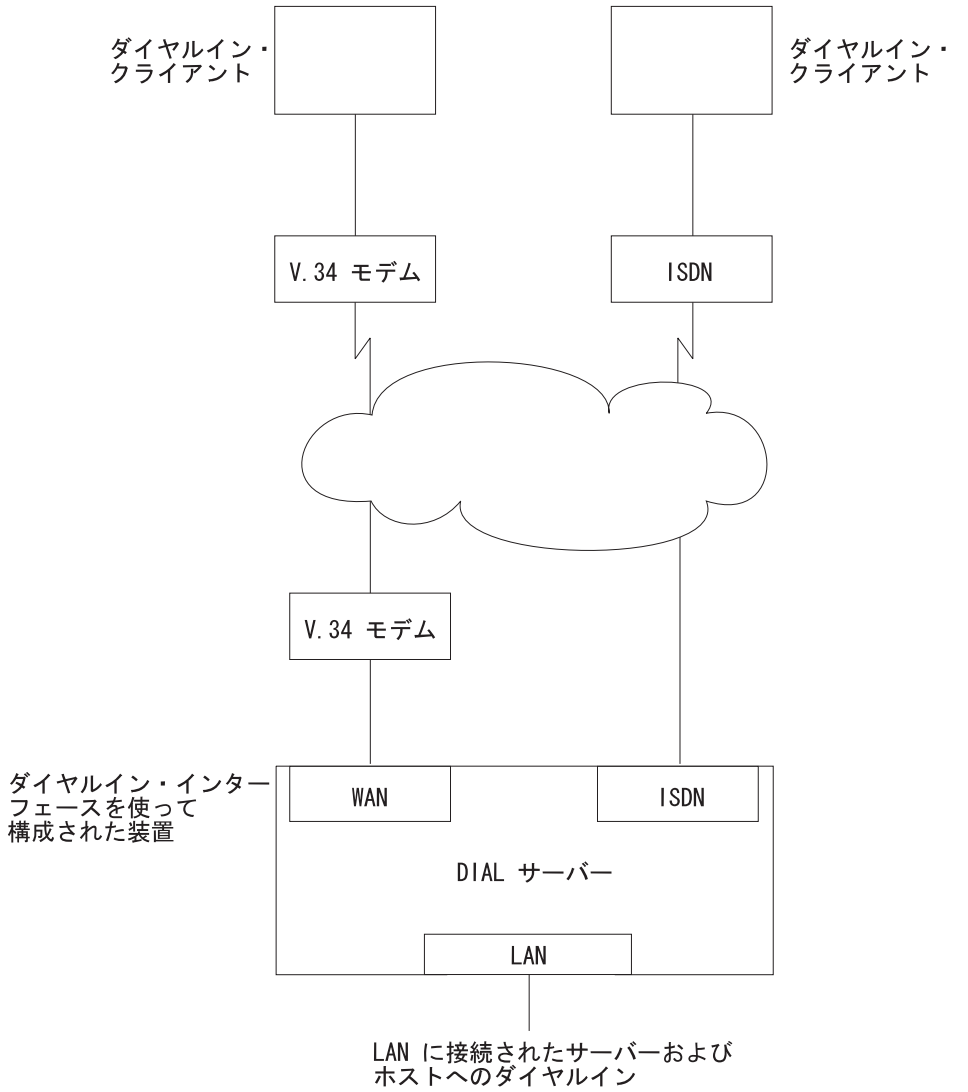


図35. ダイヤルインをサポートする DIAL サーバーの例

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。447ページの図36 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。

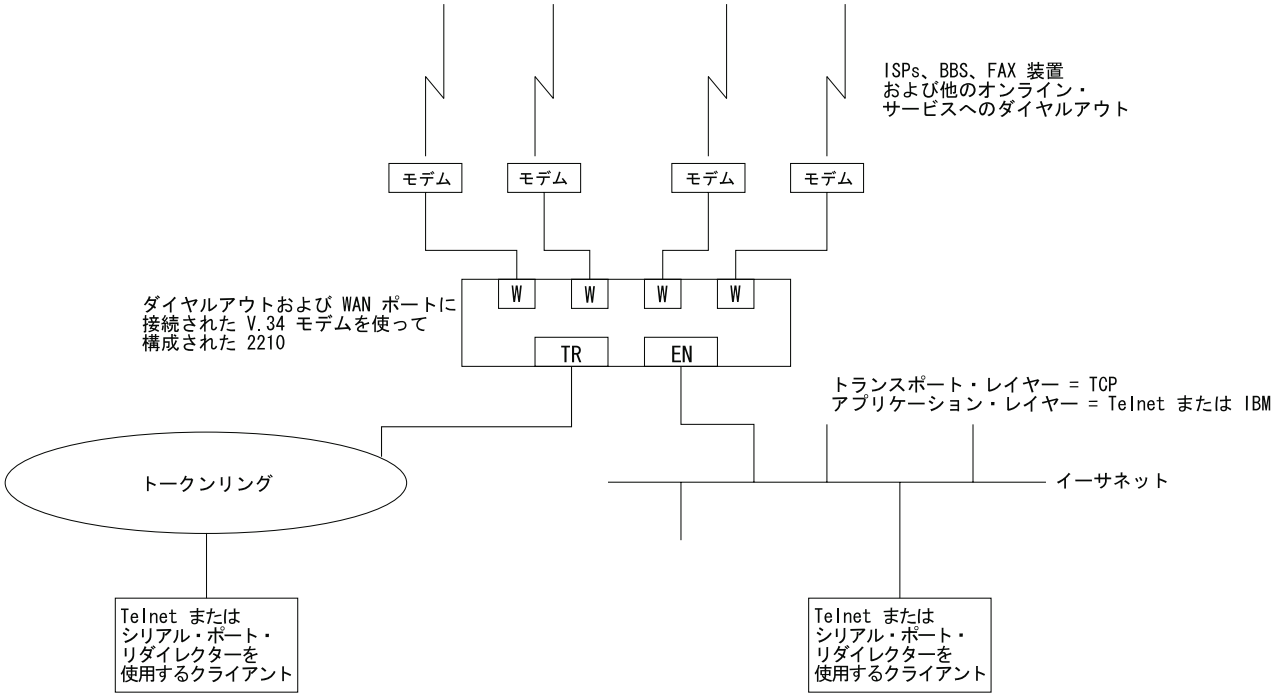


図 36. ダイヤルアウトをサポートする DIAL サーバーの例

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、ヌル・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 449 ページの『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: DIAL 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ています。

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:

1. この節で説明するパラメーターは、オーバーライドしてはなりません。オーバーライドすると、ダイヤルイン機能が正しく動作しなくなります。
2. 一部のパラメーターは、表示されなかったり、構成できない場合があります。パラメーターについての詳しい説明は、*ソフトウェア使用者の手引き* の 『ダイヤル回線の構成および監視』 の章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 コールバックが交渉された場合、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。 *ソフトウェア使用者の手引き* の 『Shiva パスワード認証プロトコル (SPAP)』 および 『マルチリンク PPP プロトコルの使用』 の項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、任意のインバウンド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。 450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。これらのコールはインバウンドであり、アウトバウンド・コール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: パラメーターについての詳しい説明は、*ソフトウェア使用者の手引き* の 『ポイント・ポイント・プロトコル・インターフェースの使用』 の章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、Windows 3.1、OS/2、および DOS バージョンの IBM DIAL ダイヤルイン・クライアント用に必要です。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・アクセスのユーザーにとって重要な機能がオンになります。 DIAL 機能の詳細については、*ソフトウェア使用者の手引き* の 『ポイント・ポイント・プロトコル・インターフェースの使用』 の章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 つに V.34 または ISDN 基本ネットを構成する。構成についての詳しい説明は、*ソフトウェア使用者の手引き* の 『V.34 ネットワーク・インターフェースの使用』 および 『ISDN インターフェースの使用』 の章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、新しいネットワークを作成し、それぞれのネットワーク番号を報告し、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: 現行の最大ネットが 3 であり、基本 2 ネットに 1 つのダイヤルイン・ネットを追加したいと想定します。

図37 は、ダイヤルイン・インターフェースの定義例です。

図 37. ダイヤルイン・インターフェースの追加

```
Config>add dev dial-in
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Base net for this circuit [0]? 2

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               CSR  81600, CSR2  80C00, vector 94
Ifc 1     V.34 Base Net          CSR  81620, CSR2  80D00, vector 93
Ifc 2     V.34 Base Net          CSR  81640, CSR2  80E00, vector 92
Ifc 3     PPP Dial-in Circuit
Ifc 4     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、またはヌル・モデム、または ISDN インターフェース。構成情報については、*ソフトウェア使用者の手引き* の 『V.34 ネットワーク・インターフェースの使用』 の章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 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。

ヌル・モデムの使用

ヌル・モデムを使用するときは、D25NM-3 フル・ハンドシェークを使用してください。

ピン・マッピング

1 から 1 へ	**1 から 1 へ**
2 から 3 へ	**3 から 2 へ**
4 から 5 へ	**5 から 4 へ**
6 から 8 と 20 へ	**8 と 20 から 6 へ**
7 から 7 へ	**7 から 7 へ**

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、*ソフトウェア使用者の手引き* の 『V.34 ネットワーク・インターフェースの使用』 の章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 基本ネットワーク上に複数の回線を構成することができます。ただし、同時に活動状態にできる回線は 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)、*ソフトウェア使用者の手引き* の 『PPP 認証プロトコル』 の項で説明しているように、PPP ユーザーを追加する。追加する 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. **feature dials** コマンドを使用して、グローバル・ダイヤルアウト・パラメーターを構成する。 *ソフトウェア使用者の手引き* の **feature** コマンドの項を参照してください。

   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. IBM DIAL ダイヤルアウト・クライアントが正しく機能するために、SNMP を 2210 上で使用可能にする必要があり、*public* と呼ばれる SNMP コミュニティーが、読み取りアクセス権を指定して 2210 上で定義される必要があります。これは、ダイヤルアウト選択アプリケーションがネットワーク上のダイヤルアウト・サーバーを見付けるために必要です。 SNMP を使用可能にする方法、および SNMP コミュニティーの構成方法については、*プロトコルの構成と監視 解説書 第 1 巻* の 『SNMP 管理』 の項を参照してください。

9. 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集合です。ユーザーがダイヤルアウトすることが必要になると、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、*ソフトウェア使用者の手引き* の 『V.34 ネットワーク・インターフェースの使用』 の章に定義されているダイヤルアウト・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 (*ソフトウェア使用者の手引き* の 『ダイヤル回線の構成および監視』 の章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。

グローバル DIAL パラメーターを構成する前に

この節では、グローバル DIAL サーバー・パラメーターについて説明します。

サーバー提供の IP アドレス

ルーターを構成して、ダイヤルイン・クライアントが接続期間中に使用する IP アドレスを提供できるようにすることが可能です。ルーターがクライアントに割り当てるアドレスは、4 通りの方法で取り出すことができます。その方法を以下に優先順に示します。

1. ユーザー ID

   IP アドレスを、各クライアントの PPP ユーザー・プロファイルに保管することができます。クライアントが接続して IP アドレスを要求したときに、ルーターはそのユーザーの PPP ユーザー・プロファイルに構成されているアドレスを取り出します。この方法では、ユーザーは毎回同じ IP アドレスを入手することができますが、各ユーザーごとに固有の IP アドレスが必要です。

   PPP ユーザー・プロファイルに IP アドレスを構成するには、Config> **add ppp-user** コマンドを使用します。

2. インターフェース

   IP アドレスを、ダイヤルイン・インターフェース構成に保管することができます。クライアントが接続して IP アドレスを要求したときに、ルーターは接続に使用されたインターフェースからアドレスを取り出します。この方法は、各ダイヤルイン・インターフェースごとに固有の IP アドレスが必要です。

   インターフェース IP アドレスを設定するには、次のようにします。

   - Config> **list devices** コマンドを使用して、ハードウェア・インターフェースに割り当てられているインターフェース番号を表示する。
   - Config> **net 'x'** コマンド ('x' は、構成されたインターフェース番号) を使用して、インターフェースのコマンド・プロンプトにアクセスする。
   - PPP Config> **set ipcp** コマンドを使用して、インターフェース IP アドレスを設定する。

3. プール

   IP アドレスの集合を、IP アドレス・プールに保管することができます。クライアントが接続してアドレスを要求したときに、ルーターはプールからアドレスを取り出します。クライアントが切断すると、アドレスはプールに戻されます。この方法は、ダイヤルイン・クライアントの IP アドレスを構成するための単一の場所を提供するので、アドレス・サーバーは必要ありません。

   IP アドレスのプールを追加するには、DIALs config> **add ip-pool** コマンドを使用します。

4. DHCP プロキシー

   IP アドレスを DHCP サーバーからリースすることができます。クライアントが接続してアドレスを要求したときに、ルーターはクライアントの代わりに DHCP サーバーからアドレスを要求します。この方法は、DHCP サーバーが LAN 上に存在するか、ルーター内に構成されていることが必要です。1 つの DHCP サーバーが、複数のルーター上のクライアントのアドレスを提供することができます。詳細については、『動的ホスト構成プロトコル (DHCP)』を参照してください。

   DHCP サーバーを追加するには、`DIALs config>` **add dhcp-server** コマンドを使用します。

IP アドレス割り当て方式

接続期間中にダイヤルイン・クライアントが使用する IP アドレスは、5 つの異なるソースから入手できます。ソースを優先順に示すと、次のようになります。

1. クライアント提供
2. ユーザー ID 割り当て
3. インターフェース割り当て
4. アドレス・プール
5. DHCP サーバー

ダイヤルイン・クライアントが接続すると、ルーターはアドレスが見つかるまで、またはすべてのソースが尽きるまで、これらのソースを順次に検索します。 IP アドレスが見つからなかった場合、IPCP ネゴシエーションは失敗します。これらの方式は、任意の組み合わせで使用できます。

デフォルト構成は、次のとおりです。

```
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
```

注: デフォルトでは、PPP ユーザー・プロファイル、インターフェース、または IP アドレス・プールには、アドレスは構成されていません。

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 フィーチャーは、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、またはリース期間が満了するまでの間、IP アドレスのリースを受けることができます。 DHCP サーバーから割り当てられる IP アドレスは、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 についての説明は、*ソフトウェア使用者の手引き* の 『IP 制御プロトコル』 の項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 を活動化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必要があります。

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 サーバーを構成して、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に注意してください)。
3. プロキシー DHCP の標準的な設定では、Client-Specified、Userid、Interface、および Pool の IP アドレス・ネゴシエーション・オプションを使用不可にする。

```
Dials Config>list ip
DIALs client IP address specification:
Client : disabled
UserID : disabled
Interface : disabled
DHCP Proxy : enabled
```

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 に送信して入手することが必要です。
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。常にリモート・アクセス・ボックスからサーバーに 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も必要です。 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上で、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。そのために、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。 454ページの『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。また、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・プールはお互いに同じサブネット内に存在することが必要です。

動的ドメイン名サーバー (DDNS)

ドメイン名サーバー (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 フィーチャーというのは、DDNS DHCP サーバーおよび DNS サーバーと共に使用した場合、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フィーチャーをいいます。このフィーチャーは、プロキシー DHCP と一緒にしか使用できません。

2210 上の動的 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 (*ソフトウェア使用者の手引き* の 『PPP 認証プロトコル』 の項を参照)、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。これにより、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29章 DIAL の構成

この章では、DIAL 構成コマンドおよびオペレーショナル・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。

DIAL グローバル構成環境へのアクセス

グローバル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、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 **feature dials** コマンドを入力して `DIALs Config>` プロンプトを表示し、DIAL グローバル・パラメーター構成環境にアクセスします。

DIAL グローバル構成コマンド

表 57. DIAL グローバル構成コマンド

コマンド	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。 xxxi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するか、または IP アドレス・プールを追加します。
Delete	DHCP サーバーをリストから削除するか、またはアドレス・ブロックを IP アドレス・プールから除去します。
Disable	IP アドレス割り当て方式、ダイヤルアウト・プロトコル、マルチシャシー MP、SPAP バナー、および動的 DNS を使用不可にします。
Enable	各種の IP アドレス割り当て方式、ダイヤルアウト・プロトコル、マルチシャシー MP、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 DIAL 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、バーチャル・コネクション (VC)、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。

表 57. DIAL グローバル構成コマンド (続き)

コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、新しいプロキシー DHCP サーバーをサーバーのリストに追加するか、または IP アドレス・プールを追加するのに使用します。

プロキシー DHCP サーバー・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。

IP アドレス・プール・フィーチャーは、ルーターがローカル定義されたアドレス・プールからダイヤルイン・クライアントへの IP アドレスを取り出すことができる方法を提供します。クライアントは、ルーターへの接続期間中、このアドレスを使用することができます。プールは、1 つまたは複数のブロックの IP アドレスから構成されます。ブロックの最大数は 20 です。各ブロックは、基本 IP アドレスとブロック内のアドレスの個数によって定義されます。各ブロック内のアドレスは、基本アドレスから始まって、昇順に連続しています。

構文:

add dhcp-server *ipaddress*

ip-pool *baseaddress #addresses*

dhcp-server *ipaddress*

指定の IP アドレスをもつ dhcp サーバーを追加します。

例:

```
DIALs Config> add dhcp-server
DIALs Proxy DHCP server address [0.0.0.0]? 10.0.0.1
```

ip-pool *baseaddress #addresses*

アドレス・ブロックを IP プールに追加します。

例:

```
DIALs Config> add ip-pool
Base address []? 192.1.100.18
Number of addresses [1]? 57
DIALs config>add ip-pool
Base address []? 192.2.200.1
Number of addresses [1]? 250
DIALs config>list ip-pools
Configured IP address pools:
          Base Address      Last Address        Number
          ------------      ------------        ------
          192.1.100.18      192.1.100.74            57
           192.2.200.1     192.2.200.250           250
```

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か、または IP アドレス・プールからアドレス・ブロックを削除するのに使用します。

構文:

delete dhcp-server *ip address*

ip-pool *baseaddress #addresses*

dhcp-server *ipaddress*

指定の IP アドレスをもつ dhcp サーバーを削除します。

例:

```
DIALs Config> delete dhcp-server
Enter the address to be deleted [0.0.0.0]? 10.0.0.1
```

ip-pool *baseaddress #addresses*

IP プールからアドレス・ブロックを削除します。

例:

```
DIALs Config> delete ip-pool
Base IP address of the block to be removed []? 192.2.200.1
```

Disable

disable コマンドは、IP アドレス割り当て方式、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-assignment *type*

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。

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、455ページの『動的ドメイン名サーバー (DDNS)』を参照してください。

IP-address-assignment ***type***

各種の IPCP アドレス割り当て方式を使用不可にします。以下のいずれも指定できます。

- Client - クライアント指定 IP アドレス割り当てを防止します。
- Userid - 認証ユーザー・プロファイルを使用して IP アドレスを調べるのを防止します。

- Interface - ルーターがインターフェースの IPCP 設定値を使用するのを防止します。
- Pool - ルーターが IP アドレス・プールを使用してクライアントにアドレスを割り当てるのを防止します。
- DHCP-proxy - ルーターが DHCP サーバーからアドレスをリースするのを防止します。

割り当て方式についての詳細は、452ページの『サーバー提供の IP アドレス』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 アドレス割り当て方式、ダイヤルアウト・プロトコル、SPAP バナー、および動的 DNS を使用可能にするのに使用します。

構文:

enable dynamic-dns
ip-address-assignment . . .
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。

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、455ページの『動的ドメイン名サーバー (DDNS)』を参照してください。

IP-address-assignment *type*
各種の IPCP アドレス割り当て方式を使用可能にします。ルーターは使用可能にされている各方式をリスト順に試行します。以下のいずれも指定できます。

- client - 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。
- Userid - ルーターは認証された PPP 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。
- Interface - ルーターはインターフェースに構成された 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。

- Pool - ルーターは IP アドレス・プールからアドレスを要求します。アドレスが利用可能の場合、それがクライアントに提供されます。
- DHCP-proxy - ルーターは DHCP からアドレスのリースを試みます。成功した場合、そのアドレスがクライアントに提供されます。

割り当て方式についての詳細は、452ページの『サーバー提供の IP アドレス』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。SPAP バナーのテキストを入力するのには、463ページの『Set』に説明されている **set spap-banner** コマンドを使用します。詳細については、*ソフトウェア使用者の手引き* 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、各ネットワークの DHCP 状態およびリース時間を監視することができます。例については、*ソフトウェア使用者の手引き* の **listipcp** コマンドの項を参照してください。

構文:

list

all

dhcp-servers

dial out

dynamic-dns

ip-address-assignment

ip-pools

name-servers

spap-banner

time-allowed

vc-parameters

例:

```
DIALs config>li all
DIALs client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled


Configured IP address pools:
     Base Address      Last Address        Number
     ------------      ------------        ------
       11.0.0.100        11.0.0.129            30
       11.0.0.210        11.0.0.229            20

Configured DHCP servers:          11.0.0.2         11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10
```

```
Dynamic DNS: Enabled

Primary Domain Name Server     (DNS): 11.0.0.2
Secondary Domain Name Server   (DNS): None
Primary NetBIOS Name Server   (NBNS): 11.0.0.2
Secondary NetBIOS Name Server (NBNS): None

Time allowed for connections: Unlimited

SPAP banner  :Enabled
Welcome to the network...

Box-level dial-out settings
Inactive timer:                                        15
LAN Protocols enabled for dial-out:         TELNET DIALs
Server name:                                          DIALOUT_SERVER

Number of Mac Addresses defined = 0
Base MAC Address: 000000000000

VC: Maximum Virtual Connections = 50
VC: Maximum suspend time (hours) (0 is unlimited) = 12
VC: Idle timeout period (seconds) = 30

Multi-chassis MP: Endpoint discriminator (0 means use box s/n) = 0

DIALs config>
```

この例は、以下のことを示しています。

DIALs client IP address specification
IP アドレス割り当て方式とそれが使用可能かどうかを表示します。このセクションおよびボックス・レベル・ダイヤルアウト設定値が入っているセクションの表示は、**list ip-address-assignment** コマンドへの応答として受け取ります。

IP address pools
構成された IP アドレス・プールを表示します。このセクションの表示は、**list ip-pool** 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。

vc connections
構成されたバーチャル・コネクションに関する情報を表示します。

multi-chassis mp
構成された終了点識別子を表示します。

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
multi-chassis-mp
nbns . . .
spap-banner . . .
time-allowed
vc-parameters

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 サーバーへの IP 接続を持つ 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、453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・ネットワーク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・ネットワーク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、接続は無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。 30 文字までの長さの任意の文字列を使用できます。デフォルト値は『2210_DIALS_SERVER』 です。これは、IBM DIAL 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 次ドメイン名サーバー (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 時に交渉されます。

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 時に交渉されます。

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・ネットワークだけです。

#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>
```

multi-chassis-mp

使用する終了点識別子を設定します。一組に結合するすべてのリンクは、同じ終了点識別子を持っていなければなりません。

例:

```
DIALs Config> set multi-chassis-mp
   Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
```

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。

spap-banner

SPAP 認証を正常に完了したすべてのクライアントに送信するメッセージを構成することができます。

例:

```
DIALs config>set spap-banner
SPAP banner  :Disabled

Enter Banner: Welcome to the network...
```

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限に接続していられることを意味します。

vc-parameters

このパラメーターは、デフォルトのグローバル・バーチャル・コネクション属性を設定するのに使用します。システムは、接続の最大数、最中断時間、および非活動タイムアウト値の入力を求めるプロンプトを出します。

例:

```
Config> feature DIALs
DIALs Config> set vc-parameters
Maximum Virtual Connections [50]? 40
Maximum suspended time (hours) (0 is unlimited) [10]? 18
Inactivity Timeout (seconds) [30]? 60
DIALs Config>
```

Maximum Virtual Connections

活動状態または中断状態にできるバーチャル・コネクションの最大数。 MP で VC を使用する場合、この値は物理接続の数より 1 だけ大きい値に構成してください。

有効値: 0 ～ 255

デフォルト値: 50

Maximum suspended time

システムが接続を終了する前に、バーチャル・コネクションを中断状態における最大時間。このパラメーターを 0 に指定すると、バーチャル・コネクションは無限に中断状態でいられます。

有効値: 0 ～ 48

デフォルト値: 12

Inactivity Timeout

中断する前に、バーチャル・コネクションを非活動状態における秒数

有効値: 10 ～ 1024

デフォルト値: 30

DIAL グローバル監視環境へのアクセス

DIAL 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。

1. OPCON プロンプトで、**talk 5** と入力します。 (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、端末に GWCON プロンプト (+) 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. + プロンプトで **feature dials** コマンドを入力して DIALS Console> プロンプトを表示して、グローバル監視環境にアクセスします。

   例:

   ```
   + feature dials
   DIALS Console>
   ```

DIAL グローバル監視コマンド

表 58. DIAL グローバル監視コマンド

コマンド	機能
Clear	特定の中断されたバーチャル・コネクションをクリアします。
List	各種のバーチャル・コネクションの状態、またはすべてのバーチャル・コネクションを表示します。
Reset	DIALS パラメーターを動的に活動化します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Clear

clear コマンドは、特定の中断されたバーチャル・コネクションをクリアするのに使用します。

構文:

clear vc *connection_id*

vc *connection_id*

終了する中断バーチャル・コネクションを指定します。 *connection_id* を入手するには、**list all-vc** または **list suspended-vcs** コマンドを入力します。

List

list コマンドは、すべてのバーチャル・コネクション、活動状態のバーチャル・コネクション、中断されたバーチャル・コネクション、または vc-parameters の値を表示するのに使用します。

構文:

list all

active-vcs

all-vcs

dhcp-servers

ip-address-assignment

ip-pool

suspended-vcs

active-vcs

すべての活動状態のバーチャル・コネクションの属性を表示します。属性の説明については、**all-vcs** パラメーターの項を参照してください。

all-vcs

すべての活動状態および中断状態のバーチャル・コネクションの属性を表示します。この表示は、**list active-vcs** コマンドと **list suspended-vcs** コマンドの表示を組み合わせたものです。

例:

```
+ feature dials
DIALS console> list all
 DIALs client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled


Current IP address pools:
     Base Address      Last Address         Total          Free
     ------------      ------------         -----          ----
*      11.0.0.100        11.0.0.129           30            30
       11.0.0.210        11.0.0.229           20            19

Current DHCP servers:           11.0.0.2         11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10


Active VCs:
Conn ID    Interface Idle-Timeout Connected Username
========== ========= ============ HHH:MM:SS ================
1656494850         8           30   0:26:15 don
7293521502         9           30   1:41:57 jane


Suspended VCs:
           Hrs.Max
Conn ID    Suspend Suspended Username
========== =======  HH:MM:SS ======================
9256166098      12   0: 4:13 joe
```

活動および中断 VC の属性は、次のとおりです。

Conn ID

バーチャル・コネクションの接続 ID。システムは、接続を確立するときに ID を割り当てます。

Username
AAA、RADIUS、またはバーチャル・コネクションを確立するローカル・リスト・ユーザー

活動 VC の場合:

Interface
バーチャル・コネクションを管理しているネットワーク・インターフェース

注: VC が中断したこのインターフェースを使用している他のユーザーが問題を起こすのを避けるために、インターフェース割り当てを使用しているダイヤルアップ・クライアントには、IP アドレスを割り当てないでください。

Idle Timeout
システムが VC を中断する前に非活動状態になっている時間数 (分)。これは **set** コマンドの非活動タイマーの値に一致しています。

Connected HHH:MM:SS
VC がインターフェースに接続されていた時間数 (時間、分、秒)

中断 VC の場合:

Hrs. Max Suspended
システムが接続を終了する前に VC が中断状態でいられる最大時間。これは **set** コマンドの最大中断時間の値に一致します。

Suspended HH:MM:SS
VC が中断されていた合計時間数 (時間、分、秒)

dhcp-servers
DHCP サーバーとその IP アドレスについて構成された情報を表示します。

ip-address-assignment
IP アドレスをクライアントに割り当てるのに使用できる方式を表示します。

ip-pool
現在のプールの使用状況を表示します。

例:

```
DIALs Console> list ip-pool
Current IP address pools:
     Base Address      Last Address         Total          Free
     ------------      ------------         -----          ----
*    192.1.100.18      192.1.100.74            57            57
      192.2.200.1     192.2.200.250           250           250

Note: The * indicates from which block the next address will be retrieved.
```

suspended-vcs
すべての中断状態のバーチャル・コネクションの属性を表示します。属性の説明については、**all-vcs** パラメーターの項を参照してください。

vc-parameters
set vc-parameters コマンドを使用して設定された vc-parameters の値を表示します。

Reset

reset コマンドは、`talk 6` で DIALs インターフェースに加えられた構成変更を動的に活動化するのに使用します。

構文:

reset all

dhcp-parameters

ip-address-assignment

ip-pool

vc-parameters

all DHCP、IP アドレス割り当て、および IP プールの構成変更を動的に活動化します。

dhcp-parameters
DHCP 構成を動的に活動化します。

ip-address-assignment
IP アドレス割り当て方式の構成を動的に活動化します。

ip-pool
IP アドレス・プールの構成を動的に活動化します。

vc-parameters
VC 構成変更を動的に更新します。

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。

表59 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 59. 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
? (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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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・プールを定義するのに使用します。*** 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、*ソフトウェア使用者の手引き* 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および監視』 の章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60 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 60. 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
? (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。 xxxi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。 xxxiページの『下位レベル操作環境の終了』 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・ネットワークの現在の状態、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

非活動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。

活動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
```

活動 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
```

DIAL サーバー動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

LAN へのダイヤルイン・アクセス (DIAL) サーバーは、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

LAN へのダイヤルイン・アクセス (DIAL) サーバーは、制限なしに、GWCON (Talk 5) **activate interface** コマンドをサポートします。

次の表は、GWCON (Talk 5) **activate interface** コマンドが起動されるときにアクティブになる、LAN へのダイヤルイン・アクセス (DIAL) サーバーの構成変更を要約しています。

GWCON (Talk 5) activate interface コマンドによって変更がアクティブになるコマンド
CONFIG, feature dials, disable spap-banner
CONFIG, feature dials, enable spap-banner
CONFIG, feature dials, set dial-out inactivity-timer
CONFIG, feature dials, set spap-banner

GWCON (Talk 5) Reset Interface

DIAL サーバーは、制限なしに、GWCON (Talk 5) **reset interface** コマンドをサポートします。

次の表は、GWCON (Talk 5) **reset interface** コマンドが起動されるときにアクティブになる、DIAL サーバーの構成変更を要約しています。

GWCON (Talk 5) reset interface コマンドによって変更がアクティブになるコマンド
CONFIG, feature dials, disable spap-banner
CONFIG, feature dials, enable spap-banner
CONFIG, feature dials, set dial-out inactivity-timer
CONFIG, feature dials, set spap-banner

GWCON (Talk 5) 構成要素リセット・コマンド

DIAL サーバーは、次の DIAL サーバー固有の GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature Dials, Reset DHCP-Parameters コマンド

説明: このコマンドは、プロキシー DHCP 機能に関連した DIAL パラメーターをリセットします。

ネットワークの影響:
なし。

制限: なし。

次の表は、**GWCON, feature dials, reset dhcp-parameters** コマンドが起動されるときにアクティブになる、DIAL サーバーの構成変更を要約しています。

GWCON, feature dials, reset dhcp-parameters コマンドによって変更がアクティブになるコマンド
CONFIG, feature dials, add dhcp-server

CONFIG, feature dials, delete dhcp-server
CONFIG, feature dials, set dhcp-gateway-address

GWCON, Feature Dials, Reset IP-Address-Assignment コマンド

説明: このコマンドは、IP アドレスの割り当て方式の変更をアクティブにするのに使用されます。これは、現在割り当てられているアドレスを変更するのではなく、将来の接続で IP アドレスが割り当てられる方法を指定します。動的 DNS 構成変更も、このコマンドを使用してアクティブになります。

ネットワークの影響:
なし。

制限: なし。

次の表は、**GWCON, feature dials, reset ip-address-assignment** コマンドが起動されるときにアクティブになる、DIAL サーバーの構成変更を要約しています。

GWCON, feature dials, reset ip-address-assignment コマンドによって変更がアクティブになるコマンド
CONFIG, feature dials, enable dynamic-dns
CONFIG, feature dials, enable ip-address-assignment
CONFIG, feature dials, disable dynamic-dns
CONFIG, feature dials, disable ip-address-assignment

GWCON, Feature Dials, Reset IP-Pools コマンド

説明: このコマンドは、ネットワーク接続を中断することなく、IP アドレス・プールの定義をリセットします (アドレスの追加または除去)。新しい IP アドレス・プール定義に、そのプールにすでに入っていて、現在使用されているアドレスが含まれていない場合、そのアドレスは、リセット後も使用されたままです。これらのアドレスがインターフェースによって解放されても、IP アドレス・プールに戻らず、再び割り当てられることもありません。

ネットワークの影響:
なし。

制限: なし。

次の表は、**GWCON, feature dials, reset ip-pools** コマンドが起動されるときにアクティブになる、DIAL サーバーの構成変更を要約しています。

GWCON, feature dials, reset ip-pools コマンドによって変更がアクティブになるコマンド
CONFIG, feature dials, add ip-pool
CONFIG, feature dials, delete ip-pool

GWCON, Feature Dials, Reset VC-Parameters コマンド

説明: このコマンドは、バーチャル・コネクション・パラメーターとテーブル・サイズをリセットします。

ネットワークの影響:
テーブル・サイズが縮小すると、一部のバーチャル・サーキットが終了する場合があります。

制限: なし。

次の表は、**GWCON, feature dials, reset vc-parameters** コマンドが起動されるときにアクティブになる、DIAL サーバーの構成変更を要約しています。

GWCON, feature dials, reset vc-parameters コマンドによって変更がアクティブになるコマンド
CONFIG, feature dials, set vc-parameters

GWCON, Feature Dials, Reset All コマンド

説明: このコマンドは、DIAL reset コマンドを使用してリセットできるすべてのパラメーターをリセットします。

ネットワークの影響:
個々の reset コマンドを参照してください。

制限: なし。

次の表は、**GWCON, feature dials, reset all** コマンドが起動されるときにアクティブになる、LAN へのダイヤルイン・アクセス (DIAL) サーバーの構成変更を要約しています。

GWCON, feature dials, reset all コマンドによって変更がアクティブになるコマンド
CONFIG, feature dials, add dhcp-server
CONFIG, feature dials, add ip-pool
CONFIG, feature dials, delete dhcp-server
CONFIG, feature dials, delete ip-pool
CONFIG, feature dials, enable dynamic-dns
CONFIG, feature dials, enable ip-address-assignment
CONFIG, feature dials, disable dynamic-dns
CONFIG, feature dials, disable ip-address-assignment
CONFIG, feature dials, set dhcp-gateway-address
CONFIG, feature dials, set ip-pools
CONFIG, feature dials, set vc-parameters

CONFIG (Talk 6) 即時変更コマンド

DIAL では、装置の操作状態を即時に変更する次の CONFIG コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、これらの変更は保管され、保存されます。

コマンド
CONFIG, feature dials, set dns

CONFIG, feature dials, set nbns
CONFIG, feature dials, set time-allowed

動的再構成不能コマンド

次の表は、動的に変更できない DIAL サーバー構成コマンドを記述しています。これらのコマンドを活動化するには、装置を再ロードまたはリスタートする必要があります。

コマンド
CONFIG, feature dials, set dial-out servername
CONFIG, feature dials, set laa
CONFIG, feature dials, set multi-chassis-mp
CONFIG, feature dials, disable dial-out dials
CONFIG, feature dials, disable dial-out Telnet
CONFIG, feature dials, enable dial-out dials
CONFIG, feature dials, enable dial-out Telnet

ダイヤルアウト動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface コマンド

ダイヤルアウトは、制限なしに、CONFIG (Talk 6) **delete interface** コマンドをサポートします。

GWCON (Talk 5) Activate Interface コマンド

ダイヤルアウトは、GWCON (Talk 5) **activate interface** コマンドをサポートしますが、次の考慮事項があります。

- 基本ネットがすでにアクティブである場合を除いて、ダイヤルアウト・ネットを活動化することはできません。
- 基本ネット・タイプが V34 である場合を除いて、ダイヤルアウト・ネットを活動化することはできません。

ダイヤルアウト・インターフェース固有コマンドはすべて、GWCON (Talk 5) **activate interface** コマンドによってサポートされます。

GWCON (Talk 5) Reset Interface コマンド

ダイヤルアウトは、GWCON (Talk 5) **reset interface** コマンドをサポートします。ただし、次の考慮事項があります。

基本ネットが変更されている場合、ダイヤルアウト・ネットをリセットすることはできません。

ダイヤルアウト・インターフェース固有コマンドはすべて、GWCON (Talk 5) **reset interface** コマンドによってサポートされます。

第30章 DHCP サーバーの使用

この章では、DHCP サーバーの使用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。

DHCP の紹介

動的ホスト構成プロトコル (DHCP) は、ブートストラップ・プロトコル (BOOTP) にもとづいたクライアント・サーバー・プロトコルです。DHCP サーバーは、中央制御の再使用可能 IP アドレスのほか、その他の TCP/IP 構成情報を DHCP クライアントに提供します。新規または既存のユーザーに対する構成情報の配布作業について、ネットワーク管理者の作業負荷を軽減します。このフィーチャーは、RFC 2131 に準拠していますが、RFC 2131 には含まれていないその他の多くのフィーチャーもサポートします。 RFC 951 に定義されている BOOTP クライアントもサポートします。

DHCP をサポートするクライアントは、ブロードキャスト DISCOVER メッセージを送信し、ネットワーク内の DHCP サーバーを検出して、ネットワークを通して構成情報を動的に提供 (OFFERED) してもらえます。DHCP で要求や応答を通信するには、よく知られている BOOTP UDP ポートを使用します (サーバーは 68、クライアントは 67)。DHCP のクライアントとサーバーは、既存の BOOTP リレー・エージェントを使って、サービス範囲を拡張できます。DHCP は、ネットワークの変更など、統計的に構成されたネットワーク上で数多くの利点があります。IP アドレスは、クライアントにリースされるので、クライアントが IP アドレスを必要としなくなったり、ほかのサブネットに移ってしまうと、アドレスは解放されて (RELEASED)、ほかのクライアントが使用します。

DHCP の操作

クライアントは、DHCP を使って IP アドレスなどの IP ネットワーク構成情報を中央の DHCP サーバーから取得できます。DHCP サーバーは、クライアントに提供するアドレスを恒久的に割り当てるのか、あるいは特定の期間だけリースするのかを管理します。リース・アドレスを受け取ったクライアントは、アドレスの再確認とリースの更新をサーバーに定期的に要求しなければなりません。

アドレスの割当、リース、リースの更新などの処理は、すべて DHCP サーバーとサーバー・プログラムが実行し、この内容はエンド・ユーザーに透過的に扱われます。DHCP サーバーが提供するオプションをクライアントが受けたり、使用するときは、RFC アーキテクチャーによるメッセージを使用します。たとえば、次のように入力します。

1. クライアントは、メッセージ (クライアント ID を含める) をブロードキャストして自分の存在を公表します (DHCPDISCOVER メッセージ)。ここで、サブネ

ット・マスク、ドメイン・ネーム・サーバー、ドメイン・ネーム、静的ルートなどの希望オプションとあわせて、IP アドレスを要求します。

2. オプションとして、DHCP および BOOTP のメッセージを転送するようにネットワーク上のルーターを構成しておくと (BOOTP リレーを使用する)、ブロードキャスト・メッセージは、付加ネットワーク上の DHCP サーバーにも転送されます。
3. 各 DHCP サーバーは、クライアントから DHCPDISCOVER メッセージを受け取ると、クライアントに DHCPOFFER メッセージを送って、IP アドレスを提供します。 DHCP サーバーは、IP アドレスを提供する前に、ネットワーク上に同じ IP アドレスがないかどうかを確認します。 サーバーは、構成ファイルを確認して、クライアントに割り当てるアドレスを静的アドレスにするか動的アドレスにするかを決めます。動的アドレスにする場合は、サーバーは、 アドレス・プールの中から、もっとも過去に使われたアドレスを選択します。アドレス・プールは、クライアントにリースする IP アドレスの集合体です。静的アドレスの場合は、サーバーは、DHCP サーバーの構成にあるクライアントのステートメントを使って、クライアントにオプションを割り当てます。DHCP サーバーは、アドレスを提供するときは、提供したアドレスを確保しておきます。
4. クライアントは、提供メッセージを受け取ると、使用するサーバーを選択します。DHCP クライアントは、提供を受けると、要求したオプションに対して、提供されたオプションがいくつあるかをメモしておきます。DHCP クライアントは、最初の提供を受けてから 4 秒間のあいだ、DHCP サーバーから連続的に提供を受け取り、それぞれの提供について、要求したオプションに対していくつのオプションが提供されているかをメモにとります。これが終わると、DHCP クライアントは、すべての提供内容を比較し、自分の基準にあったものを選択します。
5. クライアントは、メッセージをブロードキャストして、選択したサーバーを表示し、そのサーバーが提供した IP アドレスの使用を要求します (DHCPREQUEST メッセージ)。
6. サーバーに送る DHCPREQUEST メッセージで、クライアントがサーバーの提供内容を受け入れたことを示すと、サーバーはそのアドレスをリース・アドレスとしてマークを付けます。サーバーに送る DHCPREQUEST メッセージで、クライアントがほかのサーバーの提供を受けたことを示した場合、サーバーは提供したアドレスをプールに戻します。規定時間内にメッセージが到着しなかった場合は、サーバーはアドレスをプールに戻します。選択されたサーバーは、肯定応答をクライアントに送りますが、この中には構成に関する追加情報が含まれています。
7. クライアントは、構成情報が有効かどうかを確認します。DHCP クライアントは、DHCPACK メッセージを受け取ると、提供された IP アドレスにアドレス・レゾリューション・プロトコル (ARP) 要求を送り、アドレスがすでに使われていないかどうかを確認します。クライアントは、ARP 要求に対する応答を受け取った場合は、提供内容を拒否して (DHCPDECLINE メッセージ)、このプロセスをはじめからやり直します。応答がなければ、構成情報を受け入れます。
8. クライアントは、有効なリースを受け入れると、DHCP サーバーとバインド関係 (BINDING) に入り、IP アドレスとオプションを使用します。DHCP クライアントが動的アドレス・クライアントの場合は、DHCP クライアントは、ホスト名から IP アドレスへのマッピングを動的ドメイン名サーバーに通知します。

オプションを要求する DHCP クライアントに対して DHCP サーバーが提供するオプションには、サブネット・マスク、ドメイン名サーバー、ドメイン名、静的ルート、クラスの識別子 (メーカー名を示す)、ユーザーのクラスなどが含まれます。

しかし、DHCP クライアントは、独自のオプションの組み合わせを要求することもできます。オプションを要求するには、Windows NT 3.5.1 DHCP クライアントなどが必要になります。クライアントに要求され、IBM がデフォルトで提供する DHCP オプションには、サブネット・マスク、ドメイン名サーバー、ドメイン名、静的ルートが含まれています。オプションの説明については、485ページの『DHCP のオプション』を参照してください。

リースの更新

DHCP クライアントは、リースの残余時間を管理します。リース期限前のある特定時期になると、これは多くはリース期間の中間時点ですが、クライアントはリースを提供するサーバーに更新要求を送信します。これには、現在の IP アドレスと構成情報が含まれています。サーバーが応答してリースを提供すると、DHCP クライアントのリースは更新されます。

DHCP サーバーがこの要求をはっきりと拒否した場合は、DHCP クライアントは、リース期限になるまで IP アドレスを継続して使用できます。期限になると、クライアントは、アドレス要求をブロードキャストして、再びアドレス要求の手続きを開始します。クライアントは、サーバーに到達できない場合は、リースの期限になるまで割り当てられたアドレスを使用できます。

クライアントの移動

DHCP の長所として、クライアント・ホストは、サブネットからサブネットへ自由に移動でき、しかも新しいサブネットで必要になる IP 構成情報を事前に知っておく必要がありません。ホストが移動する先のサブネットが DHCP サーバーにアクセスできさえすれば、DHCP クライアントは、そのサブネットへのアクセスを自動的に正しく構成できます。

新しいサブネットへのアクセスで、DHCP クライアントが再構成するためには、クライアント・ホストをリブートしなければなりません。ホストが新しいサブネットを使ってリスタートすると、DHCP クライアントは、アドレスを割り当てた DHCP サーバーとの古いリースを更新しようとします。新しいサブネットではアドレスが無効になるので、サーバーは更新要求を拒否します。クライアントは、DHCP サーバーからの応答や命令がないので、新たな IP アドレスを取得してネットワークにアクセスするために、IP アドレス要求処理を開始します。

サーバー・オプションの変更

DHCP では、サーバーで変更ができます。サーバーを再初期化し、変更内容を必要なすべてのクライアントに配布します。DHCP クライアントは、DHCP サーバーが割り当てた DHCP オプションの値をリース期間中は保存しておきます。クライアントがすでにアップ状態で実行しているときにサーバーで構成を変更すると、DHCP クライアントは、クライアントがリースの更新を試みるか、リスタートをするまでは、変更を処理しません。

注: サーバーにハード・ファイルまたはフラッシュ記憶域カードが含まれていないときに、サーバーが再初期化される (t 5 **reset dhcp** コマンドを使用して) と、ルーターによって表示されるリース期間情報は、DHCP クライアントがリースの更新をするまで表示されなくなります。

DHCP サーバーの数量

必要なサーバーの数量は、サブネットの数、サポートする DHCP クライアントの数、 BOOTP リレーを使用するかどうか、および選択するリース期間などにより変わります。現在の DHCP プロトコルでは、サーバーからサーバーへの通信は定義されないことに注意してください。そこで、情報を共有したり、1 台の DHCP サーバーが故障したときにほかの DHCP サーバーが 『hot backup』 となることはできません。 DHCP クライアントは、ブロードキャスト・メッセージを送信します。設計上、ブロードキャスト・メッセージがサブネット間を渡ることはできません。クライアントのメッセージをサブネットの外に転送するためには、ルーターを追加して、BOOTP リレー・エージェントを使って、DHCP 要求を転送するように構成します。このようにしないと、各サブネットの DHCP サーバーを構成しなければなりません。

単一 DHCP サーバー

1 台の DHCP サーバーでサブネット上のホストに対応する場合は、そのサーバーが故障したときのことを考えておく必要があります。一般的に、サーバーが故障して影響を与えるのは、そのときにネットワークに入ろうとしている DHCP クライアントだけです。通常は、すでにネットワークにある DHCP クライアントは、リース期限が切れるまでは影響なく機能します。しかし、リース期間の短いクライアントでは、サーバーをリスタートする前に、ネットワークへのアクセスができなくなることがあります。サブネットの DHCP サーバーが 1 台だけのときにサーバーが故障したときの影響を最小限にとどめるには、故障した DHCP サーバーのリスタートや応答の時間を確保するために、リース期間を長くしておきます。

複数の DHCP サーバー

故障が一点に集中するのを避けるためには、1 つのサブネットに対して 2 台以上の DHCP サーバーを構成します。1 台のサーバーが故障しても、ほかのサーバーがサブネットの機能を継続します。各 DHCP サーバーは、サブネットに直接的に接続するか、BOOTP リレー・エージェントを使ってアクセスできるようにしておきます。

同じアドレスに 2 台の DHCP サーバーを対応させることはできないので、サブネットに定義するアドレス・プールは、DHCP サーバーに対して固有でなければなりません。そこで、1 つのサブネットで 2 台以上の DHCP サーバーを使用するときは、そのサブネットの全アドレスをサーバー間で分割します。たとえば、サブネットの全アドレスの 70% を 1 台のサーバーに構成し、もう 1 台のサーバーには残りの 30% のアドレスを構成することができます。

複数の DHCP サーバーを使用すると、DHCP 関連のネットワーク・アクセス障害の発生確率は低くなりますが、障害の防止を保証することはできません。ある特定のサブネットに対する 1 台の DHCP サーバーが故障したときに、新たなクライアントの要求をすべてのほかの DHCP サーバーで対応することは、そのサーバーのアドレスに限界があるので必ずしも可能ではありません。

しかし、どちらの DHCP サーバーのアドレス・プールを先に使い切るかについて、バイアスをかけることができます。DHCP クライアントは、提供オプションの多い DHCP サーバーを選択する傾向があります。たとえば、全アドレスの 70% を割り当てた DHCP サーバーが対応するようにバイアスをかけるには、全アドレスの 30% が割り当てられている DHCP サーバーが提供するオプションの数を少なくします。

BOOTP サーバー

BOOTP のクライアントとサーバーがすでにネットワークにある場合は、BOOTP サーバーを DHCP サーバーに取り替えることができます。DHCP サーバーは、BOOTP クライアントに現在の BOOTP サーバーと同じ IP 構成情報を提供できます。 BOOTP サーバーを DHCP サーバーに代えることができず、両者を使用してネットワークに対応する場合は、以下の事項に注意してください。

- DHCP サーバーの BOOTP サポートを無効にする。
- BOOTP サーバーと DHCP サーバーが同じアドレスを提供しないようにする。
- ルーターに BOOTP リレーのサポートを構成し、BOOTP と DHCP のサーバーに BOOTP ブロードキャストを転送できるようにする。

DHCP サーバー は、BOOTP クライアントに恒久的な IP アドレスを割り当てます。サブネットの番号が変わり、BOOTP の割当アドレスが使えなくなったときは、BOOTP クライアントはリスタートして、新たな IP アドレスを取得する必要があります。

特殊 DHCP クライアント

DHCP クライアントやネットワーク・サーバーの管理で、以下のような個別または特別の必要事項を付加することができます。

- 永久リース

  ホストに無限のリース期間を指定すると、永久リースを割り当てることができます。 BOOTP クライアントへのサポートを有効にしておけば、永久リースを要求をすれば、DHCP サーバーから BOOTP クライアントに永久リースを割り当てることができます。 DHCP サーバーは、DHCP ホストにもはっきりとした要求があれば、永久リースを割り当てます。
- 特定の IP アドレス

  特定のサブネット上の DHCP または BOOTP のクライアント・ホストについて、特定のアドレスと構成パラメーターを保留しておくことができます。
- 特定の構成パラメーター

  サブネットとは無関係に、特定の構成情報をクライアントに割り当てることができます。
- 手動定義のワークステーション

  IP ネットワークへのアクセスの構成で DHCP や BOOTP を使用しない既存ホストについては、DHCP のサブネットからアドレスを削除します。DHCP のサーバーとクライアントは、IP アドレスを割り当てたり使用する前にそのアドレスが使われていないかどうかを自動的に確認しますが、手動で定義されたホストのアドレスでネットワーク上で無効になっているもの、あるいは一時的に外されている

ものは検出しません。この場合、IP アドレスを除外せずに手動定義のホストがネットワークへのアクセスを再開すると、同じアドレスが複数できるという問題が発生する可能性があります。

リース期間

デフォルトのリース期間は 24 時間です。DHCP のリース期間がネットワークの操作や性能に影響することに注意してください。

- リース期間が短いと、DHCP のリース更新要求のためにネットワークの通信量が増加します。たとえば、リース期間を 5 分にすると、クライアントは 5 分おきに更新要求を送信します。
- リース期間が長すぎると、IP アドレスの再利用度が低下します。リース期間を非常に長くすると、クライアントがリスタートしたりリースを更新したときに、構成の変更に時間がかかるようになります。

リース期間は、以下を考慮して必要に応じて選択します。

- 利用可能なアドレスの数量とサポートするホストの数量。ホストの数がアドレスの数よりも多いときは、リース期間は 1 時間か 2 時間程度に短くしておきます。これで、使われなくなったアドレスは、できるだけ早くプールに戻されます。
- ネットワークの変更に要する時間。ホストは、リスタートまたはリースの更新を実行すると、構成情報の変更内容を受信します。こうした変更の実施に必要な時間を十分に確保するように時間をとってください。たとえば、夜のあいだに変更を行うのであれば、リース期間を 12 時間にしておきます。
- 使用可能な DHCP サーバーの数量。大きなネットワークで使用している DHCP サーバーの台数が少ない場合は、サーバーが休止したときの影響を抑えるために、リース期間を長くしておきます。

複数のホストのリース条件をサポートする必要があるような複雑なネットワークでは DHCP クラスを定義します。

概念と用語

DHCP サーバー機能について、以下の概念を使って説明します。

スコープ

DHCP サーバーの構成でスコープという用語は、パラメーター値の属する内容を示すときに使用されます。483ページの図38には、以下のスコープが示されています。

- グローバル・オプション 1
- グローバル・オプション 3
- グローバル・クラス ClassA

  ClassA は、オプション 1 を再定義しますが、グローバル・スコープのオプション 3 の値を継承します。
- グローバル・クライアント ClientA

  ClientA は、オプション 3 を再定義しますが、グローバル・スコープのオプション 1 の値を継承します。
- サブネット SubA

- オプション 1 を再定義します。
- グローバル・スコープのオプション 3 の値を継承します。
- SubA のスコープ内で ClassB を定義します。

  オプション 1 の値を再定義しますが、SubA のオプション 3 の値を継承します (これはさらにグローバル・スコープから継承します)。
- SubA のスコープ内で ClientB を定義します。

  ClientB は、オプション 3 を再定義しますが、SubA のオプション 1 の値を継承します。

• メーカー・オプション vendorA

  メーカー・オプションは例外です。メーカー・オプションは独立しており、メーカー・オプションのスコープの外では継承されません。

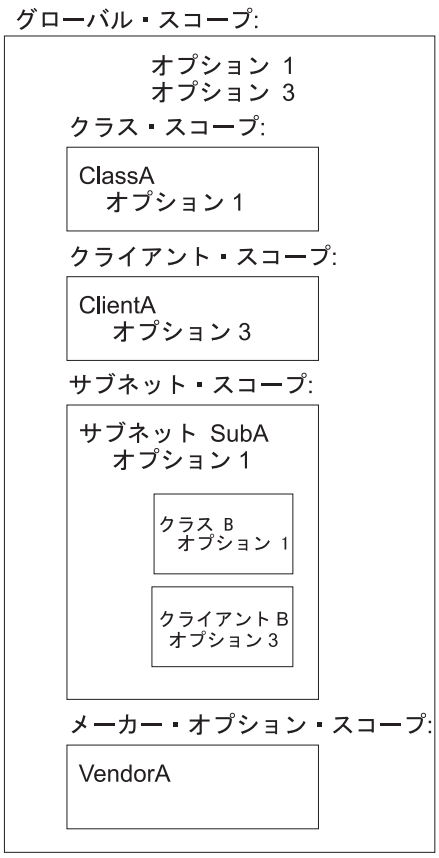


図 38. スコープの概念

サブネット

サブネットは、DHCP サーバーが管理するアドレス・プールについて、パラメーターを定義します。アドレス・プールは、クライアントにリースする IP アドレスの集合体です。指定可能なパラメーターとしては、アドレス・プールを使用するクライアントのためのリース期間やその他のオプションがあります。リース期間やその他のオプションは、グローバル・スコープから継承することができます。

サブネット・グループ

サブネット・グループは、同じインターフェースにまとめられる複数のサブネットを識別する手段です。1 つのグループに属する各サブネットは、同一のサブネット・グループ名と固有の優先順位を与えられます。アドレスは、グループに関連するアドレス・ポリシーにしたがって与えられますが、優先順位はそのアドレスの順序を決めるのに使用されます。サブネットには、2 つのアドレス・ポリシーがあります。

- インオーダー (整列)

  デフォルト設定のポリシーです。インオーダー・ポリシーは、優先順位の低いサブネットから優先順位の高いサブネットの順にアドレスを処理します。

- バランス

  バランス・ポリシーは、ラウンドロビンで定義されたサブネット・グループのアドレスを処理します。優先順位がもっとも低いサブネットのアドレスから処理します。次に、優先順位が次に低いサブネットのアドレスを処理し、そしてその次へと続きます。優先順位がもっとも高いサブネットのアドレスを処理すると、ポリシーは、優先順位がもっとも低いサブネットに戻り、グループ内のサブネットのすべてのアドレスがなくなるまでこれを続けます。

クラス クラスは、ユーザーが定義し、DHCP サーバーが管理するクライアント・グループについて、パラメーターを定義します。クラスは、グローバル・スコープまたはサブネット・スコープのもとに定義します。クラスをサブネット・スコープのもとで定義すると、DHCP サーバーは、ある特定のサブネット内のクライアントでクラスを要求するクライアントだけに対応します。サブネット・スコープで定義されたクラスだけが一定範囲のアドレスを指定できます。範囲は、サブネット範囲内のサブセット、またはサブネット範囲全体となります。クライアントがあるクラスの IP アドレスを要求したときに、そのクラスの範囲がなくなってしまった場合は、サブネット範囲に使用可能な IP アドレスがあれば、その IP アドレスが提供されます。そのときクライアントに提供されるオプションは、空になったクラスに関連付けられたオプションです。

クライアント

クライアントは、以下のように使用されます。

- 特定のエンド・ステーションについて、静的 IP アドレスと DHCP オプションを定義する。
- 特定のエンド・ステーションをサービスから除外する。
- 使用可能なIP アドレスのある範囲から 1 つの IP アドレスを除外する。

それぞれのクライアントには、特定のハードウェア・タイプ、クライアント ID、および IP アドレスがあります。ハードウェア・タイプは、RFC 1340 に定義されたハードウェア・タイプで、以下に示したとおりです。ハードウェア・タイプは、0 を除いて、クライアント ID がエンド・ステーションのハードウェア・アドレスになっています (あるいは MAC アドレス)。ハードウェア・タイプが 0 のものは、クライアント ID は文字列になっています。通常、これはドメイン名です。

クライアントを定義するときは、IP アドレス、*any*、または *none* のいずれかを入力します。IP アドレスを定義すると、その IP アドレスがそのクライアント用に確保されます。 *any* を選択すると、サブネット内の使用可能な任意の IP アドレスがクライアントに与えられます。同じサブネット内に複数のサブネット・レコードが定義されていて、それぞれに固有の範囲があるときは、 *any* で構成したクライアントには、サブネット内で最初に使用可能になったアドレスが与えられます。これはクライアントが定義されているサブネット・レコードの範囲とは必ずしも一致しません。*none* を選択すると、そのエンド・ステーションには IP アドレスは与えられません。 IP アドレスが処理されないようにするには、クライアント・レコードのハードウェア・タイプとクライアント ID を 0 に定義します。

RFC1340 に定義済みで IBM 2210 で扱っているハードウェア・タイプは以下の通りです。

Hardware Type	Value
Reserved	0
Ethernet	1
IEEE 802 Networks (Token Ring 含む)	6

全リストを見るには、RFC 1340 を参照してください。

DHCP サーバーとリースのパラメーター

以下の DHCP サーバー・パラメーターは、グローバル・レベルで定義できます。

- bootstrapserver
- canonical
- lease expire interval
- lease time default
- ping time
- support unlisted clients
- support bootp
- used ip address expire interval

以上のパラメーターについては、527ページの『Set』を参照してください。

DHCP のオプション

DHCP では、オプションを指定して、クライアントにさらに構成情報を提供できます。オプションは、RFC 2132 およびその他のさまざまな RFC で定義します。

オプションのフォーマット

すべてのオプションは、構成データが以下のいずれかのフォーマットで書かれていることを前提としています。

フォーマット	定義
IP アドレス	小数点表記による 1 つの IP アドレス
複数のIP アドレス	小数点表記による 1 つ以上の IP アドレスで、空白で分離する。

IP アドレス・ペア	小数点表記による 2 つの IP アドレスで、空白で分離する。
複数の IP アドレス・ペア	1 つ以上の IP アドレス・ペアで、各ペアは空白で分離する。
ブール値	0 または 1 (真または偽)。
バイト	-128 から 127 までの 10 進数 (-128 と 127 を含む)
無符号のバイト	0 から 255 までの 10 進数 (0 と 127 を含む)。無符号のバイトには、負の数値は指定できません。
無符号のバイトのリスト	0 から 255 (0 と 255 を含む) までの 1 つ以上の 10 進数で空白で分離する。無符号のバイトには、負の数値は指定できません。
Short	-32768 から 32767 までの 10 進数 (-32768 と 32767 を含む)
無符号のショート	0 から 65535 までの 10 進数 (0 と 65535 を含む)。 無符号のショートには、負の数値は指定できません。
無符号のショートのリスト	0 から 65535 (0 と 65535 を含む) までの 1 つ以上の 10 進数で空白で分離する。無符号のショートには、負の数値は指定できません。
Long	-2147483648 から 2147483647 までの 10 進数 (-2147483648 と 2147483647 を含む)
無符号のロング	0 から 4294967295 までの 10 進数 (0 と 4294967295 を含む)。無符号のロングには、負の数値は指定できません。
文字列	文字列
N/A	クライアントが情報を作成するので、指定する必要がないことを示す。

各 DHCP オプションは、数字コードで識別します。

アーキテクチャー上のオプション 0 から 125、およびオプション 255 は、RFC の定義用として保留となっています。DHCP サーバー、DHCP クライアント、または両者のサーバーとクライアントは、この組み合わせでオプションを使用します。アーキテクチャー上のオプションには、管理者によって変更されるものがあります。そのほかのオプションは、クライアントとサーバーだけが使用します。

注: 16 進値は、既知のフォーマットによるアーキテクチャー上のオプションには使用できません。

以下のオプションは、管理者が DHCP サーバーで構成できない、または構成してはいけないオプションです。

52 オプションのオーバーロード

53 DHCP メッセージ・タイプ

54 サーバーの識別子

55 パラメーター要求リスト

56 メッセージ

57 最大 DHCP メッセージ・サイズ

60 クラスの識別子

オプションの 128 から 254 は、ユーザー定義のオプションです。このオプションは、管理者が情報を DHCP クライアントに渡してサイトごとの構成パラメーターを実装するときに定義します。

このほか、192: TXT RR など、IBM 専用のオプションが IBM から提供されています。

ユーザー定義のオプションのフォーマットは以下の通りです。

構文:

オプション *code value*

ただし、

code 1 から 254 の任意のコード。ただし、RFC にすでに定義されているコードを除く。

value これは文字列にします。サーバーでは、ASCII 文字列または16 進数ストリングです。しかし、クライアントでは、処理プログラムに渡されるので、これは常に16 進数の文字列になります。

サーバーは、指定値をクライアントに渡します。しかし、値を処理するには、プログラムまたはコマンド・ファイルを作成します。

クライアントに与えられる基本オプション

クライアントには、以下の基本オプションが与えられます。構成フォーマットについては、485ページの『オプションのフォーマット』 を参照してください。

1 **Subnet Mask** このオプションは、DHCP サーバーに指定します。32 ビットの小数点表記で指定するクライアントのサブネット・マスクです。必須事項ではありませんが、多くの構成で、DHCP サーバーは DHCP クライアントにサブネット・マスクのオプション 1 を送ります。クライアントが DHCP サーバーからサブネット・マスクを受け取らずに、実際にはサブネットに不適当なサブネット・マスクを前提として処理を進めると、クライアントは、予測不可能なオペレーションを行います。これを指定しないと、クライアントはデフォルトのサブネット・マスクを使用します。

- Class A network 255.0.0.0
- Class B network 255.255.0.0
- Class C network 255.255.255.0

オプション・フォーマット: IP アドレス

2 **Time Offset** このオプションは、DHCP サーバーに指定します。クライア

ントのサブネットの協定世界時 (UTC) に対するオフセット (秒) です。オフセットは、32 ビットの符号付き整数です。

オプション・フォーマット: ロング

3 **Router** このオプションは、DHCP サーバーに指定します。クライアントのサブネット上のルーターの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

4 **Time Server** このオプションは、DHCP サーバーに指定します。クライアントが使用できるタイム・サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

5 **Name Server** このオプションは、DHCP サーバーに指定します。クライアントが使用できる IEN 116 ネーム・サーバーの IP アドレス (優先順位順)。

注: これはドメイン名サーバーのオプションではありません。ドメイン名サーバーを指定するには、オプション 6 を使用します。

オプション・フォーマット: IP アドレス

6 **Domain Name Server** このオプションは、DHCP サーバーに指定します。クライアントが使用できるドメイン・ネーム・システム・サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレスまたは番号付けのない IP インターフェース・アドレス (たとえば、0.0.0.2)

注: PPP インターフェースの IP 構成で Dynamic-Address が使用可能になっている場合、IPCP を使ってインターネット・サービス・プロバイダー (ISP) から 1 次と 2 次の DNS アドレスを取り出すことができます。 DHCP クライアントにこうした DNS アドレスを渡すには、Dynamic-Address インターフェースに対応する、番号付けのない IP インターフェース・アドレス (0.0.0.n など) を使用してオプション 6 を構成する必要があります。クライアントが要求を送信すると、DHCP サーバーは、この値を、ISP から取り出した値に変換します。 IP 構成で Simple-Internet-Access を使用可能にすると、番号付けのない IP インターフェースを使用してオプション 6 が自動的に構成されます。クライアントが、PPP インターフェースをアクティブにする前にこのサーバーに構成情報を要求すると、PPP 接続と IPCP が完了できる、短縮したリース期間 (3 分) が与えられます。 DNS アドレスが確認された後、構成されたリース期間が与えられます。

7 **Log Server** このオプションは、DHCP サーバーに指定します。クライアントが使用できる MIT-LCS UDP Log サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

8 **Cookie Server** このオプションは、DHCP サーバーに指定します。クライアントが使用できる Cookie の IP アドレス (優先順位順)、または quote-of-the-day (その日のことわざ) サーバー。

オプション・フォーマット: IP アドレス

9 **LPR Server** このオプションは、DHCP クライアントと DHCP サーバーの両方に指定できます。しかし、DHCP クライアントだけで指定すると、構成は不完全になります。クライアントが使用できるライン・プリンター・サーバーの IP アドレス (優先順位順)。クライアントは、オプション 9 を使うと、LPR_SERVER 環境変数を指定する必要はありません。

オプション・フォーマット: IP アドレス

10 **Impress Server** このオプションは、DHCP サーバーに指定します。クライアントが使用できる Imagen Impress サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

11 **Resource Location Server** このオプションは、DHCP サーバーに指定します。クライアントが使用できるリソース・ロケーション (RLP) サーバーの IP アドレス (優先順位順)。クライアントは、 RLP サーバーを使うと、ドメイン名サーバーなどの特定のサービスを提供するリソースを探し出せます。

オプション・フォーマット: IP アドレス

12 **Host Name** このオプションは、DHCP クライアントと DHCP サーバーの両方に指定できます。DHCP クライアントがホスト名を提供しないときは、DHCP サーバーはオプション 12 を無視します。クライアントのホスト名です (ローカル・ドメイン名を含むことがあります)。ホスト名オプションの文字数は、最短で 1 オクテット、最長で 32 オクテットです。文字数の制約については、RFC 1035 を参照してください。

オプション・フォーマット: 文字列

13 **Boot File Size** このオプションは、DHCP サーバーに指定します。クライアントのデフォルト・ブート構成ファイルの長さ (512 オクテットのブロック)。

オプション・フォーマット: 無符号のショート

14 **Merit Dump File** このオプションは、DHCP サーバーに指定します。クライアントが破壊したときにクライアントのコア・イメージを保管するメリット・ダンプ・ファイルのパス名。パスは、ネットワーク仮想端末装置 (NVT) ASCII 文字を使って、文字列としてフォーマットします。最短長さは 1 オクテットです。

オプション・フォーマット: 文字列

15 **Domain Name** このオプションは、DHCP クライアントと DHCP サーバーの両方に指定できます。DHCP サーバーのオプション 15 に値が指定されないと、クライアントは、オプション 12 のホスト名とオプション 15 のドメイン名を数値で提供しなければなりません。このステートメントは、グローバル・スコープ内に表示されたり、またはサブネット、クラス、クライアント・スコープと合わせて表示されます。

オプション・フォーマット: 文字列

16 **Swap Server** このオプションは、DHCP サーバーに指定します。クライアントのスワップ・サーバーの IP アドレス。

オプション・フォーマット: IP アドレス

17 **Root Path** このオプションは、DHCP サーバーに指定します。クライアントのルート・ディスクを含むパス。パスは、NVT ASCII 文字を使って、文字列としてフォーマットします。最短長さは 1 オクテットです。

オプション・フォーマット: 文字列

18 **Extension Path** このオプションは、DHCP サーバーに指定します。エクステンション・パス・オプションは、トリビアル・ファイル転送プロトコル (TFTP) を使って読み込み可能なファイルを識別するための文字列を指定します。最短長さは 1 オクテットです。

オプション・フォーマット: 文字列

ホスト・オプションの IP レイヤー・パラメーター

19 **IP Forwarding** このオプションは、DHCP サーバーに指定します。クライアントの IP パケット・レイヤー転送を使用可能 (1) または使用不可 (0) にします。

オプション・フォーマット: ブール値

20 **Non-Local Source Routing** このオプションは、DHCP サーバーに指定します。クライアントの非ローカル・ソース・ルートによる IP レイヤー・データグラム転送を使用可能 (1) または使用不可 (0) にします。

オプション・フォーマット: ブール値

21 **Policy Filter** このオプションは、DHCP サーバーに指定します。非ローカル・ソース・ルートによるデータグラムのフィルター処理に使用する IP アドレス・ネットマスク・ペア。ネクスト・ホップ・アドレスがどのフィルター・ペアにも一致しないデータグラムは、クライアントが破棄します。このポリシー・フィルター・オプションは、最短で 8 オクテットです。

オプション・フォーマット: IP アドレス・ペア

22 **Maximum Data gram Reassembly Size** このオプションは、DHCP サーバーに指定します。クライアントが組み立てられるデータグラムの最大サイズです。最小値は 576 です。

オプション・フォーマット: 無符号のショート

23 **Default IP Time-to-Live** このオプションは、DHCP サーバーに指定します。クライアントが発信データグラムに使用するデフォルトの活動時間 (TTL) です。TTL は、1 オクテットで、1 から 255 のあいだです。

オプション・フォーマット: 無符号のバイト

24 **Path MTU Aging Timeout** このオプションは、DHCP サーバーに指定します。 RFC 1191 に記述された方法で発見されるパス最大伝送単位 (MTU) 値の経年処理を行うためのタイムアウトの秒数。

オプション・フォーマット: 無符号のロング

25 **Path MTU Plateau Table** このオプションは、DHCP サーバーに指定します。 RFC 1191 に定義された方法で、パス MTU の発見を求めるときの MTU サイズの表。 最小 MTU 値は 68 です。パス MTU プラトー・テーブル・オプションは、最短で 2 オクテットです。長さは、2 の倍数にします。

オプション・フォーマット: 無符号のショート

インターフェース・オプションの IP レイヤー・パラメーター

26 **Interface MTU** このオプションは、DHCP サーバーに指定します。 このインターフェースに求める最大伝送単位 (MTU)。最小 MTU 値は 68 です。

オプション・フォーマット: 無符号のショート

27 **All Subnets are Local** このオプションは、DHCP サーバーに指定します。 すべてのサブネットが同じ最大伝送単位 (MT) を使用することをクライアントが前提とする (1)、前提としない (0) を選択します。この値を 0 にすると、MTU の小さなサブネットがあることをクライアントは想定します。

オプション・フォーマット: ブール値

28 **Broadcast Address** このオプションは、DHCP サーバーに指定します。クライアントのサブネットで使用されるブロードキャスト・アドレスです。

オプション・フォーマット: IP アドレス

29 **Perform Mask Discovery** このオプションは、DHCP サーバーに指定します。 クライアントがインターネット制御メッセージ・プロトコル (ICMP) を使って、サブネット・マスクのディスカバリーを実行する (1)、実行しない (0) を選択します。

オプション・フォーマット: ブール値

30 **Mask Supplier** このオプションは、DHCP サーバーに指定します。 クライアントがインターネット制御メッセージ・プロトコル (ICMP) を使って、サブネット・マスク要求に応答する (1)、応答しない (0) を選択します。

オプション・フォーマット: ブール値

31 **Perform Router Discovery** このオプションは、DHCP サーバーに指定します。 クライアントが RFC 1256 に定義された方法で、ルーター・ディスカバリーを使って、ルーターに対してアドバタイズ要求する (1)、要求しない (0) を選択します。

オプション・フォーマット: ブール値

32 **Router Solicitation Address** このオプションは、DHCP サーバーに指定します。 クライアントがルーターに対してアドバタイズ要求を送信する宛先アドレスです。

オプション・フォーマット: IP アドレス

33 **Static Route** このオプションは、DHCP サーバーに指定します。 クライアントがルーティング・キャッシュに設置する静的ルートです (優先順位にしたがった指定アドレス・ルーターのペア)。 最初のアドレスは宛先アドレス、2 番目のアドレスは宛先のルーターです。 デフォルトの宛先ルートに 0.0.0.0 を指定しないでください。

オプション・フォーマット: IP アドレス・ペア

インターフェース・オプションのリンク・レイヤー・パラメーター

34 **Trailer Encapsulation** このオプションは、DHCP サーバーに指定します。

アドレス解決プロトコル (ARP) を使用するときに、トレーラーの使用について、クライアントがネゴシエーションする (1)、しない (0) を選択します。詳しくは、RFC 893 を参照してください。

オプション・フォーマット: ブール値

35 **ARP Cache Timeout** このオプションは、DHCP サーバーに指定します。アドレス解決プロトコル (ARP) のキャッシュ入力に対するタイムアウトの秒数です。

オプション・フォーマット: 無符号のロング

36 **Ethernet Encapsulation** このオプションは、DHCP サーバーに指定します。 イーサネットのインターフェースについて、クライアントが IEEE 802.3 を使って (1) RFC 1042 に記述されたイーサネットのカプセル化をするか、Ethernet V2 を使って (0) RFC 894 に記述されたカプセル化をするかを選択します。

オプション・フォーマット: ブール値

TCP パラメーターのオプション

37 **TCP Default** このオプションは、DHCP サーバーに指定します。 クライアントが TCP セグメントを送信するときに使用するデフォルトの活動時間 (TTL) です。

オプション・フォーマット: 無符号のバイト

38 **TCP Keep-alive Interval** このオプションは、DHCP サーバーに指定します。 TCP 接続で、キープアライブ・メッセージを送信するまでのクライアントの待ち時間となる秒数の間隔。 値を 0 にすると、アプリケーションが要求しなければ、クライアントはキープアライブ・メッセージを送信しないことを意味します。

オプション・フォーマット: 無符号のロング

39 **TCP Keep-alive Garbage** このオプションは、DHCP サーバーに指定します。 前回の実装と比較するために、1 オクテットのガーベッジが入った TCP キープアライブ・メッセージをクライアントが送信する (1)、送信しない (0) を選択します。

オプション・フォーマット: ブール値

アプリケーションとサービスのパラメーター・オプション

40 **Network Information Service Domain** このオプションは、DHCP サーバーに指定します。 クライアントのネットワーク情報サービス (NIS) ドメインです。 パスは、NVT ASCII 文字を使って、文字列としてフォーマットします。最短長さは 1 オクテットです。

オプション・フォーマット: 文字列

41 **Network Information Service Domain** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるネットワーク情報サービス (NIS) の IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

42 **Network Time Protocol Servers** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるネットワーク・タイム・プロトコル (NTP) サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

43 **Vendor-Specific Information** オプション 43 は、DHCP サーバーに指定します。DHCP サーバーは、このオプションをクライアントに返し、クライアントはオプション 60 のクラス ID を送信します。 この情報オプションは、メーカー・オプション定義に指定されているメーカー固有の情報を交換するために、クライアントとサーバーが使用します。 オプション 43 を使用してメーカー情報をカプセル化するときには、以下のことにご注意ください。

- 異なるメーカーのクライアントとサーバーのあいだで、インターオペラビリティーを可能にするためには、各メーカーが RFC 2132 の標準フォーマットを使用して、オプション 43 の内容を明確に文書化する必要があります。
- 各メーカーは、他のメーカーの DHCP サーバーが簡単に実装できるような形態で、オプション 43 の範囲でカプセル化できる特定のオプションを指定する必要があります。 たとえば、メーカーは以下のようにする必要があります。
  - DHCP オプションにすでに定義されたデータ・タイプ、またはその他のしっかりと定義されたデータ・タイプでオプションを提出する。
  - ほかのメーカーのサーバーと交換する構成ファイル内に簡単にコード化できるようなオプションを選択する。
  - すべてのサーバーが簡単にサポートできること。

サーバーは、クライアントが送信したメーカー固有の情報を解釈できないときは、それを無視しなければなりません。 クライアントは、希望していたメーカー固有の情報を受信できないときは、その情報なしに操作するように試みなければなりません。 このオプションに関する追加情報について、RFC 2131 と RFC 2132 を参照してください。

注: 以上のような注意が必要なため、IBM は IBM 固有のオプションについては、オプション 192 と 200 を使用します。

オプション・フォーマット: 文字列

44 **NetBIOS over TCP/IP Name Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できる NetBIOS ネーム・サーバー (NBNS) の IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

45 **NetBIOS over TCP/IP Datagram Distribution Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できる NetBIOS データグラム・ディストリビューション (NBDD) ネーム・サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

46 **NetBIOS over TCP/IP Node Type** このオプションは、DHCP サーバーに指定します。 RFC 1001 および RFC 1002 に記述されている NetBIOS

over TCP/IP 構成可能なクライアントに使用するノード・タイプです。クライアントのタイプを指定する値には以下のものがあります。

- 0x1 B-node
- 0x2 P-node
- 0x4 M-note
- 0x8 H-node

オプション・フォーマット: 無符号のバイト

47 **NetBIOS over TCP/IP Scope** このオプションは、DHCP サーバーに指定します。 RFC 1001/1002 に指定されているクライアントのための NetBIOS over TCP/IP 範囲パラメーターです。 最短長さは 1 オクテットです。

オプション・フォーマット: 無符号のバイト

48 **X Window System Font Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できる X Window System フォント・サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

49 **Window System Display Manager** このオプションは、DHCP サーバーに指定します。 クライアントが使用できる X Window System ディスプレイ・マネージャーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

DHCP 拡張機能オプション

50 **Requested IP Address** このオプションは、 DHCP サーバーに指定します。 DHCP サーバーは、特定の IP アドレスについて、DHCP クライアントの要求を拒否できます。 クライアントは、特定の IP アドレスを要求できます (DHCPDISCOVER)。

オプション・フォーマット: N/A

51 **IP Address Lease Time** このオプションは、DHCP クライアントと DHCP サーバーの両方に指定できます。 DHCP クライアントは、オプション 51 を使って、DHCP サーバーが提供する defaultLeaseInterval の値を上書きできます。 クライアントは、IP アドレスのリース期間を要求することができます (DHCPDISCOVER または DHCPREQUEST)。 DHCP サーバーは、応答するときに (DHCPOFFER)、オプションを使ってリース期間を提案します。 このオプションは、グローバル、サブネット、クラス、クライアントなどのスコープ内で指定します。 永久 (恒久) のリースを指定するときは、X'ffffffff' を使います。

オプション・フォーマット: 無符号のロング

58 **Renewal (T1) Time Value** このオプションは、DHCP サーバーに指定します。 サーバーがアドレスを割り当ててからクライアントが更新状態に移るまでのあいだの秒数。

オプション・フォーマット: 無符号のロング

59 **Rebinding (T2) Time Value** このオプションは、DHCP サーバーに指定します。 サーバーがアドレスを割り当ててからクライアントが再バインド状態に移るまでのあいだの秒数。

オプション・フォーマット: 無符号のロング

60 **Class-Identifier** このオプションは、DHCP サーバーに指定します。 この情報は、クライアントによって作成され、指定する必要はありません。 クライアントがサーバーに提供するクライアントのタイプと構成。 たとえば、クライアントのメーカー固有のハードウェア構成を識別子でコード化できます。 この情報は、*n* オクテットの文字列で、サーバーがこの情報を解釈します。 たとえば、hex: X'01' X'02' X'03'。 クライアントが送信するクラス固有の情報を解釈できるようになっていないサーバーは、この情報を無視します。最短長さは 1 オクテットです。

オプション・フォーマット: N/A

61 **Client Identifier** このオプションは、DHCP クライアントと DHCP サーバーの両方に指定できます。 DHCP クライアントは、オプション 61 を使って固有のクライアント識別子を指定します。 DHCP サーバーは、オプション 61 を使ってアドレスのバインド・データベースに索引を付けることができます。 この値は、1 つの管理定義域のなかのすべてのクライアントに対して固有の値でなければなりません。

オプション・フォーマット: 文字列

62 **NetWare/IP Domain Name** このオプションは、DHCP サーバーに指定します。 Netware/IP ドメイン名です。 最短長さは 1 オクテット、最長長さは 255 オクテットです。

オプション・フォーマット: 文字列

63 **NetWare/IP** このオプションは、DHCP サーバーに指定します。 NetWare/IP ドメイン名を除く NetWare/IP 関連のすべての情報を伝えるときに使用する汎用のオプション・コードです。 オプション・コードを使って、多数の NetWare/IP サブオプションを伝えることができます。 最短長さは 1、最長長さは 255 です。

オプション・フォーマット: 文字列

64 **NIS domain Name** このオプションは、DHCP サーバーに指定します。 ネットワーク情報サービス (NIS)+ V3 クライアント・ドメイン名。 パスは、NVT ASCII 文字を使って、文字列としてフォーマットします。最短長さは 1 です。

オプション・フォーマット: 文字列

65 **NIS Servers** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるネットワーク情報サービス (NIS)+ V3 サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

66 **Server Name** このオプションは、DHCP サーバーに指定します。 DHCP ヘッダーに DHCP オプションとして 『sname』 フィールドが使用されたときに使われるトリビアル・ファイル転送プロトコル (TFTP) サーバー名。

オプション・フォーマット: 文字列

67 **Boot File Name** このオプションは、DHCP サーバーに指定します。 DHCP ヘッダーに DHCP オプションとしてファイル・フィールドが使用されたときに使われるブート・ファイルの名前。 最短長さは 1 です。

注: ブート・ファイル名を DHCP クライアントに渡すにはこのオプションを使います。 ブート・ファイル名は、資格の完全なパス名を含めるときに必要になり、長さは 128 文字以内にします。 たとえば、オプション 67 c:\path\boot_file_name。 このファイルには、BOOTP 応答のなかの 64 オクテットのメーカー拡張フィールドと同じ方法で解釈できる情報がありますが、例外として、ファイルの長さは BootP ヘッダーにより 128 文字に制限されます。

オプション・フォーマット: 文字列

68 **Home Address** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるモバイル IP ホーム・エージェントの IP アドレス (優先順位順)。このオプションで、モバイル・ホストは、モバイル・ホーム・アドレスを引き出し、ホーム・ネットワークのサブネット・マスクを決定することができます。通常の長さは 4 オクテットで、1 つのホーム・エージェントのホーム・アドレスを含みますが、長さは 0 にすることもできます。 長さが 0 のときは、ホーム・エージェントがないこと意味します。

オプション・フォーマット: IP アドレス

69 **SMTP Servers** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるシンプル・メール転送プロトコル (SMTP) サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

70 **POP3 Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるポスト・オフィス・プロトコル (POP) サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

71 **NNTP Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるネットワーク・ニュース転送プロトコル (NNTP) サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

72 **WWW Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できる World Wide Web (WWW) サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

73 **Finger Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるフィンガー・サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

74 **IRC Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるインターネット・リレー・チャット (IRC) サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

75 **StreetTalk Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できるStreetTalk サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

76 **STDA Server** このオプションは、DHCP サーバーに指定します。 クライアントが使用できる StreetTalk ディレクトリー・アシスタンス (STDA) サーバーの IP アドレス (優先順位順)。

オプション・フォーマット: IP アドレス

77 **User Class** このオプションは、DHCP サーバーに指定します。 DHCP クライアントは、オプション 77 を使ってホストがどのクラスのメンバーなのかを DHCP サーバーに示します。 ユーザー・クラスは、クラス用に定義されたパラメーターを DHCP サーバーで受け取るためには、オプション 77 で \DHCPCD.CFG ファイルに数値を手動で入力します。 DHCPCD.CFG ファイルは、ONDEMAND\SERVER\ETC ディレクトリーにあります。

オプション・フォーマット: 文字列

78 **Directory Agent** このオプションは、DHCP サーバーに指定します。 動的ホスト構成プロトコルは、TCP/IP ネットワーク上のホストに構成情報を渡すためのフレームワークを提供します。 サービス・ロケーション・プロトコルを使用するエンティティーがメッセージをやり取りするためには、ディレクトリー・エージェントのアドレスを探し出す必要があります。 そのほか、サービス・ロケーション・プロトコルを使って交換するサービス属性と URL とともに使用する正しいスコープと命名機関を発見する必要があります。 ディレクトリー・エージェントには特定のスコープがあって、特定の命名機関が定義した体系に関する知識を持っていることがあります。

オプション・フォーマット: IP アドレス

79 **Service Scope** このオプションは、DHCP サーバーに指定します。 この拡張機能は、サービス・ロケーション・プロトコルで指定された通りに、サービス要求メッセージに対して応答するときに、サービス・エージェントが使用すべきスコープを示します。

オプション・フォーマット: 文字列

80 **Naming Authority** このオプションは、DHCP サーバーに指定します。 この拡張機能は、URL で使用できる体系の構文を指定する命名機関を示し、これはサービス・ロケーション・プロトコルでエンティティーが使用します。

オプション・フォーマット: 文字列

IBM 固有のオプション

IBM は、ユーザー定義の範囲で (128-254) オプションを定義することで、IBM 固有のオプションを提供します。 これらのオプションは、IBM 用のメーカー・オプション (オプション 43) を定義する代わりに使用します。 これらのオプションの再定義はしないでください。

192 **TXT RR** DHCP サーバーでこのオプションを指定すると、DHCP クライアント・ユーザーは、システム管理者情報フィールドをすべて記入しなければなりません。 注意: OS/2 のクライアントでこのオプションをサポートして

いるのは、TCP/IP バージョン 4.1 だけです。 このオプションには、ユーザー名、ユーザーの電話番号、DDNS クライアント構成プログラムがユーザーに求めるそのほかのフィールドなど、テキスト・ラベルまたは入力フィールドが最大 4 つまで使用できます。 これらのフィールドで、システム管理者は、ホスト名やその他のデータを実際に構成する人を識別できます。 DDNS 構成プログラムは、システム管理者が指定しないと、これらのフィールドを表示しません。 情報は、DNS 内にテキスト・レコードとして保管されます。 ペアを構成するフィールド・ラベルとデータは、1 つの TXT リソース・レコード内に入らなければなりません。使用可能な場所は、それぞれのペアに等分に分割されます。 また、この数値は、動的アドレス・クライアントの DDNSCLI.CFG ファイル内で更新されます。

オプション・フォーマット: 文字列

メーカーのオプション

DHCP プロトコルは、RFC アーキテクチャーのオプション 43 と 60 を使って、DHCP クライアントにメーカー固有の情報を与える方法を提供します。

60 **Option 60** は、DHCP クライアントで構成し、DHCP サーバーに送信して、特定のメーカーがクライアントのときにこのクライアントを識別します。

43 **Option 43** は、DHCP サーバーで構成し、クライアントがオプション 60 を要求したときにメーカー固有の情報をクライアントに返すように定義します。 共通コードの DHCP サーバーでは、オプション 43 は、add vendor-option コマンドを使って構成します。メーカー・オプションを定義できるのは、グローバル・スコープの中だけです。 メーカー・オプションは、メーカー名とオプション・データで構成されています。 オプション・データには、以下の 2 つのフォーマットがあります。

16 進法データ
このデータは、add vendor-optionコマンドが発行されたときに、メーカー名を使って入力します。 16 進法データは、16 進数の文字列を使い、バイトのあいだには空白を入れます。『01 AA 55』

オプション
DHCP オプションは、add option コマンドを使って、メーカー・オプションのスコープに追加できます。

注: 16 進法データとオプションは、メーカーの定義内で両立しません。どちらか一方を定義できますが、両方を定義することはできません。

DHCP で IP を構成する

クライアントのために DHCP サーバーが IP アドレスと構成情報を、追加されたサブネット上にうまく割り当てるためには、IP を正しく構成する必要があります。DHCP サーバーがサブネットをサポートするように構成されているときに、サブネットに直接に接続されていると、こうしたことが必要になります。

この DHCP サーバーに DHCP 要求メッセージを転送するために BOOTP リレー・エージェントが使われている場合は、サブネットとサーバーは直接には接続されていないので、サブネットをサポートするための IP 構成は必要ありません。

IP アドレスの追加

DHCP を構成したサブネット内の IP アドレスは、接続インターフェースに追加する必要があります。

例:

- DHCP がサブネットを以下のように追加しました。

```
DHCP Server config> list subnet all
subnet      subnet          subnet          starting        ending
name        address         mask            IP Addr         IP Addr
-------------------------------------------------------------------------
net-one     192.168.8.0     255.255.255.0   192.168.8.2     192.168.8.50
```

- IP は以下のように要求します。

```
IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list add
IP addresses for each interface:
intf     0   192.168.8.1     255.255.255.0    Local wire broadcast, fill 1
intf     1                                    IP disabled on this interface
intf     2   0.0.0.2         255.255.255.255  Local wire broadcast, fill 1
intf     3                                    IP disabled on this interface
```

IP シンプル・インターネット・アクセスの使用

IP でシンプル・インターネット・アクセスを使用可能にし、これまでに DHCP を構成したことがない場合は、DHCP サーバー内で以下の構成が自動的に作成されます。シンプル・インターネット・アクセスが NAT フィーチャー、IP フィルター、アクセス制御を自動的に構成します。 DHCP がすでに構成されている場合は、DHCP の構成に追加や変更はありません。 詳細と制約については、*プロトコルの構成と監視 解説書 第 1 巻*の 『IP の使用』 の章にあるシンプル・インターネット・アクセスの使用を参照してください。

- IP を以下のように構成しました。

```
IP config>enable simple-internet-access
Interface to Service Provider [0]? 3
SIMPLE-INTERNET-ACCESS enabled on interface 3

IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list add
IP addresses for each interface:
intf     0   192.168.8.1     255.255.255.0    Local wire broadcast, fill 1
intf     1                                    IP disabled on this interface
intf     2                                    IP disabled on this interface
intf     3   0.0.0.3         255.255.255.255  Local wire broadcast, fill 1
                                              SIMPLE-INTERNET-ACCESS Enabled
```

- DHCP サーバーには、以下の構成が作成されます。

```
DHCP Server config> list global
.
.
DHCP Server enabled: Yes
.
.
```

```
DHCP Server config> list subnet all
subnet      subnet          subnet          starting        ending
name        address         mask            IP Addr         IP Addr
-------------------------------------------------------------------------
simple-net  192.168.8.0     255.255.255.0   192.168.8.2     192.168.8.50

DHCP Server config> list option subnet
Enter the subnet name []? simple-net
     option option
     code      data
-----------------------------------------------------------------
 1       255.255.255.0
 3       192.168.8.1
 6       0.0.0.3
```

DHCP サーバーの構成例

ASCII テキスト・ファイル

この節では、ASCII テキスト・フォーマットを使って、DHCP サーバーの代表的な構成の例を示します。 この例は、ユーザーにわかりやすいフォーマットを使った構成を示すための 1 つの例として参照してください。 IBM 2210 は、ASCII による構成をサポートしていません。

この ASCII の例の各機能は、それぞれのタイトルの番号が 501ページの『OPCON (Talk 6) の構成』の talk 6 の構成例の番号と共通になっているので、この番号 (**1**) を使って両者を参照してください。

1 サーバー・パラメーターの構成

```
leaseTimeDefault          120                  # 120 minutes
leaseExpireInterval       20 seconds
supportBOOTP              yes
supportUnlistedClients  yes
```

2 グローバル・オプション。下位のスコープで上書きがなければ、
各クライアントに渡されます。

```
option 15       "raleigh.ibm.com"         # domain name
option 6         9.67.1.5                         # dns server

                 class manager
{
  option 48   6.5.4.3
  option 9    9.37.35.146
  option 210  "manager_authority"   # site specific option given to all managers
}
```

3 メーカー・オプション

```
vendor  XI-clients hex"01 02 03"

vendor XA-clients
{
   option 23 100   # IP TTL
}
```

4 代表的なサブネット

```
subnet  9.2.23.0  255.255.255.0        9.2.23.120-9.2.23.126
```

```
{
        option 28       9.2.23.127         # broadcast address
        option 9   5.6.7.8
        option 51  200
```

5 サブネット・スコープで定義されたクラス・マネージャー。
このオプション 9 は、グローバル・マネージャー・クラスに指定されたグローバル 9 を上書きします。

```
                class manager

        {
                option 9   9.2.23.98
        }
```

6 プログラマーには、それぞれサブネット範囲があります。

```
        class developers  9.2.23.125-9.2.23.126
        {
                option 51       -1                # infinite lease.
                option 9        9.37.35.1         # printer used by the developers
        }
}
```

7 すべてのアドレスを受け入れるが固有のオプションがあるクライアントの例。

```
client 6        0x10005aa4b9ab  ANY
{
        option 51 999
        option 1 255.255.255.0
}
```

8 サービスからアドレスを除外します。

```
client 0       0               9.2.23.121
```

OPCON (Talk 6) の構成

上記と同じ構成を talk 6を使って以下に示します。

1 サーバー・パラメーターの構成

```
Config>f dhcp-server
DHCP server user configuration
DHCP Server config> enable dhcp
DHCP Server config>

DHCP Server config> set lease-time-default hours 2
DHCP Server config>set lease-expire-interval seconds 20
DHCP Server config>set support-bootp yes
DHCP Server config>set support-unlisted-clients global yes

DHCP Server config>li glob
DHCP server Global Parameters
============================

DHCP server enabled: Yes

Balance:  No subnet groups defined

Inorder:  No subnet groups defined

Canonical: No
```

```
Lease Expire Interval:  20 second(s)
Lease Time Default:     2 hour(s)


Support BOOTP Clients: Yes
Bootstrap Server: Not configured

Support Unlisted Clients: Yes

Ping Time: 1 second(s)
Used IP Address Expire Interval: 15 minute(s)
```

2 グローバル・オプション。下位のスコープで上書きがなければ、各クライアントに渡されます。

```
DHCP Server config>add option global 15 raleigh.ibm.com
DHCP Server config>add option global 6 9.67.1.5

DHCP Server config>li option global
option option
code      data
-------------------------------------------------------------
15      raleigh.ibm.com
6       9.67.1.5
DHCP Server config> add class global
Enter the class name []? manager
Class record with name manager has been added

DHCP Server config> add option class-global
Enter the class name []? manager
Enter the option code [1]? 48
Enter the option data []? 6.5.4.3

DHCP Server config>add option class-global 9 9.37.35.146
DHCP Server config>add option class-global manager 210 manager_authority

DHCP Server config>li class global manager
class
name
-------------------------------------------------------------
manager

 Number of Options: 3
 option  option
 code    data
 -------------------------------------------------------------
 48       6.5.4.3
 9        9.37.35.146
 210     manager_authority
```

3 メーカー・オプション

```
DHCP Server config>add vendor-option XI-client
Enter the vendor hex data []? 01 02 03
Vendor-option record with name XI-client has been added

DHCP Server config> add vendor-option XA-client
Enter the vendor hex data []?
Vendor-option record with name XA-client has been added
DHCP Server config> add option vendor-option XA-client 23 100

DHCP Server config>li vendor-option all
vendor      hex
name        data
```

```
-------------------------------------------------------------
XI-client   01 02 03
XA-client
DHCP Server config>li vendor-option det XA-client
vendor      hex
name        data
-------------------------------------------------------------
XA-client

 Number of Options: 1
 option  option
 code    data
 -------------------------------------------------------------
 23      100
```

4 代表的なサブネット

```
DHCP Server config> add subnet
Enter the subnet name []? sub1
Enter the IP subnet []? 9.2.23.0
Enter the IP subnet mask [255.255.255.0]?
Enter start of IP address range [9.2.23.1]? 9.2.23.120
Enter end of IP address range [9.2.23.150]? 9.2.23.126
Enter the subnet group name []?
Subnet record with name sub1 has been added
DHCP Server config>
DHCP Server config> add option subnet
Enter the subnet name []? sub1
Enter the option code []? 28
Enter the option data []? 9.2.23.127
DHCP Server config> add option subnet 9 5.6.7.8
DHCP Server config>add option subnet sub1 51 200

DHCP Server config> add class subnet
Enter the subnet name []? sub1
Enter the class name []? manager
Enter start of IP address range []?
Class record with name manager has been added

DHCP Server config>add option class-subnet sub1 manager
Enter the option code [1]? 9
Enter the option data []? 9.2.23.98
```

6 プログラマーには、それぞれサブネット範囲があります。

```
DHCP Server config> add class subnet
Enter the subnet name []? sub1
Enter the class name []? developers
Enter start of IP address range []? 9.2.23.125
Enter end of IP address range []? 9.2.23.126
Class record with name developers has been added

DHCP Server config>add option class-subnet sub1 developers 51 -1
DHCP Server config>add option class-subnet sub1 developers 9 9.37.35.1

DHCP Server config>li subnet detailed sub1
subnet      subnet          subnet          starting        ending
name        address         mask            IP Addr         IP Addr
-------------------------------------------------------------------------
sub1        9.2.23.0        255.255.255.0   9.2.23.120      9.2.23.126


 Number of Classes: 2
 class
 name
```

```
-------------------------------------------------------------
manager

 Number of Options: 1
 option  option
 code    data
 -------------------------------------------------------------
 9       9.2.23.98
developers
 starting IP address: 9.2.23.125
 ending   IP address: 9.2.23.126

 Number of Options: 2
 option  option
 code    data
 -------------------------------------------------------------
 51      -1
 9       9.37.35.1

Number of Options: 3
option  option
code    data
-------------------------------------------------------------
28      9.2.23.127
9       5.6.7.8
51      200
```

7 すべてのアドレスを受け入れるが固有のオプションがある
クライアントの例。

```
DHCP Server config> add client global
Enter the client name []? any-addr
Enter the client's hardware type (0 - 21) [1]? 6
Enter the client ID (MAC address or string) []? 10005aa4b9ab
Enter the client's IP address (IP address, any, none) []? any

DHCP Server config>add option client-global any-addr 51 999
DHCP Server config>add option client-global any-addr 1 255.255.255.0
```

8 サービスからアドレスを除外します。

```
Enter the client name []? excl-addr
Enter the client's hardware type (0 - 21) [1]? 0
Enter the client ID (MAC address or string) []? 0
Enter the client's IP address (IP address, any, none) []? 9.2.23.121

 DHCP Server config>li cli all
client      client  client                          attached    IP
name        type    identifier                      to subnet   address
-------------------------------------------------------------------------------
any-addr    6       10005aa4b9ab                                Any
excl-addr   0       0                                           9.2.23.121


DHCP Server config>li client global any-addr
client      client  client                          IP
name        type    identifier                      address
-------------------------------------------------------------------
any-addr    6       10005aa4b9ab                    Any

 Number of Options: 2
 option  option
 code    data
 -------------------------------------------------------------
 51      999
 1       255.255.255.0
```

第31章 DHCP サーバーの構成と監視

この章では、DHCP サーバーの構成コマンドおよびオペレーショナル・コマンドの使用方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。

- 『DHCP サーバー構成環境へのアクセス』
- 『DHCP サーバー構成コマンド』
- 535ページの『DHCP サーバー監視環境へのアクセス』
- 535ページの『DHCP サーバー監視コマンド』
- 539ページの『DHCP 動的再構成サポート』

DHCP サーバー構成環境へのアクセス

DHCP サーバーの*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。

1. OPCON プロンプトで、**talk 6** と入力する。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、構成プロンプト (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. 構成プロンプトで、**feature dhcp-server** コマンドを入力し、DHCP Server config> プロンプトを表示します。

DHCP サーバー構成コマンド

表 61. DHCP サーバー構成コマンドの概要

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。
Add	クラス、クライアント、サブネット、またはメーカー・オプションを追加します。
Change	クラス、クライアント、サブネット、またはメーカー・オプションの定義を変更します。
Default	特定のグローバル変数をデフォルト値に戻します。
Delete	クラス、サブネット、またはメーカー・オプションを削除します。
Disable	DHCP サーバーをグローバルに使用不可にします。
Enable	DHCP サーバーをグローバルに使用可能にします。
List	クラス、クライアント、サブネット、またはメーカー・オプションの定義を表示します。
Set	特定のスコープのもとに、グローバル・パラメーターまたはグローバル・オプションの定義を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、クラス、サブネット、メーカー・オプションを追加します。

構文:

add class
client
option
subnet
vendor-option

class *scope [subnet_name] class_name [range_start] [range_end]*
クラスを定義します。

scope クラスを追加するスコープを指定します。

有効値: グローバルまたはサブネット

デフォルト値: なし

subnet_name
scope が *subnet* のときだけ有効になります。 クラスを追加するサブネットの名前を示します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

class-name
クラスの名前を示します。

有効値: 最長 40 文字の ASCII 文字列

デフォルト値: なし

range-start
scope が *subnet* のときだけ有効になります。 クライアントを割り当てる IP アドレス・プールのなかから、最初の IP アドレスを指定します。

有効値: クラスを追加するサブネット範囲内の任意の有効な IP アドレス。

デフォルト値: 特定のサブネットに属するサブネット範囲にある最初の IP アドレス。

range-end
scope が *subnet* のときだけ有効になります。 クライアントを割り当てる IP アドレス・プールのなかから、最後の IP アドレスを指定します。

有効値: クラスを追加するサブネット範囲内の任意の有効な IP アドレス。 この値は、**range-start** に指定した値よりも大きくなります。

デフォルト値: 特定のサブネットに属するサブネット範囲にある最初の IP アドレスに 5 を足した値。 5 を足した IP アドレスがサブネット範囲にない場合は、サブネット範囲の最後の IP アドレスがデフォルト値になります。

例:

```
DHCP Server config> add class global
Enter class name? ClassA

DHCP Server config> add class subnet
Enter the subnet name[]? subA
Enter class name[]? ClaA
Enter start of IP address range[10.1.1.1]?
Enter end of IP address range[10.1.1.6]?
```

client *scope [subnet_name] client_name id-type id-value address*

クライアントを定義します。

scope クラスを追加するスコープを指定します。

有効値: グローバルまたはサブネット

デフォルト値: なし

subnet-name

scope が *subnet* のときだけ有効になります。 クライアントを追加するサブネットの名前を示します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

client-name

クライアントの名前を示します。

有効値: 任意の 10 文字の ASCII 文字列

デフォルト値: なし

id-type

クライアントのハードウェア・タイプを示します。 RFC 1340 に定義されていて、IBM 2210 で使用できるハードウェアを以下に有効値として示します。

有効値:

0 未指定。 クライアントの記号名を示します。

1 イーサネット

6 IEEE 802 ネットワーク (802.5 トークンリングを含む)

デフォルト値: 1

id-value

クライアントの識別子を指定します。 **id-type** が *0* の場合は、**id-value** は 64 文字の文字列になります。 それ以外のときは、**id-value** は MAC アドレスになります。

注: **id-type** が *0* で、**id-value** が *0* の場合は、指定したIP アドレスをサーバーに送ってはいけないことを示します。

有効値: 0 または、任意の MAC アドレス (12 文字の 16 進数字)

デフォルト値: なし

address

クライアントに提供する IP アドレスを指定する場合と、クライアントにサービスが与えられないことを示す文字列、またはクライアントに IP アドレスのプールから任意のアドレスが与えられることを示す文字列を示す場合があります。

有効値:

任意の有効な IP アドレス

小数点付き 10 進数。 クライアントがサブネット・スコープ内に定義されている場合は、IP アドレスはサブネット範囲内になければなりません。

なし 一致するクライアントには、サービスが与えられないことを示します。

any クライアントには、サブネット・プール内の任意の IP アドレスが与えられることを示します。

デフォルト値: なし

注: **id-type** が *0* で、**id-value** が *0* の場合は、指定したIP アドレスをサーバーに送ってはいけないことを示します。

例:

```
DHCP Server config> add client global
     Enter the client name []? ClientA
     Enter the client's hardware type (0 - 21) [1]? 0
     Enter the client ID (MAC address or string) []? ClientA
     Enter the client's IP address (IP address, any, none) []? 9.1.1.1
     Client record with name ClientA has been added

DHCP Server config> add client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the client's hardware type (0 - 21) [1]? 1
     Enter the client ID (MAC address or string) []? 400000000010
     Enter the client's IP address (IP address, any, none) []? 10.1.1.10
     Client record with name CliA has been added
```

option *scope [subnet-name] [class-name] [client-name] [vendor-name] code data*

オプションを定義します。 オプションは、グローバルに存在したり、サブネット、クラス、クライアント、またはメーカー・オプションなどのスコープ内に存在できます。

scope オプションを追加するスコープを指定します。

有効値:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet

- vendor-option

デフォルト値: なし

subnet-name

scope が *subnet*、 *class-subnet*、または *client-subnet* のときに有効になります。 クライアントを追加するサブネットの名前を示します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

class-name

scope が *class-global* または *class-subnet* のときに有効になります。オプションを追加するクラスの名前を示します。

有効値: 任意の既存クラスの名前

デフォルト値: なし

client-name

scope が *client-global* または *client-subnet* のときに有効になります。オプションを追加するクライアントの名前を示します。

有効値: 任意の既存クライアントの名前

デフォルト値: なし

vendor-name

scope が *vendor-option* のときに有効になります。オプションを追加するメーカーの名前を示します。

有効値: 任意の既存メーカーの名前

デフォルト値: なし

code オプション・コードを指定します。 DHCP オプションは、RFC 2132 に定義されています。 オプションとオプションのフォーマットについては、485ページの『DHCP のオプション』を参照してください。

有効値: 1 〜 255

デフォルト値: 1

data オプション・データを指定します。 オプション・データの定義には、 3 つの方法があります。

- ASCII 文字列を使って、RFC 2132 に定義されている特定のフォーマットをする方法。
- 初期化のときに 16 進数変換を行う方法。 データは、*hex: 01 aa 04* のように入力します。
- 文字列を使う方法。 データは、*abcdef* のように入力します。

例:

```
DHCP Server config> add option global
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option subnet
     Enter the subnet name []? subA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option class-global
     Enter the class name []? ClassA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option client
     Enter the client name []? ClientA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 85
     Enter the option data []? hex:01 AA 04
```

例:

```
DHCP Server config> add option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 86
     Enter the option data []? 9.67.85.4
```

subnet *subnet_name subnet-address subnet-mask range-start range-end [subnet_group_name] [subnet_group_priority] [policy-list]*

サブネットを定義します。

subnet-name

サブネットの名前を示します。

有効値: 任意の 10 文字の ASCII 文字列

デフォルト値: なし

subnet-address

サブネットのアドレスを示します。 アドレスは、小数点付き 10 進数で示します。

有効値: 任意の有効な IP サブネット・アドレス

デフォルト値: なし

subnet-mask

サブネット・アドレス・マスクを指定します。 サブネット・アドレスは、サブネット・マスク内におき、マスクよりも多くのビットを含むことはできません。

有効値: 小数点付き 10 進数による任意の有効な IP マスク

デフォルト値: サブネット・アドレスをもとにした計算値

range-start

このサーバーがこのサブネットのために管理する IP アドレス・プールの最初の IP アドレスを指定します。 *range-start* を指定しないと、サーバーはサブネット内のすべてのアドレスを管理します。

有効値: 指定したサブネット内の任意の有効な IP ホスト・アドレスで、小数点付き 10 進数で表す。

デフォルト値: サブネットの最初の IP アドレス

range-end

このサーバーがこのサブネットのために管理する IP アドレス・プールの最後の IP アドレスを指定します。

有効値: 指定したサブネット内の任意の有効な IP ホスト・アドレスで、小数点付き 10 進数で表す。

デフォルト値: range-start に 50 を足した値。 50 を足した IP アドレスがサブネットにない場合は、サブネット内の最後の IP アドレスがデフォルト値になります。

subnet-group-name

このサブネットが属するサブネット・グループの名前を指定します。

有効値: 最長 64 文字の任意の ASCII 文字列

デフォルト値: なし

subnet-group-priority

サブネット・グループ内のサブネットの優先順位を指定します。 この優先順位は、特定のサブネット・グループ内でアドレスが割り当てられるときの順序を決めるのに使用します。

有効値: 1 〜 65535

デフォルト値: 1

policy-list

サブネット・グループを追加するポリシー・アドレス・リストをバランスにするかインオーダーにするかを識別します。 サブネット・グループがすでにリスト上にあり、その他を指定すると、サブネット・グループは新しいリストに移動されます。

有効値: インオーダーまたはバランス

デフォルト値: 新しいサブネットの場合、デフォルトはインオーダーです。新しくない場合は、サブネット・グループは現行ポリシーに属します。

例:

```
DHCP Server config> add subnet
 Enter the subnet name []? subA
 Enter the IP subnet []? 10.1.1.0
 Enter the IP subnet mask [255.255.255.0]?
 Enter start of IP address range [10.1.1.1]?
 Enter end of IP address range [10.1.1.31]?
 Enter the subnet group name []? group1
 Enter the subnet group priority (1 - 65535) [1]?
 Enter the access policy list (Inorder or Balance) [Inorder]?
 Subnet record with name sub1 has been added
 Subnet group group1 is being added to the Inorder List
```

vendor-option *vendor_name [hex_value]*

メーカー・オプションを追加します。 メーカー・オプションを提供する方法は 2 つあります。

- プロンプトで 16 進数のデータを入力する。
- **add option vendor** コマンドを使って、メーカーに特定のオプションを追加する。 オプションについては、 508ページを参照してください。

vendor_name

メーカーの名前を指定します。

有効値: 最長 40 文字の ASCII 文字列

デフォルト値: なし

hex-value

16 進数の ASCII 文字列で、オプションのデータ部分の 16 進数を指定します。

有効値:任意の16 進数文字列。書式は *01 aa 04* のようにする。

デフォルト値: なし

例:

```
DHCP Server config> add vendor-option
     Enter the vendor name []? XA-client
     Enter the vendor hex data [] 01 aa 04?
     Vendor-option record with name XA-client has been added
```

Change

change コマンドは、クラス、クライアント、サブネット、またはメーカー・オプションの構成を変更するときに使用します。

構文:

change class
client
subnet
vendor-option

class *scope [subnet_name] class_name new_class_name [new_range_start] [new_range_end]*

クラスを変更します。

scope 変更するクラスのスコープを指定します。

有効値: グローバルまたはサブネット

デフォルト値: なし

subnet-name

scope が *subnet* のときだけ有効になります。 クラスが属するサブネットの名前を示します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

class-name

クラスの名前を示します。

有効値: 既存クラスの名前

デフォルト値: なし

new-class-name

クラスの新しい名前を示します。

有効値: 最長 40 文字の ASCII 文字列

デフォルト値: 既存のクラスの名前

new-range-start

scope が *subnet* のときだけ有効になります。 クライアントを割り当てる IP アドレス・プールのなかから、新規の最初の IP アドレスを指定します。

有効値: サブネット範囲内の任意の IP アドレス

デフォルト値: 既存の range-start

new-range-end

クライアントを割り当てる IP アドレス・プールのなかから、新規の最後の IP アドレスを指定します。

有効値: サブネット範囲内の任意の有効な IP アドレスで、**new-range-end** よりも大きな値。

デフォルト値: 既存の range-end

例:

```
DHCP Server config> change class global
     Enter the class name []? ClassA
     Enter the new class name [ClassA]?
```

例:

```
DHCP Server config> change class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the new class name [ClaA]?
     Enter start of IP address range [10.1.1.1]?
     Enter end of IP address range [10.1.1.6]?
```

client *scope [subnet_name] client_name new-client_name new-id-type new-id-value new-address*

クライアントを変更します。

scope 変更するクライアントのスコープを指定します。

有効値: グローバルまたはサブネット

デフォルト値: なし

subnet-name

scope が *subnet* のときだけ有効になります。 クライアントが属するサブネットの名前を示します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

client-name

クライアントの名前を示します。

有効値: 任意の既存クライアントの名前

デフォルト値: なし

new-client-name

クライアントの新しい名前を示します。

有効値: 最長 10 文字の ASCII 文字列

デフォルト値: 既存のクライアントの名前

new-id-type

クライアントの新しいハードウェア・タイプを示します。

有効値: 0 ～ 21、 507 ページを参照してください。

デフォルト値: クライアントの既存のハードウェア・タイプ

new-id-value

クライアントの新しい識別子を指定します。

有効値: 0 または、任意の MAC アドレス (12 文字の 16 進数字)

デフォルト値: 既存のクライアントの id-type

注: **id-type** が *0* で、**id-value** が *0* の場合は、指定したIP アドレスをサーバーに送ってはいけないことを示します。

new-address

クライアントに提供する新しい IP アドレスを指定する場合と、クライアントにサービスが与えられないことを示す文字列、またはクライアントに IP アドレスのプールから任意のアドレスが与えられることを示す文字列を示す場合があります。

有効値:

任意の有効な IP アドレス

なし 一致するクライアントには、サービスが与えられないことを示します。

any クライアントには、サブネット・プール内の任意の IP アドレスが与えられることを示します。

デフォルト値: なし

注: **id-type** が *0* で、**id-value** が *0* の場合は、指定したIP アドレスをサーバーに送ってはいけないことを示します。

例:

```
DHCP Server config> change client global
     Enter the client name []? ClientA
     Enter the new client name [ClientA]?
     Enter the new client hardware type (0 - 21) [0]?
     Enter the new client ID  [ClientA]?
     Enter the client's new IP address (IP address, any, none) [9.1.1.1]?
     Client ClientA has been changed
```

例:

```
DHCP Server config> change client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the new client name [ClientA]?
     Enter the new client hardware type (0 - 21) [1]?
     Enter the new client ID  [400000000010]?
     Enter the client's new IP address (IP address, any, none) [10.1.1.10]?
     Client CliA has been changed
```

subnet *subnet_name new_subnet_name new_subnet_address new_subnet_mask new-range_start new-range_end*

サブネットを変更します。

subnet_name

変更する特定のサブネットの名前を指定します。

有効値: 既存サブネットの名前

デフォルト値: なし

new_subnet_name

特定のサブネットの新しい名前を示します。

有効値: 任意の 10 文字の ASCII 文字列

デフォルト値: サブネットの元の名前

new_subnet_addresss

サブネットの新しいアドレスを指定します。 アドレスは、小数点付き 10 進表記で指定します。

有効値: 任意の有効な IP サブネット・アドレス

デフォルト値: 既存のサブネット・アドレス

new_subnet_mask

新しいサブネット・アドレス・マスクを指定します。 サブネット・アドレスは、サブネット・マスク内におき、マスクよりも多くのビットを含むことはできません。

有効値: 任意の有効な IP マスク

デフォルト値: 既存のサブネット・マスク

new-range-start

このサーバーがこのサブネットのために管理する IP アドレス・プールの新しい最初の IP アドレスを指定します。 *range-start* を指定しないと、サーバーはサブネット内のすべてのアドレスを管理します。

有効値: サブネット範囲にある任意の有効な IP アドレス

デフォルト値: 既存のプールの最初のアドレス

new-range-end

このサーバーがこのサブネットのために管理する IP アドレス・プールの新しい最後の IP アドレスを指定します。

有効値: サブネット範囲にあり、プールの最初のアドレスよりも大きな任意の有効な IP アドレス

デフォルト値: 既存のプールの最後のアドレス

例:

```
DHCP Server config> change subnet
     Enter the subnet name []? subA
     Enter the new subnet name [subA]?
     Enter the new IP subnet[10.1.1.0]?
     Enter the new IP subnet mask[255.255.0.0]?
     Enter new start of IP address range [10.1.1.1]?
     Enter new end of IP address range [10.1.1.31]?
     Enter the new subnet group name [group11]?
     Enter the new subnet group priority [1]?
     Enter the new access policy list (Inorder or Balance) [Inorder]?
```

vendor-option *vendor_name new_vendor_name [new_hex_value]*

メーカー・オプションを変更します。

vendor_name

メーカー・オプションの新しい名前を指定します。

有効値: 任意の既存メーカーの名前

デフォルト値: なし

new_vendor_name

メーカー・オプションの新しい名前を指定します。

有効値: 最長 40 文字の ASCII 文字列

デフォルト値: 既存のメーカー・オプションの名前

new_hex_value

新しい 16 進数の ASCII 文字列で、オプションのデータ部分の16進数を指定します。 このメーカー・オプションに特定のオプションがすでに追加されているときは、16 進数を追加できません。

有効値: 任意の有効な 16 進数文字列

デフォルト値: 既存の 16 進数文字列

例:

```
DHCP Server config> change vendor-option
     Enter the vendor name []? XA-clients
     Enter the new vendor name [XA-clients]?
     Enter the new vendor data [01 aa 04]?
```

Delete

delete コマンドは、クラス、クライアント、オプション、サブネット、サブネット・グループ、またはメーカー・オプションを削除するときに使用します。

構文:

delete class

client

option

subnet

subnet-group

vendor-option

class *scope [subnet_name] class_name*
スコープに定義された 1 つのクラスとすべてのオプションを削除します。

scope クラスを削除するスコープを指定します。

有効値: グローバルまたはサブネット

デフォルト値: なし

subnet-name
scope が *subnet* のときだけ有効になります。 クラスを削除するサブネットの名前を示します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

class-name
削除するクラスの名前を示します。

有効値: 任意の既存クラスの名前

デフォルト値: なし

例:

```
DHCP Server config> delete class global
     Enter the class name []? ClassA
```

例:

```
DHCP Server config> delete class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
```

client *scope [subnet_name] client_name*
スコープに定義された 1 つのクライアントとすべてのオプションを削除します。

scope クライアントを削除するスコープを指定します。

有効値: グローバルまたはサブネット

デフォルト値: なし

subnet_name
scope が *subnet* のときだけ有効になります。 クライアントを削除するサブネットの名前を示します。

有効値: 既存サブネットの名前

デフォルト値: なし

client_name
削除するクライアントの名前を示します。

有効値: 任意の既存クライアントの名前

デフォルト値: なし

例:

```
DHCP Server config> delete client global
     Enter the client name []? ClientA
```

例:

```
DHCP Server config> delete client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
```

option *scope [subnet_name] [class_name] [client_name] [vendor_name] code*
特定のスコープ内の 1 つのオプションを削除します。

scope オプションを削除するスコープを指定します。

有効値:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

デフォルト値: なし

subnet-name

scope が *subnet*、 *class-subnet*、または *client-subnet* のときに有効になります。 クライアントを削除するサブネットの名前を指定します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

class-name

scope が *class-global* または *class-subnet* のときに有効になります。 オプションを削除するクラスの名前を示します。

有効値: 任意の既存クラスの名前

デフォルト値: なし

client-name

scope が *client-global* または *client-subnet* のときに有効になります。 オプションを削除するクライアントの名前を示します。

有効値: 任意の既存クライアントの名前

デフォルト値: なし

vendor-name

scope が *vendor-option* のときに有効になります。 オプションを削除するメーカーの名前を示します。

有効値: 任意の既存メーカーの名前

デフォルト値: なし

code オプション・コードを指定します。 DHCP オプションは、RFC

2132 に定義されています。 オプションとオプションのフォーマットについては、485ページの『DHCP のオプション』を参照してください。

有効値: 1 ～ 255

デフォルト値: 1

例:

```
DHCP Server config> delete option global
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option subnet
     Enter the subnet name []? subA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option class-global
     Enter the class name []? ClassA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option client
     Enter the client name []? ClientA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option vendor-option
          Enter the vendor name []? XI-clients
     Enter the option code [1]? 85
```

例:

```
DHCP Server config> delete option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 86
```

subnet *subnet_name*

スコープ内に定義された 1 つのサブネットとすべてのクラス、クライアント、オプションを削除します。

subnet_name

削除するサブネットの名前を指定します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

例:

```
DHCP Server config> delete subnet
     Enter the subnet name []? subA
```

```
You are about to delete a subnet subA
and all the associated class, client, and option records associated with it
Are you sure you want to continue? [No]:
```

subnet-group *subnet_group_name*

特定のサブネット・グループに関連したすべてのサブネットとサブネット・スコープに定義されたすべてのクラス、クライアント、オプションを削除します。

subnet_group_name

サブネット・グループを識別する名前を指定します。

有効値: 既存サブネット・グループの名前

デフォルト値: なし

例:

```
DHCP Server config> delete subnet-group
     Enter the subnet group name []? group2
     You are about to delete a all subnets in group group2
     and all the associated class, client, and option records associated with them
     Are you sure you want to continue? [No]:
```

vendor-option *vendor_name*

スコープに定義されたメーカー・オプションと任意のオプションを削除します。

vendor_name

メーカーの名前を指定します。

有効値: 最長 40 文字の ASCII 文字列

デフォルト値: なし

例:

```
DHCP Server config> delete vendor-option
     Enter the vendor name []? XA-clients
```

Disable

disable コマンドは、DHCP サーバーをグローバルに無効にします。

構文:

disable dhcp-server

例:

```
DHCP Server config> disable dhcp-server
```

Enable

enable コマンドは、DHCP サーバーをグローバルに使用可能にします。

構文:

enable dhcp-server

例:

```
DHCP Server config> enable dhcp-server
```

List

list コマンドは、クラス、クライアント、グローバル・パラメーター、サブネット、またはメーカー・オプション、およびその他の関連オプションについて、構成情報を表示します。

構文:

list class
client
global
option
subnet
vendor-option

class all
global *class-name*
subnet *class-name*

構成されたすべてのクラスの概要を表示したり、特定のクラスの詳細情報を表示します。

class-name
表示するクラスの名前を示します。

有効値: 任意の既存クラスの名前

デフォルト値: なし

例:

```
DHCP Server config> list class all

     class              attached
     name               to subnet
     ------------------------------------------------------------
     ClassA
     ClaA               subA
```

例:

```
DHCP Server config> list class global
     Enter the class name []? ClassA

     class
     name
     ------------------------------------------------------------
     ClassA
     Bootstrap Server: 100.100.100.100
     Canonical: Yes
     Support Unlisted Clients: Yes
     Number of Options: 1
     option    option
     code      data
     ------------------------------------------------------------
     1         255.255.0.0
```

例:

```
DHCP Server config> list class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA

     class
     name
     ----------------------------------------------------------------
     ClaA
     starting IP address: 10.1.1.3
     ending IP address: 10.1.1.5
     Bootstrap Server: 100.100.100.100
     Canonical: Yes
     Support Unlisted Clients: DHCP

     Number of Options: 1
     option    option
     code      data
     ----------------------------------------------------------------
     6         9.67.100.1
```

client all

global *client-name*

subnet *client-name*

構成されたすべてのクライアントの概要を表示したり、特定のクライアントの詳細情報を表示します。

client-name

表示するクライアントの名前を示します。

有効値: 任意の既存クライアントの名前

デフォルト値: なし

例:

```
DHCP Server config> list client all
     client   client   client         attached    IP
     name     type     identifier     to subnet   address
     ------------------------------------------------------------------------------
     ClientA   0       ClientA                    9.1.1.1

     CliA      1       400000000010    subA       10.1.1.10
```

例:

```
DHCP Server config> list client global
     Enter the client name []? ClientA
```

例:

```
DHCP Server config> list client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA

     client client    client        IP
     name   type      identifier    address
     ---------------------------------------------------------------------
     CliA       1     400000000010  10.1.1.10
      Bootstrap Server: 200.200.200.200
      Canonical: Yes

     Number of Options: 1
```

```
option   option
code     data
-----------------------------------------------------------
6        9.67.100.1
```

global

グローバル・パラメーターを表示します。

例:

```
DHCP Server config> list global

    DHCP server Global Parameters
    =============================
    DHCP server enabled: Yes

    Balance: group2

    Inorder: group1

    Canonical: No

    Lease Expire Interval: 1 minute(s)
    Lease Time Default: 1 day(s)

    Support BOOTP Clients: No
    Bootstrap Server: Not configured

    Support Unlisted Clients: Yes
    Ping Time: 1 second(s)
    Used IP Address Expire Interval: 15 minute(s)
```

option *scope [subnet-name] [class-name] [client-name] [vendor-name] code*

scope オプションを表示するスコープを指定します。

有効値:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

デフォルト値: なし

subnet-name

scope が *subnet*、*class-subnet*、または *client-subnet* のときに有効となります。オプションが属するサブネットの名前を示します。

有効値: 任意の既存サブネットの名前

デフォルト値: なし

class-name

scope が *class-global* または *class-subnet* のときに有効になります。 表示するオプションが属するクラスの名前を示します。

有効値: 任意の既存クラスの名前

デフォルト値: なし

client-name

scope が *client-global* または *client-subnet* のときに有効になります。 表示するオプションが属するクライアントの名前を示します。

有効値: 任意の既存クライアントの名前

デフォルト値: なし

vendor-name

scope が *vendor-option* のときに有効になります。 表示するオプションが属するメーカーの名前を示します。

有効値: 任意の既存メーカーの名前

デフォルト値: なし

code オプション・コードを指定します。 DHCP オプションは、RFC 2132 に定義されています。 オプションとオプションのフォーマットについては、485ページの『DHCP のオプション』を参照してください。

有効値: 1 〜 255

デフォルト値: 1

例:

```
DHCP Server config> list option global

     option   option
     code     data
     ----------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option class-global
     Enter the class name []? ClassA
     option   option
     code     data
     ----------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? claA

     option   option
     code     data
     ----------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option client-global
     Enter the client name []? ClientA
```

```
     option   option
     code     data
     ----------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? cliA

     option   option
     code     data
     ----------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option subnet
     Enter the subnet name []? subA


     option   option
     code     data
     ----------------------------------------------------------------
     6        9.67.100.1
```

例:

```
DHCP Server config> list option vendor-option
          Enter the vendor name []? XI-clients


     option   option
     code     data
     ----------------------------------------------------------------
     85        hex:01 aa 04
     86        9.67.85.4
```

subnet

all

detailed *subnet-name*

構成されたすべてのサブネットの概要を表示したり、特定のサブネットの詳細情報を表示します。

subnet-name

表示するサブネットの名前を示します。

有効値: 既存サブネットの名前

デフォルト値: なし

例:

```
DHCP Server config> list subnet all

     name    address    mask          IP Addr    IP Addr
     ------------------------------------------------------------------------
     subA    10.1.1.0   255.255.0.0   10.1.1.1   10.1.1.31
     subB    11.1.1.0   255.255.0.0   11.1.1.1   11.1.1.31
```

例:

```
DHCP Server config> list subnet detailed
     Enter the subnet name []? subA

     subnet    subnet     subnet        starting      ending
     name      address    mask          IP Addr       IP Addr
     ------------------------------------------------------------------------
     subA      10.1.1.0   255.255.0.0   10.1.1.1      10.1.1.31
     Subnet Group: group1/1

     Number of Classes: 1
     class
     name
    ----------------------------------------------------------------
     ClaA
     starting IP address: 10.1.1.1
     ending   IP address: 10.1.1.6
     Bootstrap Server: 100.100.100.100
     Canonical: Yes
     Support Unlisted Clients: DHCP

     Number of Options: 1
     option   option
     code     data
     ----------------------------------------------------------------
     6        9.67.100.1

     Number of Clients: 1
     client     client     client            IP
     name       type       identifier        address
     ------------------------------------------------------------------------
     CliA       1          400000000010      10.1.1.10
     Bootstrap Server: 200.200.200.200
     Canonical: Yes

     Number of Options: 1
     option   option
     code     data
     ----------------------------------------------------------------
     6        9.67.100.1

     Number of Options: 1
     option option
     code   data
     ----------------------------------------------------------------
     1      255.255.255.0
```

vendor-option all

detailed *vendor-name*

構成されたすべてのメーカーの概要を表示したり、特定のメーカーの詳細情報を表示します。

vendor-name

表示するメーカー・オプションの名前を示します。

有効値: 既存の vendor-name

デフォルト値: なし

例:

```
DHCP Server config> list vendor-option all

          vendor          hex
```

```
          name            data
          ----------------------------------------------------------------
          XA-clients      01 AA 04
          XI-clients

DHCP Server config> list vendor-option detailed
          Enter the vendor name []? XI-clients
          vendor          hex
          name            data
          ----------------------------------------------------------------
          XI-clients

          Number of Options: 2
          option    option
          code      data
          ----------------------------------------------------------------
          85        hex:01 AA 04
          86        9.67.85.4
```

Set

set コマンドは、グローバル・パラメーターの数値を指定したり、バランスとインオーダーのリストにサブネット・グループを追加するときに使用します。

構文:

set balance
bootstrapserver
canonical
inorder
lease-expire-interval
lease-time-default
ping-time
support-bootp
support-unlisted-clients
used-ip-address-expire-interval

balance *subnet_group_name*

サブネット・グループをバランス・リストに追加します。 アドレスは、サブネット・グループ内に定義されたグループに関連付けられたすべてのサブネットから、優先順位にしたがってラウンドロビン方式によって割り当てられます。

subnet_group_name

このサブネットが属するサブネット・グループの名前を指定します。

有効値: 既存サブネット・グループの名前

デフォルト値: なし

例:

```
DHCP Server config> set balance
     Enter the subnet group name []? group1
```

bootstrapserver *scope [subnet-name] [class-name] [client-name] address*

DHCP サーバーがクライアントのためにブートストラップ・サーバーを指定するかどうかを指定します。 DHCP サーバーにブートストラップ・サーバーを指定させるには、サーバーの IP アドレスを定義します。このパラメーターは、グローバル、サブネット、クラス、クライアントなどのスコープ内で指定します。

scope ブートストラップ・サーバー・パラメーターのスコープを指定します。

有効値:

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

デフォルト値: なし

subnet-name

スコープが *subnet*、*class-subnet*、または *client-subnet* のときに有効になります。ブートストラップ・サーバーを指定するサブネットの名前を示します。

有効値: 既存サブネットの名前

デフォルト値: なし

class-name

スコープが *class-global* または *class-subnet* のときに有効になります。ブートストラップ・サーバーを指定するクラスの名前を示します。

有効値: 任意の既存クラスの名前

デフォルト値: なし

client-name

スコープが *client-global* または *client-subnet* のときに有効になります。ブートストラップ・サーバーを指定するクライアントの名前を示します。

有効値: 任意の既存クライアントの名前

デフォルト値: なし

サーバーの IP アドレス

ブートストラップ・サーバーの IP アドレスを指定します。

有効値: 小数点付き 10 進数による任意の有効な IP アドレス

デフォルト値: なし

例:

```
DHCP Server config> set bootstrap-server class-global
     Enter the class name []? ClassA
```

```
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClassA
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server client-global
     Enter the client name []? ClientA
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server client-subnet
     Enter the subnet name []? subA
     Enter the client name []? ClientA
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server global
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server subnet
     Enter the subnet name []? subA
     Enter the IP address of the server []? 100.100.100.100
```

canonical *scope [subnet-name] [class-name] [client-name] value*

DHCP サーバーが MAC アドレスを標準フォーマットに変換するかどうかを指定します。

イーサネット 802.3 クライアント用の MAC アドレスは、標準フォーマットで保存します (バイトは最小重みビットで始まります)。 トークンリングのクライアント用の MAC アドレスは、非標準フォーマットで保存します (バイトは最大重みビットで始まります)。 このパラメーターは、DHCP サーバーとクライアントが両者のあいだで異なるメディア・タイプにあるとき (片方がトークンリングでもう一方がイーサネット 802.3 のときなど) で、両者のあいだに変換ブリッジがあるときに使用します。このパラメーターを *yes* にすると、DHCP サーバーにより、クライアントの MAC アドレスが標準フォーマットから非標準フォーマット、あるいは非標準フォーマットから標準フォーマット書式へと入れ代わります。 DHCP サーバーは、MAC アドレスがもともとどちらのフォーマットなのかを知らないので、このパラメーターを *yes* にしても、アドレスは単に双方向に入れ代わるだけです。標準フォーマットは、グローバル、サブネット、クラス、クライアントなどのスコープに設定できます。

scope ブートストラップ・サーバー・パラメーターのスコープを指定します。

有効値:

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

デフォルト値: なし

subnet-name

スコープが *subnet*、*class-subnet*、または *client-subnet* のときに有効になります。標準フォーマットを指定するサブネットの名前を示します。

有効値: 既存サブネットの名前

デフォルト値: なし

class-name

スコープが *class-global* または *class-subnet* のときに有効になります。標準フォーマットを指定するクラスの名前を示します。

有効値: 任意の既存クラスの名前

デフォルト値: なし

client-name

スコープが *client-global* または *client-subnet* のときに有効になります。標準フォーマットを指定するクライアントの名前を示します。

有効値: 任意の既存クライアントの名前

デフォルト値: なし

value MAC アドレスを標準フォーマットに変換するかどうかを指定します。

有効値: yes、no

デフォルト値: **scope** が *global* のときは no。 あるいは、デフォルト値は、スコープの階層によって決定されます。 スコープについては、482ページの『概念と用語』を参照してください。

例:

```
DHCP Server config> set canonical class-global
 Enter the class name []? ClassA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical class-subnet
 Enter the subnet name []? subA
 Enter the class name []? ClassA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical client-global
 Enter the client name []? ClientA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical client-subnet
 Enter the subnet name []? subA
 Enter the client name []? ClientA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical global
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical subnet
 Enter the subnet name []? subA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

inorder *label-list*

サブネット・グループをインオーダー・リストに追加します。 アドレスは、そのサブネットに割り当てられた優先順位にしたがって、サブネット・グループ内のサブネットから割り当てられます。

subnet_group_name

このサブネットが属するサブネット・グループを指定します。

有効値: 既存サブネット・グループの名前

デフォルト値: なし

例:

```
DHCP Server config> set inorder
     Enter the subnet group name []? g2
```

lease-expire-interval *time length*

アドレス・プールのすべてのアドレスについて、リースの期限切れを見るためにリース状態を調査する間隔を指定します。 リースの期限切れ間隔は、グローバル・レベルで設定します。

time 時間測定の単位を指定します。

有効値: 秒、分、時間

デフォルト値: なし

length 間隔の長さを指定します。

有効値: 15 秒 ～ 12 時間

デフォルト値:

- 15 (時間単位が秒の場合)
- 1 (時間単位が分の場合)
- 1 (時間単位が時間の場合)

例:

```
DHCP Server config> set lease-expire-interval seconds
     How long is the interval in seconds (max:59) [15]? 59
```

例:

```
DHCP Server config> set lease-expire-interval minutes
     How long is the interval in minutes (max:59) [1]? 45
```

例:

```
DHCP Server config> set lease-expire-interval hours
     How long is the interval in hours (max:12) [1]? 2
```

lease-time-default *time length*

DHCP サーバーが発行したリースについて、デフォルトのリース期間を指定します。 間隔を無限大にすると、リースの期限がなくなります。 リースのデフォルト期間は、グローバル・レベルで設定します。

time 時間測定の単位を指定します。

有効値: 分、時間、日、週、月、年、無限大

デフォルト値: なし

length 間隔の長さを指定します。

有効値: 3 分 ～ 無限大

デフォルト値:

- 3 (時間単位が分の場合)
- 1 (時間単位が時間の場合)
- 1 (時間単位が日の場合)
- 1 (時間単位が月の場合)
- 1 (時間単位が年の場合)

例:

```
DHCP Server config> set lease-time-default minutes
     How long is the interval in minutes (max:59) [3]? 2
```

例:

```
DHCP Server config> set lease-time-default hours
     How long is the interval in hours (max:23) [1]?
12
```

例:

```
DHCP Server config> set lease-time-default days
     How long is the interval in days (max:6) [1]? 2
```

例:

```
DHCP Server config> set lease-time-default weeks
     How long is the interval in weeks (max:3) [1]? 1
```

例:

```
DHCP Server config> set lease-time-default months
     How long is the interval in months (max:11) [1]? 3
```

例:

```
DHCP Server config> set lease-time-default years
     How long is the interval in years (max:10) [1]? 3
```

例:

```
DHCP Server config> set lease-time-default infinity
```

ping-time *time length*

DHCP サーバーは、IP アドレスを割り当てる前に、その IP アドレスが使われていないことを確認します。 この値は、DHCP サーバーがアドレスを利用する前に PING 応答を待つ時間を指定します。 値を 0 にすると、PING が無効になり、DHCP サーバーは、アドレスを割り当てる前にそのアドレスのをテストしません。

time 時間測定の単位を指定します。

有効値: 秒数

デフォルト値: なし

length 間隔の長さを指定します。

有効値: 0 ～ 5 秒

デフォルト値: 1

例:

```
DHCP Server config> set ping-time seconds
   How long is the interval in seconds (max:5) [1]? 3
```

support-bootp *value*

サーバーが BOOTP クライアントの要求に応答するかどうかを指定します。 DHCP サーバーが BOOTP クライアントをサポートするように構成した後に BOOTP クライアントをサポートしないように再構成した場合は、再構成する前に BOOTP クライアントとのバインドを確立したアドレスについては、BOOTP クライアントがさらに要求を送るまでは (リスタートのとき)、このバインドは維持されます。 そのとき、サーバーは応答せず、バインドは解除されます。 このパラメーターは、グローバル・レベルで設定します。

有効値: yes または no

デフォルト値: no

例:

```
DHCP Server config> set support-bootp
     Would you like the server to support BOOTP clients? [No] yes
```

support-unlisted-clients *scope [subnet-name] [class-name] value*

この構成に明記してあるクライアント ID 以外の DHCP クライアントからの要求にサーバーが応答するかどうかを指定します。 このパラメーターには、複数の設定値があります。

scope **support-unlisted-clients**パラメーターのスコープを指定します。

有効値:

- class-global
- class-subnet
- global
- subnet

デフォルト値: なし

subnet-name

スコープが*subnet*、*class-subnet*、または*client-subnet* のときは有効になります。 パラメーターを指定するサブネットの名前を示します。

有効値: 既存サブネットの名前

デフォルト値: なし

class-name

スコープが*class-global*、または *class-subnet* のときに有効になります。パラメーターを指定するクラスの名前を示します。

有効値: 任意の既存クラスの名前

デフォルト値: なし

value

yes DHCP サーバーは、タイプや構成してあるしていないにかかわらず、すべてのクライアントに応答します。

no DHCP サーバーは、構成されている DHCP クライアントからの要求だけに応答します。

bootp DHCP サーバーは、リストにない BOOTP クライアントをサポートしますが、リストにない DHCP クライアントはサポートしません。

dhcp DHCP サーバーは、リストにない DHCP クライアントに応答しますが、リストにない BOOTP クライアントには応答しません。

有効値: yes、no、bootp、dhcp

デフォルト値: **scope** が *global* のときは yes。 あるいは、デフォルト値は、スコープの階層によって決定されます。 スコープについては、482ページの『概念と用語』を参照してください。

例:

```
DHCP Server config> set support-unlisted-clients class-global yes
     Enter the class name []? ClassA
```

例:

```
DHCP Server config> set support-unlisted-clients class-subnet no
     Enter the subnet name []? subA
     Enter the class name []? ClassA
```

例:

```
DHCP Server config> set support-unlisted-clients global bootp
```

例:

```
DHCP Server config> set support-unlisted-clients subnet dhcp
     Enter the subnet name []? subA
```

used-ip-address-expire-interval *time length*

サーバーがアドレスを割り当てる前に、使用中の IP アドレスを保留する時間を指定します。 サーバーは、IP アドレスを割り当てる前に、アドレスがネットワークで使われていないことを確認するために、アドレスを PING します。次に、サーバーは取っておいた使用中のアドレスにマークを付けます。 このパラメーターは、アドレスを割り当てる前に、使用中のアドレスを保留にしておく時間を指定します。 このパラメーターは、グローバル・レベルで設定します。

time 時間測定の単位を指定します。

有効値: 秒、分、時間、週、日、年、無限大

デフォルト値: なし

length 間隔の長さを指定します。

有効値: 30 秒 ～ 無限大

デフォルト値:

- 30 (時間単位が秒の場合)
- 15 (時間単位が分の場合)
- 1 (時間単位が時間の場合)
- 1 (時間単位が日の場合)

- 1 (時間単位が月の場合)
- 1 (時間単位が年の場合)

例:

```
DHCP Server config> set used-ip-address-expire-interval seconds
     How long is the interval in seconds (max:59) [30]? 2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval minutes
     How long is the interval in minutes (max:59) [15]? 2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval hours
     How long is the interval in hours (max:23) [1]? 5
```

例:

```
DHCP Server config> set used-ip-address-expire-interval days
     How long is the interval in days (max:6) [1]? 2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval weeks
     How long is the interval in weeks (max:3) [1]? 1
```

例:

```
DHCP Server config> set used-ip-address-expire-interval months
     How long is the interval in months (max:11) [1]? 3
```

例:

```
DHCP Server config> set used-ip-address-expire-interval years
     How long is the interval in years (max:10) [1]? 3
```

例:

```
DHCP Server config> set used-ip-address-expire-interval infinity
```

DHCP サーバー監視環境へのアクセス

DHCP サーバーの監視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 5** と入力します。 たとえば、次のように入力します。

   ```
   * talk 5
   Config>
   ```

   talk 5 コマンドを入力すると、端末に CONFIG プロンプト (+) 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. + プロンプトで、**feature dhcp-server** コマンドを入力して DHCP Server> プロンプトを表示します。

DHCP サーバー監視コマンド

表 62. DHCP サーバー監視コマンドの概要

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。

表 62. DHCP サーバー監視コマンドの概要 (続き)

コマンド	機能
Disable	DHCP サーバーを動的に使用不可にします。
Enable	DHCP サーバーを動的に使用可能にします。
List	クラス、クライアント、グローバル、サブネット、メーカー・オプションなどのパラメーターを表示します。
Reset	DHCP サーバーの構成を動的にリセットします。
Request	
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Disable

disable コマンドは、DHCP サーバーを動的に使用不可にします。

構文:

disable	dhcp

Enable

enable は、DHCP サーバーを動的に使用可能にします。

構文:

enable	dhcp

List

list コマンドは、クラス、クライアント、グローバル・パラメーター、サブネット、またはメーカー・オプション、およびその他の関連オプションについて、構成情報を表示します。 **list** コマンドの例については、 521ページの『List』を参照してください。

構文:

list	class
	client
	global
	option
	subnet
	vendor-option

Reset

reset コマンドは、DHCP サーバーの構成を動的にリセットします。

構文:

reset	dhcp

例:

```
DHCP Server> reset dhcp
You are about to reset the DHCP Server.
Are you sure you want to continue? [No]: y
DHCP Server has been reset
DHCP Server>
```

Request

request コマンドは、管理情報を表示します。

構文:

request clientid

delete

ipquery

poolquery

stats

status

clientid *client_id*

クライアントのために情報を表示します。

client_id

クライアントの識別子を示します。

有効値: 既存のクライアント ID

デフォルト値: なし

例:

```
DHCP Server> request clientid
     Enter the client name []? 0020351FB371

     Client id:             1-0x0020351FB371
     Status: BOUND
     Address last assigned: 192.9.200.10
     Most recent lease time: 16:41:25 December 3, 1998
     Proxy flag: FALSE
     Hostname: Win-XY-1
     Domain name: city.net
```

delete *address*

特定のクライアントの IP アドレスについて、リースを削除します。

address

削除するクライアントの IP アドレスを示します。

有効値: 既存クライアントの任意の有効 IP アドレス

デフォルト値: なし

例:

```
DHCP Server> request delete
       Enter the client's IP address []? 194.3.200.10
```

ipquery *address*

IP アドレスのために情報を表示します。

例:

```
DHCP Server>req ipquery 192.168.8.3
IP address:       192.168.8.3
Status:           RECLAIMED
Lease time:       86400 seconds
Start time:       Not Leased
Last time leased: 04:16:33  March 9, 1999
DHCP Server>
```

poolquery *address*

IP アドレスのプールについて、情報を表示します。

address

表示するプールの IP アドレスを示します。

有効値: 表示するプールの任意の有効 IP アドレス

デフォルト値: なし

例:

```
DHCP Server> request poolquery

Enter the client's IP address []? 194.3.200.10
     IP address:            194.3.200.10
     Status:                LEASED
     Lease time:            86400 seconds
     Start time:            16:41:25 December 3, 1998
     Last time leased:      16:41:25 December 3, 1998
     Client id:             1-0x0020351FB371
     Hostname:              Win-XY-1
     Domain name:           city.net
     IP address:            194.3.200.11
     Status:                STOCKED
     IP address:            194.3.200.12
     Status:                STOCKED
```

stats サーバーが管理するアドレス・プールについて、統計情報を表示します。統計には、処理した発見パケット数、応答のない発見パケット数、実行した提供の数、許可したリースの数、否定応答 (NAK) の数、処理済み情報の数、肯定応答 (ACK) のあった情報の数、更新の数、解放したリースの数、BOOTP クライアントの処理数、proxyARec を試みた数、サポートされていないパケットの数などが含まれます。 構文: request stats

例:

```
DHCP Server> request stats
       Number of DISCOVER requests received:      8
       Number of OFFER responses sent:            4
       Number of ACK responses sent:              3
       Number of NACK responses sent:             0
       Number of RELEASE requests received:       0
       Number of DECLINE packets received:        0
       Number of INFORM requests received:        0
       Number of BOOTP requests received:         0
       Number of requests received via proxy:     0
       Number of UNSUPPORTED requests received:   0
       Total number of request/responses:        15
       Number of lease expirations:               0
```

status アドレス・プールに関する情報を表示します。

例:

```
DHCP Server> request status

     IP address:            194.3.200.10
     Status:                LEASED
     Lease time:            86400 seconds
     Start time:            16:41:25 December 3, 1998
     Last time leased:      16:41:25 December 3, 1998
     Client id:             1-0x0020351FB371
     Hostname:              Win-XY-1
     Domain name:           city.net
```

```
IP address:             194.3.200.11
Status:                 STOCKED

IP address:             194.3.200.12
Status:                 STOCKED

IP address:             194.3.200.10
Status:                 STOCKED
```

DHCP 動的再構成サポート

この節では、Talk 6 および Talk 5 コマンドに影響を与える動的再構成 (DR) について説明します。

CONFIG (Talk 6) Delete Interface

動的ホスト構成プロトコル (DHCP) は、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、動的ホスト構成プロトコル (DHCP) には適用されません。 DHCP 構成は、個々のインターフェースに基づくものではありません。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、動的ホスト構成プロトコル (DHCP) には適用されません。 DHCP 構成は、個々のインターフェースに基づくものではありません。

GWCON (Talk 5) 構成要素リセット・コマンド

動的ホスト構成プロトコル (DHCP) は、次の動的ホスト構成プロトコル (DHCP) 固有の GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature DHCP, Reset DHCP コマンド

説明: DHCP サーバーをリセットし、変更された構成を使用して初期化します。

ネットワークの影響:

変更された構成が同じクライアントをサポートする場合、そのクライアントには、更新時に新しいリースが提供されます。変更された構成が同じクライアントをサポートしない場合は、そのクライアントのリースは期限が切れます。

制限:

- ハード・ファイルまたはフラッシュ記憶域カードのないルーター上では、リセット後、DHCP クライアントは引き続きそのリースを使用して動作しますが、DHCP サーバーが認識しなくなります。
- ハード・ファイルまたはフラッシュ記憶域カードのないルーター上では、DHCP サーバーによって以前にリースされた IP アドレスは、そのアドレスの再リースを試行するときに、“GWCON, feature DHCP, request status” コマンドで “USED” のマークが付けられます。

DHCP サーバー監視コマンド (Talk 5)

次の表は、**GWCON, feature DHCP, reset dhcp** コマンドが起動されるときにアクティブになる、動的ホスト構成プロトコル (DHCP) の構成変更を要約しています。

GWCON, feature DHCP, reset dhcp コマンドによって変更がアクティブになるコマンド
CONFIG, feature DHCP, add class
CONFIG, feature DHCP, add client
CONFIG, feature DHCP, add option
CONFIG, feature DHCP, add subnet
CONFIG, feature DHCP, add vendor-option
CONFIG, feature DHCP, change class
CONFIG, feature DHCP, change client
CONFIG, feature DHCP, change subnet
CONFIG, feature DHCP, change vendor-option
CONFIG, feature DHCP, delete class
CONFIG, feature DHCP, delete client
CONFIG, feature DHCP, delete option
CONFIG, feature DHCP, delete subnet
CONFIG, feature DHCP, delete subnet-group
CONFIG, feature DHCP, delete vendor-option
CONFIG, feature DHCP, disable dhcp-server
CONFIG, feature DHCP, enable dhcp-server
CONFIG, feature DHCP, set balance
CONFIG, feature DHCP, set bootstrapserver
CONFIG, feature DHCP, set canonical
CONFIG, feature DHCP, set inorder
CONFIG, feature DHCP, set lease-expire-interval
CONFIG, feature DHCP, set lease-time-default
CONFIG, feature DHCP, set ping-time
CONFIG, feature DHCP, set support-bootp
CONFIG, feature DHCP, set support-unlisted-clients
CONFIG, feature DHCP, set used-ip-address-expire-interval

GWCON (Talk 5) 一時変更コマンド

動的ホスト構成プロトコル (DHCP) は、装置の操作状態を一時的に変更する次の GWCON コマンドをサポートします。装置が再ロードされるか、リスタートされる場合、または動的に再構成可能なコマンドを実行する場合、常にこれらの変更は失われます。

コマンド
GWCON, feature DHCP, disable dhcp
GWCON, feature DHCP, enable dhcp

動的再構成不能コマンド

動的ホスト構成プロトコル (DHCP) 構成パラメーターはすべて、動的に変更することができます。

第32章 VCRM の構成および監視

バーチャル・サーキット・リソース・マネージャー (VCRM) は、リソース ReSerVation プロトコル (RSVP) をサポートするフィーチャーです。このプロトコルについては、*プロトコルの構成と監視 解説書 第 1 巻*の 『RSVP の使用』 および 『RSVP の構成および監視』 の章で説明しています。 RSVP からの予約要求に基づいて、VCRM は物理インターフェースを介したデータ・フローのための接続を作成します。その場合、最初に VCRM は予約を収容できる十分な帯域幅が得られるかどうかを調べることが必要です。

注: フレーム・リレーや X.25 のような WAN インターフェースを使用している場合、利用可能な帯域幅の量が VCRM に分かるようにするために、回線速度を設定する必要があります。回線速度の設定手順は、*ソフトウェア使用者の手引き* のフレーム・リレーおよび X.25 インターフェースの構成および監視の章で説明しています。

インターフェースが ATM SVC の場合、VCRM は RSVP QoS 要求を SVC セットアップ要求にマップします。 SVC のセットアップに成功すると、RSVP 予約要求は成功します。 VCRM は、QoS パケット用の適切なバッファー・スペースが得られること、およびパケットが正しい SVC を介して伝送されることを確認します。

インターフェースが PPP リンク、LAN、または WAN の場合、VCRM は QoS のソフトウェア待ち行列化およびベストエフォート・パケットを使用して、アウトバウンド・リンク上のパケットを優先順位付けします。

この章には、以下の節が含まれています。

VCRM 構成環境へのアクセス

VCRM 構成環境にアクセスするには、`Config>` プロンプトで、次のコマンドを入力します。

```
Config> feature vcrm
VC & Resource Management config console
  --Currently no configurable objects.
Config>
```

表示されるメッセージの目的は、VCRM は別個には構成できないことを示すことです。 RSVP を使用可能にすると VCRM も使用可能になり、そのパラメーターを RSVP 構成から入手します。

VCRM 監視環境へのアクセス

VCRM 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、次のコマンドを入力します。

VCRM の監視 (Talk 5)

```
+ feature VCRM
VCRM console
VCRM Console>
```

VCRM Console> プロンプトが表示されます。

VCRM 監視コマンド

この節では、VCRM 監視コマンドについて説明します。以下のコマンドは VCRM> プロンプトで入力します。

表 63. VCRM 監視コマンド

コマンド	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。 xxxiページの『ヘルプの入手』 を参照してください。
Clear	待ち行列統計をリセットします。
Queue	ATM 以外のソフトウェア待ち行列統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxiページの『下位レベル操作環境の終了』 を参照してください。

Clear

clear コマンドは、ソフトウェア待ち行列統計をリセットするのに使用します。

構文:

clear

clear コマンドの例は、**queue** コマンドの項を参照してください。

Queue

queue コマンドは、ATM 以外のトラフィック・フローのソフトウェア待ち行列を表示するのに使用します。

構文:

queue

ATM 以外のソフトウェア待ち行列の表示に使用される用語の定義を以下に示します。

Quota 予約された帯域幅の量。当初は、ベストエフォート (B.E.) がすべての quota (割り当て量) を所有します。予約されると、予約帯域幅 (b/w) が B.E. quota から QoS quota にシフトします。

Max-q パケットに記述されている最大待ち行列長さ

Curr-q
パケットに記述されている現行の待ち行列長さ

In quota
割り当てられた帯域幅内で送信されたパケット数または K バイト数

Outside quota

割り当てられた帯域幅外で送信されたパケット数または K バイト数 (アイドル帯域幅が利用可能の場合)

Packets/bytes dropped

ソフトウェア待ち行列によって廃棄されたパケット数またはバイト数

DLC packets/bytes dropped

パケットがソフトウェア待ち行列を通過した後で DLC によって廃棄されたパケット数またはバイト数

例:

```
*t 5

+feature vcrm
VCRM console
VCRM Console>?
CLEAR
QUEUE
EXIT
VCRM Console>queue
Flow-control Queues at sys-clock 346781 Second:
---------
Intf    B.E. Quota:       10000 Kbps           QoS Quota:        0     Kbps
0/Eth   B.E. Max-q        0                    QoS Max-q         0
        B.E. curr-q       0                    QoS curr-q        0
        B.E. pkts/Kbytes sent:                 QoS pkts/Kbytes sent:
        in quota:        54169/   3926         in quota:            0/      0
        outside quota:       0/      0         outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0           QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0     QoS: 0/0
Intf    B.E. Quota:       2048  Kbps           QoS Quota:        0     Kbps
2/PPP   B.E. Max-q        0                    QoS Max-q         0
        B.E. curr-q       0                    QoS curr-q        0
        B.E. pkts/Kbytes sent:                 QoS pkts/Kbytes sent:
        in quota:           62/      6         in quota:            0/      0
        outside quota:       0/      0         outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0           QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0     QoS: 0/0
Intf    B.E. Quota:       2032  Kbps           QoS Quota:        16    Kbps
3/FR    B.E. Max-q        1                    QoS Max-q         1
        B.E. curr-q       0                    QoS curr-q        0
        B.E. pkts/Kbytes sent:                 QoS pkts/Kbytes sent:
        in quota:        53160/   4920         in quota:       346596/  31886
        outside quota:       0/      0         outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0           QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0     QoS: 0/0
Intf    B.E. Quota:       2048  Kbps           QoS Quota:        0     Kbps
4/PPP   B.E. Max-q        1                    QoS Max-q         1
        B.E. curr-q       0                    QoS curr-q        0
        B.E. pkts/Kbytes sent:                 QoS pkts/Kbytes sent:
        in quota:           66/      6         in quota:          109/     1
        outside quota:       0/      0         outside quota:       0/
        B.E. pkts/bytes dropped: 0/0           QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0     QoS: 0/0

Max total queue length=1;  current total length=0
VCRM Console>clear
Flow-control Queues cleared at sys-clock 346786 Second:
-------
VCRM Console>
```

VCRM の監視 (Talk 5)

付録. リモート AAA 属性

ここでは、Radius、TACACS、および TACACS+ サーバーによって使用されるリモート AAA 属性を識別しています。

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
	1	PPTP
	2	L2F
	3	L2TP
TUNNEL_MEDIUM_TYPE		整数
	1	IP
TUNNEL_SERVER_EP		文字列
		IP アドレス

IBM ベンダー特定

NAS_TUNNEL_PASSWORD	101
INBYTES_AH	110
INBYTES_ESP	111
OUTBYTES_AH	112
OUTBYTES_ESP	113
INPKTS_BAD	114
OUTPKTS_BAD	115
INPKTS_BAD_AH	116
INPKTS_BAD_ESP	117
OUTPKTS_BAD_AH	118
OUTPKTS_BAD_ESP	119
INPKTS_AH	120
AH INPKTS_ESP	121

OUTPKTS_AH	122
AH OUTPKTS_ESP	123
INPKTS_BAD_AH_RPLY	124
INPKTS_BAD_ESP_RPLY	125
INBYTES_WRAP	128
OUTBYTES_WRAP	129
INB_AH_WRAP	130
INB_ESP_WRAP	131
OUB_AH_WRAP	132
OUB_ESP_WRAP	133
POLICY_NAME	135
P1_ID	136
TRANSFORMS	137
REFR_CNT	138
COMPR	139
ESP_ALGO	140
AH_ALGO	141
ESPAUTH_ALGO	142
P1_NAME	143
VC-ACTIVE	177
VC-IDLETIME	179
VC-SUSPENDTIME	180
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、ベンダー特定のフィールド `<keyword>=<value>` に入力できるキーワードが使用されます。

KWD_VC_ACTIVE	VCN
KWD_VC_IDLETIME	VCI
KWD_VC_SUSPENDTIME	VCS
KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN
KWD_DIALOUT	DOF
KWD_SUBNETMASK	SNM
KWD_PRIVILEGE	PRV

値

CALLBACK_FLAGS

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)

PRIVILEGE:
ADMIN
OPER
MONITOR

RADIUS 構成ファイル例

以下は、RADIUS 構成ファイルの例です。

VENDOR IBM 211			
ATTRIBUTE	User-Name	1	文字列
ATTRIBUTE	User-Password	2	文字列
ATTRIBUTE	CHAP-Password	3	文字列
ATTRIBUTE	NAS-IP-Address	4	ipaddr
ATTRIBUTE	NAS-Port	5	整数
ATTRIBUTE	Service-Type	6	整数
ATTRIBUTE	Framed-Protocol	7	整数
ATTRIBUTE	Framed-IP-Address	8	ipaddr
ATTRIBUTE	Framed-IP-Netmask	9	ipaddr
ATTRIBUTE	Framed-Routing	10	整数
ATTRIBUTE	Filter-Id	11	文字列
ATTRIBUTE	Framed-MTU	12	整数
ATTRIBUTE	Framed-Compression	13	整数
ATTRIBUTE	Login-IP-Host	14	ipaddr
ATTRIBUTE	Login-Service	15	整数
ATTRIBUTE	Login-TCP-Port	16	integer #
ATTRIBUTE	Old-Password	17	文字列
ATTRIBUTE	Reply-Message	18	文字列
ATTRIBUTE	Callback-Number	19	文字列
ATTRIBUTE	Callback-Id	20	string #
ATTRIBUTE	Unassigned	21	文字列
ATTRIBUTE	Framed-Route	22	文字列
ATTRIBUTE	Framed-IPX-Network	23	整数
ATTRIBUTE	State	24	文字列
ATTRIBUTE	Class	25	文字列
ATTRIBUTE	Vendor-Specific	26	文字列
ATTRIBUTE	Session-Timeout	27	整数
ATTRIBUTE	Idle-Timeout	28	整数
ATTRIBUTE	Termination-Action	29	整数
ATTRIBUTE	Called-Station-Id	30	文字列
ATTRIBUTE	Calling-Station-Id	31	文字列
ATTRIBUTE	NAS-Identifier	32	文字列
ATTRIBUTE	Proxy-State	33	文字列
ATTRIBUTE	Login-LAT-Service	34	文字列
ATTRIBUTE	Login-LAT-Node	35	文字列
ATTRIBUTE	Login-LAT-Group	36	文字列

```
ATTRIBUTE       Framed-Appletalk-Link       37      整数
ATTRIBUTE       Framed-Appletalk-Net        38      整数
ATTRIBUTE       Framed-Appletalk-Zone       39      文字列
ATTRIBUTE       Acct-Status-Type            40      整数
ATTRIBUTE       Acct-Delay-Time             41      整数
ATTRIBUTE       Acct-Input-Octets           42      整数
ATTRIBUTE       Acct-Output-Octets          43      整数
ATTRIBUTE       Acct-Session-Id             44      文字列
ATTRIBUTE       Acct-Authentic              45      整数
ATTRIBUTE       Acct-Session-Time           46      整数
ATTRIBUTE       Acct-Input-Packets          47      整数
ATTRIBUTE       Acct-Output-Packets         48      整数
ATTRIBUTE       Acct-Terminate-Cause        49      整数
ATTRIBUTE       Acct-Multi-Session-Id       50      文字列
ATTRIBUTE       Acct-Link-Count             51      整数
ATTRIBUTE       CHAP-Challenge              60      文字列
ATTRIBUTE       NAS-Port-Type               61      整数
ATTRIBUTE       Port-Limit                  62      整数
ATTRIBUTE       Login-LAT-Port              63      文字列
--------------------- START IBM -----------------------
ATTRIBUTE       Tunnel-Type                 64      整数
ATTRIBUTE       Tunnel-Medium               65      整数
ATTRIBUTE       Tunnel-Client-EP            66      文字列
ATTRIBUTE       Tunnel-Server-EP            67      文字列
ATTRIBUTE       Tunnel-Conn-ID              68      文字列
ATTRIBUTE       Tunnel-Password             69      文字列
ATTRIBUTE       Tunnel-NAS-Password         101     文字列
ATTRIBUTE       VC-ACTIVE                   177     整数
ATTRIBUTE       VC-IDLETIME                 179     整数
ATTRIBUTE       VC-SUSPENDTIME              180     整数
ATTRIBUTE       IBM-Callback-Flags          210     文字列
ATTRIBUTE       IBM-Encryption              211     文字列
ATTRIBUTE       IBM-DialOut                 214     文字列
ATTRIBUTE       IBM-Hostname                213     文字列
ATTRIBUTE       IBM-Subnetmask              215     文字列
ATTRIBUTE       IBM-Privilege               216     文字列
ATTRIBUTE       IBM-ipsec-inb-ah            110     整数
ATTRIBUTE       IBM-ipsec-inb-esp           111     整数
ATTRIBUTE       IBM-ipsec-ob-ah             112     整数
ATTRIBUTE       IBM-ipsec-ob-esp            113     整数
ATTRIBUTE       IBM-ipsec-ip-bad            114     整数
ATTRIBUTE       IBM-ipsec-op-bad            115     整数
ATTRIBUTE       IBM-ipsec-ip-bad-ah         116     整数
ATTRIBUTE       IBM-ipsec-ip-bad-esp        117     整数
ATTRIBUTE       IBM-ipsec-op-bad-ah         118     整数
ATTRIBUTE       IBM-ipsec-op-bad-esp        119     整数
ATTRIBUTE       IBM-ipsec-ip-ah             120     整数
ATTRIBUTE       IBM-ipsec-ip-esp            121     整数
ATTRIBUTE       IBM-ipsec-op-ah             122     整数
ATTRIBUTE       IBM-ipsec-op-esp            123     整数
ATTRIBUTE       IBM-ipsec-ip-bad-ah-r       124     整数
ATTRIBUTE       IBM-ipsec-ip-bad-esp-r      125     整数
ATTRIBUTE       IBM-ipsec-inb-wrap          128     整数
ATTRIBUTE       IBM-ipsec-ob-wrap           129     整数
ATTRIBUTE       IBM-ipsec-ib-ah-wrap        130     整数
```

ATTRIBUTE	IBM-ipsec-ib-esp-wrap	131	整数
ATTRIBUTE	IBM-ipsec-ob-ah-wrap	132	整数
ATTRIBUTE	IBM-ipsec-ob-esp-wrap	133	整数
ATTRIBUTE	IBM-ipsec-policy-name	135	文字列
ATTRIBUTE	IBM-ipsec-p1-id	136	文字列
ATTRIBUTE	IBM-ipsec-p1-name	143	文字列
ATTRIBUTE	IBM-ipsec-esp-algo	140	文字列
ATTRIBUTE	IBM-ipsec-ah-algo	141	文字列
ATTRIBUTE	IBM-ipsec-esp-algo	142	文字列
VALUE	Tunnel-Type	L2TP	3
VALUE	Tunnel-Type	L2F	2
VALUE	Tunnel-Type	PPTP	1
VALUE	Tunnel-Medium	IP	1
VALUE	VC-ACTIVE	YES	1
VALUE	VC-ACTIVE	NO	0
VALUE	IBM-Callback-Flags	Required	REQ
VALUE	IBM-Callback-Flags	Roaming	OAM
VALUE	IBM-Dialout	Enable	TRUE
VALUE	IBM-Dialout	Disable	FALSE
VALUE	IBM-Dialout	ONLY	ONLY
VALUE	IBM-Privilege	Administrator	ADMIN
VALUE	IBM-Privilege	Operator	OPER
VALUE	IBM-Privilege	Monitor	MONITOR

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	0 (monitor privilege), 1 (operator privilege), 15 (administrator privilege)
callback-dialstring	

IBM 特定の属性

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

AAL ATM アダプテーション・レイヤー (ATM Adaptation Layer)

AAL-5 ATM アダプテーション・レイヤー 5 (ATM Adaptation Layer 5)

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 アドレッシング (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 拡張ピアツーピア・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・ルーティング透過型 (adaptive source routing transparent)

ASYNC
非同期 (asynchronous)

ATCP AppleTalk 制御プロトコル (AppleTalk Control Protocol)

ATM 非同期転送モード (Asynchronous Transfer Mode)

ATMARP
クラシカル IP 中の ARP (ARP in Classical IP)

ATP AppleTalk トランザクション・プロトコル (AppleTalk Transaction Protocol)

AUI 接続ユニット・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 相手確認 (are you there)

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)

BCM ブロードキャスト・マネージャー (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)

BGP ボーダー成長プロトコル (Border Growth 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 コール・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 防衛データ・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・レディー (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)

E&M Ear & Mouth

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)

ELSCon
2 次 ELS コンソール (Secondary ELS Console)

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 (Ethernet)

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)

FXO Foreign Exchange Office

FXS Foreign Exchange Station

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)

IETF インターネット技術特別調査委員会 (Internet Engineering Task Force)

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)

ILMI インターリム・ローカル管理インターフェース (Interim Local Management Interface)

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 平衡型リンク・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)

LCS LAN チャネル・ステーション (LAN Channel Station)

LCP リンク制御プロトコル (Link Control Protocol)

LE LAN エミュレーション (LAN Emulation)

LEC LAN エミュレーション・クライアント (LAN Emulation Client)

LED 発光ダイオード (light-emitting diode)

LECS LAN エミュレーション構成サーバー (LAN Emulation Configuration Server)

LES LAN エミュレーション・サーバー (LAN Emulation Server)

LES-BUS
LAN エミュレーション・サーバー - ブロードキャストおよび未知サーバー (LAN Emulation Server - Broadcast and Unknown Server)

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)

LSA リンク・サービス体系 (Link Services Architecture)

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
軍事ネットワーク (military network)

MOS マイクロ・オペレーティング・システム(Micro Operating System)

MOSDBG
マイクロ・オペレーティング・システム・デバッグ・ツール (Micro Operating System Debugging Tool)

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)

MPC マルチパス・チャネル (Multi-Path Channel)

MPC+ ハイパフォーマンス・データ転送 (HPDT) マルチパス・チャネル (High performance data transfer (HPDT) Multi-Path Channel)

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)

MSS マルチプロトコル・スイッチ・サービス (Multiprotocol Switched Services)

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)

NAS Nways スイッチ管理ステーション (Nways Switch Administration station)

NBMA 非ブロードキャスト・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)

NDPS 非介入パス・スイッチ (non-disruptive path switching)

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 国立科学財団 (National Science Foundation)

NSFNET
国立科学財団ネットワーク (National Science Foundation NETwork)

NVCNFG
不揮発性構成 (nonvolatile configuration)

OOS アウト・オブ・サービス (out of service)

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)

PCA 並列チャネル・アダプター (parallel channel adapter)

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 プロセス識別子(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)

Qos サービス品質 (Quality of Service)

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 コメント要求 (Request for Comments)

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)

s 秒 (second)

SAF 発信元アドレス・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)

SDU サービス・データ単位 (Service Data Unit)

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)

SLIP シリアル・ライン IP (Serial Line IP)

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・ルーティング透過型 (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)

SVN スイッチド・バーチャル・ネットワーキング (Switched Virtual Networking)

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 point 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)

TLV タイプ/長さ/値 (Type/Length/Value)

TMO タイムアウト (timeout)

TOS サービスのタイプ (type of service)

TSF 透過型スパンニング・フレーム (transparent spanning frames)

TTL 活動回数 (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)

UNI ユーザー・ネットワーク・インターフェース (User-Network Interface)

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)

VoFR ボイス・オーバー・フレーム・リレー (Voice over Frame Relay)

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 レストラル / リルート (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。

拡張ピアツーピア・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 ピア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。

拡張ピアツーピア・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。

拡張ピアツーピア・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。

拡張ピアツーピア・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・サーバーへのドメイン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、そのネットワーク内のネットワークが、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 ネットワークの中間ルーティング・サービス

拡張ピアツーピア・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、*ブロードキャスト・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). *拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク (Advanced Peer-to-Peer Networking (APPN) network)* を参照。

APPN ネットワーク・ノード (APPN network node). *拡張ピアツーピア・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、出荷時設定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 (AUI) (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 のインターオペラビリティー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とルーターの集まり。このようなネットワーク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

BCM. ブロードキャスト・マネージャー (BroadCast Manager)。ブロードキャスト・フレームの効果を制限するために設計された、LAN エミュレーションの IBM 拡張版。

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) ネットワークをより大規模なインターネット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)). 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。

ブロードキャスト (broadcast). (1) すべての宛先に同じデータを伝送すること。 (T) (2) 複数の宛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。

ブロードキャスト・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。

BUS. ブロードキャストおよび未知サーバー (Broadcast and Unknown Server)。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。

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。

コール・リクエスト・パケット (call request packet). (1) コール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コール監視パケット。 (2) X.25 通信において、ネットワークを通してコール設定を要求するために、DTE によって伝送されるコール監視パケット。

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。

チャネル化 (channelization). 通信回線上の帯域幅を多数のチャネル (サイズが異なる場合もある) に分割するプロセス。***時分割多重方式 (time division multiplexing)*** (TDM) とも呼ばれる。

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。

CIP. クラシカル IP (Classical IP)。

CIPC. クラシカル IP クライアント (Classical IP Client)。

クラシカル IP (Classical IP). ATM 上で IP を使用して通信するための ATM 接続ホストの IETF 標準。

クラシカル IP クライアント (Classical IP Client). 論理 IP サブネットのユーザーを表すクラシカル IP コンポーネント。

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管理ベクトル移送 *(NMVT) (network management vector transport (NMVT))* も参照。

CU 論理アドレス (CU Logical Address). 2216 に対してホストによって定義された制御装置アドレス。この値は、ホスト入出力構成プログラム (IOCP) の CNTLUNIT マクロ命令の CUADD ステートメントによって定義される。制御装置アドレスは、同じホスト上で定義された各論理区画ごとに固有でなければならない。

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・パケットまたはコール・リクエスト・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) *物理回線 (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・レディー (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宛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。*発信元サービス・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。

装置アドレス (device address). 2216 装置を選択するためにチャネル・パスで伝送される装置アドレス。S/370 入出力アーキテクチャーでは、サブチャネル番号とも呼ばれる。この値は、ホストIOCP 内の実装置に対する CNTLUNIT マクロ命令の UNITADD ステートメントによって定義される。

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信コール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) *管理ドメイン (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。

ELAN. エミュレートされたローカル・エリア・ネットワーク (Emulated Local Area Network)。 ATM 技術で実施された LAN セグメント。

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) *拡張ピアツーピア・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。

等価容量 (equivalent capacity). NBBS 体系において、パケット紛失率を限界値以下にするために、コネクションに必要な帯域幅の最少量。

ESI. エンド・システム識別子 (End System Identifier)。ATM アドレスの 6 バイトのコンポーネント。

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、宛先サブエリア・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、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 つまたは複数の宛先フィールド、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 (HPR) (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、拡張ピアツーピア・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、宛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、宛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。

ホット・プラグ可能、常時交換可能 (hot pluggable). 該当するコンポーネントに接続されていない、あるいは依存していない他のリソースの動作を妨害せずに、取り付けや取り外しを行うことができるハードウェア・コンポーネントを表す用語。

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)。

IETF. インターネット技術特別調査委員会 (Internet Engineering Task Force)。インターネット仕様を作成する機関。

ILMI. インターリム・ローカル管理インターフェース (Interim Local Management Interface)。ユーザー・ネットワーク・インターフェース (UNI) を管理するための SNMP ベースの手順。

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。

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) および最短パス最優先オープン (OSPF) がある。

インターリービング (interleaving). (1) いくつかのコンピューター設備を同時に使用して、複数の処理や機能を交互に実行すること。 (2) データ伝送において、あるデータ・ストリームからのパケットと別のデータ・ストリームからのパケットを交互に処理すること。

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として機能することができるネットワークの集合体。*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宛先が、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の信頼性も保証しない。

インターオペラビリティー (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。発信元とあて信先のアドレス、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 宛先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 (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。

J

ジッター (jitter). (1) ディジタル信号の有意瞬間における、その理想位置からの短時間の非累積的な変動。 (2) 伝送されたディジタル信号の好ましくない変動。 (3) ネットワーク遅延の変動。

L

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 宛先を 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・マネージャー (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 宛先を 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・アドレス (Link Address). ESCON チャネル・アダプター付きの 2216 の場合は、次のように決められたポート番号である。つまり、通信パスに ESCD が 1 つある場合は、ホストに接続された ESCON ディレクター (ESCD) ポート番号。通信パスに ESCD が 2 つある場合は、動的接続で定義された ESCD のホスト側ポート番号。通信パスに ESCD がない場合、この値は X'01' に設定する必要がある。

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の使用可能なインターフェースおよび到達可能な近隣に関する、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。

LIS. 論理 IP サブネット (Logical IP Subnet)。ATM 技術のスイッチド・バーチャル・ネットワーキング (SVN) 構成で 実現された IP サブネット。

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で、さらに大きなネットワーク

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 (MAN) (metropolitan area network (MAN))* および*広域ネットワーク (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、宛先サービス・アクセス・ポイント (DSAP)、発信元サービス・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。

論理区画 (logical partition). 論理区分 (LPAR) モードで動作できる、ホスト内の区画に割り当てられた番号。 LPAR モードでは、ESCON アダプターは複数のホスト区画と論理ファイバー接続を共用することができる。

論理区分 (LPAR) モード) (Logically Partitioned (LPAR) mode). 処理を論理区画 (LP) に分割して、複数のプロセッサーがあるように見せる、一部のホスト・プロセッサーの機能。 LPAR モードでは、ESCON アダプターは複数のホスト区画と論理ファイバー接続を共用することができる。

LP. 論理区画 (logical partition)

LP 番号 (LP number). 論理区画番号 (Logical partition number)。これによって、複数の論理ホスト区画 (LP) が 1 つの ESCON ファイバーを共用することができる。この値は、ホスト入出力構成プログラム (IOCP) の RESOURCE マクロ命令によって定義される。ホストで EMIF を使用していない場合は、 LP 番号としてデフォルト値 0 を使用する。

LPAR. 論理区分 (logically partitioned)。

LPAR モード (LPAR mode). 論理区分 (LPAR) モード。

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、基本ピア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、ピア・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

管理アクセス (management access). ネットワーク管理ステーション、または変更制御サーバーを NBBS ネットワークに接続する Nways スイッチ。

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 (MAN) (metropolitan area network (MAN)). 2 つ以上のネットワーク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 (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。 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・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。

モジュール (module). Nways スイッチにおいて、論理カード、コネクター、およびライトが含まれている、パッケージされたハードウェア装置。モジュールは、アダプター、回線インターフェース・カプラー、音声サーバー拡張、およびその他のコンポーネントをパッケージするのに使用される。すべてのモジュールが論理サブラックに**ホット・プラグ可能**。

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。

MSS. マルチプロトコル交換サービス (Multiprotocol Switched Services)。IBM のスイッチド・バーチャル・ネットワーキング (SVN) 構成のコンポーネント。

マルチキャスト (multicast). (1) 選択された宛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宛先のサブセットだけに伝達される、特殊な形式のブロードキャスト。

マルチパス・チャネル (multipath channel) (MPC). VTAM-VTAM 間両方向通信用として複数の単一方向サブチャネルを使用するチャネル・プロトコル。

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・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 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。

ネットワーク制御 (network control). 以下の目的のために Nways スイッチのコントロール・ポイントによって実行される NBBS 体系の機能。
- Nways スイッチ資源の割り振りと制御
- トポロジーおよびディレクトリー・サービスの提供
- ルートの選択
- 輻輳 (ふくそう) の制御

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 (NMS) (network management station (NMS)). NetView/AIX および Nways スイッチ管理プログラムを稼働するステーション。 NBBS ネットワーク・トポロジー、会計、効率、構成の更新、および問題分析を管理する。

ネットワーク管理ステーションは、イーサネット LAN を介して管理アクセス Nways スイッチに接続される。

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・マネージャー (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)). *拡張ピアツー・ピア・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。

ネクスト・ホップ解決プロトコル (NHRP) (Next Hop Resolution Protocol (NHRP)). RFC としての認定を受けるために提出されている、インターネット草案バージョン 10 に指定されているルーティング・プロトコル。ネクスト・ホップ解決プロトコルでは、発信元ステーションが、宛先の方向にある『NBMA ネクスト・ホップ』の非ブロードキャスト・マルチアクセス (NBMA) アドレスを判別する方式を定義する。NBMA ネクスト・ホップは、宛先自体である場合もあれば、 NBMA ネットワーク内にあって、宛先に『最も近い』ルーターである場合もある。こうして、発信元ステーションは、宛先またはルーターとの間に直接 NBMA バーチャル・サーキットを確立し、NBMA ネットワーク上のルーティング・ホップの数を減らすことができる。

ネットワーク・サポート・センター (Network Support Center). IBM が NBBS ネットワークにリモート・サポートを提供する場所。

ネットワーク・サポート・ステーション (network support station). ローカルで動作し、Nways スイッチにサービスするために使用される処理装置。 Nways スイッチの管理者またはサービス担当者が使用する。

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。

ネットワーキング広帯域サービス (NBBS) (Networking BroadBand Services (NBBS)). ATM 標準を補完して以下の機能を提供する、高速ネットワーキング用の IBM 体系。
- アクセス・サービス
- トランスポート・サービス
- ネットワーク制御

NHRP. ネクスト・ホップ解決プロトコル (Next Hop Resolution Protocol)。

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。

Nways スイッチ (Nways Switch). IBM 2220 Nways ブロードバンド・スイッチ (IBM 2220 Nways BroadBand Switch) と同義。

Nways スイッチ構成端末 (Nways Switch configuration station). Nways Switch 構成ツール (NCT) の独立バージョンを稼働している専用 OS/2 端末。ネットワーク構成データベースを生成するのに使用され、リモート・コンソールに導入する必要がある。

O

最短パス最優先オープン (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。*宛先 (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). パケットが指定の宛先に到達しない、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。コール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、データ・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・アダプター (port adapter). ポート回線に NBBS 体系のアクセス・サービスを提供するコードを実行している、Nways スイッチの 2216 以外の型式のモジュール。 2216 では、ポート・アダプターとトランク・アダプターの機能が結合された多重化ポート/トランク・アダプター (MPTA) が使用されている。

ポート回線 (port line). 外部ユーザー装置を Nways スイッチに接続し、それにより NBBS ネットワークへの接続を可能にする通信回線。回線エミュレーション・サービス (CES)、パルス符号変調 (PCM)、ハイレベル・データ・リンク制御 (HDLC)、またはフレーム・リレー (FR) など、各種のアクセス・サービスおよびインターフェースを使用できる。

Nways スイッチでは、各ポート回線は 1 つの (または、複数の) NBBS ポートに関連付けられている。

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。

ポテンシャル接続 (potential connection). NBBS 体系において、NBBS ネットワークの外部の 2 つの装置間の事前定義された接続。エンドポイント Nways スイッチの 1 つに保管されている構成パラメーターによって定義される。

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)

パルス符号変調 (PCM) (pulse code modulation (PCM)). アナログ音声信号のディジタル化のために採用された標準。 PCM では、音声は 8 kHz の速度でサンプリングされ、各サンプルは 8 ビット・フレームに符号化される。

Q

サービス品質 (QOS) (quality of service (QoS)). NBBS 体系では、サービス品質でネットワーク接続の特性を保証する。これは、エンド・エンド遅延、ジッター、およびパケット紛失率などを表わす。

サービス品質 (QoS) (Quality of Service (QoS)). 性能パラメーターを使用してアクセスされる、エンド・エンド・サービスのユーザー指向の性能。ATM ネットワークでは、セル損失比率、セル伝送遅延、およびセル遅延変動といった性能パラメーターによって、エンド・エンド ATM 接続の QoS が決まる。

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・コンソール (remote console). OS/2、TCP/IP、およびリモート Nways スイッチ資源制御プログラムを実行しているステーション。任意のネットワーク・サポート・ステーションに接続し、リモートから Nways スイッチの操作と保守を行うことができる。

接続は、以下を介して行う。
- モデムを使用する交換回線を介して

任意のネットワーク・サポート・ステーションを、別のネットワーク・サポート・ステーションのリモート・コンソールとして使用することができる。

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。

資源 (resource). Nways スイッチにおいて、ハードウェア要素または制御プログラムによって作成される論理エンティティー。たとえば、アダプター、LIC、および伝送路は物理資源である。コントロール・ポイント、およびコネクションは論理資源である。

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宛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、発信元ノードから宛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宛先アドレスなど) 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) メッセージを宛先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 (伝送ヘッダー内の宛先ネットワーク・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宛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。

NBBS ネットワークでは、SLIP は、ネットワーク・サポート・ステーションと IBM ネットワーク・サポート・センター (NSC) の間の接続にまたがって使用される。

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、照会をブロードキャストできる機構。
- 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。

SLIP. シリアル・ライン IP (Serial Line IP)。シリアル通信リンク上で実行中の IP に関する IETF 標準。

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。

SNAP. (1) サブネットワーク・アクセス・プロトコル (SubNetwork Access Protocol)。 (2) サブネットワーク接続点 (SubNetwork Attachment Point)。

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、発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、発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。

発信元サービス・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、最終宛先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、最終宛先に渡される。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。

サブネットワーク接続点 (SubNetwork Attachment Point). フレームのプロトコル・タイプを識別する LLC ヘッダー拡張部。

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。

同期光ネットワーク (synchronous optical network) (SONET). 光インターフェースを介してディジタル情報を伝送するための米国標準。これは、同期ディジタル階層 (SDH) 勧告と密接な関連がある。

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宛先 (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。

時分割多重 (TDM) (time division multiplexing (TDM)). ***チャネル化 (channelization)*** を参照。

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。

TLV. タイプ/長さ/値 (Type/Length/Value)。LAN エミュレーション・パケットの中の汎用情報要素。

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・ノード間にブロードキャストされ、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、パケット交換通信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、ピア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。

トランスポート・サービス (transport services). 以下の目的のために Nways スイッチのコントロール・ポイントによって実行される NBBS 体系の機能。

- トランク・ラインと Nways スイッチの接続サポート
- 帯域幅の使用率の最大化
- サービス品質の保証
- Nways スイッチ間のパケット転送
- 論理待ち行列の管理と、伝送のスケジューリング

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。

トランク・アダプター (trunk adapter). トランク・ラインに NBBS 体系のトランスポート・サービスを提供するコードを実行する、Nways スイッチの 2216 以外の型式のモジュール。 2216 では、ポート・アダプターとトランク・アダプターの機能が結合された多重化ポート/トランク・アダプター (MPTA) が使用されている。

トランク・ライン (trunk line). 2 つの Nways スイッチを接続する高速伝送路。同軸ケーブル、ファイバー・ケーブル、または無線を使用でき、通信会社からリースすることもできる。

Nways スイッチでは、各トランク・ラインは 1 つの NBBS トランクに関連付けられている。

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コール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コール装置を定義する CCITT の仕様。

V.34. 標準の市販の音声グレードの 33.6 Kbps (およびそれより低速の) チャネルを介してのモデム通信に関する ITU-T 勧告。

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。

VCC. バーチャル・チャネル・コネクション (Virtual Channel Connection)。当事者 (通話者) 間の接続。

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・ローカル・エリア・ネットワーク (VLAN) (Virtual Local Area Network (VLAN)). プロトコルおよびサブネットに基づく、1 つまたは複数の LAN の論理的グループ化で、ネットワーク・トラフィックを、こうしてできるグループ内に分離する場合に使用される。

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、パス情報単位 (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 (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。

特殊文字 (Special Characters)

2216 Nways ブロードバンド・スイッチ (2216 Nways BroadBand Switch). NBBS ネットワークでの高速通信を可能にする高速パケット交換機。 2220 Nways ブロードバンド・スイッチでは、ネットワーキング・ブロードバンド・サービス体系で定義されている機能を実装している。 ***Nways スイッチ (Nways Switch)*** と同義。

索引

日本語, 数字, 英字, 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］

［ラ行］

A

B

C

D

E

I

L

M

N

P

Q

R

S

T

U

V

W

Printed in Japan

SD88-6111-02

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 V3.4 フィーチャーの使用