Nways
マルチプロトコル・ルーティング・サービス

プロトコルの構成と監視
解説書 第 1 巻
バージョン 3.2

SC88-6371-06
(英文原典：SC30-3680-08)

Nways
マルチプロトコル・ルーティング・サービス

プロトコルの構成と監視
解説書 第 1 巻
バージョン 3.2

SC88-6371-06
(英文原典：SC30-3680-08)

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。

第 9 版 (1998 年 11 月)

本書は IBM Nways マルチプロトコル・ルーティング・サービス の バージョン 3.2、また新版あるいは TNL でお知らせしない限り、これ以降のすべてのリリースおよび修正にも適用されます。

原　典： SC30–3680–08
Nways Multiprotocol Routing Services
Protocol Configuration and Monitoring
Reference Volume 1
Version 3.2

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 1999.5

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

本書のオンライン・バージョンのご使用条件

弊社は、お客様に対して以下のことを許諾します。

本媒体に収められた文書 (IBM プログラムを除く。以下、「資料」という) をお客様の社内使用のために複製し、改変し、印刷することができます。ただし、資料のすべての複製物上には、全文複製か部分複製かを問わず、著作権表示、すべての注意書きのほか必要な表示をそのまま複製するものとします。

上記の条件に違反があった場合は、本使用権は終了するものとします。この場合、お客様は、ただちに複製物のすべてを破棄し、本媒体を弊社に返却するものとします。

商標

以下の用語は IBM Corporation の商標です。

Advanced Peer-to-Peer Networking	IBM	PS/2
AIX	Micro Channel	RS/6000
AIXwindows	NetView	System/370
APPN	AS/400	Nways
VTAM	BookManager	

UNIX は、X/Open Company Limited. を通じて排他的にライセンス許可された、米国およびその他の諸国における登録商標です。

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

その他の会社名、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、Nways 装置 上にブリッジングとルーティングの機能を構成する場合に必要になる情報が記載してあります。本書には、ソフトウェアに入っているすべてのフィーチャーおよび機能が記載されています。ただし、Nways 装置 によっては、本書に記載されているフィーチャーや機能をすべてサポートしているとは限らない場合があります。フィーチャーまたは機能が装置に固有な場合は、該当する章または節にある注意でそのような制限を示しています。

本書は IBM 2210 をサポートしており、このプロダクトを “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、実際の出力は異なる場合があります。 例は、装置の構成時に表示されるものの指針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および操作に当たる方々を対象として書かれています。 コンピューター・ネットワークのハードウェアおよびソフトウェアを扱った経験があれば役に立ちますが、プロトコル・ソフトウェアの使用にはプログラミング経験は必要ありません。

追加情報の入手 : 資料の印刷後に資料に変更が加えられる場合があります。追加情報が使用可能な場合、または資料の印刷後に変更が必要になった場合は、変更は構成プログラム・ディスケットのディスケット 1 上の (README という名前の) ファイルに入れられます。このファイルは、ASCII テキスト編集プログラムを使用して見ることができます。

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あります。

- 基本コード。これは次のものから構成されます。
  - 装置用のルーティング、ブリッジング、データ・リンク、交換、および SNMP エージェントの各機能を提供するコード。
  - ルーター・ユーザー・インターフェース。これにより、装置に導入されたマルチプロトコル・ルーティング・サービスの基本コードを構成し、監視し、使用することができます。 ルーター・ユーザー・インターフェースにアクセスするには、ローカルの場合はサービス・ポートに接続された ASCII 端末またはエミュレーターを介して、リモートの場合は Telnet セッションまたはモデム接続された装置を介して行います。

  基本コードは工場で 2210 に導入されています。
- IBM Nways マルチプロトコル・ルーティング・サービス 用の構成プログラム (本書では *構成プログラム* と呼ぶ) は、グラフィカル・ユーザー・インターフェースの一種であり、独立型ワークステーションでこれを使用して装置を構成できます。構成プログラムにはエラー検査およびオンライン・ヘルプ情報が組み込まれています。

構成プログラムは工場でプリロードされていません。構成プログラムは装置とは別個に、ソフトウェア発注の一部として出荷されます。

IBM Nways マルチプロトコル・ルーティング・サービス 用の構成プログラムは、「IBM Networking Technical Support」ホーム・ページからも入手できます。サーバー・アドレスとディレクトリーについては、*Nways マルチプロトコル・アクセス・サービス、ルーティング・サービス、スイッチ・サービス 構成プログラム 使用者の手引き*、GC88-6657 を参照してください。

本書における表記法

コマンド構文およびプログラム応答を示すために本書では次の表記法を使用します。

1. コマンドの省略形には、次の例に示すように下線が引いてあります。

   ```
   reload
   ```

   この例では、コマンド全体 (reload) とその省略形 (rel) のいずれを入力しても構いません。

2. パラメーターのキーワード選択項目は、大括弧で囲まれ、語 or で区切られています。例えば、次のように示されます。

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

   キーワードのいずれかをパラメーターの値として選びます。

3. オプションに続く 3 つのピリオドは、オプションの後に追加データ (例えば、変数) を入力することを意味します。 例えば、次のように示されます。

   ```
   time host ...
   ```

   この例では、コマンドの記述で説明されているように、ピリオドの位置にホストの IP アドレスを入力します。

4. コマンドに応答して表示される情報の中で、オプションについての省略時値は、オプションの直後の大括弧の中に入れて示します。 例えば、次のように示されます。

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

   この例では、STP を指定しないかぎり、媒体は UTP に省略時設定されます。

5. キーボードのキーの組み合わせについては、本書では次のように示します:

   - **Ctrl-P**
   - **Ctrl -**

   キーの組み合わせ **Ctrl -** では、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。状況によっては、このキーの組み合わせを使用すると、コマンド行プロンプトが変わります。

6. キーボードのキーの名前は、例えば、**Enter** のように示してあります。

7. 変数 (つまり、ユーザーが定義するデータを表すのに使用する名前) は、イタリックで示してあります。例えば、次のように示されます。

   File Name: *filename.ext*

IBM 2210 Nways マルチプロトコル・ルーターの資料

次のリストは IBM 2210 をサポートする資料を示しています。

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 2210」ホーム・ページにアクセスしてください。

```
http://www.networking.ibm.com/220/220prod.html
```

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。

SC88-6657

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

GA88-6313

IBM 2210 入門と計画の手引き

GC88-6228

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。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 3.2 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。この変更は、以下のもので構成されます。

- **新規機能**
  - IP バージョン 6
    - TCP6、UDP6、Telnet、PING-6 と traceroute-6、ICMPv6、IPsec
    - 近隣ディスカバリー・プロトコル (Neighbor discovery protocol (NDP)) (ホスト自動構成用)
    - 静的ルート、RIPng、プロトコル独立マルチキャスト高密度モード (PIM-DM)、マルチキャスト・リスナー・ディスカバリー (MLD)
    - IPv4 ネットワークによる IPv6 パケットの構成トンネル伝送または自動トンネル伝送
    - イーサネット、トークンリング、PPP の各インターフェースに対するサポート

- 資源予約プロトコル (Resource ReSerVation Protocol (RSVP))
  - IPv4 ネットワーク上のアプリケーションが、ネットワーク資源を予約して、必要なサービス品質のパケット送達を達成できるようにする信号メカニズム
  - ATM ポイント・ポイント SVC、PPP、フレーム・リレー、X.25、トークンリング、イーサネットでのサポート
- BSC に対するバイナリー同期リレー (BRLY) サポート

  IPv4 ネットワークでのパートナー 2210 または 2212 ルーターへの BISYNC 同期 (BSC) 送信のトンネル伝送に対するバイナリー同期リレー (BRLY) サポート

• 拡張機能

- 基本サービス
  - イベント・ログ・システム (ELS) の機能強化による大量の ELS メッセージの取り込み、フォーマット、オフロード
  - 再ロードや再始動を経ても消えることのない、構成ツールからの時限構成変更サポート
  - PPP、フレーム・リレー、V.34 の各インターフェースに対するパケット・トレース・サポート
- フレーム・リレーによるソース・ルート・ブリッジング用マルチアクセス・ブリッジ・ポートに対するブリッジング・サポート。マルチアクセス・ポートでは、 1 つのブリッジ・ポートに多くの DLCI が組み込まれ、拡張容易性が向上しています。
- DIAL
  - Microsoft Dial-Up Network Clients でサポートされている機能に対する DIAL サポート
    - コールバック制御プロトコル (Callback Control Protocol (CBCP)) に対するサポート
    - Microsoft Point-to-Point Encryption (MPPE) と Microsoft PPP CHAP (MS-CHAP) に対するサポート
  - Shiva パスワード認証プロトコル (Shiva Password Authentication Protocol (SPAP)) の使用時にダイヤルアップ接続の中断と再開を行うためのバーチャル・コネクション
- IP 項目
  - IP 優先/TOS フィルター機能強化
  - ポリシー・ベースのルーティング
  - インターフェース別 IP MTU の構成
  - IBM 6611 ルーター・ネットワークの移行を容易に行うための OSPF 機能強化
  - 近隣ごとのポリシー数とパス選択のための追加属性に対する BGP-4 サポート
  - DVMRPv3 サポート
  - IGMP プルーニング (技取り)/グラフティング (技付け)・サポート
- コーラー ID とコール・ブロッキングを基にしたコールバックに対する ISDN サポート

- 2210 がそれ自体と別のルーターの間に L2TP トンネルを作成できる、 L2TP クライアント・モデルに対する L2TP サポート。このトンネルは、2210 に着信するすべてのトラフィックに使用できます。L2TP ネットワーク・サーバー (LNS) 機能も拡張されて、L2TP ネットワーク・アクセス・コンセントレーター (LAC) への発信コールを開始できます。
- ネットワーク・ディスパッチャー項目
  - ステートレス UDP アプリケーションに対するサポート
  - ネットワーク・ニュース転送プロトコル (Network News Transfer Protocol (NNTP))、Post Office Protocol (POP3)、シンプル・メール転送プロトコル (SMTP)、 Telnet に関する新しいプロトコル・アドバイザー
  - TN3270 サーバーの平衡化時には、TN3270 サーバーの 1 つが、ネットワーク・ディスパッチャー機能と同じ 2210 にあっても構わない。
- ACE/サーバーを使用する PPP 認証に対するサポート
- セキュリティー機能強化
  - セキュリティー・アソシエーションを最大 2 つのネスト・レベルまで作成するための IPsec トンネル内トンネル (tunnel-in-tunnel) サポート
  - IPsec ESP NULL アルゴリズム・サポート
  - 「*don't fragment* (断片化禁止)」ビットの設定とパス MTU の伝送に対する IPsec サポート
  - IPsec の動的再構成の改善
- PPP 専用線、ISDN、V.25bis、V.34 接続をバンドルするための媒体混在マルチリンク PPP サポート
- APPN 機能強化
  - APPN SDLC 2 次マルチポイント・サポート
  - すべてのリンク・ステーション・タイプを対象にする、 APPN 伝送グループ (TG) 番号の構成
  - Talk 5 での APPN PING (APING) コマンドに対するサポート
  - 新しいトレース・オプション
- TN3270 機能強化

  注: ここに示してある TN3270 機能強化は、初期リリースの V3.2 では使用できませんが、98/12/31 までには 2210 Web サーバーで利用できるようになります。

  - SNA LU が名前付きプールにグループ分けできる、 TN3270 LU プーリング・サポート
  - TN3270 IP アドレスの LU 名マッピング
  - 自己定義従属 LU (SDDLU) と動的定義従属 LU (DDDLU) のサポート
  - 複数 TCP ポート・サポート
- DLSw 機能強化
  - 重複 MAC アドレスに対するサポート
  - リモート SDLC 装置によって接続が行われるまで SDLC 装置のポーリングを遅らせるためのサポート
- X.25 機能強化

PVC の範囲の定義に対する構成サポート
  - スイッチド・バーチャル・サーキットに対するフレーム・リレー・サポート
  - フレーム・リレー・パーマネント・バーチャル・サーキット (PVC) での IPXWAN サポート (番号制 RIP、非番号制 RIP、静的ルーティングに対するサポートを含む)
- **説明および訂正**

  技術的な変更および追加がなされている場合は、変更個所の左側余白に縦線 (|) を引いて示してあります。

編集上の変更

今回の新版を機に、本書だけでなく他のソフトウェア資料にも、次のように編集上の変更が数多く加えられることになりました。

- 資料を再編成する
- 不要な情報および冗長な情報を取り除く
- 検索を容易にする
- 一部の情報に補足説明を追加する

再編成の第一歩は、次のようにして完了しています。

- 表題が「**Understanding, Using and Configuring Features**」の部分は、*ソフトウェア使用者の手引き* から *フィーチャーの使用と構成* に転載する。
- 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* に転載する。

この再編成は、版を重ねた場合も継続されます。このような変更についてご意見がおありの場合は、本書の巻末のご意見記入用紙にご記入の上、郵便かファックスでお送りください。

ヘルプの入手

コマンド・プロンプトでは、該当のレベルで使用できるコマンドのリストの形式でヘルプを表示させることができます。この場合は、**?** (**help** コマンド) を入力した上で、**Enter** を押します。現行レベルから使用可能なコマンドをリストするには、**?** を使用してください。 通常、特定のコマンド名の後に **?** を入力して、そのオプションをリストすることもできます。 例えば、* プロンプトに **?** を入力すると、以下の情報が表示されます。

```
*?

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

RESTART

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

下位レベル環境の終了

ソフトウェアの複数レベルの性質により、2210 を構成または動作するときに、2 次、3 次、さらに下位のレベル環境になります。 次に高いレベルに戻るためには、**exit** コマンドを入力してください。 2 次レベルまで戻るためには、2 次レベル・プロンプト (Config> または +) が表示されるまで **exit** を入力し続けます。

例えば、IP プロトコル構成プロセスを終了するには、以下のようにします。

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

1 次レベル (OPCON) に戻る必要がある場合は、インターセプト文字 (省略時値では **Ctrl P**) を入力します。

第1部 ブリッジ機能の構成と監視

第1章 ブリッジングの基本

この章では、ブリッジおよびブリッジング操作の基本について説明します。この章には次の節が含まれています。

- 『ブリッジングの概要』
- 4ページの『ブリッジングおよびルーティング』
- 6ページの『ブリッジのタイプ』
- 8ページの『基本ブリッジ操作』
- 10ページの『MAC ブリッジ・フレーム形式』

ブリッジングの概要

ブリッジとは 2 つ以上のローカル・エリア・ネットワークをつなぐ装置です。 ブリッジは、接続された各ネットワークからデータ・フレームを受け入れ、フレームに含まれる媒体アクセス制御 (MAC) ヘッダーに基づいて各フレームを転送するかどうかを決定します。ブリッジは本来、2 つ以上の同種のネットワークを結合するものでした。用語*同種 (homogeneous)* は、接続されたネットワークが同じブリッジング方式および媒体タイプを使用することを意味します。これらの例としては、ソース・ルーティング・ブリッジング方式***のみ*** または透過ブリッジング・アルゴリズム***のみ*** をサポートするネットワークがあります (これらの方式については後ほど説明します)。

現在のブリッジでは非同種のネットワーク間の通信も可能です。*非同種 (non-homogeneous)* とは、異なるブリッジング方式を混用することができ、より多くの構成オプションも提供することができるネットワークのことをいいます。 4ページの図1 に、単純ブリッジ構成および複合ブリッジ構成の例を示します。

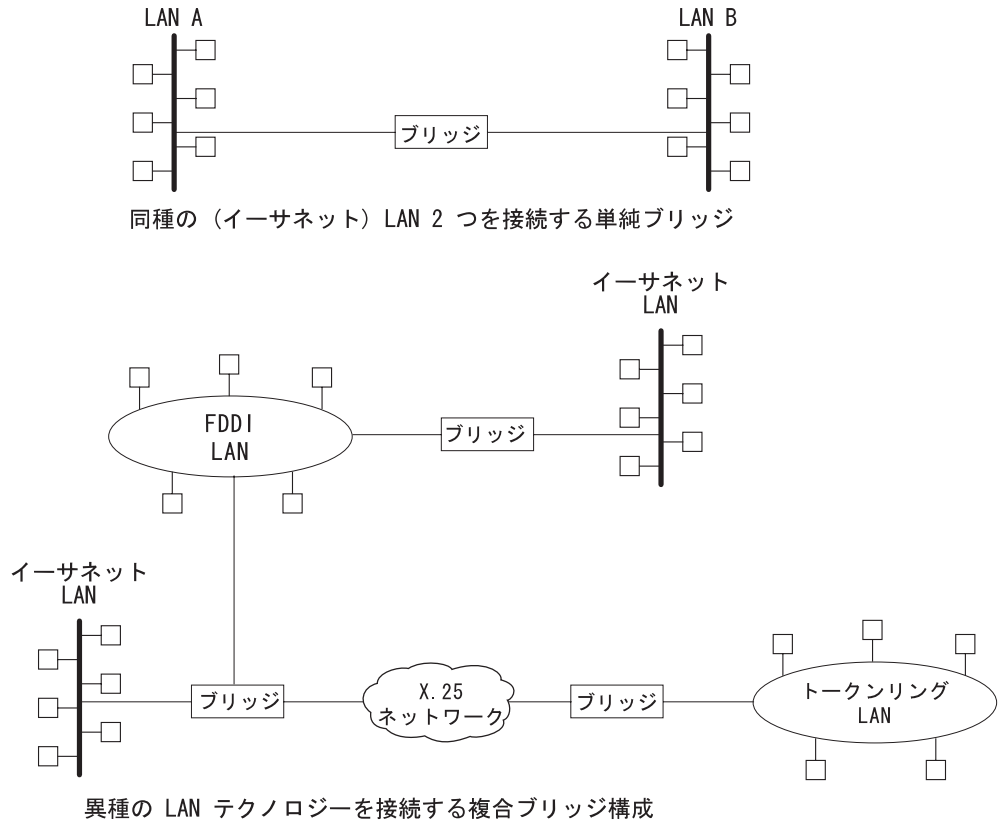


図 1. 単純および複合ブリッジ構成

ブリッジングおよびルーティング

2210 はブリッジングとルーティングの両方を実行できます。プロトコル・フィルター処理とは、着信するデータがルートされるか、ブリッジされるかを決定するプロセスです。

プロトコル・フィルター処理

着信データの処理中に、以下のアクションが起こります。

- 特定のプロトコル転送側がグローバルに使用可能になっている場合には、パケットはルートされます。
- 特定のプロトコル・フィルターが構成されている場合には、パケットはフィルターされます。
- ルートまたはフィルターされないパケットは、宛先媒体アクセス制御 (MAC) アドレスによりブリッジされる候補となります。

5ページの表1 は、あて先アドレスの内容に基づき、『ブリッジまたはルートのどちらか ?』 という問いにどのようにして答えるかを示しています。

表 1. ルート/ブリッジのデシジョン・テーブル

受信したフレームのあて先 MAC アドレスの内容	ブリッジが取るアクション
ブリッジ・アドレス	ブリッジは、フレームをルートする構成済みのプロトコルにフレームを渡します。
マルチキャスト・アドレスまたは同報通信アドレス	フレーム内に構成済みのプロトコルがある場合には、そのフレームがルートされます。その他の場合は、フレームはブリッジされます。
ユニキャスト	フレームはブリッジされます。

インターフェース単位でのルーティングおよびブリッジング

IP、IPX、AppleTalk の場合は、次の規則が特定のインターフェースを介するルーティングやブリッジングに適用されます。

- プロトコルは、特定のプロトコルが受信インターフェースに合わせて構成されている場合にルートされる
- パケットは、受信インターフェース上に特定のプロトコル・フィルターを構成した場合にフィルターされる
- ルートまたはフィルターされないパケットは、あて先媒体アクセス制御 (MAC) アドレスによりブリッジされる候補となります。

ルーター接続

ルーターを使用してレイヤー 3 で接続すると、地理的に離れた区域にあるエンド・ステーション間での接続とパス選択ができます。ルーティング・プロトコルを使用して、長距離で多様な LAN を接続するための最良のパスを選択します。大規模なネットワークではネットワークおよびサブネットワークの構成オプションが多様であるため、LAN を接続するのにネットワーク・レイヤーを介して行うのが、通常好ましい方法です。ネットワーク・レイヤー・プロトコルは、大規模で多様なネットワーク構成の中で情報を移動する場合も、非常に効率的であることが証明されています。

ブリッジ接続

レイヤー 2 でブリッジと接続すると、物理リンクを通じての接続性が得られます。 この接続は、ネットワークに接続されているホストからは本質的に『透過的』です。

注: ソース・ルーティング・ブリッジは完全に 『透過的』 とは見なされません。ソース・ルーティング・ブリッジと透過型ブリッジについて詳しくは、 13ページの『第2章 ブリッジング方式』 を参照してください。

リンク・レイヤーは、(レイヤー 3 での論理アドレス指定方式に対する) 物理アドレス指定方式、伝送制御手順、トポロジー報告、エラー通知、フロー制御、およびデータ・フレームの順序付けられた送達を維持します。上位レイヤーのプロトコルからの分離は、ブリッジングの利点の 1 つです。ブリッジはリンク・レイヤーで機能するので、上位レイヤーで発生するプロトコル情報を調べようとはしません。これにより、ネットワーク・レイヤー・プロトコル・トラフィックの処理オーバーヘッドがより低く、通信は高速になります。 ブリッジは第 3 レイヤーの情報には無関心な

ので、(ルーターがするように) 2 つ以上のネットワーク間で異なるタイプのプロトコル・トラフィック (例えば、 IP または IPX) を転送することもできます。

ブリッジは、レイヤー 2 のフィールドに基づいてフレームをフィルターすることもできます。 つまり、ブリッジは特定のタイプのフレームまたは特定のネットワークからのフレームのみを受け入れて転送するように構成することができます。フィルターを構成できるこの機能は、効率的なトラフィックの流れを維持するために非常に便利です。

ブリッジは大規模ネットワークを管理可能なセグメントに分割するのに有利です。 大規模ネットワーク内でのブリッジングの利点は次のように要約できます。

- ブリッジングにより、特定のネットワーク・エリアを分離して、個々のネットワーク・エリアの問題を大きなネットワークの問題に発展しないようにすることができます。
- フィルターにより、特定のセグメントに転送されるトラフィック量を調整することができます。
- ブリッジの使用によって、単一の LAN を 1 つのブリッジに接続したのではサポートしきれない台数のインターネットワーキング装置間での通信が可能になります。
- ブリッジングは、ノード制限 (セグメント上のノードの総数) を除去します。ローカル・ネットワークのトラフィックは他の接続されたネットワークのすべてに渡されるわけではありません。
- ブリッジは、長距離の LAN セグメントの接続を可能にすることにより、 LAN の接続される 『長さ』 を拡張します。 ブリッジはレイヤー 2 で 2 つの LAN セグメントを接続して、より大規模なネットワークを形成できるようにします。 これにより、イーサネット上でのステーションの数が多すぎることによる輻輳 (ふく輳) の問題およびトークンリング体系でのステーション数が 256 という制限を克服することができます。

ブリッジとルーターの比較

ブリッジやルーターなどのネットワーク間装置は、ネットワーク・セグメントを接続するという点で同様の機能をもっています。 ただし、各装置は、LAN 間接続を確立し維持するのに、異なる方式を使用します。 ルーターは OSI モデルのレイヤー 3 (ネットワーク・レイヤー) で LAN を接続するのに対し、ブリッジはレイヤー 2 (リンク・レイヤー) で LAN を接続します。

ブリッジのタイプ

以下の項では、特定のタイプのブリッジ、およびそれらがハードウェアおよびソフトウェアの機能によりどのように分類できるかについて説明します。

単純ブリッジ

単純ブリッジは、ローカル・エリア・ネットワークを接続する 2 つ以上の結合されたネットワーク・インターフェースから構成されます (4ページの図1)。 ブリッジは、ブ

リッジされた LAN の個別の MAC (媒体アクセス制御) エンティティー間でデータ・フレームを中継することにより個別のローカル・エリア・ネットワーク (LAN) を相互接続します。

単純ブリッジの主な機能は次のように要約できます。

- ブリッジは、LAN A で送信されたすべてのデータ・フレームを読み取り、LAN B にアドレス指定されたすべてのデータ・フレームを受信します。単純ブリッジは、受信するデータ・フレームの内容または形式に変更を加えません。追加のヘッダーを使ってフレームをカプセル化することもしません。

  ほとんどの単純ブリッジには、ルーティングのアドレスおよび情報が含まれています。少なくとも、ブリッジはどこへフレームを渡したらよいか分かるように、接続された各ネットワークにどのアドレスがあるかを知っている必要があります。
- ブリッジは LAN B にアドレス指定されたデータ・フレームを LAN B へと再伝送するのに、その LAN 用の MAC プロトコルを使用します。データ・フレームをブリッジが送信できるよりデータ・フレームが速く到着することがあるので、ブリッジは、ピーク時のデータ・トラフィック要求を満たす十分なバッファー・スペースをもつ必要があります。
- ブリッジは、LAN B から LAN A へのデータ・フレーム・トラフィックについても同様のことを行います。

複合ブリッジ

複合ブリッジは、単純ブリッジよりも高度な機能を実行します。これらの機能には、ブリッジが他のブリッジに関する状況情報を維持することも含まれます。この情報には、通信パスのコストならびに接続された各ネットワークに達するのに要するホップの数が含まれます。ブリッジ間で情報を定期的に交換することにより、すべてのブリッジ情報が更新されます。これらのタイプの交換によって、ブリッジ間での動的ルーティングが可能になります。

また、複合ブリッジでは、フレームを修正し、異なる LAN テクノロジー (例えば、トークンリング、イーサネットなど) からのパケットを認識して伝送することもできます。この場合には、ブリッジは*変換 (translational)* ブリッジと呼ばれることもあります。

適応ソース・ルーティング透過型 (ASRT) ブリッジは、2210 でブリッジ技術を具体的に実現したものです。ASRT ブリッジは、上記のブリッジング・オプションのいくつかだけでなく、追加のオプションも使用できるソフトウェア構成要素の集まりです。これらの機能すべてについては、この章で後ほどさらに詳しく説明します。

ローカル・ブリッジ

ローカル・ブリッジは、同じ地理的区域内のいくつかの LAN セグメント間を接続することができます。 この例としては、企業の本社にあるさまざまな LAN を接続するのに使用されるブリッジがあります。

リモート・ブリッジ

リモート・ブリッジは、異なる地域にある複数の LAN セグメントを接続します。企業の本社にある LAN を国内各地の事業所にある LAN に接続する場合に使用するブリッジなどは、この例になります。地理的な違いがあるので、この構成は、ローカル・エリア・ネットワーク構成から広域ネットワーク (WAN) 構成に移ります。

リモート・ブリッジはいくつかの点でローカル・ブリッジとは異なることがあります。 大きな違いの 1 つは、データが転送される速度です。WAN 接続は LAN 接続より遅い場合があります。この速度の違いが大きな意味をもつ可能性があるのは、時間が重要なアプリケーションを実行するときです。もう 1 つの違いは、リモート・ブリッジとローカル・ブリッジが LAN に接続される物理的な方法にあります。ローカル・ブリッジでは、接続はローカル配線媒体 (例えば、イーサネット、Thinet) を介して行われます。 リモート・ブリッジでは、接続はシリアル回線を通じて行われます。

基本ブリッジ操作

IEEE 802 LAN 標準に従うと、端末アドレスはすべて MAC レベルで指定されます。LLC (論理リンク制御) レベルでは、SAP (サービス・アクセス・ポイント) アドレスのみが指定されます。したがって、MAC レベルはブリッジが機能するレベルです。以下の例では、このレベルでブリッジ機能がどのように進行するかを説明しています。

操作例 1: 2 つの LAN を接続するローカル・ブリッジ

9ページの図2は、2 つの別個の LAN のエンド・ステーションを接続する 2 ポートのブリッジ・モデルを示しています。この例では、ローカル・ブリッジは、同一の LLC レイヤーおよび MAC レイヤーをもつ LAN (つまり、2 つのトークンリング LAN) を接続しています。概念的には、このブリッジは、接続された LAN の媒体アクセス制御 (MAC) サブレイヤーと物理チャネルの間でフレームを転送することにより、それらの間でデータ・リンク接続性を提供するデータ・リンク・リレーと考えることができます。

ブリッジングのプロセスを要約すると、ブリッジは、あて先アドレスがローカル LAN 上にない MAC フレームを取り込みます (つまり、LAN が、伝送されたフレームを受信するインターフェースに接続されます)。 ブリッジは次にフレームを該当するあて先 LAN に転送します。 このプロセスを通じて、2 つのエンド・ステーションにある対等 LLC エンティティー間で対話が行われます。 体系的には、LLC レイヤーの機能は OSI モデルの上のレベルから渡される MAC フレームを中継することだけなので、ブリッジは LLC レイヤーを含んでいる必要はありません。

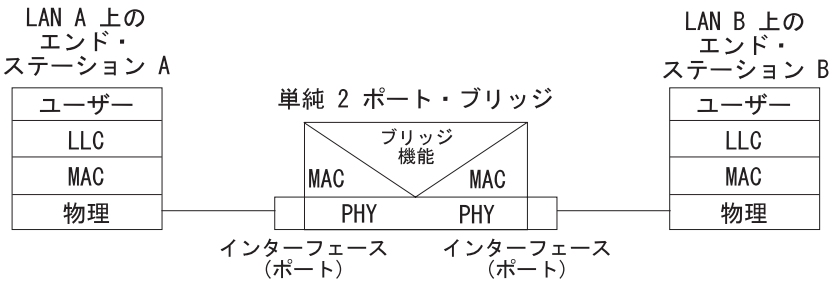


図2. 2 つの LAN を接続する 2 ポートのブリッジ

操作例 2: シリアル・リンクを介するリモート・ブリッジ

図3 は、シリアル・リンクを介して接続された 1 対のブリッジを示しています。これらのリモート・ブリッジは同一の LLC レイヤーおよび MAC レイヤーをもつ LAN (つまり、 2 つのトークンリング LAN) を接続しています。

要約すると、ブリッジはローカル LAN 上にあて先アドレスがない MAC フレームを取り込んでから、そのフレームを該当するあて先 LAN へとその LAN 上のブリッジを介して伝送します。 このプロセスを通じて、2 つのエンド・ステーションの対等 LLC エンティティー間で対話が行われます。 体系的には、LLC レイヤーの機能は OSI モデルの上のレベルから渡される MAC フレームを中継することだけなので、ブリッジは LLC レイヤーを含んでいる必要はありません。

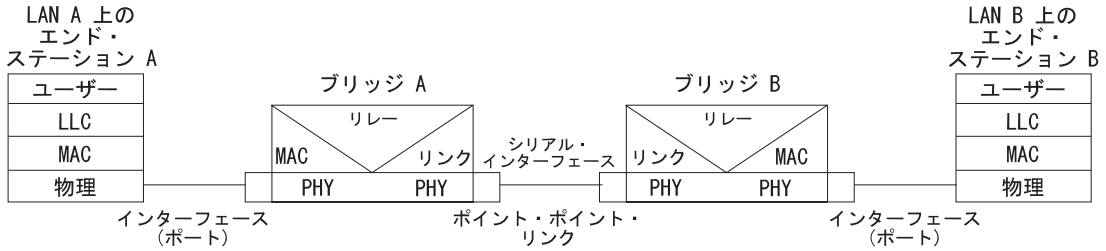


図3. ポイント・ポイント・リンクを介してのブリッジング

ブリッジがシリアル・リンクを介してデータを通信するとき、データはカプセル化されます。 10ページの図4 はカプセル化のプロセスを示しています。

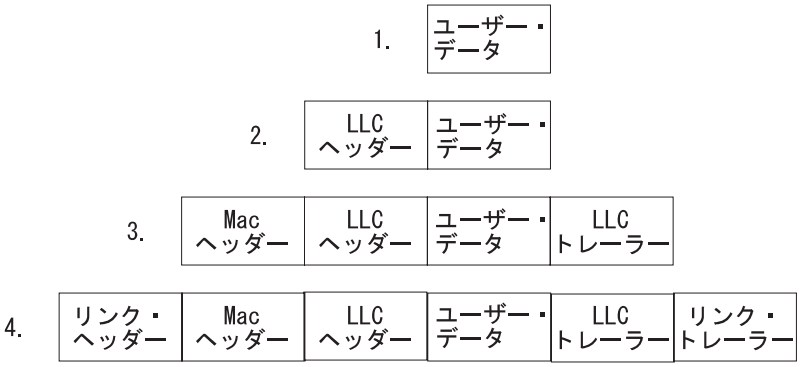


図4. ポイント・ポイント・リンクを介するデータのカプセル化

カプセル化は次のように進行します。

1. エンド・ステーション A はその LLC にデータを提供します。
2. LLC はヘッダーを追加し、その結果生じたデータ単位を MAC レベルに渡します。
3. MAC は次にヘッダー (3) およびトレーラーを追加して、MAC フレームを形成します。 ブリッジ A はフレームを取り込みます。
4. ブリッジ A の機能は MAC フレームをそのままあて先 LAN に中継することなので、ブリッジ A が MAC フィールドを除去することはありません。 ただし、ポイント・ポイント構成では、ブリッジはリンク・レイヤー (例えば、HDLC) のヘッダーおよびトレーラーを追加し、リンクを介して MAC フレームを伝送します。

データ・フレームがブリッジ B (目標ブリッジ) に到達すると、リンク・フィールドは除去され、ブリッジ B は元の未変更の MAC フレームをそのあて先であるエンド・ステーション B に送信します。

MAC ブリッジ・フレーム形式

前述したように、ブリッジはデータ・フレーム、特に MAC フレームを、ブリッジされた LAN の別々の MAC エンティティーの間で中継することにより LAN 相互を接続します。 MAC フレームは、発信元アドレスとあて先アドレスの形でフレームを転送するために必要な『どこ?』の情報を提供します。この情報は、データを正常に送受信するために不可欠です。

IEEE 802 は次の 3 つのタイプの MAC フレームをサポートします。 CSMA/CD (802.3)、トークン・バス (802.4)、およびトークンリング (802.5)。 11ページの図5 では、ブリッジによってサポートされる CSMA/CD およびトークンリングの MAC フレーム形式を示します。特定のフレームについては次の節で詳述します。

注: LLC レベルでは別のフレーム形式が使用されます。 次に、このフレームは、該当する MAC フレームに組み込まれます。

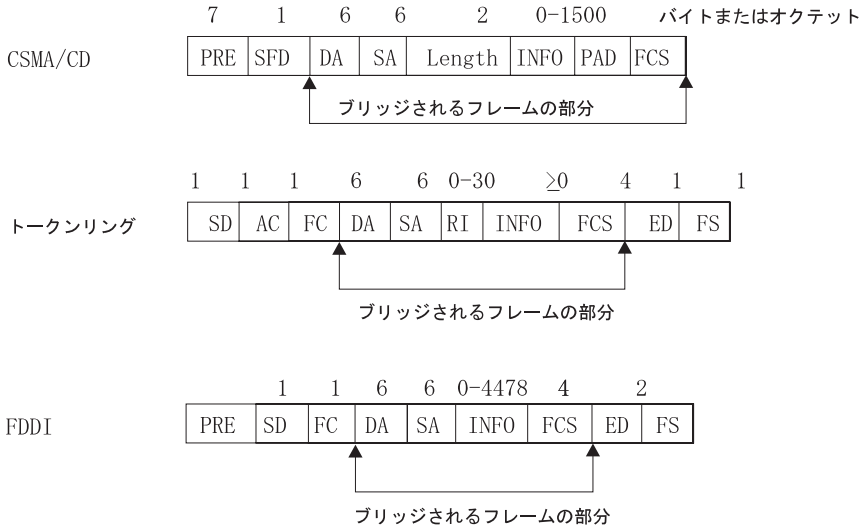


図 5. MAC フレーム形式の例

CSMA/CD (イーサネット) MAC フレーム

以下の情報は、CSMA/CD (イーサネット) MAC フレームにある各フィールドについて説明しています。

- *プリアンブル (PRE)*。 受信側エンド・ステーションがビット同期を確立してフレームの最初のビットを見つけるのに使用する 7 バイトのパターン。
- *フレーム開始区切り文字 (SFD)*。 フレームの開始を示します。

フレームのうち実際にブリッジされる部分は、次のフィールドから構成されます。

- *あて先アドレス (DA)*。フレームのあて先のエンド・ステーションを指定します。このアドレスは、固有な物理アドレス (1 つのあて先の場合)、マルチキャスト・アドレス (エンド・ステーションのグループが 1 つのあて先である場合)、またはグローバル・アドレス (すべてのステーションがそのあて先である場合) となります。形式は 16 ビットまたは 48 ビット (2 オクテットまたは 6 オクテット) のいずれかであり、特定の LAN 上のすべてのステーションについて同一でなければなりません。
- *発信元アドレス (SA)*。 フレームを送信したエンド・ステーションを指定します。形式は、あて先アドレス形式と同一でなければなりません。
- *長さ*。 後続する LLC バイトの数を指定します。
- *情報 (INFO)*。 LLC レベルで作成される組み込みフィールドで、サービス・アクセス点情報、制御情報、およびユーザー・データを含みます。
- *埋め込み (PAD)*。フレームが十分に長く、正しい衝突検出 (CD) 操作が行われることを保証するバイト・シーケンス。
- *フレーム検査シーケンス (FCS)*。32 ビットの巡回冗長検査値。この値は、あて先アドレスから始まるすべてのフィールドに基づいています。

トークンリング MAC フレーム

以下の情報は、トークンリング MAC フレームにある各フィールドについて説明しています。

- *開始区切り文字 (SD)*。 フレームの開始を示す固有の 8 ビット・パターン。
- *アクセス制御 (AC)*。 PPPTMRRR の形式をもつフィールド。ここで、PPP および RRR は 3 ビットの優先度変数および予約変数、M はモニター・ビット、T はこれがトークン・フレームまたはデータ・フレームのいずれかであることを示します。 これがトークン・フレームの場合は、他の唯一のフィールドは終了区切り文字 (ED) です。
- *フレーム制御 (FC)*。 これが LLC データ・フレームであるかどうかを示します。そうでない場合は、このフィールド内のビットは、トークンリング MAC プロトコルの操作を制御します。

フレームのうち実際にブリッジされる部分は、次のフィールドから構成されます。

- *あて先アドレス (DA)*。CSMA/CD およびトークン・バスと同様です。
- *発信元アドレス (SA)*。フレームの発信元である特定のステーションを識別します。フィールドの長さは、2 オクテットまたは 6 オクテットのアドレスです。 どちらのアドレス長でも、ルーティング情報フィールド (RIF) がフレーム内にあるかどうかを示すルーティング情報標識 (RII) ビットが入っています。

  RII=1　ルーティング情報フィールドがあります。

  RII=0　ルーティング情報フィールドがありません。

  このフィールドについては、23ページの『ソース・ルート・ブリッジング (SRB)』でさらに詳しく説明します。

- *ルーティング情報フィールド (RIF)*。 ソース・ルーティング・プロトコルには RIF が必須です。これは、2 オクテットのルーティング制御フィールドおよび一連の 2 オクテットのルーティング機能フィールドから構成されます。このフィールドについては、23ページの『ソース・ルート・ブリッジング (SRB)』でさらに詳しく説明します。
- *情報 (INFO)*。LLC レベルで作成される組み込みフィールドで、サービス・アクセス点情報、制御情報、およびユーザー・データを含みます。
- *フレーム検査シーケンス (FCS)*。32 ビットの巡回冗長検査値。 この値は、あて先アドレスから始まるすべてのフィールドに基づいています。

最後に、*終了区切り文字 (ED)* には、エラー検出 (E) ビット、および中間フレーム (I) ビットが含まれています。 I ビットは、これが複数のフレーム伝送のうち最後のフレーム以外のフレームでないことを示します。 *フレーム状況 (FS)* には、識別されたアドレス (A) ビットおよびコピーされたフレーム (C) ビットが含まれています。

第2章 ブリッジング方式

この章では、適応ソース・ルーティング透過型 (ASRT) ブリッジによってサポートされるブリッジング方式について説明します。各節では、特定の技術の概要を示し、その技術によってサポートされるデータ・フレームの説明が続きます。この章には次の節が含まれています。

- 『透過ブリッジング』
- 23ページの『ソース・ルート・ブリッジング (SRB)』
- 32ページの『ソース・ルーティング透過型 (SRT) ブリッジ』
- 35ページの『ASRT ブリッジの概要』
- 35ページの『適応ソース・ルーティング透過型ブリッジ (ASRT) (SR-TB 変換)』

透過ブリッジング

透過型ブリッジはスパンニング・ツリー・ブリッジ (STB) としても一般に知られています。用語*透過*は、ブリッジが接続された LAN に非ローカル・トラフィックをそっと転送し、それがユーザーにとって*透過*的つまり見えないことを指しています。エンド・ステーションのアプリケーションは、ブリッジの存在について知りません。ブリッジは、トラフィックが通過するのを listen することにより、エンド・ステーションの存在を知ります。この listen プロセスから、ブリッジはその LAN に接続されたエンド・ステーション・アドレスのデータベースを作成します。

受信する各フレームについて、ブリッジはフレームのあて先アドレスをそのデータベース上のあて先アドレスと突き合わせて検査します。フレームのあて先が同じ LAN 上のエンド・ステーションである場合には、そのフレームは転送されません。あて先が別の LAN である場合には、フレームが転送されます。あて先アドレスがデータベースに存在しない場合には、フレームは、ブリッジに接続されているすべての LAN (フレームの発信元の LAN を除く) に転送されます。

透過型ブリッジはすべて、スパンニング・ツリーのプロトコルおよびアルゴリズムを使用します。 スパンニング・ツリー・アルゴリズムは、ブリッジされたネットワーク (その物理設計自体はループを含むことがある) 内でループのないトポロジーを生成し、維持します。 2 つの LAN 間で複数のブリッジが接続されているメッシュ・トポロジー内では、*ループ* が発生します。 そのような場合には、データ・パケットは 2 つの LAN の並列ブリッジの間で行ったり来たりします。 これは、余分なデータ・トラフィックを作り、ループとして知られる現象を生じさせます。

ループが発生する場合は、ローカルまたはリモートあるいはその両方の LAN を構成して物理ループを除去する必要があります。 スパンニング・ツリーでは、自己構成アルゴリズムにより、ループを作成することなく LAN 内のどこでもブリッジを追加することができます。 新しいブリッジを追加すると、スパンニング・ツリーは LAN 上のすべてのブリッジを自動的に再構成し、単一のループのないスパンニング・ツリー にします。

ブリッジング方式

スパンニング・ツリーでは、2 つのエンド・ステーション間に複数のアクティブなデータ・ルートは決して存在しないので、データ・ループは除去されます。 各ブリッジごとに、アルゴリズムで、どのブリッジ・ポートがデータを転送できるか、またどのブリッジ・ポートがブロックされてループのないトポロジーを形成するかを決定します。スパンニング・ツリーが提供するフィーチャーには、次のものがあります。

- *ループ検出*。拡張 LAN 構成における物理データ・リンク・ループを検出し、除去します。
- *データ・パスの自動バックアップ*。冗長パスに接続しているブリッジは自動的にバックアップ・モードに入ります。1 次ブリッジに障害が起こると、バックアップ・ブリッジがアクティブになります。
- *ユーザーの構成機能*。ユーザーはネットワーク・トポロジーを自分で調整できます。 場合により、省略時の設定値では、必要なネットワーク・トポロジーが生成されないことがあります。ブリッジ優先度、ポート優先度、およびパスのコストのパラメーターを調整して、ユーザーのネットワーク・トポロジーに合ったスパンニング・ツリーを形成することができます。
- *シームレス (直接) 相互運用性*。多様な通信環境によって生じる構成上の制限なしに LAN を相互に運用できます。
- *非ルーティング・プロトコルのブリッジング*。非ルーティング・プロトコルのコスト効率が良いブリッジングを可能にします。

ルーターおよび透過型ブリッジ

スパンニング・ツリー・オプションを備えるルーターの操作時には、ブリッジおよびルーターのソフトウェアが同時並行して稼働します。 このモードではルーターはブリッジおよびルーターです。

この操作時に、次のことが起こります。

- 特定のプロトコル転送側がグローバルに使用可能になっている場合には、パケットはルートされます。
- 特定のプロトコル・フィルターが構成されている場合には、パケットはフィルターされます。
- ルートまたはフィルターされないパケットは、宛先媒体アクセス制御 (MAC) アドレスによりブリッジされる候補となる

ネットワーク要件

透過型ブリッジは、IEEE 802.1D 標準に適合するスパンニング・ツリー・ブリッジを採用しています。ネットワーク上の透過型ブリッジ (イーサネットトークンリングなど) は、すべて 802.1D スパンニング・ツリー・ブリッジであることが必要です。このスパンニング・ツリー・プロトコルは、一部の旧式のブリッジで使用される Digital Equipment Corporation が使用権をもつスパンニング・ツリー・プロトコルを実施するブリッジとは互換性がありません。

透過型ブリッジの操作

2 つの LAN 間で複数のブリッジが接続されているメッシュ・トポロジーでは、 2 つの LAN の並列ブリッジの間でパケットが行ったり来たりするループ現象が発生することがあります。 ループとは、2 つの LAN 間に複数のデータ・パスが存在する状態です。 スパンニング・ツリー・プロトコルの運用では、自動的に余分なパスをブロックしてループを除去します。

始動時に、ネットワークに参加するすべてのブリッジは、各ブリッジについての構成情報を提供する Hello ブリッジ・プロトコル・データ単位 (BPDU) を交換します。BPDU には、ブリッジ ID、ルート ID、およびルート・パス のコストなどの情報が含まれています。この情報は、どのブリッジがルート・ブリッジで、どのブリッジがそれが接続されている LAN の指定ブリッジであるかを、ブリッジが統一的に判別するのに役立ちます。

HELLO メッセージで交換されたすべての情報のうち、スパンニング・ツリーを計算するためには、次のパラメーターが最も重要です。

- *ルート・ブリッジ ID* ルート・ブリッジ ID はルート・ブリッジのブリッジ ID です。ルート・ブリッジとは、それが接続されているすべての LAN に対する指定ブリッジです。
- *ルート・パスのコスト*。このブリッジのルート・ポートを介するルートへの指定パスのコストの合計。この情報は、トポロジーが変更されると、ルート・ブリッジおよび指定ブリッジの両方によって送信され、パス上のすべてのブリッジの情報が更新されます。
- *ブリッジ ID*。 スパンニング・ツリー・アルゴリズムがスパンニング・ツリーを判別するために使用する固有の ID。ネットワーク内の各ブリッジには、固有のブリッジ識別子が割り当てられます。
- *ポート ID*。 現行の HELLO BPDU メッセージの送信元ポートの ID。

この情報が入手できると、スパンニング・ツリーはその形状と方向を判別し始め、次に論理パス構成を作成します。このプロセスは次のように要約できます。

1. ネットワーク用のルート・ブリッジは、ネットワーク内の各ブリッジのブリッジ ID を比較することによって選択されます。最も低い ID (つまり、最も高い値) をもつブリッジが選択されます。
2. スパンニング・ツリー・アルゴリズムは、次に各 LAN に対して指定ブリッジを選択します。同じ LAN に複数のブリッジが接続されている場合には、ルートへのパス・コストが最小のブリッジが指定ブリッジとして選択されます。同じパス・コストの場合は、最も低いブリッジ ID をもつブリッジが指定ブリッジとして選択されます。
3. LAN 上の非指定ブリッジは、ルート・ポートとして選択されなかった各ポートを BLOCKED (ブロックされた) 状態にします。BLOCKED (ブロックされた) 状態では、ブリッジは Hello BPDU をまだ listen しているので、ネットワークで行われるいかなる変更 (例えば、指定ブリッジに障害が起こる) にも対処し、その状態を BLOCKED から FORWARDING に変更することができます (つまり、データを転送することができます)。

このプロセスを通じて、スパンニング・ツリー・アルゴリズムは、任意のトポロジーのブリッジされた LAN ネットワークを単一のスパンニング・ツリーに形成します。

スパンニング・ツリーでは、どの 2 つのエンド・ステーション間でもアクティブなデータ・パスが複数存在することは決してないので、データ・ループが除去されます。ネットワーク上の各ブリッジについて、スパンニング・ツリーは、ループが形成しないようにするのにどのブリッジ・ポートをブロックしたらよいかを判別します。

この新しい構成は時間の要素によって拘束されています。指定ブリッジが故障するか、物理的に除去された場合、LAN 上の他のブリッジが、ブリッジの最大経過時間として設定された時間内で Hello BPDU を受信しない状況を検出します。この事象により新しい構成プロセスが開始されて、別のブリッジが指定ブリッジとして選択されます。新しい構成は、ルート・ブリッジが故障したときにも作成されます。

スパンニング・ツリーの形成

スパンニング・ツリーがその省略時設定値を使用するときは、スパンニング・ツリー・アルゴリズムは通常受け入れ可能な結果を作成します。しかし、このアルゴリズムはネットワークのパフォーマンスが不良なスパンニング・ツリーを生成することもあります。この場合には、ブリッジ優先度、ポート優先度、およびパス・コストを調整して、ユーザーが予期するネットワーク・パフォーマンスに合うようスパンニング・ツリーを形成することができます。次の例はこれがどのようにして行われるかを説明しています。

17ページの図6 は、3 つのブリッジを使用してネットワーク化された 3 つの LAN を示しています。各ブリッジは、そのスパンニング・ツリー構成に省略時のブリッジ優先度の設定値を使用しています。この場合、各ブリッジのブリッジ優先度は同じなので、物理アドレスが最も低いブリッジがルート・ブリッジとして選択されます。この例では、これはブリッジ 2 です。

新しく構成されたスパンニング・ツリーは変更されないでいます。これは、ルート・ブリッジから Hello BPDU が事前設定された時間間隔 (ブリッジ・ハロー時間) で繰り返し送信されるからです。このプロセスを通じて、指定ブリッジはすべての構成情報を使って更新されます。指定ブリッジは次に Hello BPDU からの情報を再生成し、それらが指定ブリッジである LAN へと情報を配布します。

表 2. スパンニング・ツリーの省略時値

ブリッジ 1 ブリッジ優先度 : 32768 アドレス : 00:00:90:00:00:10	**ブリッジ 2** ブリッジ優先度 : 32768 アドレス : 00:00:90:00:00:01	**ブリッジ 3** ブリッジ優先度 : 32768 アドレス : 00:00:90:00:00:05
ポート 1 優先度: 128 パス・コスト: 100	**ポート 1** 優先度: 128 パス・コスト: 100	**ポート 1** 優先度: 128 パス・コスト: 100
ポート 2 優先度: 128 パス・コスト: 17857	**ポート 2** 優先度: 128 パス・コスト: 17857	**ポート 2** 優先度: 128 パス・コスト: 17857
ポート 3 優先度: 128 パス・コスト: 17857	**ポート 3** 優先度: 128 パス・コスト: 17857	**ポート 3** 優先度: 128 パス・コスト: 17857

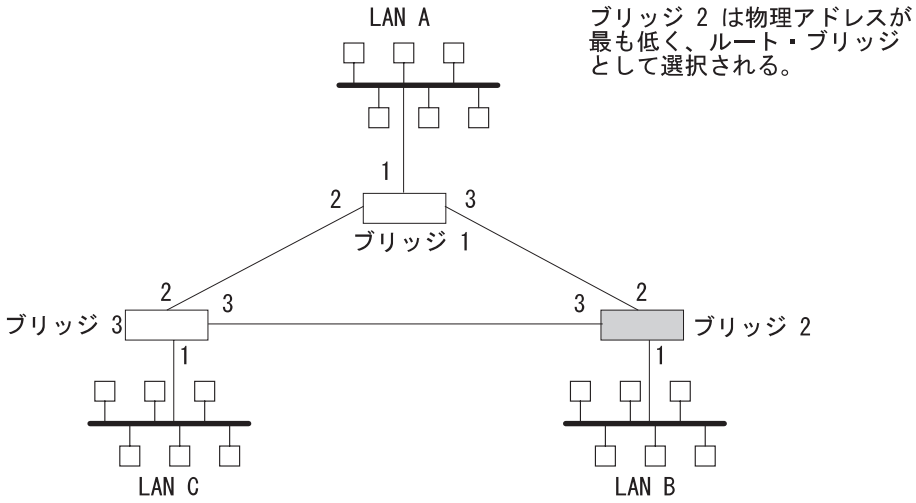


図 6. スパンニング・ツリー以前のネットワークされた LAN

スパンニング・ツリー・アルゴリズムはブリッジ 1 をブリッジ 3 に接続するポート (ポート 2) をバックアップ・ポートとして指定し、ループ状態を生じさせるようなフレームをそのポートが転送しないようブロックします。16ページの表2 の省略時値を使用してアルゴリズムによって作成されたスパンニング・ツリーは、図7 では、ブリッジ 1 をブリッジ 2 に接続し、ついでブリッジ 2 をブリッジ 3 に接続する太線として示してあります。ルート・ブリッジはブリッジ 2 です。

このスパンニング・ツリーによるネットワークのパフォーマンスは良くありません。というのは、LAN C 上のワークステーションが LAN A 上のファイル・サーバーに到達するには、ブリッジ 1 とブリッジ 3 の間の直接接続を使用せずにブリッジ 2 を介して間接的に進むしかないからです。

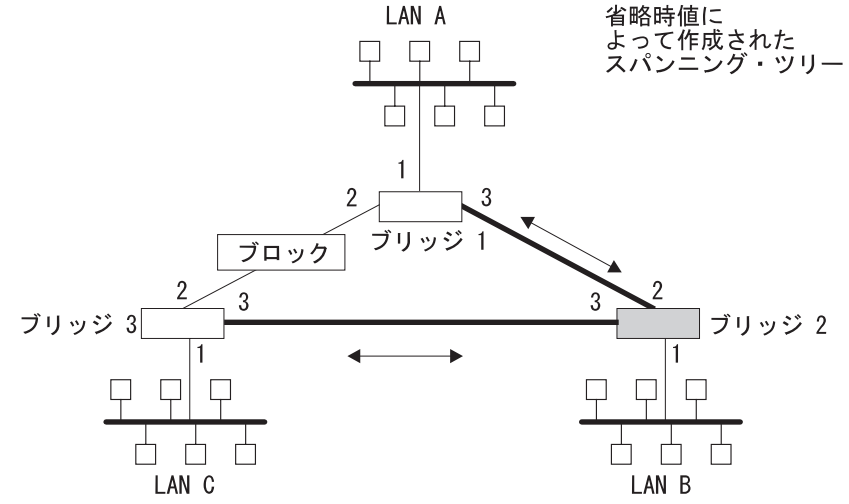


図 7. 省略時値を使用して作成されたスパンニング・ツリー

通常、このネットワークはブリッジ 2 とブリッジ 3 の間のポートを頻繁には使用しません。したがって、ブリッジ 1 をスパンニング・ツリーのルート・ブリッジにすると、ネットワークのパフォーマンスを改善できます。これは、ブリッジ 1 を最も高い

優先度の 1000 を使って構成することにより行うことができます。この修正によって生じたスパンニング・ツリーは、図8 にブリッジ 1 をブリッジ 3 に接続し、ブリッジ 1 をブリッジ 2 に接続する太線によって示されています。ルート・ブリッジは今度はブリッジ 1 になります。 ブリッジ 2 とブリッジ 3 の間の接続は今度はブロックされており、バックアップ・データ・パスとして使用されます。

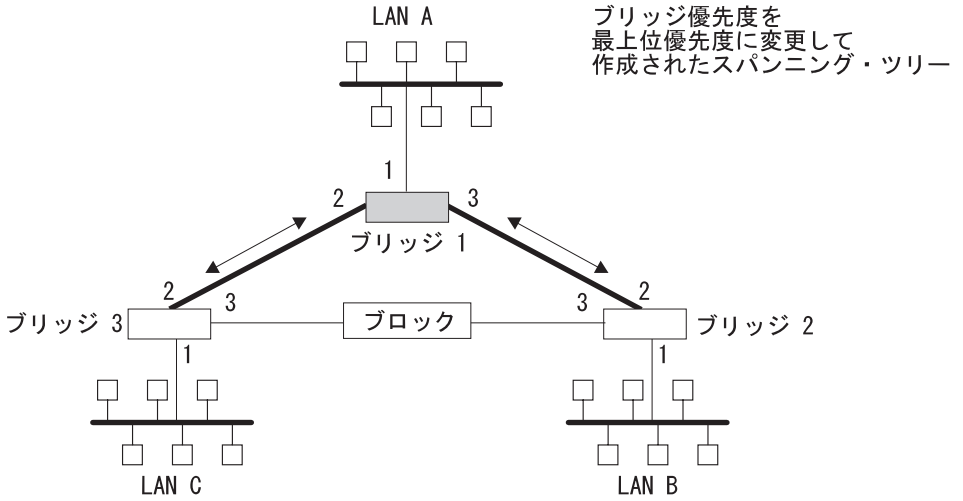


図 8. ユーザーが調整したスパンニング・ツリー

スパンニング・ツリー・ブリッジおよびイーサネット・パケット形式の変換

2210 スパンニング・ツリー・ブリッジ・プロトコルは、IEEE 標準 802.1D-1990 媒体アクセス制御 (MAC) ブリッジに準拠したパケットを転送するブリッジ・ルーター機能を提供します。このプロトコルにより適正なイーサネット・パケットのヘッダーの変換機能も提供されます。

イーサネット/IEEE 802.3 ネットワークは、MAC ヘッダーの長さ/タイプ・フィールドの値に基づいて、イーサネット・データ・リンク・レイヤーおよび IEEE 802.2 データ・リンク・レイヤーを同時にサポートすることができます。ブリッジは、混合された LAN タイプを通じての透過性を与えるために、イーサネット形式に変換したり、イーサネット形式から変換したりする必要があります。使用されるアルゴリズムは、新しい IEEE 標準に基づいています。

基本アプローチは、IEEE 802 SNAP SAP を使用して、イーサネット・パケットを IEEE 802.2 の無番号情報 (UI) パケットに変換します。SNAP プロトコル識別子は、00-00-00の組織で固有な識別子 (OUI) をもっており、最後の 2 つのバイトはイーサネット・タイプの値です。

SNA トラフィック用の IBM RT フィーチャー

一部の IBM パーソナル・コンピューター (AIX を実行する IBM RT PC または OS/2 EE を実行する任意の PC) は、IEEE 802.3 イーサネット・カプセル化を使用する代わりにイーサネット・タイプ 2 のパケット内に SNA をカプセル化します。これに

は、MAC ユーザー・データの長さを含む特殊な Ethertype ヘッダーが必要です。このヘッダーの後には IEEE 802.2 (LLC) ヘッダーが続きます。

これらのフレームの処理はポートごとに使用可能/使用不能にできます。使用可能モードでは、ブリッジは送信元ステーションの行動を学習します。フレームがそのようなステーションにターゲットされるときは、ブリッジは正しいフレーム形式を生成します。ステーションの行動についての情報がない場合 (マルチキャストまたは未知のステーションの場合のように)、ブリッジは重複フレームを作成します。一方は IEEE 802.3 および IEEE 802.2 形式で、もう一方は IBM-RT ヘッダーが付いています。

XNS フレームの UB カプセル化

XNS イーサネット・フレームは イーサネット・タイプ 0x0600 を使用します。トークンリング形式に変換されると、これらのフレームは IEEE 802.1H で指定されるような SNAP を入手します。一部のトークンリング・エンド・ステーションはそのようなフレーム用の SNAP で Ungermann-Bass OUI を使用するので、このカプセル化を活動化する構成スイッチがあります。このカプセル化を活動化するためのスイッチは、**frame token_ring_SNAP** コマンドを用いて設定します。

透過ブリッジングおよびフレーム・リレー

フレーム・リレー・インターフェースがイーサネット・ネットワークトークンリング・ネットワークからの透過フレームを転送するのは、ブリッジングが回線上で使用可能になっている場合です。 IP トンネルを使用する必要はありません。

透過ブリッジング用として構成されている各回線ごとに、それぞれ Hello BPDU の生成と伝送が行われます。スパンニング・ツリー・プロトコルによって、アクティブ・データ・パスの一部として指定されていないフレーム・リレー回線がブロックされ、したがって、ループが除去されます。

透過ブリッジングおよび ATM

ATM インターフェースがイーサネット・ネットワークトークンリング・ネットワークからの透過フレームを転送するのは、バーチャル・チャネル・コネクション (VCC) 上でブリッジングが使用可能になっている場合です。 IP トンネルを使用する必要はありません。

透過ブリッジング用に構成された各 VCC に Hello BPDU が生成され、伝送されます。スパンニング・ツリー・プロトコルによって、アクティブ・データ・パスの一部として指定されていない ATM VCC がブロックされ、したがって、ループが除去されます。

透過型ブリッジの用語および概念

この項では、透過ブリッジングで通常使用される用語および概念を説明します。

経過時間

項目をもつポートが転送状態にあるときに動的項目がフィルター・データベースから除去されるまでの時間の長さ (経過時間)。動的項目が経過時間によって示されていない場合には、その項目は削除されます。

ブリッジ

ローカル・エリア・ネットワーク (LAN) を接続するプロトコルに依存しない装置。これらの装置はデータ・リンク・レイヤーで作動し、LAN 間でデータ・パケットを保管し、転送します。

ブリッジ・アドレス

スパンニング・ツリー・アルゴリズムがネットワーク上のブリッジを識別するのに使用する、ブリッジ識別子の下位 6 オクテットの部分。省略時解釈では、ブリッジ・アドレスは最も番号が小さいポートの MAC アドレスに設定されます。**set bridge** 構成コマンドを使用することで、省略時アドレスを指定変更できます。

ブリッジ・ハロー時間

ブリッジ・ハロー時間は、ブリッジがスパンニング・ツリーにおけるルート・ブリッジになるときにブリッジが Hello BPDU (ブリッジ構成情報を含む) を送信する回数を指定します。 ルート・ブリッジがスパンニング・ツリー内のすべてのブリッジのハロー時間を制御するので、この値はルート・ブリッジにとってのみ有効です。ブリッジ・ハロー時間を設定するには、**set protocol bridge** コマンドを使用します。

ブリッジ転送遅延

ブリッジ転送遅延は、ブリッジ・ポートが待機状態および学習状態でどれだけ時間を費やすかを指定します。転送遅延は、ブリッジ・ポートがスパンニング・ツリー・トポロジーを調整するために待機状態にある時間の量です。転送遅延は、スパンニング・ツリーが構成されている間にブリッジが受信する各パケットの発信元アドレスをブリッジが学習するのに費やす時間の量でもあります。 ルート・ブリッジはスパンニング・ツリー内のすべてのブリッジの転送遅延を制御するので、この値はルート・ブリッジにとってのみ有効です。

ルート・ブリッジはこの値をすべてのブリッジに伝達します。 この時間は、**set protocol bridge** コマンドを使って設定されます。 このパラメーターを設定する手順については、次の章で詳しく説明します。

ブリッジ識別子

スパンニング・ツリー・アルゴリズムがスパンニング・ツリーを判別するために使用する固有の識別子。ネットワーク内の各ブリッジは固有のブリッジ識別子をもっている必要があります。

ブリッジ識別子は次の 2 つの部分から構成されます。下位 6 オクテットのブリッジ・アドレスおよび上位 2 オクテットのブリッジ優先度です。 省略時解釈では、ブリッジ・アドレスは最も番号が小さいポートの MAC アドレスに設定されます。 **set bridge** 構成コマンドを使って、省略時のアドレスを指定変更することができます。

ブリッジの最大経過時間

プロトコルが情報を廃棄し、トポロジーが変化するまで、スパンニング・ツリー・プロトコル情報が有効と見なされている時間の量。スパンニング・ツリー内のすべてのブリッジは、そのデータベースに受信した構成情報をタイムアウトにするためにこの経過時間を使用します。こうして、スパンニング・ツリー内のすべてのブリッジに一律のタイムアウトを生じさせることができます。ブリッジの最大経過時間を設定するには、**set protocol bridge** コマンドを使用します。

ブリッジ優先度

set protocol bridge コマンドによって設定されるブリッジ識別子の上位 2 オクテットの部分。 この値は、各ブリッジがネットワークのルート・ブリッジになれるかどうかの可能性を示しています。ブリッジ優先度を設定する際、スパンニング・ツリー・アルゴリズムは優先度の値が最も大きなブリッジをスパンニング・ツリーのルート・ブリッジに選択します。数値が最も小さいブリッジが最も高い優先度値をとります。

指定ブリッジ

特定の LAN 上でルート・ブリッジの最も近くにある必要があるブリッジ。この近さは、ルート・ブリッジの累積パス・コストにより測定されます。

指定ポート

LANに接続された指定ブリッジのポート ID

フィルターおよび永続データベース

LAN に接続されたポートの特定のポート番号に属するステーション・アドレスについての情報が含まれているデータベース

フィルター・データベースは永続データベースからの項目を使って初期設定されます。これらの項目は永続的であり、電源のオン/オフまたはシステム・リセットを行っても残っています。これらの項目の追加または削除は、スパンニング・ツリー構成コマンドを使って行うことができます。永続データベース内の項目は静的ランダム・アクセス・メモリー (SRAM) レコードとして保管され、項目の数は SRAM のサイズによって制約されます。

注: 監視コマンドを使用しても項目 (静的) を追加できますが、これらの項目は、電源のオン/オフおよびシステム・リセットを行うと***残りません***。

フィルター・データベースも、ブリッジによって学習された項目 (動的項目) を累積します。これらの項目にはそれらに関連する経過時間が含まれています。特定の時間 (経過時間) を超えて項目が参照されないと、削除されます。静的項目は経過時間はなく、動的項目がそれらを上書きすることはできません。

フィルター・データベースおよび永続データベース内の項目には、次の情報が含まれます。

- *アドレス*。項目の 6 バイトの MAC アドレス。
- *ポート・マップ*。その項目に関連するすべてのポート番号を指定します。

- *項目のタイプ*。以下のタイプのうち 1 つを指定します。
  - 予約済み項目。IEEE 802.1d 委員会によって予約済みです。
  - 登録済み項目。ボックスに接続された通信ハードウェアに属するユニキャスト・アドレス、またはプロトコル転送側によって使用可能になるマルチキャスト・アドレスから構成されます。
  - 永続項目。構成プロセスでユーザーが入力します。電源のオン/オフおよびシステム・リセットが行われても残っています。
  - 静的項目。監視プロセスでユーザーが入力します。静的項目は電源のオン/オフおよびシステム・リセットを行うと消え、経過時間はありません。
  - 動的項目。ブリッジが動的に学習します。電源のオン/オフおよびシステム・リセットを行うと消え、関連する経過時間があります。
  - 空き。アドレス項目を入れられる空のデータベース内のロケーション
- *アドレス経過時間 (動的項目のみ)*。アドレス項目が廃棄される前に経過する時間のレゾリューション。ユーザーはこの値を設定できます。

永続データベースに対する変更は、スパンニング・ツリー構成コマンドを用いて行い、フィルター・データベースに対する変更は、GWCON 監視プロセスを経て行います。

並列ブリッジ

同じブリッジを接続する 2 つ以上のブリッジ

パス・コスト

各ポート・インターフェースには関連するパス・コストがあります。これは、ブリッジされたネットワーク内でこのポートを使用してルート・ブリッジに到達するまでの相対値です。スパンニング・ツリー・アルゴリズムはこのパス・コストを使用して、ネットワーク・トポロジーにおいてルート・ブリッジから他のすべてのブリッジへのコストを最小化するパスを計算します。すべての指定コストおよびルート・ポートのパス・コストの総和は、ルート・パス・コストと呼ばれます。

ポート

接続された各 LAN または WAN へのブリッジの接続。ブリッジが、ブリッジとして機能するためには少なくとも 2 つのポートが必要です。

ポート ID

2 オクテットのポート識別子。上位の 1 オクテットがポート優先度を表し、下位の 1 オクテットがポート番号を表します。ポート番号とポート優先度は両方ともユーザーが割り当てることができます。ポート ID はブリッジ内で固有でなければなりません。

ポート番号

ポート ID のうち、ユーザーが割り当てる 1 オクテットの部分で、その値は物理媒体への接続を表します。ポート番号でゼロは使えません。

ポート優先度

ポート ID のうち 2 番目の 1 オクテットの部分。この値は、スパンニング・ツリー・アルゴリズムが、ポートの選択とブロックの決定のために比較を行う際に使用するポートの優先度を表します。

レゾリューション

動的項目がデータベース内で経過する時間を計る時間要素。範囲は 1 秒から 60 秒です。

ルート・ブリッジ

最高の優先度のブリッジ ID を所有しているため、スパンニング・ツリーの*根*として選択されるブリッジ。このブリッジは、定期的に Hello BPDU (ブリッジ構成情報を含む) を出すことにより、スパンニング・ツリーを完全に保つ役目をもっています。ルート・ブリッジとは、それが接続されているすべての LAN に対する指定ブリッジです。

ルート・ポート

ブリッジのうちルート・ブリッジへの最低コストのパスを提供するポートのポート ID

スパンニング・ツリー

任意の 2 つのエンド・ステーション間にあるデータ・ルートが 1 つだけである、ブリッジのトポロジー

透過ブリッジング

このタイプのブリッジングには、エンド・ステーション・アプリケーションにとって*透過* のメカニズムを使用しています。透過ブリッジングは、スパンニング・ツリー・アルゴリズムを通じてデータ・フレームを転送するよう指定したブリッジによって、ローカル・エリア・ネットワークのセグメントを相互接続しています。

ソース・ルート・ブリッジング (SRB)

ソース・ルーティングは、ブリッジされたネットワークを通じてフレームを転送する方式で、発信元ステーションがフレームに、そのフレームがたどるルートを識別します。分散ルーティング方式では、各ブリッジにあるルーティング・テーブルが、ネットワークを通じてデータが通るパスを決定します。それに対して、ソース・ルーティング方式では、発信元ステーションが伝送されるフレーム内にその全ルートを定義します。

ソース・ルーティング・ブリッジ (SRB) は、24ページの図9 に示すように、4 Mbps および 16 Mbpsのトークンリングを介してのローカル・ブリッジングを提供します。また、最高 E1 の速度で稼働する通信リンクを介してリモート LAN を接続することもできます。

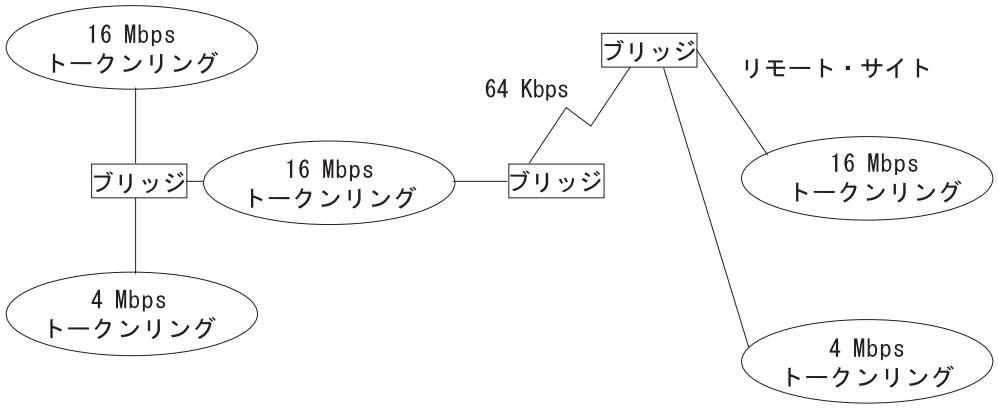


図 9. ソース・ルーティング・ブリッジの接続性の例

ソース・ルーティング・ブリッジには次のような特長があります。

- *ブリッジ互換性*。OS/2、PC LAN 管理プログラム、および NetBIOS などのシステムを稼働する IBM PC LAN に接続するためにこのブリッジを使用できます。このブリッジは PC LAN とメインフレーム間で IBM SNA トラフィックも搬送できます。
- *パフォーマンスおよび速度*。ブリッジングはネットワーク・レイヤーではなくデータ・リンク・レイヤーで行われるので、パケット変換およびアドレス・テーブルの維持は必要でありません。これには、オーバーヘッドが削減され、ルーティングの決定がより迅速に行われることが必要です。
- *ブリッジ・トンネル伝送*。 ソース・ルーティング・パケットをカプセル化することにより、ブリッジ/ルーターは、性能低下またはネットワーク・サイズの制約なしに、これらのパケットをインターネットワークを通じて所望のあて先エンド・ステーションに動的にルートします。

  ソース・ルーティング・エンド・ステーションは、ネットワークの複雑さとは無関係に、このパスを単一のホップと見なします。これにより、ソース・ルーティング構成で検出される通常の 7 ホップの距離の制限を克服することができます。この特長により、ソース・ルーティング・エンド・ステーション間を非ソース・ルーティング媒体 (例えば、イーサネット・ネットワーク) を介して接続することもできます。

ソース・ルーティング・ブリッジの操作

前述したように、ソース・ルーティング構成では発信元ステーションが伝送されるフレームの全ルートを定義します。ソース・ルーティング・ブリッジは動的です。エンド・ステーションとブリッジの両方が、ルート発見および転送のプロセスに参加します。以下のステップはこのプロセスを説明しています。

1. 発信元ステーションはフレームを送信しようとして、そのフレームの宛先がそれ自体の (ローカルの) セグメントまたはリングにないことを見つけます。
2. 発信元ステーションは*ルート発見* 同報通信フレームを作成し、それをローカル・セグメントに伝送します。
3. ローカル・セグメント上のすべてのブリッジがルート発見フレームを取り込み、接続されたネットワークを通じてフレームを送信します。

ルート発見フレームがあて先エンド・ステーションへの探索を続けている間、フレームを転送する各ブリッジはそのフレームのルーティング情報フィールド (RIF) に自身のブリッジ番号およびセグメント番号を追加します。フレームがブリッジされたネットワークを通過し続ける間、RIF はあて先へのパスを記述するブリッジ番号とセグメント番号の対のリストをコンパイルします。

同報通信フレームが最後にそのあて先に到達すると、そのフレームには、発信元からあて先への正しいアドレス・シーケンスが含まれることになります。

4. あて先のエンド・ステーションがフレームを受信すると、通信用のルート・パスを含めた応答フレームを生成します。ブリッジされたネットワークの他の部分にさまようフレーム (その間、不適切なルーティング情報を累積していきます) は、決してあて先エンド・ステーションには到達せず、どのステーションもそれらのフレームを受け取りません。
5. 発信元のステーションは学習されたルート・パスを受信します。そのステーションは、その後この確立されたパスを通じて情報を伝送できます。

ソース・ルーティング・フレーム

前述したように、ブリッジはデータ・フレーム、特に MAC フレームを、ブリッジされた LAN の別々の MAC エンティティーの間で中継することにより LAN 相互を接続します。MAC フレームは、発信元アドレスとあて先アドレスの形でフレームを転送するために必要な『どこ?』の情報を提供します。この情報は、データを正常に送受信する上で不可欠です。

ソース・ルーティングでは、データ・フレームを転送する決定は、フレーム内のルーティング情報に基づいています。フレームが転送される前に、エンド・ステーションは、*ルート発見* プロセスによってあて先ステーションまでのルートを得ています。フレームを発生させた発信元ステーションは、転送されるフレームのルーティング情報フィールド (RIF) にルートの記述を組み込むことにより、フレームがたどるルートを指定します。各種のソース・ルーティング・ブリッジ・フレームを詳しく調べると、ブリッジがこのルーティング情報をどのように入手し、送信するかをさらによく理解することができます。

ソース・ルーティング MAC フレームは複数リングの環境を通じてデータ通信するのに必要なルーティング情報を含んでいるので、それらは典型的なトークンリング MAC フレームと比べて形式が少し異なっています。発信元アドレス・フィールド内の RII に 『1』 がある場合には、ルーティング情報を含む RIF が発信元アドレスの後にあることを示しています。26ページの図10 では、ソース・ルーティング・フレームの送信元アドレス・フィールドの形式を詳しく示しています。

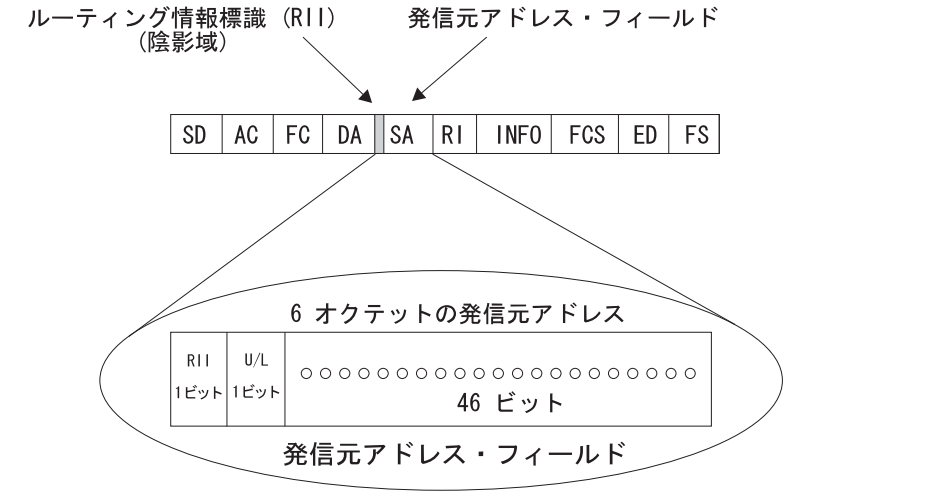


図 10. 802.5 の発信元アドレス形式

発信元アドレス・フィールド内の RII が 1 に設定されている場合は、発信元アドレスの後に RIF があります。RIF は、ソース・ルーティング時のルート情報を提供するため、必要です。RIF は 2 オクテットのルーティング制御 (RC) フィールドおよび一連の 2 オクテットのルート指定子 (RD) フィールドから構成されます。図11 では、ルーティング情報フィールドの形式を詳しく示しています。

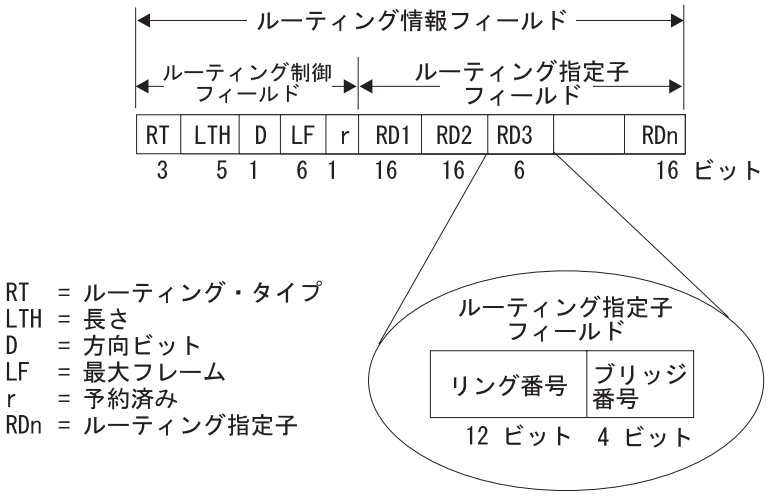


図 11. 802.5 のルーティング情報フィールド

以下の情報は、RIF にある各フィールドを説明しています。

- **ルーティング・タイプ (RT)。**

  フレームがネットワークを通じて、特定ルートに沿って転送されるのか、またはすべての相互接続 LAN に到達するルート (複数の場合もある) に沿って転送されるのかを、ビットの設定値によって示しています。このフィールドのビット設定値により、ソース・ルーティング・フレームは次のタイプの 1 つとして識別されます。

- 全パス探索フレーム (探索フレーム)
- スパンニング・ツリー探索フレーム (探索フレーム)
- 特定ルーティング・フレーム (ルーティング・フレーム)
- スパンニング・ツリー・ルーティング・フレーム (ルーティング・フレーム)

RT ビットが 100 に設定されている場合は、*全パス探索フレーム*が存在します。このフレームが生成されると、ネットワーク内の重複しない全ルートに沿って (発信元からあて先まで) 転送されます。このプロセスの結果、発信元のエンド・ステーションからの異なるルート数と同じだけの数のフレームがあて先のエンド・ステーションに到達します。このルーティング・タイプは、スパンニング・ツリーに沿って使用可能なすべてのルートを使用して現在の発信元ステーションに送信されたルート発見フレームを受信したことに対する応答です。転送するブリッジはフレームにルート指定子を付け加えます。

RT ビットが 110 に設定されている場合は、*スパンニング・ツリー探索フレーム* が存在します。 スパンニング・ツリー・ブリッジだけがフレームを 1 つのネットワークから別のネットワークに中継します。つまり、このフレームはネットワーク内の全リングで一度だけ現れ、したがってあて先エンド・ステーションでも一度だけ現れます。ルート発見プロセスを開始するステーションはこのフレーム・タイプを使用します。ブリッジはフレームにルート指定子フィールドを追加します。このフレーム・タイプはグループ・アドレスを使用するステーションに送信されるフレームにも使用されます。グループ・アドレスについては、次の節でさらに詳しく説明します。

最初の RT ビットが 0 に設定されている場合は、*特定ルーティング・フレーム*が存在します。この場合、特定のルーティング情報を含むルート指定子 (RD) フィールドがフレームをネットワークを通じてあて先アドレスまでガイドします。フレームがそのあて先に到達し、ルート・パスを発見すると、あて先ステーションは特定ルーティング・フレーム (SRF) を発信元ステーションに戻します。発信元ステーションはその後データを特定ルーティング・フレームに入れて伝送します。

- **長さビット (LTH)**。RI フィールドの長さ (オクテット単位) を示します。
- **方向ビット (D)**。フレームが接続されたネットワークを通過するのにとる方向を示します。このビットが 0 に設定されている場合、フレームは接続されたネットワークをルーティング情報フィールドに指定された順序で (例えば、RD1 から RD2 へ... RDn へ) 進んでいきます。方向ビットが 1 に設定されている場合は、フレームはネットワークを逆の順序で進みます。
- **最大フレーム・ビット (LF)**。特定のルート上で通信する 2 つのエンド・ステーション間で伝送できる INFO フィールドの最大フレーム・サイズを示します。LF ビットが意味をもつのは、STE フレームと ARE フレームについてだけです。特定ルーティング・フレーム (SRF) では、ブリッジは LF ビットを無視し、LF ビットを更新できません。探索フレームを発信するステーションは、LF ビットをそれが扱うことができる最大サイズに設定します。転送するブリッジは LF ビットを次のうち最も小さいものを超えることがない最大値に設定します。
  - 受信された LF ビットの指示値
  - ブリッジでサポートされる最大の最大サービス・データ単位 (MSDU) サイズ
  - そこからフレームが受信されたポートによってサポートされる最大 MSDU サイズ
  - フレームの伝送先のポートによってサポートされる最大 MSDU サイズ

必要な場合は、あて先ステーションは最大フレーム容量を示すために、LF 値をさらに減少させます。

LF ビットのコードは 3 ビットの基本コードおよび 3 ビットの拡張コードから構成されます (全体で 6 ビット)。 SRT ブリッジ (これについては後の節で説明します) には LF モード標識が含まれているので、ブリッジは基本 LF ビットまたは拡張 LF ビットのどちらかを選択できます。 LF モード標識が基本モード に設定されているときには、ブリッジは最大のフレーム基本値を使って探索フレーム内の LF ビットを設定します。 LF モード標識が拡張モードに設定されているときには、ブリッジは最大のフレーム拡張値を使って探索フレーム内の LF ビットを設定します。

- **ルート指定子フィールド (RDn)** は、RD フィールドの順序列に従ってネットワークを通過する特定ルートを示します。各 RD フィールドには、固有のネットワークの 12 ビットのリング番号および 4 ビットのブリッジ番号が含まれています。これらの番号は、同じ 2 つのリングを接続するときの 2 つ以上のブリッジ (並列ブリッジ) を識別します。ルーティング情報フィールドの最後のブリッジ番号は空値 (すべてゼロ) になっています。

スパンニング・ツリー探索オプション

スパンニング・ツリー探索フィーチャーにより、ネットワークに同じ LAN を接続する 2 つ以上のブリッジがあるときに宛先への単一のルートを選択できます。このフィーチャーを使用可能にすると、選択したブリッジだけがスパンニング・ツリー探索 (STE) フレームを受信します。スパンニング・ツリー・プロトコルと混同しないでいただきたいのですが、このオプションでは次のことができます。

- スパンニング・ツリー・ネットワークのシミュレート
- トラフィック負荷の平衡化

スパンニング・ツリー・ネットワークのシミュレート

スパンニング・ツリー・ネットワークには、任意の 2 つのエンド・ステーション間の単一のデータ・ルートが含まれています。ネットワークが、29ページの図12 に示すような 2 つ以上の並列ブリッジを使用する場合は、ネットワーク上の発見フレームの重複を避けることにより、手動でネットワーク内の 1 つのスパンニング・ツリーを構成することができます。スパンニング・ツリー探索を使用可能にしないと、ステーション Q がステーション R に発見フレームを伝送する場合、ブリッジ A とブリッジ B の両方がそのフレームを再送します。その場合、セグメント 2 は同じフレームの 2 つのコピーを受信します。

スパンニング・ツリー探索を使用可能にすると、ネットワーク上の各 LAN セグメントは伝送されたフレームの 1 つのコピーだけを受信します。選択したブリッジのみが STE フレームを受信できるので、無駄なフレームを作成しないで済み、ネットワークのオーバーヘッドが低減されます。

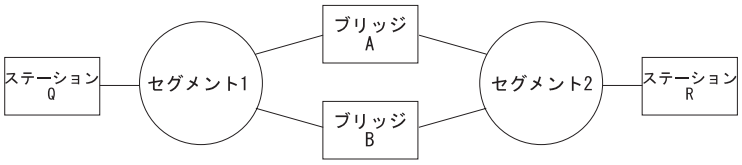


図 12. 並列ブリッジの例

トラフィック負荷の平衡化

負荷平衡化にもスパンニング・ツリー探索オプションを使用できます。例えば、図 13 では、ブリッジ A は、セグメント 2 を接続するインターフェースを介して STE フレームを受け入れるよう構成されています。ブリッジ B は、セグメント 1 に接続するインターフェースを介して STE フレームを受け入れるよう構成されています。トラフィックは矢印の方向に進みます。この構成では、並列ブリッジがトラフィック負荷を分担できます。

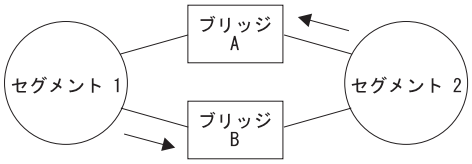


図 13. 負荷平衡化のためのスパンニング・ツリー探索の使用

注: ソース・ルーティングが機能するためには、IBM PC LAN プログラムなど一部のエンド・ノード・アプリケーションは、接続されたインターフェースでスパンニング・ツリー探索を使用可能にすることが必要です。並列ブリッジ構成では、スパンニング・ツリー探索オプションは並列インターフェースの 1 つにおいてのみ使用可能にする必要があります。ただし、スパンニング・ツリー用に使用可能なインターフェースが多過ぎても、(トラフィックが余分になる以外は) 重大な障害は生じません。

スパンニング・ツリー探索オプションを使用していて、単一ルート・パス上のどれかのブリッジが故障すると、ソース・ルーティング・トラフィックはそのあて先に到達できません。手動で代替パスを再構成する必要があります。

ソース・ルーティング・ブリッジングおよびフレーム・リレー

ソース・ルーティング・ブリッジングが使用可能になっていると、ソース・ルーテッド・フレームがフレーム・リレー・インターフェースとブリッジング転送側の間で転送されます。ブリッジがそれぞれのフレーム・リレー・バーチャル・サーキットを固有のリング番号をもつブリッジ・ポートとして処理するように構成できます。さらに、ブリッジ・ポートとして構成されていないフレーム・リレー・バーチャル・サーキットは、固有のリング番号をもつ単一のマルチアクセス・ブリッジ・ポートとしてグループにまとめることができます。詳しくは、60ページの『マルチ

アクセス・ブリッジ・ポートについて』 を参照してください。アクティブ・データ・パスの一部になっていないバーチャル・サーキットは、ループの内トポロジーを維持するためにブロックされます。

ソース・ルーティング・ブリッジングおよび ATM

ソース・ルーティング・ブリッジングがバーチャル・チャネル・コネクション (VCC) 上で使用可能になっていると、ソース・ルーテッド・フレームが ATM インターフェースとブリッジング転送側の間で転送されます。固有のあて先リング番号がそれぞれの VCC ごとに構成されます。 VCC にはアクティブ・データ・パスの一部になっていないものがあり、ループのないトポロジーを維持するためにブロックされています。

ソース・ルーティング・ブリッジの用語および概念

この節ではソース・ルーティング・ブリッジングで一般に使用される用語および概念について説明します。

ブリッジ・インスタンス

ブリッジ・インスタンスは、ソフトウェアに定義されたブリッジのシーケンスを識別します。例えば、2 つの構成済みブリッジの 1 つのブリッジ内では、ブリッジ・インスタンスは 1 および 2 になります。

単一のブリッジ内のブリッジ・インスタンスは独立しており、通信することはありません。例えば、図14 では、ステーション A はブリッジ・インスタンス 2 のどちらのステーションにもデータを渡すことができません。ステーション B にだけフレームを渡すことができます。実際、ブリッジ・インスタンスにより、2 つの別のネットワークを作成できます。これらのネットワークはどこか他の点で物理的に相互接続されない限り、通信することはありません。

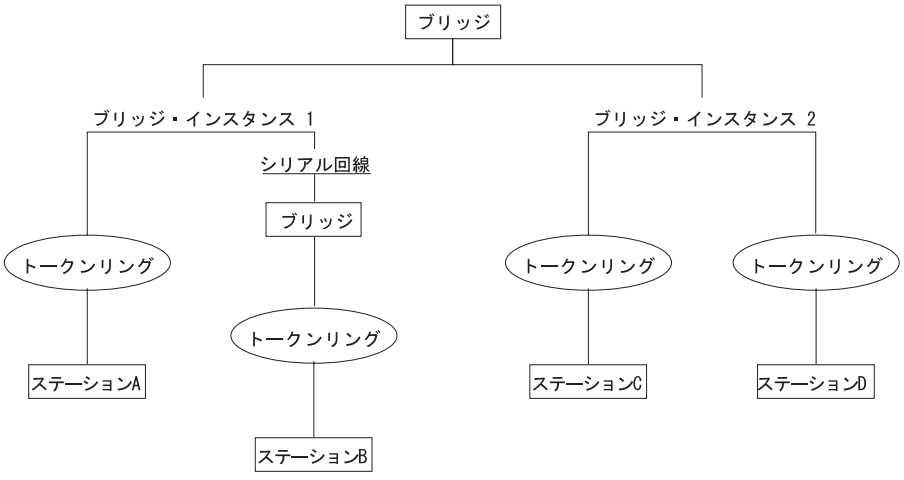


図 14. ブリッジ内のブリッジ・インスタンス

ブリッジ番号

ブリッジ番号はブリッジを識別する 4 ビットの 16 進値です。同じリングに接続されたブリッジは同じブリッジ番号をもつ場合があるとはいえ、並列ブリッジ (同じ 2 つのリングに接続されているブリッジ) は固有なブリッジ番号をもつ必要があります。

探索フレーム

ソース・ルーティング・ブリッジは、フレームをネットワークを通じてそのあて先のエンド・ステーションに転送するときに、探索フレームにルーティング情報を追加します。探索フレームはルートを発見するのに使用されます。探索フレームには次の 2 つのタイプのものがあります。全ルート探索 (ARE) フレームおよびスパンニング・ツリー探索 (STE) フレームです。 ARE フレームはすべてのポートによって転送されるのに対し、STE フレームはスパンニング・ツリー・プロトコルによりフレームを転送するよう割り当てられているポートによってのみ転送されます。

インターフェース番号

インターフェース番号は、ハードウェア・プロダクト内の『物理的』インターフェースを識別し、ブリッジ (つまり、ポート) によって理解される『論理的』インターフェースに結合される必要があります。ルーターのソフトウェアを構成するとき、ルーター/ブリッジはポートに順次番号を付けます。ソース・ルーティング・ブリッジを使用する場合は、ポート番号を使用して、各ネットワーク・セグメントを接続するインターフェースを識別する必要があります。

ルート

ルートは一連の LAN およびブリッジ (例えば、SRB ブリッジ) を通過するパスです。

ルート発見

ルート発見とは、あて先エンド・ステーションへのルートが学習されるプロセスです。

セグメント番号

セグメント番号は、個々の LAN (単一のトークンリングまたはシリアル回線など) を識別します。セグメントはブリッジに接続していますが、独立して動作することもできます。

ソース・ルーティング

ソース・ルーティングとは、フレーム内にそれが進むルートを指定することによって、複数 LAN ネットワークを通じてフレームを転送するブリッジング・メカニズムです。

ソース・ルーティング透過型 (SRT) ブリッジ

標準化された技術 (イーサネットおよびトークンリングは両方とも IEEE によって定義されています) を採用する作業を行うと、それらのネットワークを接続しようとするときに所有権の分野に立ち戻らなければならないことがあります。これは、ブリッジがトークンリング・ネットワークとイーサネット・ネットワークで機能の仕方が異なるためです。

ビット配列、パケット・サイズ、および確認ビットなどの違いのほかに、ブリッジング方式の違いがもう 1 つの障害になります。イーサネットのブリッジは透過ブリッジング方式を使用し、ブリッジがネットワークを通じてのトラフィックのルートを決定します。トークンリング・ネットワークは透過ブリッジングを一部の場合にだけ使用するので、基本のブリッジング方式としては一般にソース・ルーティングに依存しています。

透過パケットにはルーティング情報が含まれていないので、ソース・ルーティングは透過環境では作動することができません。この場合、ブリッジはパケットを転送すべきかどうか知ることができません。透過ブリッジングはソース・ルーティング環境で操作することができますが、エンド・ステーションへ何のルーティング情報も渡さないでこれを行います。重要な情報 (例えば、パケット・サイズ) が欠落しており、問題を起こす可能性があります。

IEEE は、ソース・ルーティング透過型 (SRT) と呼ばれる 802.1D 透過ブリッジング標準の拡張を批准しました。 SRT は、トークンリングとイーサネット のブリッジングに固有の非互換性の大部分の解決を試みる、ブリッジング・テクノロジーの 1 つです。透過ブリッジング標準に (代替ブリッジ・アーキテクチャーではなく) 並列ブリッジング・アーキテクチャーを追加することにより 2 つのタイプのトラフィックをサポートすることは、多数のブリッジングおよび個別リンクを導入するコストを節減することになります。

概説

ソース・ルーティング透過型 (SRT) ブリッジは、ルーティング情報をもつソース・ルーティング・フレームが受信されたときはソース・ルーティングを行い、ルーティング情報のないフレームが受信されたときは透過ブリッジングを行う、MAC ブリッジです。 SRT では、イーサネット とトークンリングの間のブリッジは、すべて透過型です。ブリッジはデータ・リンク・レイヤーの MAC サブレイヤーで働き、エンド・ステーションには完全に見えません。

SRT ブリッジは、フレームの RII フィールドの値を検査することにより、2 つのタイプのフレームを区別します (詳しくは、25ページの『ソース・ルーティング・フレーム』を参照してください)。RII の値が 1 の場合はフレームがルーティング情報を運んでいることを示すのに対し、RII の値が 0 の場合はルーティング情報がないことを示します。この方式では、SRT ブリッジは、発信媒体 (トークンリングを含む) と対話せずに、透過ブリッジング・フレームを転送します。ソース・ルーティング・フレームはソース・ルーティング・ブリッジング・ドメインに制限されています。

スパンニング・ツリー・プロトコルおよびアルゴリズムは、SRT ブリッジにより接続されているすべてのネットワークを含む単一のツリーを形成します。SRT ブリッジ接

続ネットワークはソース・ルーティングのサブドメインをもつ、より大きなドメインの透過ブリッジングを提供します。このようにして、透過フレームは、SRT および TB ブリッジ接続 LAN の一番端まで到達できるのに対し、ソース・ルーティング・フレームは SRT および SRB ブリッジ LAN のみに限定されます。SRT ブリッジングのモデルでは、ソース・ルーティング・ブリッジングおよび透過ブリッジングの部分は同じスパンニング・ツリーを使用しています。SRT ブリッジ接続定義域では、エンド・ステーションが 『ソース・ルーティング透過型ブリッジ』の質問に答える役目をします。

ソース・ルーティング透過型ブリッジの操作およびアーキテクチャー

SRT ブリッジでは、各ブリッジ・ポートは、ポートに関連する個々の MAC エンティティーによって提供される MAC サービスを使用して、接続されたローカル・エリア・ネットワークとフレームをやり取りします。MAC リレー・エンティティーは、ブリッジ・ポート間でフレームを中継する、MAC とは独立したタスクを担当します。受信されたフレームがソース・ルーティングされていない場合 (つまり、RII = 0) には、ブリッジ・フレームは透過ブリッジング論理を使用して転送または廃棄されます。受信されたフレームがソース・ルーティングされている場合 (RII = 1) には、フレームはソース・ルーティング論理に従って取り扱われます。このプロセスは 図15 に示されています。矢印はデータ・ルートを表します。

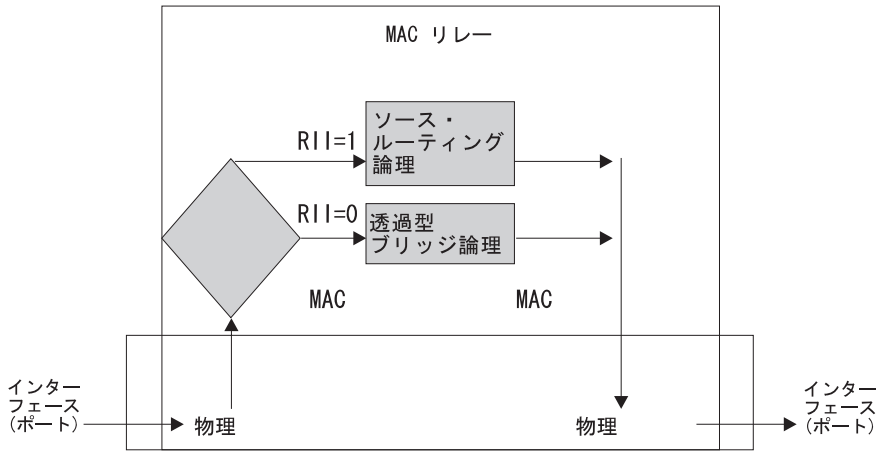


図 15. SRT ブリッジの操作

SRT はフレームごとにソース・ルーティングされたトラフィックとソース・ルーティングされていないトラフィックとを区別します。パケットがソース・ルーティングされている場合には、ブリッジはそれをそのようなものとして転送します。それが透過型ブリッジ・パケットである場合には、ブリッジはあて先アドレスを判別し、それをイーサネットとして処理します。

ソース・ルーティング透過ブリッジングおよびフレーム・リレー

SRT ブリッジングが回線上で使用可能になっていると、ソース・ルーテッド・フレームと透過フレームがフレーム・リレー・インターフェースとブリッジング転送側の間で転送されます。

ソース・ルーティング透過ブリッジングおよび ATM

SRT ブリッジングがバーチャル・チャネル・コネクション (VCC) 上で使用可能になっていると、ソース・ルーテッド・フレームと透過フレームが ATM インターフェースとブリッジング転送側の間で転送されます。

ソース・ルーティング透過型ブリッジの用語

この項では、SRT ブリッジで一般に使用される用語および概念を説明します。

探索フレーム

ソース・ルーティング・ブリッジは、フレームをネットワークを通じてそのあて先のエンド・ステーションに転送するときに、探索フレームにルーティング情報を追加します。 探索フレームはルートを発見します。探索フレームには次の 2 つのタイプのものがあります。

- 全ルート探索 (ARE) フレーム
- スパンニング・ツリー探索 (STE) フレーム

ARE フレームはすべてのポートによって転送されるようになっているのに対し、STE フレームはスパンニング・ツリー・プロトコルによってそれを転送するよう割り当てられているポートによってのみ転送されます。

ルーティング情報フィールド (RIF)

ソース・ルーティングでは、データ・フレームを転送する決定は、フレーム内のルーティング情報に基づいています。フレームが転送される前に、エンド・ステーションは、*ルート発見* プロセスによってあて先ステーションまでのルートを得ています。フレームを発信するステーション (つまり、*発信元* ステーション) は、伝送されるフレームのルーティング情報フィールド (RIF) にルートの記述を埋め込むことによりフレームがたどるルートを指定します。

ルーティング情報標識 (RII)

ソース・ルーティング MAC フレームは複数リングの環境を通じてデータ通信するのに必要なルーティング情報を含んでいるので、それらの形式は典型的なトークンリング MAC フレームと比べて少し異なっています。ルーティング情報標識と呼ばれる発信元アドレス・フィールドに 1 がある場合には、ルーティング情報を含むルーティング情報フィールドが発信元アドレスの後にあることを示しています。SRT ブリッジは、RII フィールドの 1 または 0 の値を検査することにより、ソース・ルーティングされたフレームとソース・ルーティングされていないフレームを区別します。

ソース・ルーティング

フレーム内にそれが進むルートを指定することによって、複数 LAN ネットワークを通じてフレームを転送するブリッジング・メカニズム

スパンニング・ツリー

任意の 2 つのエンド・ステーション間にあるデータ・ルートが 1 つだけである、ブリッジのトポロジー

透過ブリッジング

エンド・ステーションにとって透過のメカニズムを使用するブリッジングのタイプの 1 つ。透過ブリッジングは、ローカル・エリア・ネットワークのセグメントを、スパンニング・ツリー・アルゴリズムを通じてデータ・フレームを転送するよう指定されたブリッジによって相互接続します。

ASRT ブリッジの概要

適応ソース・ルーティング透過型 (ASRT) ブリッジは、いくつかのブリッジング・オプションのソフトウェアの集まりです。ASRT ブリッジ・ソフトウェアは、透過ブリッジングとソース・ルーティングとを組み合わせたもので、両者を別個に機能させることもできれば、両者を結合して単一の ASRT ブリッジとすることもできます。この拡張機能により、厳密なソース・ルーティング・エンド・ステーションと透過エンド・ステーションの間の通信が、ASRT ブリッジ経由で可能になります。 使用される構成コマンドの組み合わせに応じて、ASRT ブリッジは次のブリッジング・オプションを提供します。

- 透過型ブリッジ (STB)
- ソース・ルーティング・ブリッジ (SRB)
- ソース・ルーティング透過型ブリッジ (SRT)
- ソース・ルーティング - 透過型ブリッジ (SR-TB)

ASRT ブリッジは、SRT の IEEE 802.5M/草案 6 (1991 年) に記述されているソース・ルーティング透過型ブリッジに従って作成されます。ASRT ブリッジには、 SRT 標準への適合にとどまらない拡張機能をユーザーに提供する修正が組み込まれています。 ASRT ブリッジでは、導入済み基本のソース・ルーティング・ブリッジとの互換性を可能にしながら、なおそれらのブリッジがイーサネット LAN、トークンリング LAN とリンクできるようにします。 ASRT による基本 SRT 機能の拡張は、以下のので説明するような追加の重大な方法によっても行われています。

適応ソース・ルーティング透過型ブリッジ (ASRT) (SR-TB 変換)

ソース・ルーティングは SRT モデルで使用できるとはいえ、隣接するソース・ルーティング・トークンリング間でしか使用できません。ソース・ルーティング専用のブリッジは、イーサネット LAN とトークンリング LAN をリンクする SRT ブリッジとは共存できません。トークンリング・エンド・ノードは、イーサネット ノードと通信する必要があるため、RIF を省略するように構成する必要があります。同様にして、エンド・ノードが RIF を省略するように構成されていると、RIF を必要とする通常のソース・ルーティング・ブリッジを通じて通信できません。

概説

ソース・ルーティング - 透過型ブリッジ (SR-TB) オプションは、ソース・ルーティング・ブリッジング (ソース・ルーティング・ドメイン) および透過ブリッジング (透過ブリッジング・ドメイン) を使用してネットワークを相互接続します。このオプションは両方のドメインを透過的に結合します。操作中、両方のドメインのステーションは相互の存在または SR-TB ブリッジの存在には気付きません。1 つのステーションから見ると、結合されたネットワーク上のどのステーションもそれ自体のドメインにあるように見えます。

ブリッジは、透過ブリッジング・ドメインからのフレームをソース・ルーティング・フレームに変換してから、ソース・ルーティング・ドメインに転送する (およびその逆) ことによって、この機能を果たします。これは、ブリッジがエンド・ステーションのアドレスのデータベースをそれぞれそのルーティング情報フィールドとともにソース・ルーティング・ドメイン内に維持しておくことによって行われます。ブリッジは、透過ブリッジング・ドメインにあるエンド・ステーションに代わってルート発見を行うこともします。ソース・ルーティング・ドメイン内のあて先ステーションへのルートを見つけるためにルート発見プロセスが使用されます。不明の宛先に送信されるフレームは、スパンニング・ツリー探索 (STE) 形式で送信されます。

SR-TB ブリッジは、次の 3 つのタイプのスパンニング・ツリーを予期します。

- 透過ブリッジング・ドメインによって形成されたスパンニング・ツリー
- ソース・ルーティング・ブリッジ・ドメインによって形成されたスパンニング・ツリー
- すべての SR-TB ブリッジの特別なスパンニング・ツリー

以下の項では、SR-TB ブリッジの操作をさらに詳しく説明します。

ソース・ルーティング - 透過型ブリッジの操作

SR-TB の操作中、ネットワークは 2 つ以上の個別のドメインに区分されます。各ドメインはブリッジによって相互接続された LAN セグメントの集まりから構成されます。これらの LAN セグメントはすべて共通のブリッジング方式で操作されます。したがって、次の 2 つのタイプのドメイン (ブリッジング方式に応じて決まる) からなるネットワークが作成できます。

- ソース・ルーティング・ドメイン
- 透過ブリッジング・ドメイン

37ページの図16 は、これらのドメインの例を示しています。個々のドメインについて、各ソース・ルーティング・ドメインは、そのブリッジ用にセットアップされた単一ルート同報通信トポロジーをもちます。そのソース・ルーティング・スパンニング・ツリーに属するブリッジのみが、単一ルート同報通信フレームを転送するように指定されます。この場合には、単一ルート同報通信標識を運ぶフレームはソース・ルーティング・ドメインの各セグメントに転送されます。ソース・ルーティング・スパンニング・ツリーはドメイン内の任意の 2 つのステーション間で複数のパスを認めないので、各セグメントにはフレームの 1 つのコピーしか到達しません。

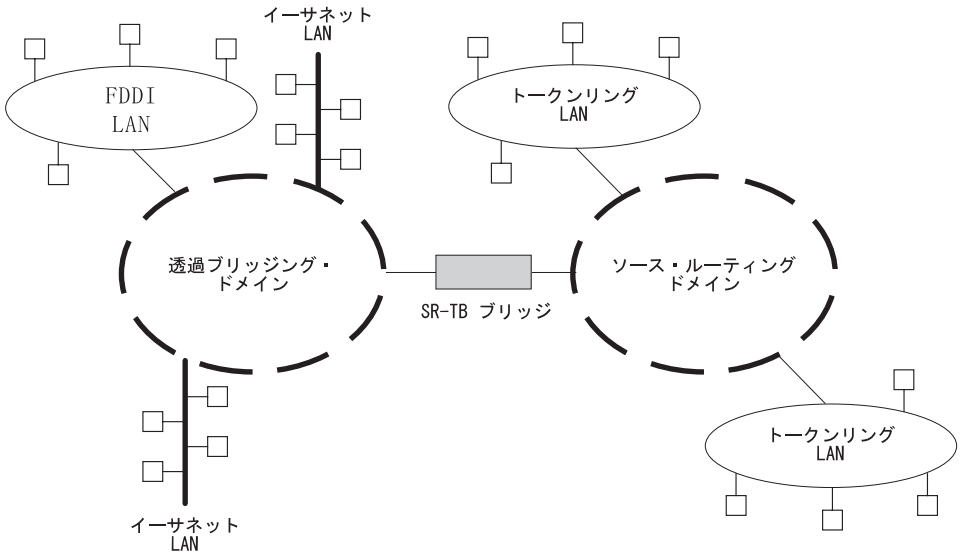


図 16. 2 つのドメインを接続する SR-TB ブリッジ

特定のソース・ルーティングおよび透過ブリッジングの操作

SR-TB ブリッジは *2 ポート装置* であり、1 つの MAC インターフェースがソース・ルーティング側の LAN セグメントに割り当てられ、もう 1 つのインターフェースが透過ブリッジング側の LAN セグメントに割り当てられています。各エンド・ステーションは、その LAN セグメント用の該当する MAC レイヤーを読み取ります。つまり、ブリッジング機能は、次の 2 つのタイプの操作に分けることができます。

- 透過ブリッジングの操作
- ソース・ルーティング・ブリッジングの操作

透過ブリッジング側では、SR-TB ブリッジが他の透過型ブリッジと同様に操作されます。ブリッジは、それが透過ブリッジング・ステーションであることを知っているステーションについてアドレスのテーブルをもっています。2 つ以上の SR-TB ブリッジが異なるドメインを結合するので、SR-TB ブリッジはネットワーク・スパンニング・ツリーを作成し、維持するのに必要な*ブリッジ間*プロトコルに従います。

SR-TB ブリッジがその透過ブリッジング・ステーションから受信したフレームをブリッジのソース・ルーティング側に転送するのは、フレームに入れて運ばれるあて先アドレスがブリッジの透過ブリッジング側のアドレス・テーブルに見つからない場合だけです。

ソース・ルーティング・ブリッジング側では、SR-TB ブリッジはソース・ルーティング・ブリッジおよびソース・ルーティング・エンド・ステーションの機能を特定の方法で結合します。ソース・ルーティング・エンド・ステーションとして、ブリッジはあて先アドレスとルーティング情報の関連をソース・ルーティング側に維持します。ブリッジは、ブリッジ自体の中のアプリケーション (例えば、ネットワーク管理) 用のエンド・ステーションとして、または透過型ブリッジング側のステーション用の仲介として通信します。

ブリッジング方式

SR-TB ブリッジがその透過ブリッジング・ステーションから受信したフレームをブリッジのソース・ルーティング側に転送するのは、フレームに入れて運ばれるあて先アドレスがブリッジの透過ブリッジング側のアドレス・テーブルに見つからない場合だけです。ブリッジのソース・ルーティング側によって伝送されるフレームは、ブリッジに関するルーティング情報がブリッジによって認知され、保持される場合に、それらの情報を運びます。

ソース・ルーティング・ブリッジとして、SR-TB ブリッジはルート発見プロセスに参加し、すでにルーティング情報を運んでいるフレームのルーティングに参加します。SR-TB ブリッジに固有なルート指定子は、そのソース・ルーティング側の個別の LAN の LAN 番号およびブリッジの個別のブリッジ番号から構成されます。

ブリッジは同様に、透過ブリッジング側のすべての LAN を表す単一の LAN 番号も維持します。SR-TB ブリッジは、表3に記述されているように、受信フレームと転送フレームの各ケースを別々に扱います。

表 3. SR-TB ブリッジのデシジョン・テーブル

受信されたフレームのタイプ	SR-TB ブリッジがとる処置
非ルーティング・フレームがソース・ルーティング・ステーションによって受信された。	ルーティング情報を運ぶフレームを複写または転送しない。
全ルート同報通信フレームがソース・ルーティング・ステーションによって受信された。	フレームを複写し、繰り返されたフレームの中で同報通信標識の A ビットおよび C ビットを設定する。あて先アドレスが透過ブリッジング・テーブルにある場合は、ブリッジはルーティング情報なしに透過ブリッジング・ネットワークにフレームを転送する。その他の場合は、フレームは転送されない。
単一ルート同報通信フレームがソース・ルーティング・ステーションによって受信された。 ブリッジは単一ルート同報通信ブリッジとして指定されていない。	フレームを複写または転送しない。
単一ルート同報通信フレームがソース・ルーティング・ステーションによって受信された。ブリッジは単一ルート同報通信ブリッジとして指定されている。	フレームを複写し、同報通信標識内の A ビットと C ビットを設定し、ルーティング情報をフレームから除去し、修正されたフレームを透過ブリッジング側に送る。保管されたルーティング情報フィールドにブリッジ番号と、透過ブリッジング側の LAN 番号を追加する。同報通信標識を非同報通信に変更し、D ビットを補足し、このルーティング情報をフレームの発信元アドレスに保管する。

表 3. SR-TB ブリッジのデシジョン・テーブル (続き)

受信されたフレームのタイプ	SR-TB ブリッジがとる処置
非同報通信フレームがソース・ルーティング・ステーションによって受信された。	フレームに特定のルートが含まれている場合は、ブリッジがルーティング情報を調べる。SR-TB ブリッジがルートの一部であり、ソース・ルーティング側の LAN 番号と透過ブリッジング側の LAN 番号の間にある場合は、ブリッジがフレームを複写し、その繰り返しフレーム内の A ビットと C ビットを設定する。フレームをルーティング情報なしで透過ブリッジング側に送る。ブリッジがその発信元アドレスの永続ルートをもっていない場合は、ブリッジがルーティング情報を複写し、D ビットを補足し、そのルーティング情報をフレームの発信元アドレスに保管する。
フレームが透過ブリッジング側から受信された。	フレームをソース・ルーティング側に送る場合、ブリッジはまず、あて先アドレスに関するルーティング情報をフレームがもっているかを判別する。もっている場合には、ブリッジはフレームにルーティング情報を追加し、RII を 1 に設定し、フレームをソース・ルーティング側の伝送の待ち行列に入れる。もっていない場合は、ブリッジはフレームに、単一ルート同報通信の標識および最初の 2 つの LAN 番号とそれ自身のブリッジ番号を含む 2 つのルート指定子をルーティング制御フィールドに追加する。

SR-TB ブリッジ : 4 つの例

SR-TB ブリッジは、ドメインの透過的結合により、ソース・ルーティング・ドメインと透過ブリッジング・ドメインを相互接続します。操作中、両方のドメインのステーションは相互の存在または SR-TB ブリッジの存在には気付きません。エンド・ステーションから見ると、結合されたネットワーク上のどのステーションも自分と同じドメインにあるように見えます。

以下の項では、SR-TB ブリッジで転送されるフレームの特定の例を記載します。これらの例では、SR-TB ブリッジが単一ルート同報通信ブリッジとして指定されているものと想定しています。40ページの図17 では、各項で記述される状況に付随する情報を記載します。

- Q はブリッジ自体のブリッジ番号です
- X はソース・ルーティング側の LAN の LAN 番号です
- Y は透過ブリッジング側の LAN の LAN 番号です
- A、B、C、および D はエンド・ステーションを表しています

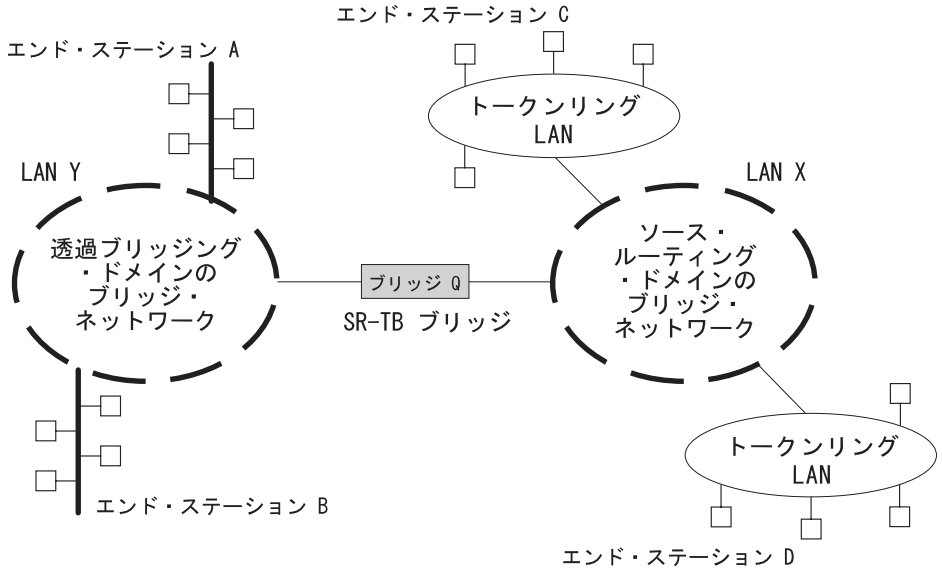


図 17. SR-TB ブリッジの例

例 1: エンド・ステーション A からエンド・ステーション B に送信されるフレーム

SR-TB ブリッジが、発信元アドレスがエンド・ステーション A であて先アドレスがエンド・ステーション B のフレームを受信すると、ブリッジはエンド・ステーション A のアドレスを透過ブリッジング側のアドレス・テーブルに入力します。このテーブルには、ブリッジの透過ブリッジング側にあることが知られているステーションのアドレスを含んでいます。これは透過ブリッジングの通常のプロセスです。

エンド・ステーション B のアドレスが透過ブリッジング側のアドレス・テーブルにある場合は、SR-TB ブリッジはフレームを転送しません。エンド・ステーション B のアドレスが透過ブリッジング側のアドレス・テーブルになく、ソース・ルーティング側のアドレス・テーブルにもない場合は、そのロケーションは SR-TB ブリッジには分かりません。この場合、フレームは、ルート探索の戻りの要求が付いていない単一ルート同報通信として、ソース・ルーティング側に転送されます。エンド・ステーション B によって送信されたフレームがあると (そのあて先とは無関係に)、そのアドレスは透過ブリッジングのアドレス・テーブルに追加されます。これにより、エンド・ステーション B にアドレス指定されたフレームが以降はソース・ルーティング側に転送されないようになります。

例 2: エンド・ステーション A からエンド・ステーション C に送信されるフレーム

この例では、エンド・ステーション A のアドレスは前の例と同様に扱われます。エンド・ステーション C のアドレスが透過ブリッジングのアドレス・テーブルにないのは確かなので、SR-TB ブリッジはフレームをソース・ルーティング側に転送します。

ブリッジは、次に、そのソース・ルーティング・アドレス・テーブルにエンド・ステーション C のアドレスがないか探します。このテーブルには、ブリッジのソース・

ルーティング側にあることが知られているステーションについて、すべての既知のアドレスが関連するルーティング情報とともに含まれています。 C のアドレスがソース・ルーティング・テーブルにある場合は、ブリッジはアドレス・テーブルにあるルーティング情報を使用してフレームを転送します。C のアドレスがソース・ルーティング・テーブルにない場合 (またはテーブルにあってもルーティング情報が空である場合)、ブリッジはフレームを、ルート探索の戻りの要求が付いていない単一ルート同報通信としてソース・ルーティング側に転送します。

エンド・ステーション C がこのフレームを受信すると、C はエンド・ステーション A のアドレスをそのソース・ルーティング・テーブルの中に、SR-TB ブリッジから作成されたルートの逆方向表示とともに入力し、それを一時的項目としてマークします。エンド・ステーション C が後でエンド・ステーション A にフレームを送信しようとするとき、この特定のルートを使用します。このルートは一時的としてマークされているので、フレームはルート探索の戻りの要求が付いた 非同報通信ルートとして送信されます。

戻ってくるフレームが SR-TB ブリッジに到達すると、フレームはルーティング情報なしに透過ブリッジング側に送られますが、エンド・ステーション C へのルートは一時的ルートとしてソース・ルーティング・テーブルに入力されます。それにより、エンド・ステーション C はエンド・ステーション A にアドレス指定されたフレーム用の最適なルーティングを選択することができます。このルーティングは、SR-TB ブリッジのソース・ルーティング・テーブルに永続ルートとして入力されることになります。

例 3: エンド・ステーション C からエンド・ステーション D に送信されるフレーム

フレームが非同報通信として送信され、 SR-TB ブリッジの接続先であるセグメントを横断する場合は、ブリッジは、RII フィールドを走査してルーティング・シーケンス (LAN X から ブリッジ Q を経て LAN Y まで) を調べます。ブリッジはこのシーケンスを見つけることができないので、フレームを送りません。

フレームが単一ルート同報通信として送信される場合、エンド・ステーション D がソース・ルーティング側にあることが既知であると、ブリッジはフレームを廃棄します。 エンド・ステーション D がソース・ルーティング側にあることが知られていない場合は、ブリッジはフレームを透過ブリッジング側に (ルーティング情報なしに) 送り、ルーティング情報に 『Q から Y へ』を追加します。最後に、ブリッジはエンド・ステーション C へのルーティング情報を一時的ルートとしてソース・ルーティング・テーブルに保管します。その際、非同報通信標識および方向ビットを補足します。

フレームが全ルート同報通信として送信される場合は、SR-TB ブリッジはフレームを廃棄し (これは、エンド・ステーション D のアドレスが透過ブリッジング・アドレス・テーブルにないためです)、エンド・ステーション C のアドレスがソース・ルーティング・テーブルにあることを学習します。

例 4: エンド・ステーション C からエンド・ステーション A に送信されるフレーム

フレームが非同報通信で送信される場合、ブリッジは RII フィールドを走査して、ルーティングのシーケンス (X から Q を経て Y まで) を調べます。ブリッジがそのシーケンスを見つけると、ブリッジはフレームを透過ブリッジング側に送ります。ブリッジはエンド・ステーション C へのルーティング情報も保管します。

フレームが単一ルート同報通信として送信される場合、ブリッジはフレームを (ルーティング情報なしに) 透過ブリッジング側に送り、ルーティング情報に 『Q から Y へ』を追加します。 またブリッジは、非同報通信標識を設定し、方向ビットを補足し、そのソース・ルーティング・テーブルの C のアドレスにルーティング情報を入力します。

エンド・ステーション C 用の一時的項目がソース・ルーティング・テーブルにすでに存在する場合は、SR-TB ブリッジはルーティング情報を更新します。フレームが全ルート同報通信として送信される場合、ブリッジはそのフレームを廃棄しますが、エンド・ステーション C のアドレスがソース・ルーティング・テーブル内にあるか確認します。

SR-TB およびフレーム・リレー

フレーム・リレー・インターフェースでは、ブリッジングが回線上で使用可能になっている限り、ブリッジされたフレームをすべて該当するブリッジング転送側に転送することによって、SR-TB ブリッジングをサポートします。

SR-TB および ATM

ATM インターフェースは、ブリッジされたフレームをすべて該当するブリッジング転送側に転送することによって、SR-TB ブリッジングをサポートします。ただし、VCC でブリッジングが使用可能になっていることが条件になります。

ソース・ルーティング - 透過型ブリッジ (SR-TB) の用語および概念

この項では、SR-TB ブリッジングで使用される用語および概念を説明します。

全ルート同報通信

ブリッジされた LAN で重複しないすべてのルートを通じてフレームを送信するプロセス。

全ステーション同報通信

フレームが現れるリング上の各ステーションがフレームを複写するように、フレームをアドレス指定する (あて先アドレスにすべて 1 を入れる) プロセス。

ブリッジ

ローカル・エリア・ネットワーク (LAN) を接続するプロトコルに依存しない装置。ブリッジはデータ・リンク・レイヤーで働き、LAN 間でデータ・パケットを保管し、転送します。

ブリッジ番号

ブリッジを識別する固有の番号。同じ 2 つのリングを接続する複数のブリッジを区別します。

探索フレーム

ソース・ルーティング・ブリッジは、フレームをネットワークを通じてその宛先のエンド・ステーションに転送するときに、探索フレームにルーティング情報を追加します。探索フレームはルートを発見します。探索フレームには次の 2 つのタイプのものがあります。全ルート探索 (ARE) フレームおよびスパンニング・ツリー探索 (STE) フレームです。 ARE フレームはすべてのポートによって転送されるのに対し、STE フレームはスパンニング・ツリー・プロトコルによりフレームを転送するよう割り当てられているポートによってのみ転送されます。

リング番号

ブリッジされたネットワーク内のリングを識別する固有の番号

ルート

一連の LAN およびブリッジ (例えば、ソース・ルーティング・ブリッジ) を通過するパス

ルート指定子

ネットワークを通過するルートを作成するのに使用される、ルーティング情報フィールド内のリング番号およびブリッジ番号

ルート発見

あて先エンド・ステーションへのルートを学習するプロセス

セグメント番号

セグメント番号は、個々の LAN (単一のトークンリングまたはシリアル回線など) を識別します。セグメントはブリッジに接続していますが、独立して動作することもできます。

単一ルート同報通信

ネットワーク内の各リングでフレームの 1 つのコピーだけが現れるようにして、ネットワークを通じてフレームを送信するプロセス

ソース・ルート・ブリッジング

フレーム内にそれが進むルートを指定することによって、複数 LAN ネットワークを通じてフレームを転送するブリッジング・メカニズム

スパンニング・ツリー

任意の 2 つのエンド・ステーション間にあるデータ・ルートが 1 つだけである、ブリッジのトポロジー

透過ブリッジング

エンド・ステーションにとって*透過*のメカニズムを使用するブリッジングのタイプの 1 つ。透過ブリッジングは、スパンニング・ツリー・アルゴリズムでデータ・フレームを転送するよう指定されたブリッジによってローカル・エリア・ネットワーク・セグメントを相互接続します。

透過-ソース・ルーティングの互換性 - 問題点および解決法

まず第一に、ASRT ブリッジは、ソース・ルーティング・ブリッジ変換 (SR-TB) を通じて、通常のソース・ルーティング・ブリッジと互換性のある透過型ブリッジを提供します。SR-TB は本来、802.5 仕様の一部として提案されたものでした。この方式は IBM の 8209 変換ブリッジと類似しており、それと相互に運用することができます。

SR-TB は透過ブリッジング・フレームをソース・ルーティング・フレームに変換し、その逆の変換も行います。つまり、必要に応じて RIF を挿入または除去することにより、透過型ブリッジまたはソース・ルーティング・ブリッジのどちらかとして機能します。この機能によって、パケットは、イーサネット LAN と SRT トークンリング LAN の間で移動でき、なお導入済み基本のソース・ルーティング・トークンリング LAN との互換性をもつこともできます。

パケット・サイズの問題の除去

SR-TB は、イーサネット・ドメインを使ってブリッジされているトークンリングのパケット・サイズの問題も除去します。この構成では、エンド・ステーションは、ソース・ルーティング・プロトコルを使用するので、エンド・ステーション間に最大フレーム・サイズが 1518 バイトのネットワークがあるかどうか動的に判別できます。エンド・ステーションは手動で再構成せずにこの限度を自動的に受け入れます。逆の状況の、イーサネットをトークンリング・ドメインを横断してブリッジする場合では、パケット・サイズは問題になりません。これはトークンリングのパケット・サイズの許容度がはるかに大きいからです。

ハードウェア・アドレス・フィルター

ASRT ブリッジによって提供されるもう 1 つの主要なフィーチャーは、ハードウェア・アドレス・フィルターです。ハードウェア・アドレス・フィルターは、イーサネットおよびトークンリングの LAN 技術にあるパケット確認方式の矛盾を解決します。これは MAC レイヤーで起こり、宛先 MAC アドレスに基づいて確認ビットを正しくセットする唯一の技法です。ASRT ブリッジは、ハードウェア・アドレス・フィ

ルターを実行するのに内容アドレス指定メモリー (CAM) を使用します。この技術により、ブリッジは、MAC アドレスを瞬時に調べることにより、パフォーマンスを損なうことなくより高度な機能を効果的にもつことになります。

STB および SRB ブリッジにおけるビット配列

異なる MAC アドレス・タイプをもつ LAN を接続するためにブリッジが継続的に構築されるため、データ伝送時のビット配列はこれらの技術の相互運用性に影響を及ぼします。

MAC アドレスを管理する際、IEEEは 48 ビットの IEEE として知られる広く割り当てられる固有の MAC アドレスを割り当てます。これらのアドレスは、802.3、802.4、802.5 の LAN でサポートされます。このアドレス指定方式が開発された時期に標準が欠けていたために、2 つの異なる状況が発生しました。

- 802.3 (イーサネット) と 802.4 の LAN では、発信元アドレスとあて先アドレスは、グループ・ビットを最初に送信し、LLC データ・フィールドは、最下位ビット (LSB) を最初に送信していました。
- 802.5 (トークンリング) LAN では、発信元アドレスとあて先アドレスは、グループ・ビットを最初に送信し、LLC データ・フィールドは、最上位ビット (MSB) を最初に送信していました。

注: 単純化するために、802.3 および 802.4 のブリッジおよび LAN は、ここでは LSB ブリッジおよび LAN と呼びます。 802.5 のブリッジと LAN は、MSB ブリッジと LAN と呼びます。

ビット伝送標準が異なるため、LSB から MSB の LAN へのブリッジは、MAC フレームの開始時にはあて先と発信元の MAC アドレスのビット配列を反転する必要があります。これは、異なる LAN タイプが MAC アドレスについて同じビット配列 (つまり、グループ・ビットが最初) を使用しているのに対し、ユーザー・データについては異なるビット配列 (LSB または MSB が最初) を使用しているからです。

ビット配列が逆であるために生じるアドレスの解釈ミスに加えて、高水準の通信プロトコルのいくつかは MAC アドレスをまったく誤って解釈します。IP や Novell IPX などのプロトコルは、ブリッジ・アドレスを誤って解釈します。これは、それらが最初に開発された時期に、MAC アドレス表示の標準がなかったからです。

ビット配列の違いは、ブリッジング技術 (データ・リンク・レイヤー技術) をルーティング技術 (ネットワーク・レイヤー技術) と組み合わせることにより、最善の解決がなされます。ユーザーに今日の通信プロトコルを『逆構築 (リバース・エンジニア) し』、各ブリッジをケース・バイ・ケースでアドレスを『反転 (フリップ)』するか逆にするよう構成するように依頼するのではなく、これらのプロトコルをルートすることによって、問題はもっと簡単に解決されます。

ルーティングは、上位レイヤーで稼働する詳細なパケット・アドレスにアクセスすることにより、ビットの配列とプロトコルのアドレス指定の問題を除去します。ルーティングだけでは、他のプロトコル (IBM フレームおよび NetBIOS など) はルーティングすることができないし、SNA ルーティングは制限されるため、完全な解決策にはなりません。したがって、SRTを、ブリッジとルーティングが協力して働く装置で実現することが重要です。

ASRT 構成の考慮事項

ASRT ブリッジは、IEEE 802.1D ブリッジの標準で記述されるスパンニング・ツリーのプロトコルおよびアルゴリズムをすべてのインターフェースを通じて使用しています。異なるタイプのブリッジが存在する環境では 2 つ以上のスパンニング・ツリーが形成されることがあります。例えば、IEEE 802.1d プロトコル (例えば、STB および SRT) を実行するすべてのブリッジのスパンニング・ツリーが IBM 8209 ブリッジの別のツリーと共存することが可能です。この構成から生じるループは、修正が必要です。

TCP/IP ホスト・サービスは SDLC リレーをサポートします。IP ルーターとしてではなく、純粋なブリッジとして稼働している場合、IP ルーターに通常関連している機能は使用できません。例えば、 BootP 転送側機能または ARP サブネットルーティング機能は使用できません。

ASRT 構成マトリックス

ASRTブリッジでは、ブリッジおよび接続されたすべてのインターフェースについての構成パラメーターの集合から、そのブリッジについての*ブリッジ固有性*が生じます。 次のマトリックスでは、ユーザーのネットワークを扱うために必要なブリッジ固有性を生じさせるため、各インターフェース・タイプの構成設定値の手引きを示します。

ブリッジ固有性	SR <-> TB 変換は使用可能か ?	インターフェース・タイプとブリッジング方式設定値			
		トークンリング	イーサネット	シリアル回線またはトンネル	ATM
STB	No	TB	TB	TB	TB
SRB	No	SR	--	SR	SR
STB & SRB	No	SR	TB	TB または SR	TB または SR
SR-TB	Yes	SR	TB	TB	TB
SR-TB	Yes	SR	TB	SR	SR
SRT	No	SR & TB	TB	SR & TB	SR & TB
ASRT	Yes	SR & TB	TB	SR & TB	SR & TB
ASRT	Yes	SR	TB	SR & TB	SR & TB
ASRT	Yes	SR または TB	TB	SR & TB	SR & TB

ブリッジ固有性のキー:
STB = 透過 (スパンニング・ツリー) ブリッジ
SRB = ソース・ルーティング・ブリッジ
SR-TB = ソース・ルーティング透過型変換ブリッジ
SRT = ソース・ルーティング透過型ブリッジ
ASRT = 適応ソース・ルーティング透過型ブリッジ

ブリッジング方式のキー:

SR = ソース・ルーティング TB = 透過ブリッジング

ブリッジング方式

第3章 ブリッジングのフィーチャー

この章では、適応ソース・ルーティング透過型 (ASRT) ブリッジで使用可能なブリッジングのフィーチャーについて説明します。この章には次の節が含まれています。

- 『ブリッジ・トンネル』
- 51ページの『TCP/IP ホスト・サービス (ブリッジ専用管理)』
- 51ページの『ブリッジ - MIB サポート』
- 52ページの『NetBIOS 名前キャッシュ』
- 52ページの『NetBIOS 重複フレーム・フィルター』
- 52ページの『NetBIOS の名前フィルターとバイト・フィルター』
- 55ページの『複数スパンニング・ツリー・プロトコル・オプション』
- 57ページの『スレッド化 (ルーター発見)』
- 59ページの『ATM を介したブリッジング』
- 60ページの『マルチアクセス・ブリッジ・ポートについて』

ブリッジ・トンネル

ブリッジ・トンネル (カプセル化) は、ASRT ブリッジ・ソフトウェアのもう 1 つのフィーチャーです。パケットを業界標準の TCP/IP パケット内のカプセルとすることにより、ブリッジ・ルーターはこれらのパケットを大きな IP インターネットワークを通じてあて先エンド・ステーションへ動的にルートすることができます。

エンド・ステーションは IP パス (トンネル) を、ネットワークの複雑さとは無関係に、単一のホップとして見ます。これにより、ソース・ルーティング構成で検出される通常の 7 ホップの距離の制限を克服することができます。これにより、ソース・ルーティング・エンド・ステーションを非ソース・ルーティング媒体 (イーサネット・ネットワークなど) 越しに接続することができます。

ブリッジ・トンネルは通常のソース・ルーティングのいくつかの制限も克服します。制限には次のものが含まれます。

- 7 ホップの距離の制限
- ソース・ルーティングが広域ネットワーク (WAN) で生じる大きいオーバーヘッド
- ソース・ルーティングが WAN の障害および故障に敏感であること (パスに障害が起こると、すべてのシステムは伝送を再始動する必要がある)

ブリッジ・トンネル・フィーチャーが使用可能になっていると、ソフトウェアはパケットを TCP/IP パケット内にカプセル化します。ルーターにとっては、パケットは TCP/IP パケットのように見えます。フレームが IP エンベロープ内にカプセル化されると、IP 転送機能は、あて先 IP アドレスに基づいて該当するネットワーク・インターフェースを選択する役目をします。このパケットは、性能低下またはネットワーク・サイズの制限なしに、大きなインターネットワークを通じて動的にルートすることができます。ソース・ルーティング・エンド・ステーションは、ネットワーク

の複雑さとは無関係に、このパスを単一のホップと見なします。 図18 は、構成内にトンネル機能を使用する IP インターネットワークの例を示しています。

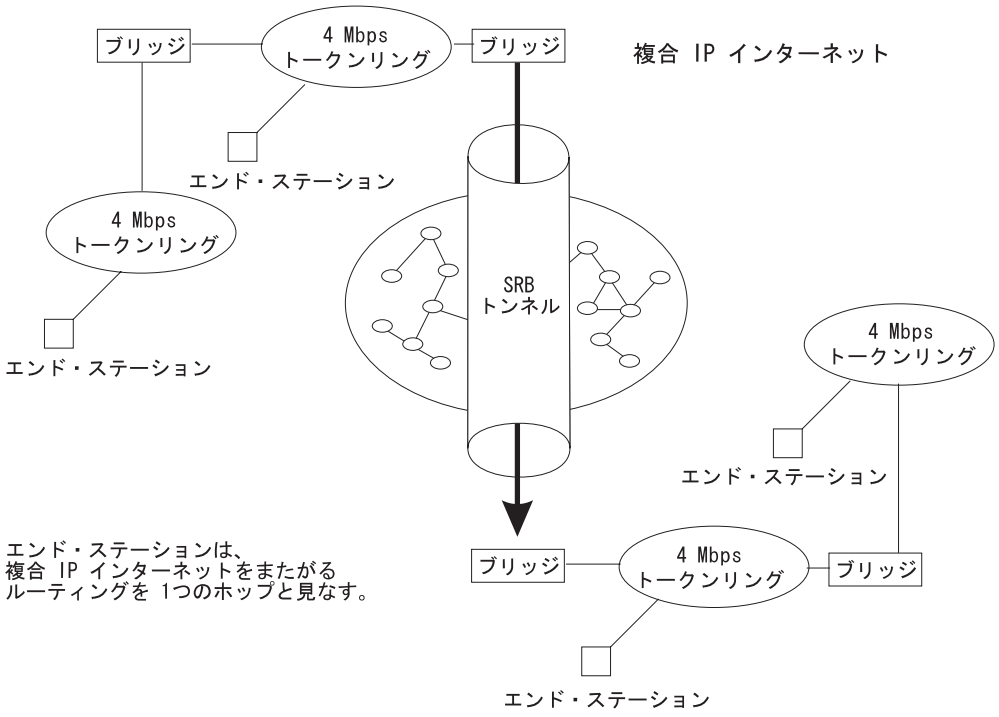


図 18. ブリッジ・トンネル・フィーチャーの例

トンネルはエンド・ステーションには透過です。トンネル・フィーチャーに参加するブリッジング・ルーターは IP インターネットをブリッジ・セグメントの 1 つとして扱います。パケットがあて先インターフェースに到達すると、TCP/IP ヘッダーは自動的に除去され、内側のパケットは標準のソース・ルーティング・パケットとして進みます。

カプセル化および OSPF

カプセル化フィーチャーの主な利点は、ルーティング・プロセスに OSPF の動的ルーティング・プロトコルを追加できることです。OSPF は、カプセル化フィーチャーとともに使用される場合に、次の利点を提供します。

- *最小コストのルーティング*。 OSPF では、遅延を最小に抑えて最高速パス (トンネル) にアクセスするので、ネットワーク管理者は、費用が最も少ないルートにトラフィックを配分できます。
- *動的ルーティング*。OSPF は最小コストのパスを探すとともに、障害を検出し、トラフィックを少ないオーバーヘッドでう回させます。
- *マルチパス・ルーティング*。負荷分担により、使用可能な帯域幅をより効率的に使用することができます。

OSPF を使用すると、トンネルはインターネットワーク内でパスを自動的に管理します。パス上の回線またはブリッジが故障している場合には、トンネル・ブリッジがトラフィックを新しいパスに沿って自動的にう回させます。パスが復元されると、トンネルは自動的に最良のパスに更新されます。このう回はエンド・ステーション

には完全に透過です。OSPF について詳しくは、333ページの『第16章 OSPF の使用』で始まる構成と監視の章を参照してください。

TCP/IP ホスト・サービス (ブリッジ専用管理)

ブリッジング・ルーターは TCP/IP ホスト・サービスもサポートします。このサービスにより、ルーティング機能が使用不能になったときに、ブリッジを構成し、管理することができます。このオプションには次の機能があります。

- SNMP を通じての管理
- Telnet サーバー機能
- TFTP プロトコルを通じての構成のダウンロードおよびアップロード
- TFTP 近隣ブート機能
- PING およびルート追跡の IP 診断ツール
- SNMP セットおよび telnet クライアントを通じての装置の制御

ブリッジの監視インターフェースから見ると、TCP/IP ホスト・サービスは、それ自体の構成と監視プロンプトをもつ新しいプロトコルとして扱われます。これらのプロンプトには、`talk 6` および `talk 5` において **protocol** コマンドを介してアクセスします。

ブリッジ専用管理機能は、ブリッジに IP アドレスを割り当て、 TCP/IP ホスト・サービスを使用可能にする (221ページの『第12章 TCP/IP ホスト・サービスの構成と監視』を参照) ことによって、活動化されます。この IP アドレスは、単一のインターフェースに関連しているのではなく、ブリッジ全体に関連しています。ネットワークを通じてブートするとき、ブリッジの IP アドレスおよび省略時のゲートウェイはブート PROM 付きの ROMCOMM インターフェースを通じて自動的に学習することができます。省略時のゲートウェイの割り当てはユーザーが構成することもできます。

TCP/IP ホスト・サービスが使用可能なのは、ルーターのソフトウェア・ロードでブリッジングの選択が任意である場合です。

ブリッジ - MIB サポート

SNMP を介するブリッジ管理の場合、IBM Nways マルチプロトコル・ルーティング・サービス は RFC 1493 および RFC 1525 で指定されている管理情報ベース (MIB) をサポートしますが、下記の MIB は***除きます***。

- dot1dStaticTable
- dot1dTpFdbTable
- dot1dPortPairTable

NetBIOS 名前キャッシュ

NetBIOS 名前キャッシュ・フィーチャーにより、ブリッジング・ルーターは、発信元リングから出され、ブリッジを介して転送される名前照会 (Name-Query) フレームの数を大幅に減らすことができます。NetBIOS 名前キャッシュの構成は、NetBIOS 構成の一環として行われます。詳細は、161ページの『NetBIOS 名前キャッシュおよびルート・キャッシュ』に記載してあります。

NetBIOS 重複フレーム・フィルター

3 つのフレーム・タイプが 6 つのグループで送信されるのが普通です。

- 名前照会
- 名前追加
- グループ名追加

重複フレーム・フィルターはタイマーを使用して、ユーザーが設定した時間内にブリッジを介して各タイプのフレームのうち 1 つのインスタンスだけが転送できるようにします。

このプロセスは名前キャッシュで使用されるデータベースとは別のデータベースを使用します。重複フレーム・データベース項目は、クライアントの MAC アドレスおよび、上述の各フレーム・タイプごとに 1 つずつ、3 つの時刻スタンプを含んでいます。重複フレーム・フィルターは名前キャッシュの前に処理されます。詳細は、153ページの『重複フレーム・フィルター』に記載してあります。

NetBIOS の名前フィルターとバイト・フィルター

NetBIOS フィルターは、その使用によって ASRT ブリッジングのパフォーマンスの向上を図ることができるフィーチャーです。このフィーチャーでは、ルーター構成プロセスを使用して特定のフィルターを構成することができます。NetBIOS フィルターは、NetBIOS パケットに適用されて、パケットをブリッジ (転送) するかフィルター (除去) するかを判別するための規則の集合です。

NetBIOS フィルターのタイプ

NetBIOS フィルターには、*ホスト名* と *バイト* の 2 つのタイプがあります。

ホスト名

ホスト名フィルターでは、ブリッジまたはフィルターしたい特定の NetBIOS ホスト名をもつパケットを選択することができる、NetBIOS パケット内のフィールドを使用します。ホスト・サービスはブリッジング専用です。ホスト名フィルターは、フレーム・タイプに応じて、NetBIOS 発信元名またはあて先名に基づいて使用することができます。

名前フィルターは、ブリッジ中またはデータ・リンク交換中の NetBIOS トラフィックに適用されます。

バイト バイト・フィルターでは、ブリッジまたはフィルターしたい特定の NetBIOS パケットが指定できる、NetBIOS パケット内のバイト (散在フィールド) を使用します。

これらのフィルターには対応するしきい値もタイマーもないので、使用不能にするか除去するかしない限り、これらのフィルターはアクティブに保たれます。NetBIOS フィルターは、3 つの部分で構成されます。つまり、実際のフィルター、フィルター・リスト、およびフィルター項目という 3 つの部分から構成されます (詳細については54ページの『フィルターの構築』の項で説明します)。

NetBIOS の構成と監視については、171ページの『第8章 NetBIOS の構成と監視』で説明します。この節の以下の各項では、NetBIOS ホスト名フィルターおよび NetBIOS バイト・フィルターについて説明します。

NetBIOS ホスト名フィルター

ホスト名の使用による NetBIOS フィルターでは、ブリッジまたはフィルターしたい、特定の NetBIOS ホスト名をもつパケットを選択することができます。特定の NetBIOS ホスト名 (または NetBIOS ホスト名の集合) をもつパケットをブリッジするかフィルターするかを指定すると、次の NetBIOS パケット・タイプの送信元名フィールドまたは宛先名フィールドが検査されます。

- ADD_GROUP_NAME_QUERY (発信元)
- ADD_NAME_QUERY (発信元)
- DATAGRAM (あて先)
- NAME_QUERY (あて先)

ホスト名フィルター・リストでは、上記の 4 つの異なるタイプの NetBIOS パケット内の発信元名フィールドまたはあて先名フィールドと比較する必要がある NetBIOS 名を指定します。上記の 4 つのタイプのいずれか 1 つではない NetBIOS パケットにホスト名フィルター・リストを適用すると、結果は*組み込み* になります。

ホスト名を使用して NetBIOS フィルターを構成するときは、どのポートにフィルターを適用するか、また、フィルターがこれらのポートの入力パケットまたは出力パケットのいずれに適用されるのかを指定します。NetBIOS 無番号情報 (UI) パケットのみがフィルターの対象と見なされます。フィルターは、ソース・ルート・ブリッジング (すべての RIF タイプ) または透過ブリッジングのいずれかについて、ルーターに到達する NetBIOS パケットに適用されます。

フィルターで NetBIOS ホスト名を指定するときは、名前の 16 番目の (最後の) 文字を、別個の引き数として、その 16 進数の形で表すことができます。こうすると、名前の最初の 15 バイトは指定されたものとみなされ、16 番目のバイト (指定されている場合) は、最終引き数によって判別されます。指定した文字数が 16 文字未満である (しかも 16 番目のバイトが指定されていない) 場合は、名前には 15 番目の文字まで ASCII ブランク文字が埋め込まれ、16 番目の文字はワイルドカードとして処理されます。

特定の NetBIOS ホスト名が評価されるとき、その名前は特定の NetBIOS パケットの特定のフィールドとだけ比較されます。フィルター項目内の NetBIOS ホスト名には、NetBIOSホスト名内の任意の点にワイルドカード文字 (?) 、または NetBIOS ホスト名

の最後の文字としてアスタリスク (*) を組み込むことができます。「?」は、ホスト名の中の任意の 1 文字に対応します。「*」はホスト名の終わりにある任意の 1 文字または複数文字に対応します。

NetBIOS バイト・フィルター

もう 1 つのフィルター・メカニズムとしてバイト・フィルターがあり、これを使用すると、MAC アドレスに関連する NetBIOS パケット内のフィールドに基づいて、ブリッジまたはフィルターするパケットを指定することができます。この場合、すべての NetBIOS パケットを調べて、構成されたフィルター基準に合うかどうかを判別します。

バイト・フィルターを構築する場合は、以下のフィルター項目を指定します。

- NetBIOS ヘッダーの先頭からのオフセット
- 突き合わせの対象となるバイト・パターン
- NetBIOS ヘッダーの選択されたフィールドに適用される任意指定のマスク

マスク (存在する場合) の長さは、バイト・パターンの長さに等しいことが必要です。マスクでは、ルーターがヘッダーのバイト数を 16 進パターンと比較して等しいかどうかを調べる前に、NetBIOS ヘッダー内のバイト数とともに論理的に AND 結合されるバイト数を指定します。マスクを指定しない場合は、すべてが 1 であるものとみなされます。16 進パターン (したがって、マスク) の最大長は 16 バイト (32 桁の 16 進数) です。

特定のバイトを使用して NetBIOS フィルターを構成するときは、フィルターがどのポートに適用されるのか、またフィルターがこれらのポートの入力パケットまたは出力パケットのいずれに適用されるかを指定します。

フィルターの構築

各フィルター・リストは 1 つ以上のフィルター項目から構成されます。各フィルター・リストは 1 つ以上のフィルター項目から構成されます。各フィルター項目は、フィルター項目が指定された順序で、パケットと比較して評価されます。

フィルター項目とパケットの間に一致が見つかった場合、ルーターにより次のことが行われます。

- フィルター・リストが*組み込み* と指定されていれば、パケットをブリッジします。
- フィルター・リストが*排除* と指定されていれば、パケットを除去します。

フィルター・リストのフィルター項目で一致が見つからない場合には、ルーターにより次のことが行われます。

- フィルターが全体として*組み込み* と指定されている場合は、パケットを転送します。
- フィルターが全体として*排除* と指定されている場合は、パケットを除去します。

フィルター項目は、NetBIOS パケットの特定のフィールドに適用される単一の規則です。規則の適用の結果は、組み込み (ブリッジ) または排除 (フィルター) の指示のど

ちらかです。以下に挙げるフィルター項目は、NetBIOS フィルターで構成できます (最初の 2 つの項目はホスト名フィルターで、後の 2 つの項目はバイト・フィルターです)。

- NetBIOS ホスト名の任意指定の 16 番目の文字 (16 進数) を組み込む。
- NetBIOS ホスト名の任意指定の 16 番目の文字 (16 進数) を排除する。
- 10 進バイト・オフセットを、そのオフセットの 16 進数マスクから始めて、NetBIOS ヘッダーの 16 進パターンに組み込む。
- 10 進バイト・オフセットを、そのオフセットの 16 進数マスクから始めて、NetBIOS ヘッダーの 16 進パターンから排除する。

フィルターの指定の一部によって、フィルター・リスト内のフィルター項目のいずれにも一致しないパケットをブリッジする (組み込む) か、フィルターする (排除する) かを指定します。これはフィルター・リストについての省略時アクションです。フィルター・リストについての省略時アクションは最初は組み込みに設定されていますが、この設定値はユーザーが変更できます。

単純フィルターおよび複合フィルター

単純フィルターは、1 つのフィルター・リストをルーター・ポート番号および入出力指定と組み合わせることにより作成されます。これは、フィルター・リストを、所定のポートで受信または送信されるすべての NetBIOS パケットに適用する必要があることを示しています。フィルター・リストが組み込みと評価される場合には、考慮されているパケットはブリッジされます。そうでない場合は、パケットはフィルターされます。

複合フィルターは、ポート番号、入出力指定、および論理演算子 and または or のどちらかによって区切られた複数のフィルター・リストを指定することによって、作成することができます。複合フィルター内のフィルター・リストは厳密に左から右へと評価され、複合フィルター内の各フィルター・リストが評価されます。各組み込みフィルター・リストの結果は、それぞれ真として扱われ、各排除フィルター・リストの結果は、それぞれ偽として扱われます。すべてのフィルター・リストおよびそれらの演算子をパケットに適用した結果は、真または偽となり、それぞれパケットがブリッジまたはフィルターされることを示します。入力/ポートまたは出力/ポートの各組み合わせがもつことのできるフィルターは、多くても 1 つです。

複数スパンニング・ツリー・プロトコル・オプション

ASRT ブリッジによりスパンニング・ツリー・プロトコル・オプションを拡張して、できるだけ多くの構成オプションに適用することができます。以下の項では、これらのフィーチャーに関する情報を提供します。

背景 : 複数スパンニング・ツリー・プロトコルの問題

ブリッジング技術は、異なるブリッジ方式をサポートするために異なるバージョンのスパンニング・ツリー・アルゴリズムを使用します。各アルゴリズムの共通の目的は、ループのないトポロジーを作成することです。

透過型ブリッジ (TB) によって使用されるスパンニング・ツリー・アルゴリズムでは、Hello BPDU およびトポロジー変更通知 (TCN) BPDU は、透過フレームに入れてすべての参加媒体 (トークンリング、イーサネット、その他) のすでに認識されているグループ・アドレスに送信されます。この交換された情報からテーブルが作成され、ループのないトポロジーが計算されます。

ソース・ルーティング・ブリッジ (SRB) は、スパンニング・ツリー探索 (STE) フレームを他の SRB ブリッジを通じて伝送して、ループのないトポロジーを判別します。このアルゴリズムはハロー BPDU を透過フレームに入れて、すでに認識されている機能アドレスに送信します。TCN BDPU は SRB によって使用されないので、このスパンニング・ツリー・アルゴリズムの結果として作成されるポート状態の設定は全ルート探索 (ARE) フレームおよび特定ルーティング・フレーム (SRF) のトラフィックに影響を及ぼしません。

IBM 8209 ブリッジを使用するブリッジ構成では、並列 8209 ブリッジを検出するのに異なるスパンニング・ツリー方式が使用されます。このアルゴリズムはトークンリング上の IEEE 802.1d グループ・アドレスに STE フレームとして送信されるハロー BPDU を使用します。イーサネット上では、同じグループ・アドレスに透過フレームとして送信されるハロー BPDU が使用されます。この方式では、8209 は透過型ブリッジやその他の IBM 8209 ブリッジを使ってスパンニング・ツリーを作成できます。 この方式は SRB スパンニング・ツリー・プロトコルに参加しませんが、SRB によって送信されるハロー BPDU はフィルターされます。したがって、8209 がルート・ブリッジになるのを防ぐ方法はありません。8209 ブリッジがルートとして*選択*された場合には、2 つの透過型ブリッジ・ドメイン間のトラフィックはトークンリング/SRB ドメインを通過しなければならない場合があります。

お分かりのように、複数のスパンニング・ツリー・プロトコルを稼働すると、アルゴリズムがそれ自体のループのないトポロジーを作成する方法について互換性の問題が生じます。

STP/8209

STP/8209 ブリッジングのフィーチャーを使用して、スパンニング・ツリー・プロトコルをさらに拡張することができます。 以前は、SRB ではトークンリングを介してのループのないツリーは手動で構成することしかできませんでした。これは、並列 SR-TB ブリッジの場合にループを防止できる唯一のメカニズムでした。STP/8209 フィーチャーを追加すると、次のスパンニング・ツリー・アルゴリズムの組み合わせが可能です。

- 純粋な透過型ブリッジ (TB) - IEEE 802.1d スパンニング・ツリー・プロトコルが使用されます。
- 純粋なソース・ルーティング・ブリッジ (SRB) - SRB スパンニング・ツリー・プロトコルが使用されます。
- 別個のエンティティーとしての透過型ブリッジおよびソース・ルーティング・ブリッジ - TB にはIEEE 802.1d スパンニング・ツリー・プロトコルが使用され、SRB には手動構成 (スパンニング・ツリー・プロトコル) が使用されます。
- SR-TB ブリッジ - TB および SR-TB の単一のツリーを作成するには、TB ポートでは IEEE 802.1d スパンニング・ツリー・プロトコルが使用され、SRB ポートでは IBM 8209 BPDU が使用されます。SRB ハロー BPDU は SR ドメインを通過

することはできますが、処理されません。IBM 8209 ブリッジはそのようなフレームをフィルターしますが、これが許されるのは、このブリッジが 2 ポートのブリッジで他のポートが TB ポートであるためです。

- 純粋な SRT ブリッジ - IEEE 802.1d スパンニング・ツリー・プロトコル**のみ** が使用されます。SRB ハロー BPDU および IBM 8209 BPDU は通過することはできますが、処理されません。
- ASRT ブリッジ - TB および SRT ブリッジを使ってツリーを作成するために、IEEE 802.1d スパンニング・ツリー・プロトコルが使用されます。『8209 類似』 BPDU はすべての SR インターフェースでも生成されます。これらの BPDU は受信されるとすぐに処理されます。これにより、すべての SR インターフェースで 2 つの BPDU が生成され、受信されます。両方の BPDU は同じ情報を運ぶので、ポート情報に矛盾は生じません。これにより、ASRT ブリッジは他の TB および SRT ブリッジに加えて、IBM 8209 および SR-TB ブリッジとともにスパンニング・ツリーを作成できます。

スレッド化 (ルーター発見)

スレッド化はトークンリングのエンド・ステーションのネットワーク・プロトコル (例えば、IP、IPX、または AppleTalk) がソース・ルーティング・ブリッジ・ネットワークを通じて別のエンド・ステーションを発見するプロセスです。

スレッド化プロセスの詳細は、エンド・ステーションのプロトコルによって異なります。以下の項では、IP、IPX、および AppleTalk についてのスレッド化のプロセスを説明します。

ARP を使用しての IP スレッド化

IP エンド・ステーションは ARP REQUEST および REPLY パケットを使用して、RIF を発見します。IP エンド・ステーションおよびブリッジは両方とも、ルート発見および転送プロセスに参加します。以下のステップは IP スレッド化プロセスを説明しています。

1. IP エンド・ステーションは ARP テーブルおよび RIF テーブルを維持します。ARP テーブル内の MAC アドレスは、RIF テーブル内のあて先 RIF を相互参照するために使用されます。その特定の MAC アドレスへの RIF が存在しない場合、エンド・ステーションは ARE (全ルート探索) または STE (スパンニング・ツリー探索) を指定した ARP REQUEST パケットをローカル・セグメントへ伝送します。
2. ローカル・セグメントにあるすべてのブリッジは ARP REQUEST パケットを取り込み、それを接続されたネットワークを通じて送信します。

   ARP REQUEST パケットがあて先エンド・ステーションの探索を継続する間、パケットを転送する各ブリッジはそれ自体のブリッジ番号およびセグメント番号をパケットの RIF に追加します。 フレームがブリッジされたネットワークを通過し続ける間、RIF はあて先へのパスを記述するブリッジ番号とセグメント番号の対のリストをコンパイルします。

   ARP REQUEST パケットが最後にそのあて先に到達するとき、パケットには発信元からあて先までのブリッジ番号とセグメント番号の正確なシーケンスが含まれています。

3. あて先エンド・ステーションがフレームを受信すると、MAC アドレスおよびその RIF をそれ自体の ARP テーブルおよび RIF テーブルに入れます。あて先エンド・ステーションが同じ発信元から他の ARP REQUEST パケットを受信するような場合は、そのパケットは除去されます。
4. あて先エンド・ステーションは、RIF を含む ARP REPLY パケットを生成し、それを発信元エンド・ステーションに送り返します。
5. 発信元エンド・ステーションは学習されたルート・パスを受信します。MAC アドレスおよびその RIF は次に ARP テーブルおよび RIF テーブルに入力されます。RIF は次にデータ・パケットに付加され、あて先に転送されます。
6. RIF 項目の経時は IP 最新表示タイマーによって扱われます。

IPX スレッド化

IPX エンド・ステーションは受信する各パケットを RIF について検査します。RIF がテーブルに存在しない場合は、テーブルにその RIF を追加し、そのルートを *HAVE_ROUTE* として指定します。パケットがローカル・リング上のエンド・ステーションから来たことを RIF が示している場合は、そのルートは *ON_RING* として指定されます。

エンド・ステーションがパケットを送出する必要があり、RIF テーブルにその MAC アドレスへの項目がない場合は、エンド・ステーションはデータを STE として伝送します。

RIF タイマーが満了すると、テーブル内の項目が消去され、その項目の RIF を含む別のパケットが到着するまで再入力されません。

AppleTalk 2 のスレッド化

AppleTalk エンド・ステーションは ARP パケットおよび XID パケットを使用してルートを発見します。AppleTalk エンド・ステーションおよびブリッジの両方がルート発見プロセスおよび転送に参加します。以下のステップは AppleTalk スレッド化プロセスを説明しています。

1. 特定の MAC アドレスについて RIF が存在しない場合、エンド・ステーションは ARE (全ルート探索) を指定した ARP REQUEST パケットをローカル・セグメントへ伝送します。
2. ローカル・セグメントにあるすべてのブリッジは ARP REQUEST パケットを取り込み、それを接続されたネットワークを通じて送信します。ARP REQUEST パケットがあて先エンド・ステーションの探索を継続する間、パケットを転送する各ブリッジはそれ自体のブリッジ番号およびセグメント番号をパケットの RIF に追加します。 フレームがブリッジされたネットワークを通過し続ける間、RIF はあて先へのパスを記述するブリッジ番号とセグメント番号の対のリストをコンパイルします。
3. あて先エンド・ステーションがフレームを受信すると、MAC アドレスおよびその RIF をそれ自体の ARP テーブルおよび RIF テーブルに入れ、項目の状態は *HAVE_ROUTE* として指定されます。あて先エンド・ステーションが同じ発信元から他の ARP REQUEST パケットを受信するような場合は、そのパケットは除去されます。

4. あて先エンド・ステーションは次に RIF を含む ARP REPLY パケットを生成し、RIF 内の方向ビットを反転させてそのパケットを発信元エンド・ステーションに送り返します。
5. 発信元エンド・ステーションは学習されたルート・パスを受信します。MAC アドレスおよびその RIF は次に ARP テーブルおよび RIF テーブルに入れられ、状態は *HAVE_ROUTE* として指定されます。パケットがローカル・リング上のエンド・ステーションから来たことを RIF が示している場合は、そのルートは *ON_RING* として指定されます。
6. RIF タイマーが満了すると、ARE を指定して XID が送信され、状態は *DISCOVERING* に変更されます。XID 応答が受信されない場合、その項目は廃棄されます。

SR-TB 重複 MAC アドレス・フィーチャー

重複 MAC アドレス (DMAC) フィーチャーを使用すると、重複 MAC アドレスが設定されている SR ブリッジ・ネットワークに SR-TB ブリッジを接続できます。重複 MAC アドレス・フィーチャーは、次の 2 つのオプションで使用可能にすることができます。

- **負荷平衡なしの重複 MAC フィーチャー**

  このオプションを選択すると、負荷平衡なしで重複 MAC アドレスを使用可能にすることができます。この場合、重複 MAC アドレスについて RIF が 1 つだけ学習され、経時はその学習された RIF に対して行われます。TB ドメインからのステーションはすべて、この 1 つの RIF を使用して、その MAC アドレスと通信します。この RIF の項目が時間切れになると、次のフレームがスパンニング・ツリー探索 (STE) フレームとして TB ドメインから送信されます。

- **負荷平衡付きの重複 MAC フィーチャー**

  このオプションを選択すると、負荷平衡付き重複 MAC アドレスを使用可能にできますが、これが使用可能にできるのは、負荷平衡なし DMAC を使用可能にした後だけに限られます。この場合、各重複 MAC アドレスごとに 2 つの RIF が学習され、保持されます。 この 2 つの RIF はどちらも、それぞれ固有の経時タイマーをもつことになります。 ブリッジが特定の RIF をもつフレームを受信すると、その RIF に対応する経時値が更新されます。 TB ドメインからのステーションが重複 MAC アドレスに初めてフレームを送信するときに、ブリッジ・ソフトウェアは、そのフレームの送信に使用する RIF を決定します。それ以降の送信側ステーションからのフレームはすべて、その同じ RIF を使用して送信されます。ブリッジは、最大 7 つの重複 MAC アドレスについて、1 次および 2 次 RIF を保持します。重複 MAC アドレスに対して別々の経時値を指定すると、該当の重複 MAC アドレスに対応する項目の経時処理には、該当する値が使用されるので、重複 MAC アドレスの経時値を調整できます。

ATM を介したブリッジング

装置は、固有の ATM (RFC 1483) を介したブリッジングをサポートします。固有の ATM を介したブリッジングの場合、単一の (物理) インターフェースについて複数の (バーチャル) ポートを設定することができます。

ブリッジングについての RFC 1483 サポート

RFC 1483 は、ブリッジされたプロトコルについて、0xAA-AA-03 という LLC 値と、0x00-80-C2 という OUI 値を指定します。SNAP ヘッダーの 2 オクテットの PID 部分は、ブリッジされたプロトコルの場合、ブリッジされた媒体を指定し、さらに、元のフレーム検査シーケンス (FCS) を元のブリッジ PDU 内に保存するかどうかも指定します。さまざまな媒体の PID 値が指定されます。詳細については、RFC 1483 を参照してください。

ATM インターフェースは、トークンリング/802.5、イーサネット/802.3 との間で、ブリッジされた MAC フレームの転送を行います。 VCC 1 つにつき、ブリッジ・ポートが 1 つ使用されます。 ATM インターフェース上にブリッジ・ポートを構成する一方で、そのポートに永続的に結び付けられる VCC を指定する必要があります。 ポート/VCC 上で受信されたブリッジ・フレームは、使用されているブリッジング・プロトコルおよびブリッジング構成どおりに 1 つまたは複数のポート/VCC 上で送出されます。 ブリッジ・ポートが ATM インターフェースで構成され、VCC がそれと関連付けられていれば、従来型の LAN 上の通常のブリッジング・ポートとして機能します。 ポートと ATM インターフェース関連付けは、ユーザーやブリッジング機能にとって透過です。

ATM インターフェース上にブリッジ・ポートを構成する場合、ユーザーは、PVC または SVC サポートを使用するかどうか指定する必要があります。PVC サポートの場合、その PVC の VPI および VCI を与える必要があります。SVC サポートの場合には、リモート ATM アドレスのほか、そのローカル・アドレスに使用されるセレクターも与える必要があります。

注: PVC サポートと異なり、SVC を使用する場合、中間スイッチでの設定は不要です。

ATM インターフェース上にポートが追加されていれば、パラメーターとしてポート番号を必要とするブリッジング構成コマンドをこのポート番号と一緒に使用できます。

ATM を介したブリッジの構成について詳しくは、593ページの『第27章 ARP の使用』および 81ページの『第6章 ブリッジングの構成と監視』を参照してください。

マルチアクセス・ブリッジ・ポートについて

マルチアクセス・ブリッジ・ポートとは、個々にはブリッジ・ポートとして構成されていないフレーム・リレーを、すべて組み込むブリッジ・ポートのことです。 マルチアクセス・ブリッジ・ポートには、固有のブリッジ・セグメント番号が割り当てられ、これがソース・ルーティング・ブリッジングで使用されます。

マルチアクセス・ブリッジ・ポートには、次のようなブリッジング特性があります。

- サポートするのは、ソース・ルーティング (SR) ブリッジングだけです。
- 全メッシュ構成では、任意間接続をサポートし、スパンニング・ツリー・プロトコルを使用してブリッジング・ループを防止することができます。

- 全メッシュ構成以外では、同一セグメント上のバーチャル・サーキットがサポートされていないため、ブランチとデータ・センターの間の接続しかサポートしません。この構成では、スパンニング・ツリー・プロトコルが使用できないので、STE フレームの転送を使用可能にする必要があります。デフォルトでは、スパンニング・ツリー・プロトコルが使用不可、STE フレームの転送が使用可能になっています。

  注: これが優先構成です。その理由は、スパンニング・ツリー・プロトコルは、WAN 帯域幅をかなり使用しますし、構成のほとんどが全メッシュではないからです。

- 1 対 N のブリッジ・バーチャル・セグメントを必要とします。
- 類似エンド・ステーション間の接続は、プロトコルに左右されませんが、媒体が異なるエンド・ステーション間の接続は、限定されます。
- 複数の IBM 2218 装置で効果的なデータ・キャッチャーが得られます (62ページの『IBM 2218 装置との相互運用』 を参照してください)。

マルチアクセス・データベース

各マルチアクセス・ブリッジ・ポートには、フレームを受信したフレーム・リレー・バーチャル・サーキットにネクスト・ホップ・セグメント番号をマップする、マルチアクセス・データベースが保持されています。ARE フレームや STE フレーム、特定ルーティング・フレームなどを回線から受信すると、データベース項目の作成や更新が行われます。 STE フレームと ARE フレームの場合は、マルチアクセス・セグメント上に転送する必要があれば、マルチアクセス・セグメント内のすべてのバーチャル・サーキットにフラッディングされます。これに対して、特定ルーティング・フレームの場合は、マルチアクセス・セグメント上に転送する必要があっても、転送が行われるのは、ネクスト・ホップ・セグメント番号をバーチャル・サーキットにマップするマルチアクセス・データベース項目がある場合だけです。

ソフトウェアによるマルチアクセス・データベース内の項目の「経時処理」は、ユーザーが **multiaccess-age** コマンドを使用して指定する速度で行われます。

マルチアクセス・ブリッジ・ポートの構成

次の例に示すのは、フレーム・リレー・インターフェース 1 と 4 にマルチアクセス・ブリッジ・ポートを構成する方法です。ポート 5 は次に使用可能なブリッジ・ポートであり、これはソース・ルーティングを初めて使用可能にしている場合です。

```
* talk 6
Config> prot asrt
ASRT Config> add multiaccess-port
ASRT Config> Interface number [0]? 1
ASRT Config> Port Number [5]?
ASRT Config> Segment Number for the port in hex (1 - FFF) [001]? 300
ASRT Config> Bridge Number in hex (0 - 9, A - F) [0]? 2
ASRT Config> Bridge Virtual Segment Number (1 - FFF) [001]? CCD
ASRT Config> add multiaccess-port
ASRT Config> Interface number [0]? 4
ASRT Config> Port Number [6]?
ASRT Config> Segment Number for the port in hex (1 - FFF) [001]? 400
```

注: 最初のマルチアクセス・ブリッジ・ポートを構成した後で、ブリッジ番号とバーチャル・セグメント番号の入力を指示するプロンプトが出ることはありません。

IBM 2218 装置との相互運用

マルチアクセス・ポートを 2210/2212/2216 装置でデータ・キャッチャーとして使用すると、ネットワーク内の 2218 の高密度、高可用性トポロジーが得られます。

- 高密度が得られるのは、単一のマルチアクセス・ブリッジ・ポートを通して、多数の 2218 装置がデータ・センターに接続できるからです。
- 高可用性が得られるのは、単一の 2218 が、1 次とバックアップのデータ・センター・ブリッジに、それらのマルチアクセス・ブリッジ・ポートを通して接続されるように構成するからです。そうしておけば、2218 がフレーム・リレー・ネットワーク内で問題を検出すると、そのつど 1 次サーキットと バックアップ・サーキットの間で切り替えができます。

2218 が、それ自体と中央ブリッジの間の LLC 接続を喪失せずに、1 次ブリッジと中央ブリッジの間で切り替えられるようにするには、次のことを行う必要があります。

- 1 次とバックアップのデータ・センター・ブリッジを、同じブリッジの 1 対 N バーチャル・セグメント番号で構成する。
- 1 次とバックアップのデータ・センター・ブリッジを、同じルート・ブリッジ番号で構成する。
- 1 次とバックアップのデータ・センター・ブリッジを、同じマルチアクセス・セグメント番号で構成する。

注: この構成では、ブランチとデータ・センター間の接続がサポートされるだけです。

63ページの図19 に、2210 と 2218 の間の標準的なネットワーク接続が図示してあります。

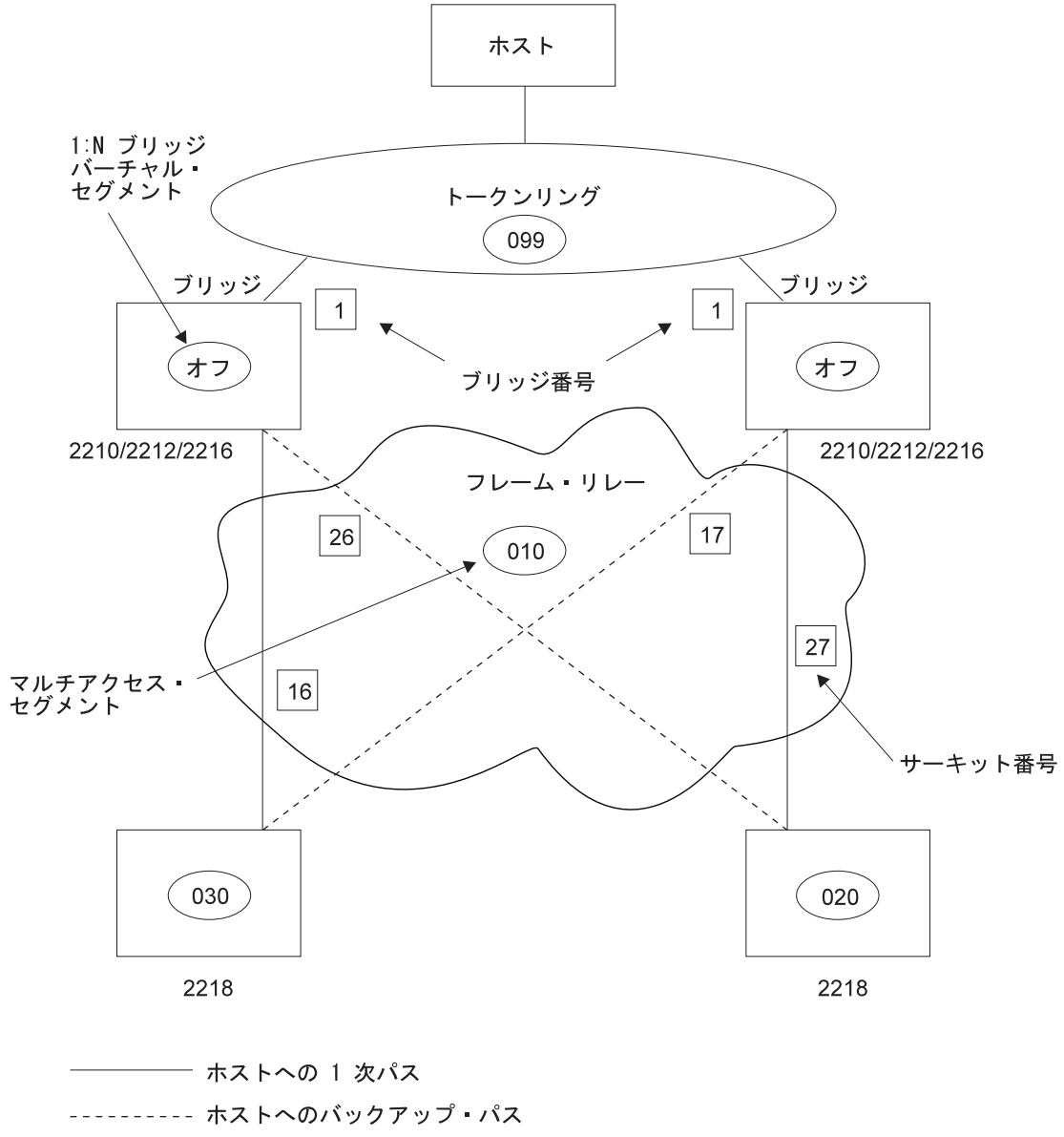


図 19. 2218 とマルチアクセス・ブリッジ・ポートによる構成例

第4章 境界アクセス・ノード (BAN) フィーチャーの使用

この章では、2210 での境界アクセス・ノード (BAN) フィーチャーについて説明します。 BAN は、接続された PU タイプ 2.0 および 2.1 のエンド・ステーションが、広域リンクを通して SNA 環境と通信する場合に、信頼性の高い低コストの手段になります。この章には次の節が含まれています。

境界アクセス・ノード・フィーチャーについて

BAN を使用すると、次の SNA ノード・タイプのいずれとも接続することができます。

- エンド・ノード
- ネットワーク・ノード
- サブエリア・ノード

IBM ネットワーク制御プログラム (NCP) はサブエリア・ノードの一例であり、VTAM とともに複合 APPN ネットワーク・ノードにもなります。

BAN フィーチャーは 2210 ソフトウェアのフレーム・リレー、DLSw、および適応ソース・ルート・ブリッジング (ASRT) 機能の拡張です。このフィーチャーにより、2210 に接続された IBM タイプ 2.0 および 2.1 のエンド・ステーションは、フレーム・リレーを介して、RFC 1490 のブリッジされた 802.5 (トークンリング) フレーム形式をサポートする SNA ノードに直接接続することができます。BAN フィーチャーは、IBM SNA 環境との通信手段として改良とコストの節減を実現しました。IBM では、この機能強化をサポートするために、IBM 3745 の IBM ネットワーク制御プログラム (NCP) ソフトウェアを修正しました。

BAN を使用すると、エンド・ステーションは、66ページの図20 に示すように、トークンリング、イーサネット、または SDLC 回線を経由して、SNA ノードに直接接続されている場合と同じように機能します。エンド・ステーションのデータは実際には 2210およびフレーム・リレー・ネットワークを通過しますが、これはエンド・ステーションにとっては透過です。

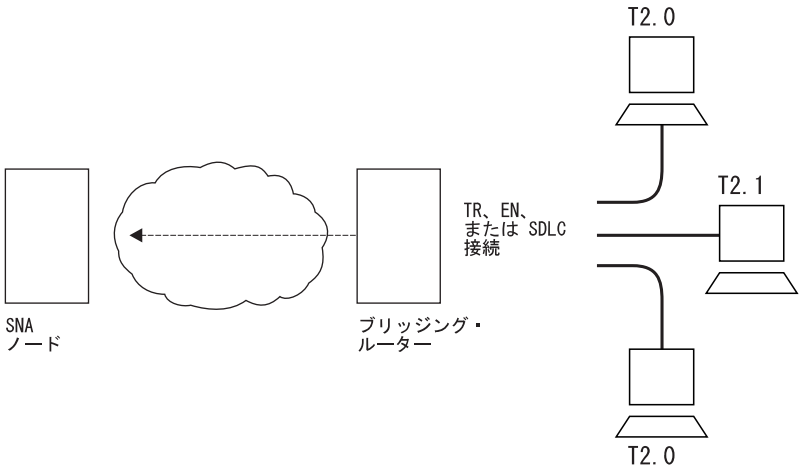


図 20. BAN を使用したエンド・ステーションと SNA ノードの直接接続

BAN の利点

BAN は、ユーザーが完全な DLSw 実施を必要としない場合の要件に見合うように設計されているため、IBM 環境との接続方式として経済的です。 BAN は完全な DLSw 機能へのパスを提供するので、IBM 環境とのインターネットワークを必要とするユーザーの場合は、BAN によって次の 3 つの主要な利点が得られます。

1. 別の DLSw ルーターによってフレーム変換しなくても、イーサネットまたはトークンリングのトラフィックを直接 SNA ノードにブリッジすることができます。したがって、別のルーターおよび中央サイトのホストを必要としなくなるため、設備投資コストを節減することができます。
2. 単一のフレーム・リレー・データ・リンク接続 ID (DLCI) を介しての多重 LLC タイプ 2 (*LLC2*) の数についてのアーキテクチャー上の制限はありません。それに対して、既存の NCP フレーム・リレー境界ノード (BN) サポートは各 DLCI ごとの LLC2 接続の数を 127 に制限しています。したがって、フレーム・リレー DLCI 提供者コストを大幅に節減することができます。
3. エンド・ステーションにローカルな DLSw ルーター上でエンド・ステーション・アドレスを構成する必要がなくなります。したがって、BAN セットアップの構成および管理が一層容易になります。

   注: IP トラフィック用に BAN DLCI を使用することができます。これにより、(BAN を介して) SNA 用に使用しているのと同じ DLCI を通じて (SNMP を介して) ルーターを管理することができます。

BAN はどのように働くか

ルーター内の BAN フィーチャーは、タイプ 2.0 または 2.1 のエンド・ステーションによって送信されたフレームをフィルターする働きをします。各 BAN フレームは、ブリッジされた 802.5 (トークンリング) フレーム形式に適合するように、ルーターによって修正されます。ルーターは各フレームを検査し、BAN DLCI MAC アドレスをもつフレームだけが、DLCI を介してメインフレームまで通過できるようにしま

す。ブリッジされた 802.5 フレーム内のあて先 MAC アドレスは、SNA ノードあてのフレーム内の境界ノード ID で置き換えられます。

BAN では、通常は 1 つの DLCI しか必要とされません。ただし、BAN はルーターと IBM 環境の間に多くの DLCI 接続を使用することができます。場合によっては、BAN トラフィックを処理するのに 2 つ以上の DLCI をセットアップしなければならないことがあります。詳細については、74ページの『複数の DLCI のセットアップ』を参照してください。

BAN フィーチャーを使用するには次の 2 つの方法があります。

- 2210 のブリッジング機能を使用した直接ブリッジング
- DLSw 終端。この場合、BAN は DLSw を稼働させているルーターで LLC2 接続を終端させます。

以下の項では、各方式を構成する方法を説明します。

ブリッジされた BAN と DLSw BAN の比較

BAN は次の 2 つの方法で実施できます。直接ブリッジングおよび DLSw 終端。直接ブリッジングでは、タイプ 2.0 またはタイプ 2.1 のエンド・ステーションから SNA ノード内まで、LLC2 フレームを直接ブリッジするように、BAN を構成します。DLSw 終端では、BAN は、DLSw を稼働させているルーターで LLC2 接続を終端させます。以下の説明では、直接ブリッジングを *BAN タイプ 1*、DLSw 終端を *BAN タイプ 2* と呼びます。

68ページの図21 は、BAN タイプ 1 の (ブリッジされた) 接続を示しています。この図では、ルーターが、接続されたエンド・ステーションから受信された LLC2 トラフィックを終端していないことに注意してください。その代わり、ルーターは、受信したフレームをブリッジされたトークンリング形式 (RFC 1490) のフレームに変換し、SNA ノードに直接ブリッジしています。

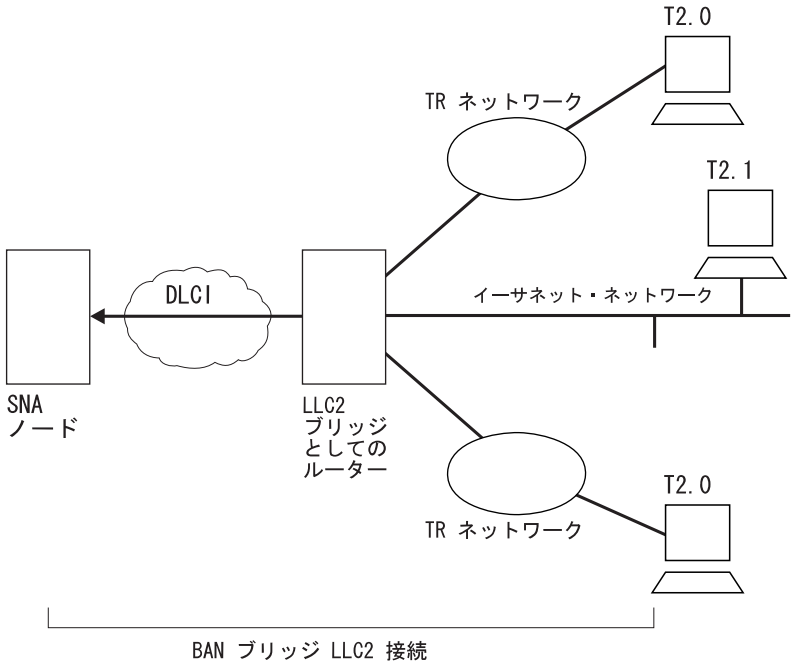


図 21. BAN タイプ 1: LLC2 ブリッジとしてのルーター

この場合、ルーターは SNA ノードとエンド・ステーションの間のブリッジとして働きます。DLSw は、BAN タイプ 2 のように、ルーターで LLC2 セッションを終端しません。エンド・ステーション・フレームは、トークンリング形式、SDLC (ピクチャー化されていない) 形式、またはイーサネット形式のいずれでも構いませんが、ブリッジが該当のタイプのフレームをサポートするように構成されている場合に限ります。

69ページの図22 は BAN タイプ 2 の (バーチャル BAN DLSw) 接続を示しています。この図では、DLSw ルーターがブリッジとして機能していないことに注意してください。ルーターは、接続されたエンド・ステーションから受信した LLC2 トラフィックを終端しています。それと同時に、ルーターは、フレーム・リレー・ネットワークを介して、SNA ノードへの新しい LLC2 接続を確立しています。したがって、2 つの LLC2 接続がトランザクション内に存在していますが、それらの間の切れ目は、SNA ノードとエンド・ステーションの両方から透過です。 結果的に、SNA ノードとエンド・ステーションの間にバーチャル LLC2 接続ができます。

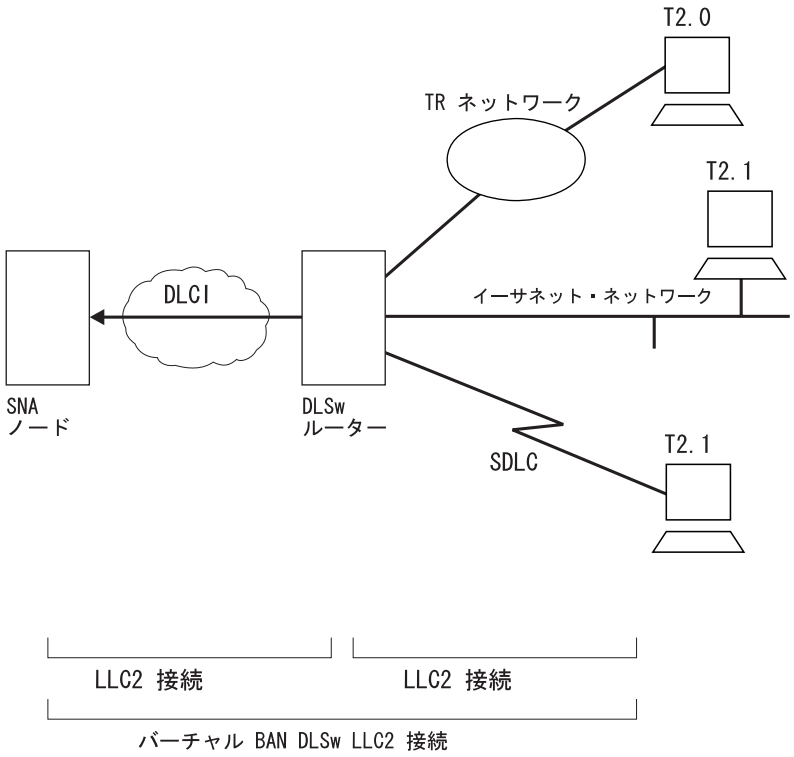


図 22. BAN タイプ 2: ローカル DLSw 変換

SDLC セッションはルーターで終端され、ルーターと SNA ノードの間に別個の LLC2 セッションが存在しています。SDLC ステーションは、SNA ノードにとってはフレーム・リレーに接続されたステーションのように見えます。

リモート DLSw は両方のタイプの BAN についてサポートされます。BAN タイプ 1 およびタイプ 2 の接続はいずれも、タイプ 2.0 または 2.1 のエンド・ステーションを SNA ノードに接続する DLSw パートナーとして機能しているルーターによって使用することができます。

どちらの方式を使用すべきか ?

フレームの直接ブリッジング (BAN タイプ 1) の方が一般的に好まれます。これは、最小のネットワーク・オーバーヘッドで高速のデータの配送を提供するからです。ただし、例外があります。DLCI 上での使用率が高すぎると、ブリッジされた構成でセッション・タイムアウトが発生します。これとは逆に、DLSw 構成 (BAN タイプ 2) では、セッション・タイムアウトが発生することはめったにありません。このタイプの構成では、LLC2 セッションをローカル (DLSw) ルーターで終端してから再作成するからです。

BAN フィーチャーの使用

BAN の構成にあたっては、システムがプロンプトによって情報の入力を指示します。システムが省略時値を用意していて、ユーザーは **Return** を押して、それを受け入れる場合も少なくありません。

BAN フィーチャーを使用するためには、次のようにする必要があります。

1. ルーターをフレーム・リレー (FR) 用に構成する
2. ルーターを適応ソース・ルート・ブリッジング (ASRT) 用に構成する
3. ルーターを BAN 用に構成する
4. ルーターを DLSw 用に構成する (BAN タイプ 2 のみ)

上記のステップを以下に例を挙げて説明します。この例では、BAN トラフィックを搬送する単一の DLCI をセットアップしているものと想定します。状況および要件に応じて、複数の DLCI をセットアップして冗長度を得たり、IBM 環境で全体の帯域幅を増やしたい場合があります。この場合、2210 の BAN DLCI MAC アドレスは ISDN バックアップ 2210 の BAN DLCI MAC アドレスに一致する必要があります。また、2210 の内部ブリッジ・セグメントの値が、バックアップ 2210 の内部ブリッジ・セグメントの値と異なっている必要があります。詳細については、74ページの『複数の DLCI のセットアップ』を参照してください。

ステップ 1: 2210 をフレーム・リレー用に構成する

フレーム・リレー構成プロンプトにアクセスするには、次の例に示すように Config> プロンプトで **network** *interface#* と入力します。(*Interface#* とはフレーム・リレー・インターフェースの番号です。)

```
Config>network 2
Frame Relay user configuration
FR Config>
```

FR Config> プロンプトで、次の例で示すように永続サーキットを追加します。ルーターは次のことを入力するようプロンプト指示します。

- サーキット番号。これは DLCI 番号です。
- コミットされた情報速度

```
FR Config>add permanent
Circuit number  [16]? 20
Committed Information Rate in bps  [64000]?
Committed Burst Size(Bc) in bits (64000)?
Excess Burst Size (Be) in bits(0)?
Assign circuit name []? 20-ncp10
Is circuit required for interface operation [N]?
FR Config>
```

作成した DLCI は、 BAN を使用したときに 2210 と SNA ノードを接続する PVC になります。 BAN 、次のステップは、この PVC をブリッジ・ポートとして構成することです。

注: 同じ SNA ノードまたは異なる SNA ノードに接続された複数の BAN DLCI をセットアップしたい場合は、各 DLCI ごとにフレーム・リレーを別々に構成する必要があります。詳細については、74ページの『複数の DLCI のセットアップ』を参照してください。

ステップ 2: ルーターを適応ソース・ルート・ブリッジング用に構成する

次に、PVC をブリッジ・ポートとして構成する必要があります。これを行うには、次に示すように Config> プロンプトで **protocol** コマンドを使用します。

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>
```

ASRT Config> プロンプトでは、次に示すようにポートを追加します。ルーターは、インターフェース番号を入力するようプロンプト指示します。割り当てる番号は、ブリッジ上の FR インターフェースの番号です。ポート番号およびサーキット番号を入力するようプロンプト指示されます。割り当てるサーキット番号は、ステップ 1 でフレーム・リレーを介してのブリッジ用にルーターを構成するときに使用した番号と同じものでなければなりません。

```
ASRT config> add port
Interface Number [0]? 2
Port Number [5]?
Assign circuit number [16]? 20
ASRT config>
```

次に、フレーム・リレー・ポート用にソース・ルーティングを使用可能にし (enable source routing と入力)、ソース・ルーティング・セグメント番号を定義します。

```
ASRT config>enable source routing
Port Number [3]? 5
Segment Number for the port in hex (1 - FFF) [1]? 456
Bridge Number in hex (1-9, A-F) [1]?
ASRT config>
```

最後に、次に示すようにブリッジ・ポート上の透過ブリッジングを使用不能にする (disable transparent bridging) を入力します。

```
ASRT config>disable transparent bridging
Port Number [3]? 5
ASRT config>
```

BAN タイプ 2 接続が使用されている場合は、DLSw をブリッジングに使用できるようにします。

```
ASRT config>enable dls
ASRT config>
```

次のステップは、ルーターを BAN 用に構成することです。

ステップ 3: ルーターを BAN 用に構成する

ASRT config> プロンプトでルーターを BAN 用に構成する必要があります。ルーター上での BAN ポートの追加は、ルーターを再始動するまで、検証されません。ステップ 1 および 2 と同様、ブリッジ・ポート 5 がこのステップを通じて使用されるポートであることに注意してください。

```
Config>protocol asrt
ASRT config>ban
BAN (Boundary Access Node) configuration
BAN config>
```

BAN config> プロンプトで、BAN フィーチャーを使用可能にしたいポート番号 (5) を追加します。次に示すように、BAN DLCI MAC アドレスおよび境界ノード ID を入力するようプロンプト指示されます。

```
BAN config>add 5
Enter the BAN DLCI MAC Address []? 400000000001
Enter the Boundary Node Identifier MAC Address [4FFF00000000]?
```

この例では、400000000001 が DLCI の MAC アドレスです。これは、接続されたエンド・ステーションがデータを送信する先のアドレスです。(68ページの図21 および 69ページの図22 を参照してください)。もう一方のアドレス 4FFF00000000 は、省略時の境界ノード ID アドレスです。これを受け入れる場合は、**Enter** を押します。

注: 境界ノード ID は、2210 から SNA ノードに送信されたブリッジされた 802.5 フレーム内に入れられた宛先 MAC アドレスに対応しています。省略時値 4FFF00000000 は、IBM ネットワーク制御プログラム (NCP) によって使用された省略時値に一致します。NCP アドレスは、NCP 定義内で物理フレーム・リレー・ポートを定義する LINE ステートメントの LOCADD キーワードで指定します。フレーム・リレーを介してブリッジされた 802.5 フレームをサポートする他の SNA ノードについては、境界ノード ID は、SNA ノードがこのバーチャル・サーキット用に構成してあった MAC アドレスに設定する必要があります。

BAN 接続タイプの指定: 次のプロンプトでは、追加したい BAN 接続のタイプ (ブリッジまたは DLSw 終端) を指定するよう指示されます。これら 2 つの方式については、前の節で BAN タイプ 1 および BAN タイプ 2 として説明しています。タイプ 1 の直接ブリッジングが省略時値です。インバウンド・トラフィックがルーターで終端するようにしたくない場合は、省略時値を受け入れる必要があります。

b または **t** を入力した後、ルーターは BAN ポートが追加されたことを通知します。

```
Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) [b]?
BAN port record added.
```

ステップ 4: ルーターを DLSw 用に構成する (BAN タイプ 2 のみ)

BAN タイプ 2 接続が使用されている場合は、DLSw を構成する必要があります。これには、DLSw の使用可能化、DLSw セグメント番号の設定、ローカル DLSw TCP パートナーの追加、さらに FR インターフェースおよび LAN インターフェースと関連付けられているサービス・アクセス・ポイント (SAP) のオープンが必要です。この DLSw 構成が実行できない場合は、BAN タイプ 2 (DLS 終端処理済み) 接続を使用できません。

`DLSw config>` プロンプトから **enable dls** コマンドを使用して、DLSw を使用可能にします。

`DLSw config>` プロンプトから **set srb** コマンドを使用して、DLSw セグメント番号を設定します。

ローカル DLSw TCP パートナーを追加するために、`DLSw config>` プロンプトで以下を入力します。

```
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0.]? 128.185.236.33
Neighbor Priority (H/M/L) [M]?
DLSw config>
```

以下の例に示すように、`DLSw config>` プロンプトから SAP をオープンします。

```
DLSw config>open
Interface # [0]?
Enter SAP in hex (range 0-ff) [0]? 4
DLSw config>
```

インターフェース 0 に **open** コマンドを出すと、LAN インターフェースで SAP がオープンします。FR インターフェースで SAP をオープンする場合も同じコマンドを出します。どちらの場合でも、SAP をオープンするのに番号 **4** を入力することに注意してください。

```
DLSw config>open
Interface # [2]?    [open on the FR interface]
Enter SAP in hex (range 0-ff) [0]? 4
DLSw config>
```

BAN トラフィック用の複数の DLCI の使用

BAN トラフィックを IBM 環境とやりとりするには通常は 1 つの DLCI で十分ですが、状況によっては 2 つ以上の DLCI をセットアップしておくと役に立ちます。

シナリオ 1: 耐障害 BAN 接続をセットアップする

複数の SNA ノードに冗長接続しておくと、単一 SNA ノードの障害から保護されます。さらに、BAN トラフィックをいくつかの DLCI の間で共用すると、1 つの SNA ノードが過負荷になる可能性が低下します。冗長 DLCI 構成では、図23 に示すように、PU タイプ 2.0 および 2.1 のエンド・ステーションは、BAN トラフィックを異なる SNA ノードに渡すことができます。

注: 各 DLCI は同じ DLCI MAC アドレスを使って別個の FR ASRT ブリッジ・ポート上に構成されます。ただし、このオプションは、SR-TB 変換が使用可能になっている場合は使用できません

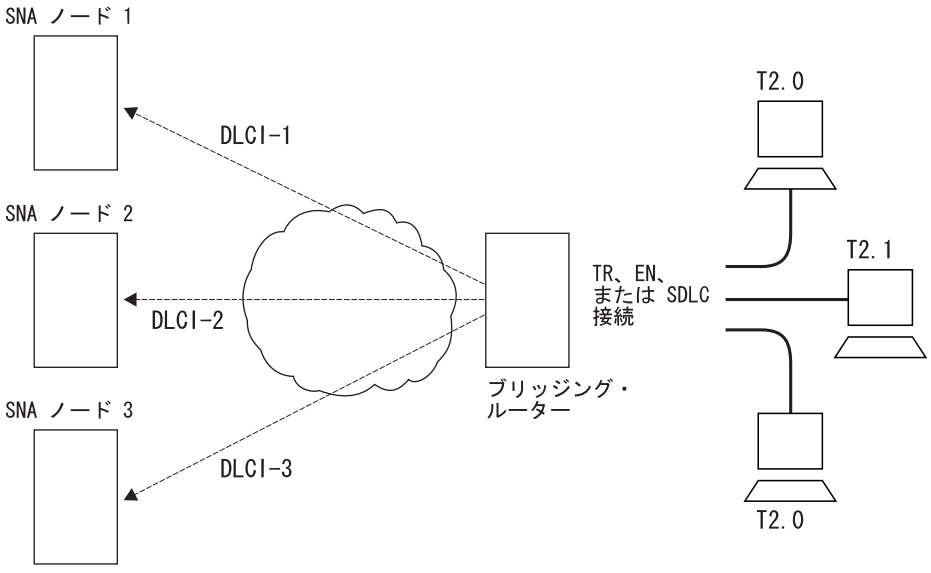


図 23. 異なる SNA ノードへの複数の DLCI をもつ BAN 構成

シナリオ 2: IBM 環境への帯域幅を広げる

同じ SNA ノードに複数の接続を行うと、IBM 環境との通信に使用できる帯域幅が広がります。したがって、単一の DLCI で輻輳 (ふくそう) が生じる可能性が低下します。

大量の BAN トラフィックがあり、別の FR 接続が使える場合には、2 つ以上の DLCI をセットアップしたい場合があります。2 番目の DLCI によって、SNA ノードに提供される全帯域幅が広がり、予期しない障害から保護されることができます。

複数の DLCI のセットアップ

複数の DLCI のセットアップは、特に初期の BAN 構成時に行えば単純です。複数の接続をセットアップする場合は、各フレーム・リレー DLCI がそれぞれ、IBM 環境の特定の SNA ノードに対応していることに留意してください。該当の SNA ノードに BAN フレームを渡すには、フレーム・リレー接続の確立時に、正しいサーキット番号を指定する必要があります。フレーム・リレー提供者は接続のそれぞれごとにサーキット番号を与えることができます。

異なる SNA ノードに対する DLCI 接続をセットアップする場合 (73ページの『シナリオ 1: 耐障害 BAN 接続をセットアップする』 を参照) は、次のようにする必要があります。

1. 次のアクションのいずれかを取ります。
   - **ASRT 構成では**、その DLCI 用のブリッジ・ポートを追加します。
   - **フレーム・リレー構成では**、第 2 のブリッジ・ポートで別のフレーム・リレー DLCI を定義します。
2. 71ページの『ステップ 3: ルーターを BAN 用に構成する』 に示すように、BAN 用のブリッジ・ポートを構成します。

同じ SNA ノードに対する 2 番目の DLCI 接続をセットアップする場合 (『シナリオ 2: IBM 環境への帯域幅を広げる』を参照) は、同じ手順に従います。 『シナリオ 2: IBM 環境への帯域幅を広げる』 では、第 2 のフレーム・リレー・ポート用に提供されたサーキット番号は第 1 のポート用のサーキット番号とは異なります。ただし、各サーキット番号ごとに、異なる DLCI および IBM 環境への別個のパスを識別します。

BAN 構成の検査

ルーターを再始動するとき、ルーターは、BAN ブリッジ・ポートがソース・ルーティング行動をもつフレーム・リレー・ブリッジ・ポートであることを妥当性検査します。 ここで示すように list コマンドを使って BAN 構成を検査する必要があります。

```
BAN config>list

bridge    BAN                 Boundary              bridged or
port      DLCI MAC Address    Node Identifier       DLSw terminated
------    ----------------    ---------------       ---------------
5         40:00:00:00:00:01   4F:FF:00:00:00:00     bridged

BAN config>
```

この例に示されているように、**list** コマンドによって、BAN 構成の各局面が表示されていて、ブリッジ・ポート (この場合は 5)、DLCI の MAC アドレスと SNA ノードの境界ノード ID、およびポートがブリッジされているか DLSw が終端されているかが示されます。

BAN が始動時に正しく初期設定されたか検証するために、GWCON を次のように使用することができます。

```
+protocol asrt
ASRT> ban
BAN (Boundary Access Node) console

BAN>list
bridge  BAN                Boundary           bridged or
port    DLCI MAC Address   Node Identifier    DLSw terminated   Status
----    ----------------   ---------------    ---------------   -------
5       40:00:00:00:00:01  4F:FF:00:00:00:00  bridged           Init Fail

BAN>
```

GWCON は次の 3 つの状況メッセージを提供します。

- Init Fail の状況は、構成問題が存在することを示します。
- Down の状況は、DLCI が稼働していないことを示します。
- Up の状況は、フレーム・リレー DLCI が活動化し、予定されたとおりに稼働していることを示します。

Up 以外の状況を受信する場合、ルーターの ELS メッセージをチェックして問題を診断する必要があります。『BAN 用のイベント・ログ・システム (ELS) メッセージを使用可能にする』 で、ELS メッセージを使用可能にする方法を説明します。

BAN 用のイベント・ログ・システム (ELS) メッセージを使用可能にする

初期 BAN 構成と再始動の後、構成が予定どおり稼働しているかどうか調べるために ELS メッセージを使用可能にするのは良い方法です。次に示すように、Config> prompt から BAN に固有のメッセージを使用可能にすることができます。

```
Config>ev
Event Logging System user configuration
ELS config>display subsystem ban all
ELS config>
```

このコマンドを入力すると、すべての BAN サブシステム・メッセージが表示されます。 これにより、ELS は BAN に関連するすべての行動を通知します。 BAN をしばらく稼働した後、一部のメッセージを消したい場合があります。 **nodisplay** コマンドおよび特定のメッセージ番号を使用することにより、特定の ELS BAN メッセージを消すことができます。 この例は ban.9 メッセージを消す方法を示しています。

```
ELS config>nodisplay event ban.9
```

すべての BAN 関連メッセージのリストおよび説明については、イベント・ログ・システム・メッセージの手引きを参照してください。

第5章 ブリッジングの使用

この章では、ASRT 構成コマンドを使用して適応ソース・ルーティング透過型 (ASRT) ブリッジ用の基本構成を作成する方法を説明します。この章には、『基本ブリッジング構成手順』が含まれています。

ASRT ブリッジ構成コマンドについてさらに詳しい情報が必要な場合は、81ページの『第6章 ブリッジングの構成と監視』を参照してください。

ASRT ブリッジングの修正に関する紹介については、52ページの『NetBIOS の名前フィルターとバイト・フィルター』を参照してください。

NetBIOS フィルターのセットアップの例については、165ページの『NetBIOS のホスト名フィルターおよびバイト・フィルターの構成手順』を参照してください。

ASRT 構成環境にアクセスする方法については、 *ソフトウェア 使用者の手引き* の「始めに」を参照してください。

基本ブリッジング構成手順

ASRT ブリッジでは、使用するコマンドの数をなるべく少なくして、基本ブリッジング構成を実行できます。例えば、**enable bridge** コマンドを使用すると、すべての正しく構成された装置を透過ブリッジングに参加させることによりこのプロセスが開始されます。それに加えて、スパンニング・ツリー・アルゴリズムについてすべての省略時値が使用可能になっています。

次に、透過ブリッジング以上のブリッジング機能が、『ポートごとに』使用可能になります。ソース・ルーティングが使用可能になっても、セグメント番号やブリッジ番号などのユーザー入力は依然として必要であり、説明されている基本コマンド以上で入力する必要があります。

ブリッジング・インターフェース

ASRT ブリッジがサポートするブリッジングのインターフェースは、以下のインターフェースの 1 つまたは複数を組み合わせたものです。

- イーサネット
- トークンリング
- シリアル回線
- ATM
- FDDI

イーサネット・インターフェースと FDDI インターフェースでは、透過ブリッジングがサポートされますが、トークンリング・インターフェースでは、ソース・ルーティングと透過ブリッジングがサポートできます。

シリアル回線のインターフェースは、透過とソース・ルーティングのトラフィックのためにポイント・ポイントを接続することができます。シリアル回線を通じての

ブリッジ構成は両方のエンドポイントで一貫しているよう注意することが重要です。つまり、両方のエンドポイントは次のように構成する必要があります。

- 透過から透過へ
- ソース・ルーティングからソース・ルーティングへ
- ソース・ルーティング/透過からソース・ルーティング/透過へ

混合したブリッジが必要な場合は、シリアル回線は両方のブリッジング方式に構成されているのがベストです。提案されるもう 1 つの指針は、ブリッジング・ルーターはブリッジング方式または特定のプロトコルのルーティングについて一貫していることを確認することです。

すぐ次の情報では、ASRT ブリッジによって提供されるブリッジング・オプションを使用可能にするのに必要な手順を概説します。さらに構成変更を行う場合について詳しくは、この章のコマンドの節に記載されています。これらの作業を完了したら、ルーターを再始動して、新しい構成を有効にする必要があります。

透過型ブリッジを使用可能にする

透過型ブリッジを使用可能にするには次のコマンドを使用してください。

- ローカル・エリア・ネットワークのすべてのインターフェースで透過型ブリッジを使用可能にするには、**enable bridge**。広域ネットワーク (WAN) インターフェース (例えば、シリアル回線) は、**add port** コマンドを使用することにより、組み込むことができます。
- 指定されたトークンリング・インターフェースを透過ブリッジングへの参加から除外するには、**disable transparent** *port#*。透過ブリッジング構成から除外したいすべてのインターフェースについてこのコマンドを繰り返してください。

ソース・ルーティング・ブリッジを使用可能にする

ソース・ルーティング・ブリッジングを使用可能にするには、次のコマンドを使用してください。

- ローカル・エリア・ネットワークのすべてのインターフェースについてブリッジングを使用可能にするには、**enable bridge**。WAN インターフェース (例えば、シリアル回線) は、**add port** コマンドを使用することによって組み込むことができます。
- すべてのポートで透過ブリッジングを使用不可にするには、**disable transparent** *port#*。
- 特定のポートについてソース・ルーティングを使用可能にするには、**Enable source-routing** *port# segment# [bridge#]*。ソース・ルーティングが 3 つ以上のポートで使用可能な場合は、1:N SRB 構成に必要な内部バーチャル・セグメントを割り当てるために追加のセグメント番号が必要です。

ソース・ルーティングが必要な唯一のフィーチャーである場合には、インターフェースでの透過ブリッジングは使用不可にする必要があります。

注: 本来ソース・ルーティングをサポートしていないインターフェースを組み込むことが**ない**ように注意する必要があります。例えば、イーサネット・ポート

で、透過ブリッジングが使用不可、ソース・ルーティングが使用可能になっていると、このポートでは、ブリッジング機能は使用不可になります。

SR-TBブリッジを使用可能にする

SR-TBブリッジを使用可能にするには、次のコマンドを使用してください。

- ローカル・エリア・ネットワークのすべてのインターフェースについてブリッジングを使用可能にするには、**enable bridge**。WAN インターフェース (例えば、シリアル回線) は、**add port** コマンドを使用することによって組み込むことができます。
- すべての基礎ソース・ルーティング・インターフェース上で透過ブリッジングを使用不可にするには、**disable transparent** *port#*。
- 特定のポートについてソース・ルーティングを使用可能にするには、 **enable source routing bridge** *port# segment# [bridge#]*。ソース・ルーティングが 3 つ以上のポートで使用可能な場合は、1:N SRB 構成に必要な内部バーチャル・セグメントを割り当てるために追加のセグメント番号が必要です。
- ソース・ルーティングされたフレームから透過フレームへの変換、およびその逆の変換を使用可能にするには、**enable sr-tb-conversion** *segment#*。また、透過ブリッジング・ドメイン全体を表すために、ドメイン・セグメント番号およびドメイン MTU サイズを割り当てることも必要です。

上記の手順のどれかを完了したら、**list bridge** コマンドを使用して、現行のブリッジ構成を表示するようお勧めします。これにより、構成を検査し、チェックすることができます。

上記のコマンドすべてについてさらに詳しくは、81ページの『第6章 ブリッジングの構成と監視』を参照してください。

第6章 ブリッジングの構成と監視

この章では、適応ソース・ルーティング透過型 (ASRT) ブリッジ・プロトコルを構成する方法および ASRT 構成コマンドを使用する方法について説明します。この章には次の節が含まれています。

- 『ASRT 構成環境へのアクセス』
- 『ASRT 構成コマンド』
- 123ページの『トンネル構成コマンド』
- 94ページの『BAN』
- 127ページの『フレーム・リレー・コマンド』

ASRT 構成環境へのアクセス

ASRT 構成環境にアクセスするには、Config> プロンプトで **protocol asrt** コマンドを入力します。

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>
```

ASRT 構成コマンド

ASRT 構成コマンドでは、ASRT ブリッジおよびそのネットワーク・インターフェース用のネットワーク・パラメーターを指定することができます。これらのコマンドでは、 ブリッジ IP トンネル、NetBIOS、およびフレーム・リレー・インターフェースのフィーチャーを使用可能にし、構成することもできます。

新しい構成を有効にするためには、ルーターを再始動する必要があります。

ASRT config> プロンプトに入力構成コマンドを入力します。コマンドには次のようにアクセスします。

- TNL config> プロンプトで IP トンネル用の構成コマンドを入力します。TNL config> プロンプトは、主要 ASRT コマンドのサブセットであり、この章で後述する ASRT config> **tunnel** コマンドを入力することによってアクセスできます。
- NetBIOS config> プロンプトで NetBIOS 用の構成コマンドを入力します。NetBIOS config> プロンプトは、主要 ASRT コマンドのサブセットであり、この章で後述する ASRT config> **netbios** コマンドを入力することによってアクセスできます。
- NetBIOS Filter config> プロンプトで NetBIOS フィルター用の構成コマンドを入力します。このプロンプトは、NetBIOS コマンドのサブセットです。
- ASRT config> プロンプトで ATM 用のブリッジング構成コマンドを入力します。

ASRT 構成コマンド (Talk 6)

表4 は、ASRT 構成コマンドを示しています。

表 4. ASRT 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	永続データベース、特定のアドレス・マッピング、LAN/WAN ポート、プロトコル・フィルター、重複 MAC アドレス、および IP インターネットワークを通じてのエンド・ステーション間のトンネルにステーション・アドレス項目を追加します。
Ban	境界アクセス・ノード (BAN) 構成プロンプトにアクセスして、BAN 構成コマンドが入力できるようにします。
Change	ユーザーがブリッジ番号およびセグメント番号を変更できるようにします。
Delete	ステーション・アドレス項目、特定のアドレス・マッピング、LAN/WAN ポート、プロトコル・フィルター、重複 MAC アドレス、および IP インターネットワークを通じてのエンド・ステーション間のトンネルを削除します。
Disable	以下の機能を使用不能にします。 • ブリッジング • 重複フレーム • グループ・アドレスと機能アドレス間のマップ • スパンニング・ツリー探索フレームの伝送 • 特定のポートでのソース・ルーティング • トンネルを介するスパンニング・ツリー探索フレームの受信 • SR-TB 変換 • 特定のポートでの透過 (スパンニング・ツリー) ブリッジング機能 • ブリッジ間のトンネル • 重複 MAC アドレス・フィーチャー • 重複 MAC 負荷平衡
Enable	以下の機能を使用可能にします。 • ブリッジング • 重複フレーム • グループ・アドレスとアドレス間のマップ • スパンニング・ツリー探索フレームの伝送 • 特定のポートでのソース・ルーティング • トンネルを介するスパンニング・ツリー探索フレームの受信 • SR-TB 変換 • 特定のポートでの透過 (スパンニング・ツリー) ブリッジング機能 • ブリッジ間のトンネル • 重複 MAC アドレス・フィーチャー • 重複 MAC 負荷平衡

表 4. ASRT 構成コマンドの要約 (続き)

コマンド	機能
List	完全なブリッジ構成または選択された構成パラメーターについての情報を表示します。
NetBIOS	NetBIOS 構成プロンプトを表示します。
Set	以下のパラメーターを設定します。 • 動的アドレス項目用の経過時間 • ブリッジ・アドレス • トンネル用の最大フレーム・サイズ • 最大フレーム (LF) ビットのコード化 • 最大フレーム・サイズ • スパンニング・ツリー・プロトコル・ブリッジおよびポートのパラメーター • ルート記述子 (RD) の値 • フィルター・データベース・サイズ • 重複 MAC アドレス・ルーティング情報フィールド (RIF) の経時値 • マルチアクセス・データベース項目の経時値
Tunnel	トンネル構成プロンプトにアクセスして、トンネル構成コマンドを入力できるようにします。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

ブリッジ構成に次の情報を追加するには、**add** コマンドを使用します。

- 永続データベースのステーション・アドレス項目
- 所定のプロトコルの特定のアドレス・マップ
- マルチアクセス・ポート
- LAN/WAN ポート
- パケットをそのプロトコル・タイプに基づいて選択的にフィルターするプロトコル・フィルター
- エンド・ステーション間で IP ネットワーク・セグメントを横断する IP トンネル
- 最大 7 つの重複 MAC アドレス

ブリッジの IP トンネル・フィーチャーでは、**add** コマンドを使用すると、 IP インターネットワークを横断してエンド・ステーション間で IP トンネルを作成できます。このトンネルは、IP インターネットを通じてのパスがいかに複雑であろうと、エンド・ステーション間での 1 つだけのホップとしてカウントされます。

構文:

add address . . .
dmac-addr
mapping . . .
multiaccess-port . . .

port . . .

prot-filter . . .

tunnel . . .

address *addr-value*

永続データベースに固有なステーション・アドレス項目を追加します。ブリッジが再始動されると、これらの項目はフィルター・データベースに永続項目として複写されます。*addr-value* は、必要な項目の MAC アドレスです。これは、個別アドレス、マルチキャスト・アドレス、または同報通信アドレスになりえます。各着信ポートについて発信転送ポート・マップを指定するオプションも与えられます。永続データベース項目は電源オフ/オンのプロセスによって破壊されることはなく、経過時間の設定値によって影響されません。永続項目が、動的項目によって取って代わられることはありません。

有効値: X'0000 0000 0000' ～ X'FFFF FFFF FFFF'

省略時値: なし

以下の各項では、**add address** コマンドを使用してアドレス項目を管理する方法の特定の例を示します。

アドレスの追加

```
add address
Address (in 12-digit hex) []? 123456789013
    Exclude destination address from all ports?(Yes or [No]):
    Use same output port mapping for all input Ports?(Yes or [No]):
    Output port mapping:
       Input Port Number [1]?
       Bridge to all ports?(Yes or [No]):
       Bridge to  port 1  Yes or [No]:
       Bridge to  port 2  Yes or [No]:
       Bridge to  port 3  Yes or [No]:
       Bridge to  port 4  Yes or [No]:
       Bridge to  port 5  Yes or [No]:
       continue to another input port? (Yes or [No]): y
       Input Port Number [2]? 3
       Bridge to all ports?(Yes or [No]): y
       continue to another input port? (Yes or [No]): y
       Input Port Number [4]?
       Bridge to all ports?(Yes or [No]):
       Bridge to  port 1  Yes or [No]:
       Bridge to  port 2  Yes or [No]:
       Bridge to  port 3  Yes or [No]:
       Bridge to  port 4  Yes or [No]:
       Bridge to  port 5  Yes or [No]:
       continue to another input port? (Yes or [No]): n
    Source Address Filtering Applies? (Yes or No): y
    ASRT config>
```

注: プロンプトに 『Yes または No』 で答える質問がある場合は、『No』 が省略時値です。省略時値を受け入れるには、**Return** を押します。

Exclude destination address ...

このプロンプトでは、その項目に宛先アドレス・フィルターを設定できます。このプロンプトに 『Yes』 と応答すると、どのポートから届いたかとは無関係に、このアドレスをあて先アドレスとして含むフレームがすべてフィルターされます。

Use same output mapping...

このプロンプトに 『Yes』 と応答すると、特定の 1 つのポートにだけマップするのではなく、すべての着信ポートについて 1 つの発信ポート・マップを作成することができます。このプロンプトに 『No』 と応答すると、さらにプロンプト (`Input Port Number [1]?`)

が出て、それぞれの入力ポートの選択を指示されます。その特定の入力ポート・プロンプトから、その入力ポート用の固有のポート・マップを作成できます。

Input Port 1, Port 2

前のプロンプトに 『No』 と応答すると、各入力ポートおよびそれに関連する発信ブリッジ・ポートを選択するために入力ポートごとのプロンプト (Input Port Number [1]?) が出されます。

Bridge to all ports?

このプロンプトに 『Yes』 と応答すると、すべてのポートを含む発信ポート・マップが作成されます。したがって、あて先アドレスとしてこのアドレスが指定されたフレームを受信したら、フレームは着信ポートを除くすべての発信転送ポートに渡されます。ポート・マップに従ってこれがどのように行われるかを示す例は以下のとおりです。

フレームがポート *1* で受信され、ポート・マップが 1 (ポート 1) を示している場合、そのフレームはフィルターされます。

同じフレームがポート *2* で受信され、ポート・マップが 1 (ポート 1) を示している場合、フレームはポート 1 に渡されます。フレームがポート 1 で受信され、突き合わせアドレス項目のポート・マップが 1、2、または 3 を示している場合は、フレームはポート 2 および 3 に渡されます。

ポート・マップがポートを指示していない (NONE/DAF) 場合は、フレームはフィルターされます。これはあて先アドレス・フィルター (DAF) として知られているものです。

受信されたフレームに一致するアドレス項目が見つからない場合には、発信元ポートを除くすべての転送ポートに渡されます。

Bridge to Port 1, Port 2, etc.

このプロンプトでは、アドレス項目を特定のブリッジ・ポートに関連させることができます。『Yes』 と応答すると、アドレスが指定されたポートにマップされ、そのポートがそのアドレス項目のポート・マップに組み込まれます。『No』 と応答すると、そのポートのアドレス・マップはスキップされます。

continue to another bridge port?

このプロンプトでは、構成する次の入力ポートを選択できます。

Source address filtering

発信元アドレス・フィルター (SAF) に対応できます。SAF が適用される (プロンプトに 『Yes』 が応答される) 場合、発信元アドレス・フィルターが使用可能にされたフィルター・データベース内のアドレス項目に一致する発信元アドレスをもつ受信フレームは廃棄されます。このメカニズムにより、ネットワーク管理プログラムは、あるエンド・ステーションのトラフィックがブリッジされないようにして、エンド・ステーションを隔離することができます。

Enabling Destination Address Filtering For Entry

この例では、ある項目に宛先アドレス・フィルターを選択するためのコマンド・プロンプトに応答する方法を示します。

```
ASRT config>add address 000000334455
Exclude destination address from all ports?(Yes or [No]): y
Source Address Filtering Applies? (Yes or [No]): y
ASRT config>
```

アドレス項目を追加した後で、**list range** コマンドを使用してアドレス項目の状況を検査することができます。 次の例は、その項目 (太字の部分) についてポート・マップが存在せず、あて先アドレス・フィルター (DAF) がオンにされていることを示しています。

```
ASRT config>list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

00-00-00-22-33-44       PERMANENT       Input Port:  3
                                        Output ports: 1, 2
                                        Input Port:  4
                                        Output ports:  1, 2

00 00 00 33 44 55       PERMANENT       NONE/DAF
```

複数の入力ポートをもつアドレス項目について作成された出力ポート・マップ

この例は、複数の入力ポートをもつアドレス項目について個別の出力ポート・マップを作成するためにコマンド・プロンプトに応答する方法を示しています。

```
ASRT config> add address 000000123456
Exclude destination address from all ports?(Yes or [No]):
Use same output port mapping for all input Ports?(Yes or [No]):
Input Port Number [1]? 1
Bridge to all ports ?(Yes or [No]):
Bridge to port 1 - Yes or [No]: y
Bridge to port 2 - Yes or [No]: y
Bridge to port 3 - Yes or [No]:
continue to another input port ? (Yes or [No]): y
Input Port Number [2]?
Bridge to all Ports?(Yes or [No]):
Bridge to Port 1 - Yes or [No]:
Bridge to port 2 - Yes or [No]:
Bridge to port 3 - Yes or [No]: y
continue to another input port ? (Yes or [No]):
Source Address Filtering Applies? (Yes or [No]):
ASRT config>
```

アドレス項目を追加した後で、**list range** コマンドを使用してアドレス項目の状況を検査することができます。次の例は、入力ポートとしてポート 1 および 2 をもち、両方の入力ポート用に個別のポート・マップをもつ項目 (太字の部分) を示しています。発信元アドレス・フィルター (SAF) も使用可能にされています。

```
ASRT config> list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF

00-00-00-12-34-56       PERM/SAF        Input Port:  1
                                             Output ports: 1, 2
                                             Input Port:  2
                                             Output ports: 3
```

アドレス項目に関連するすべての着信ポートについて作成した単一の出力ポート・マップ

この例では、アドレス項目に関連するすべての着信ポートについて単一の出力ポート・マップを作成するためのコマンド・プロンプトに応答する方法を示しています。

```
ASRT config> add address 000000556677
Exclude destination address from all ports?(Yes or [No]):
Use same output port mapping for all input Ports?(Yes or [No]): y
   Bridge to all ports?(Yes or [No]): n
   Bridge to  port 1 - Yes or [No]: y
   Bridge to  port 2 - Yes or [No]: y
   Bridge to  port 3 - Yes or [No]:
Source Address Filtering Applies? (Yes or [No]): y
ASRT config>
```

アドレス項目を追加した後で、**list range** コマンドを使用してアドレス項目の状況を検査することができます。下の例は、すべての着信ポートについて単一のポート・マップをもつ項目 (太字の部分) を示しています。発信元アドレス・フィルター (SAF) も使用可能にされています。

```
ASRT config> list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF

00-00-00-55-66-77       PERM/SAF        Input Port:  ALL PORTS
                                        Output ports:  1, 2
```

dmac-addr *addr-value*

最高 7 つの重複 MAC アドレス項目をデータベースに追加します。*addr-value* は、必要な項目の MAC アドレスです。重複 MAC アドレス・フィーチャーの詳細については、59ページの『SR-TB 重複 MAC アドレス・フィーチャー』を参照してください。

有効値: X'0000 0000 0000' ～ X'FFFF FFFF FFFF'

省略時値: なし

例:

アドレス項目を追加した後で、**list dmac** コマンドを使用して DMAC 情報を検査することができます。

```
ASRT config>add dmac-addr
Address (in 12-digit hex) []? 10005a777701
ASRT config>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-02
10-00-5A-66-66-05
10-00-5A-77-77-01
```

mapping *dlh-type type-field ga-address fa-address*

所定のプロトコル識別子について特定の機能アドレスからグループ・アドレスへのマップを追加します。アドレス・マップはトークンリングを横切る宛先アドレスでのみイーサネットに変換されます (またはその逆の変換が行われます)。

注: イーサネット・タイプにマップされた各値について、対応する SNAP タイプの値を追加する必要があります。両方向のマップにはこれが必要です。

dlh-type

(データ・リンク・ヘッダー・タイプ) は、DSAP、Etherタイプ、または SNAP 用の選択項目です。

type-field

プロトコル・タイプ・フィールド

あて先サービス・アクセス・ポイント (DSAP) のプロトコル・タイプは、1 ～ FE (16 進数) の範囲で入力します。

DSAP の有効値: X'1' ～ X'FE'

共通の値は次のとおりです。

プロトコル - SAP (16 進値)

– Banyan SAP - BC (802.5 にのみ使用されます)
– Novell IPX SAP - E0 (802.5 にのみ使用されます)
– NetBIOS SAP - F0
– ISO コネクションレス型インターネット - FE

DSAP の省略時値: 1

イーサネット (Ether) のプロトコル・タイプは、5DD ～ FFFF (16 進数) の範囲で入力します。

イーサネットの有効値: X'5DD' ～ X'FFFF'

プロトコル - イーサネット・タイプ (16 進数)

– IP - 0800
– ARP - 0806
– CHAOS - 0804
– Maintenance Packet Type - 7030
– DECnet MOP Dump/Load - 6000
– DECnet MOP Remote Console - 6002
– DECnet- 6003
– DEC LAT - 6004
– DEC LAVC - 6007
– XNS - 0600
– Apollo Domain - 8019 (イーサネット)
– Novell NetWare IPX - 8137 (イーサネット)
– AppleTalk Phase 1 - 809B
– Apple ARP Phase 1 - 80F3
– Loopback assistance - 9000

イーサネット省略時値: 1

サブネットワーク・アクセス・プロトコル (SNAP) のプロトコル・タイプは、10 桁の 16 進形式で入力します。

SNAP 有効値: X'00 0000 0000' ～ X'FF FFFF FFFF'

共通の値は次のとおりです。

– AppleTalk Phase 2 08-00-07-80-9B

– Apple ARP Phase 2 00-00-00-80-F3

SNAP 省略時値: 00 0000 0800

ga-address

6 バイト (12 桁の 16 進数) のグループ/マルチキャスト・アドレス

有効値: X'0000 0000 0000' ～ X'FFFF FFFF FFFF'

省略時値: なし

fa-address

非標準形式の機能アドレス。機能アドレスはローカルに管理されるグループ・アドレスです。これらのアドレスは、トークンリング・ネットワークで最も一般的に使用されます。

有効値: X'0000 0000 0000' ～ X'FFFF FFFF FFFF'

省略時値: なし

例:

```
ASRT config> add mapping dsap

Protocol Type in hex (1 - FE) [1]?
Group-Address (in 12-digit hex) [ ]?
Functional address (in noncanonical format) [ ]?
```

例:

```
ASRT config> add mapping ether

Protocol Type in hex (5DD - FFFF) [0800]?
Group-Address (in 12-digit hex) []?
Functional address (in noncanonical format) [ ]?
```

例:

```
ASRT config> add mapping snap

Address (in 10-digit hex) [0000000800]?
Group-Address (in 12-digit hex) []?
Functional address (in noncanonical format) [ ]?
```

multiaccess-port *interface# port# segment# [bridge#] [virtual-segment#]*

ブリッジング構成にマルチアクセス・ポートを追加します。このコマンドで、ポート番号がフレーム・リレー・インターフェースに対応付けられ、ソース・ルート・ブリッジング用のポートが使用可能になります。

interface#

マルチアクセス・ポートを構成する対象となるフレーム・リレー・インターフェースを指定します。

有効値 : 既存のフレーム・リレー・インターフェース番号のどれか

省略時値 : 0

port# ブリッジ・ポート番号を指定します。この番号は、ルーター内に構成されているブリッジ・ポートすべての間で固有であることが必要です。

有効値 : 1 ～ 254

省略時値 : 次の指定可能なポート番号

segment#

マルチアクセス・セグメントを表すソース・ルーティング・セグメント番号を 12 ビットの 16 進数で指定します。このマルチアクセス・セグメントに接続されているブリッジは、すべてが同一のセグメント番号を使用する必要があります。

有効値 : X'001' ～ X'FFF'

省略時値 : X'001'

bridge#

マルチアクセス・セグメント上でこのブリッジを表すソース・ルーティング・ブリッジ番号を 4 ビットの 16 進数で指定します。このパラメーターが必須なのは、ソース・ルーティングを初めて使用可能にするときだけです。ブリッジ番号は、マルチアクセス・セグメント上のすべてのブリッジの間で固有であることが必要です。

有効値 : X'0' ～ X'F'

省略時値 : X'0'

virtual-segment#

オプションのソース・ルーティング・セグメント番号を 12 ビットの 16 進数で指定します。このパラメーターが必須なのは、3 つ以上のブリッジ・ポート上で初めてソース・ルーティングを使用可能にするときか、マルチアクセス・ブリッジ・ポートを最初に構成するときだけです。

有効値 : X'001' ～ X'FFF'

省略時値 : X'001'

例 :

```
add multiaccess-port
Interface number [0]? 3
Port number [2]? 2
Segment number for the port in hex (1 - FFF) [001]? 200
Bridge number in hex (0-9, A-F) [0]? 1
Bridge Virtual Segment Number in hex (1-FFF) [001]? FFF
```

port *interface# port#*

ブリッジング構成に LAN/WAN ポートを追加します。 このコマンドはポート番号をインターフェース番号と関連させ、そのポートを透過ブリッジングに参加させることができます。

ポート番号の有効値: 1 ～ 254

ポート番号の省略時値: なし

例 : ポートを追加する

```
ASRT config> add port
Interface Number [0]?
Port Number [5]?
```

ATM ポートの追加については、 128ページの『ATM コマンド』 を参照し、フレーム・リレー・ポートの追加については、 127ページの『フレーム・リレー・コマンド』 を参照してください。

prot-filter snap ether dsap

ブリッジがパケットのプロトコル・タイプに応じてパケットを選択的にフィルターできるように、ブリッジを構成することができます。フィルターはすべてのポートに、または選択されたポートにだけ適用できます。

このパラメーターは、その特定のプロトコルの受信フレームにブリッジ論理を適用することなく廃棄するプロトコル識別子を指定します。このプロトコ

ル・タイプ用の ARP パケットも廃棄されます。プロトコル・フィルターは受信されたパケットにのみ適用されます。使用可能なプロトコル・フィルターには次のものが含まれます。

SNAP パケット
プロトコル・タイプが 10 桁の 16 進形式で入力されるサブネットワーク・アクセス・プロトコル

Ether パケット
プロトコル・タイプが 5DD ～ FFFF (16 進数) の範囲で入力されたイーサネット・タイプ。

DSAP パケット
プロトコル・タイプが 0 ～ FE (16 進数) の範囲で入力されたあて先サービス・アクセス・ポイント・プロトコル。

注:

1. タイプ X'AA' の DSAP フィルターを追加しても、すべての SNAP 形式パケットをフィルターすることはできません。カプセル化された SNAP プロトコルを個々にフィルターする必要があります。スライド・ウィンドウ・フィルターの使用を考えてください。 *フィーチャーの使用と構成* の『MAC フィルターの使用』 という章を参照してください。
2. 特定のインターフェースを通るルートを指定されているプロトコルの場合に、プロトコル・フィルターが構成できないのは、インターフェースがブリッジング用としても構成されている場合です。

共通のプロトコル・フィルターおよびそれらのそれぞれの値は次のとおりです。

DSAP タイプ

プロトコル	SAP (16 進値)
Banyan SAP	BC (802.5にのみ使用されます)
Novell IPX SAP	E0 (802.5にのみ使用されます)
NetBIOS SAP	F0
ISO Connectionless Internet	FE

SNAP プロトコル識別子

プロトコル	SNAP OUI/IP (10 桁)
AppleTalk Phase 2	08-00-07-80-9B
Apple ARP Phase 2	00-00-00-80-F3

イーサネット・タイプ

プロトコル	イーサネット・タイプ (16 進数)
IP	0800
ARP	0806
CHAOS	0804
Maintenance Packet Type	7030
DECnet MOP Dump/Load	6000
DECnet MOP Remote Console	6002
DECnet	6003
DEC LAT	6004

プロトコル	イーサネット・タイプ (16 進数)
DEC LAVC	6007
XNS	0600
Apollo Domain	8019 (イーサネット)
Novell NetWare IPX	8137 (イーサネット)
Apple ARP Phase 1	80F3
Loopback assistance	9000

例: ASRT config> **add prot-filter dsap** (DSAP パケットに使用)

```
Protocol Type in hex (0 - FE) [1]?
   Filter packets arriving on all ports?(Yes or [No]):
   Filter packets arriving on  port 1 - Yes or [No]:
   Filter packets arriving on  port 2 - Yes or [No]:
   Filter packets arriving on  port 3 - Yes or [No]:
Port assignment Required, filter not added
ASRT config>
```

例: ASRT config> **add prot-filter ether** (イーサネット・パケットに使用)

```
Protocol Type in hex (5DD - FFFF) [0800]?
   Filter packets arriving on all ports?(Yes or [No]):
   Filter packets arriving on  port 1 - Yes or [No]:
   Filter packets arriving on  port 2 - Yes or [No]:
   Filter packets arriving on  port 3 - Yes or [No]:
Port assignment Required, filter not added
ASRT config>
```

例: ASRT config>**add prot-filter snap** (SNAP パケットに使用)

```
Address (in 10-digit hex) [0000000800]?
Protocol Type in hex (5DD - FFFF) [0800]?
   Filter packets arriving on all ports?(Yes or [No]):
   Filter packets arriving on  port 1 - Yes or [No]:
   Filter packets arriving on  port 2 - Yes or [No]:
   Filter packets arriving on  port 3 - Yes or [No]:
Port assignment Required, filter not added
ASRT config>
```

tunnel *port#*

ブリッジ・ポートにユーザー定義の IP トンネルを作成します。ブリッジ・トンネルにより、ソース・ルート・ブリッジ・ドメインまたは透過型ブリッジ・ドメインは IP ネットワークを介して通信することができます。

IBM LAN および端末トラフィックを単一のバックボーンを介して非 IBM トラフィック (すなわち、Novell) と組み合わせることができるように、ブリッジ・ルーター・ソフトウェアのソース・ルーティング・ブリッジ・トンネルおよび SDLC (同期データ・リンク制御) リレー・フィーチャーは、業界標準 TCP/IP パケット内で IBM トラフィックをカプセル化します。次に、ブリッジング・ルーターは、大型の IP インターネットワークを介して IP パスまたはトンネル を使用してこれらのパケットをルートします。これによってもたらされる利点は、機能性とネットワーク使用効率が向上するだけでなく、ネットワークの可用性が高くなり、さらに容易に使用できるようになることです。

エンド・ステーションは IP パス (トンネル) を、ネットワークの複雑さとは無関係に、単一のホップとして見ます。これにより、ソース・ルーティング構成で検出される通常の 7 ホップの距離の制限を克服することができます。これにより、ソース・ルーティング・エンド・ステーションを非ソース・ルーティング媒体 (イーサネット・ネットワークなど) 越しに接続することができます。

ブリッジ・トンネルは通常のソース・ルーティングのいくつかの制限も克服します。制限には次のものが含まれます。

- 7 つのホップの距離制限
- ソース・ルーティングが広域ネットワーク (WAN) で生じる大きいオーバーヘッド
- ソース・ルーティングが WAN の障害および故障に敏感であること (パスに障害が起こると、すべてのシステムは伝送を再始動する必要がある)

ブリッジ・トンネル・フィーチャーが使用可能になっていると、ソフトウェアはパケットを TCP/IP パケット内にカプセル化します。ルーターにとっては、パケットは TCP/IP パケットのように見えます。フレームが IP エンベロープ内にカプセル化されると、IP 転送機能は、あて先 IP アドレスに基づいて該当するネットワーク・インターフェースを選択する役目をします。このパケットは、性能低下またはネットワーク・サイズの制限なしに、大きなインターネットワークを通じて動的にルートすることができます。ソース・ルーティング・エンド・ステーションは、ネットワークの複雑さとは無関係に、このパスを単一のホップと見なします。

トンネルはエンド・ステーションには透過です。トンネル機能に参加するブリッジング・ルーターは IP インターネットをブリッジ・セグメントの 1 つとして扱います。パケットがあて先インターフェースに到達すると、TCP/IP ヘッダーは自動的に除去され、内側のパケットは標準のソース・ルーティング・パケットとして進みます。

Add Tunnel は、ブリッジ・ポートにつながるユーザー定義の IP トンネルを作成します。このトンネルは、IP インターネットを通じたパスがどれほど複雑であっても、ブリッジ間のただ 1 つのホップとしてカウントされます。トンネル・フィーチャーを使用するには、IP 転送側が使用可能なっている必要があります。

追加できるトンネルは 1 つだけです。他の LAN ポートに使用されない *Port Number* を使用する必要があります。ブリッジング・トンネルに Port Number が割り当てられていれば、パラメーターとしてポート番号を必要とする他のすべてのブリッジング・コマンドを使用して、そのトンネル特性を構成することができます。エンドポイントの IP アドレスなど、トンネル固有の構成については、**tunnel** コマンドを使用します (121ページの『Tunnel』を参照)。

このポートでは省略時解釈で透過ブリッジングが使用可能にされます。ただし、**Enable Source-Routing** オプションを使用すると、ソース・ルーティングを使用可能にできます。

例: **add tunnel 3**

```
Port Number [1]? 3
```

Port Number
ブリッジによって使用されていない固有のポート番号

BAN

境界アクセス・ノード (BAN) 構成プロンプトへアクセスするには、**ban** コマンドを使用してください。BAN コマンドは、BAN 構成プロンプト (BAN config>) で入力します。これらのコマンドのそれぞれの説明については、121ページの『BAN 構成コマンド』を参照してください。

構文:

ban

例: **ban**

```
BAN (Boundary Access Mode) configuration
BAN config>
```

Change

change コマンドは、ブリッジング構成におけるソース・ルーティング・ブリッジ番号およびセグメント番号を変更するのに使用します。

構文:

change bridge . . .

segment . . .

bridge *new-bridge#*

ブリッジング構成内のブリッジ番号を変更します。

例: change bridge 3

segment *old-segment# new-segment#*

ブリッジング構成内のセグメント番号を変更します。

例: change segment 2 3

Delete

delete コマンドは、ブリッジング構成から次の情報を削除するのに使用します。

- 永続データベースのステーション・アドレス項目
- 所定のプロトコルの特定のアドレス・マップ
- LAN/WAN ポート
- パケットをそのプロトコル・タイプに基づいて選択的にフィルターするプロトコル・フィルター
- 重複 MAC アドレス

IP トンネル・フィーチャーでは、トンネル用のポート番号を指定した **delete port** コマンドが、IP インターネットワークを横断するブリッジ間のトンネルを除去します。

構文:

delete address

dmac-addr

mapping . . .

port . . .

prot-filter . . .

address *addr-value*

永続データベースからアドレス項目を削除します。このアドレスは削除したい項目の MAC アドレスです。削除する項目の addr-value (12 桁の 16 進形式) を入力し、**Return** を押してください。予約済みのマルチキャスト・アドレスは削除できません。存在していないアドレス項目を削除しようとすると、次のメッセージを受け取ります。

```
Record matching that address not found
```

有効値: X'0000 0000 0000' ～ X'FFFF FFFF FFFF'

省略時値: なし

例: delete address

dmac-addr *addr-value*

データベースから重複 MAC アドレス項目を削除します。*addr-value* は削除したい項目の MAC アドレスです。

有効値: X'0000 0000 0000' ～ X'FFFF FFFF FFFF'

省略時値: なし

例:

```
ASRT>list gamic
Duplicate MAC address feature is   DISABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05

ASRT config>delete dmac-address
Address (in 12-digit hex) []? 10005a666600
Address deleted

ASRT config>list dmac
Duplicate MAC address feature is   DISABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

mapping *dlh-type type-field ga-address*

所定のプロトコルの特定のアドレス・マップを削除します。

dlh-type

(データ・リンク・ヘッダー・タイプ) は、DSAP、Etherタイプ、または SNAP 用の選択項目です。

type-field

プロトコル・タイプ・フィールド

あて先サービス・アクセス・ポイント (DSAP) のプロトコル・タイプは、1 ～ FE (16 進数) の範囲で入力します。

有効値: X'1' ～ X'FE'

共通の値は次のとおりです。

プロトコル - SAP (16 進値)

省略時値: 1

イーサネット (Ether) のプロトコル・タイプは、5DD ～ FFFF (16 進数) の範囲で入力します。

有効値: X'5DD' ～ X'FFFF'

省略時値: 1

サブネットワーク・アクセス・プロトコル (SNAP) のプロトコル・タイプは、10 桁の 16 進形式で入力します。

有効値: X'00 0000 0000' ～ X'FF FFFF FFFF'

共通の値は次のとおりです。

省略時値: 00 0000 0800

ga-address

6 バイト (12 桁の 16 進数) のグループ/マルチキャスト・アドレス

有効値: X'0000 0000 0000' ～ X'FFFF FFFF FFFF'

省略時値: なし

例 : delete mapping DSAP FE <group address>

port *port#*

ブリッジング構成からポートを除去します。省略時の **enable bridge** コマンドはすべての LAN 装置がブリッジに参加するように構成するので、このコマンドにより、どの装置がブリッジに参加すべきか、または参加すべきでないかをカストマイズできます。ポート番号値は通常、インターフェース番号より 1 大きくなります。

このコマンドの後に IP tunnel port# を入力すると、ブリッジング構成から IP トンネルが除去されます。

例: delete port 2

prot-filter snap ether dsap

フィルターに使用される、以前に指定したプロトコル識別子が削除されます。すべてのポートについて、または選択されたポートについて、フィルターを削除できます。これらのフィルターには次のものが含まれます。

SNAP パケット

プロトコル・タイプが 10 桁の 16 進形式で入力されるサブネットワーク・アクセス・プロトコル

Ether パケット

プロトコル・タイプが 5DD ～ FFFF (16 進数) の範囲で入力されるイーサネット・タイプ

DSAP パケット
プロトコル・タイプが 0 ～ FE (16 進数) の範囲で入力される宛先サービス・アクセス・ポイント・プロトコル

例: ASRT config> **delete prot-filter snap** (SNAP パケットに使用)

```
Address (in 10-digit hex) [0000000800]?
   Delete filter on all ports?(Yes or [No]):
   Delete filter on  port 1 - Yes or [No]:
   Delete filter on  port 2 - Yes or [No]:
   Delete filter on  port 3 - Yes or [No]:
```

例: ASRT config> **delete prot-filter ether** (イーサネット・パケットに使用)

```
Protocol Type in hex (5DD - FFFF) [0800]?
   Delete filter on all ports?(Yes or [No]):
   Delete filter on  port 1 - Yes or [No]:
   Delete filter on  port 2 - Yes or [No]:
```

例: ASRT config> **delete prot-filter dsap** (DSAP パケットに使用)

```
Protocol Type in hex (0 - FE) [1]?
   Delete filter on all ports?(Yes or [No]):
   Delete filter on  port 1 - Yes or [No]:
   Delete filter on  port 2 - Yes or [No]:
   Delete filter on  port 3 - Yes or [No]:
```

Disable

disable コマンドは、以下のブリッジ機能を使用不能にするのに使用します。

- ブリッジング
- 重複フレーム
- グループ・アドレスと機能アドレス間のマップ
- スパンニング・ツリー探索フレームの伝送
- 特定のポートでのソース・ルーティング
- SR-TB 変換
- 特定のポートでの透過 (スパンニング・ツリー) ブリッジング機能
- 重複 MAC アドレス・フィーチャー
- 重複 MAC 負荷平衡
- DLSw

トンネル・フィーチャーについては、disable コマンドは IP インターネットワークを横断するエンド・ステーション間のトンネルを使用不能にします。

構文:

disable bridge
dls
duplicate . . .
dmac-addr
dmac-load-balance
ethertype-ibmrt-pc
fa-ga-mapping

ibm8209_spanning_tree

spanning-tree-explorer . . .

source-routing . . .

sr-tb-conversion

stp

transparent . . .

tree

ub-encapsulation

bridge

ブリッジング機能を全般的に使用不能にします。ただし、このコマンドは以前に構成されたブリッジング値を除去することはしません。

例: `disable bridge`

dls ブリッジ上での DLSw の操作を使用不能にします。(DLSw を実行するルーターは、エンド・ステーションにはブリッジから見えます。) 詳しくは、493 ページの『第25章 DLSw フィーチャーの使用』を参照してください。

例: `disable dls`

duplicate *frame-type*

混合ブリッジ環境にある重複フレームの作成を使用不能にします。802.5 インターフェースで SR-TB ブリッジング機能を使用可能にする (ソース・ルーティングおよび透過ブリッジングを使用可能にする) 場合、ブリッジ・フレームが不明の (またはマルチキャストの) あて先に向けられると、矛盾が生じます。あて先がソース・ルーティング (のみ) または透過ブリッジングの背後にあるかどうかはブリッジにとっては不明です。

この状態を修正するために、ブリッジはこれらのフレームの複写を送信します (省略時)。1 つのフレームにはソース・ルーティング・フィールドがあり (スパンニング・ツリー探索 RIF)、もう一方は透過ブリッジング用にフォーマットされています (RIF はありません)。**disable duplicate** コマンドにより、これらのフレームの 1 つの作成を使用不能にできるようにして、この重複を除去することができます。 **disable duplicate** コマンドを使用して、両方のタイプのフレームを同時に使用不能にすることはできません。

コマンドの後に **STE** を入力すると、ブリッジに対して、ソース・ルーティング環境用に作成されたスパンニング・ツリー探索フレームの送信を控えるよう指示がなされます。コマンドの後に **TSF** を入力すると、ブリッジに対して、透過ブリッジング環境用に作成された透過スパンニング・フレームの送信を控えるよう指示がなされます。両方の場合のいずれも、通常ならば両方のタイプのフレームが送信されたであろう状態です。インターフェース上で透過ブリッジングを使用不能にすると、透過フレームの作成も使用不能になります。

例: `disable duplicate TSF`

```
Port Number [1]?
```

dmac-addr

重複 MAC アドレス・フィーチャーを使用不能にします。

例: disable dmac-addr

```
ASRT>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05

ASRT config>disable dmac-addr

ASRT>list dmac
Duplicate MAC address feature is   DISABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

dmac-load-balance

重複 MAC アドレス・フィーチャーについて重複 MAC 負荷平衡を使用不能にします。

例: disable dmac-load-balance

```
ASRT>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
ASRT config>disable dmac-load-balance
ASRT>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

ethertype-ibmrt-pc

SNA フレームの、OS/2 EE で稼働する IBM RT によって使用されるようにイーサネット・タイプ 2 形式への変換を使用不能にします。

例: disable ethertype-ibmrt-pc

```
    Port Number [1]?
```

fa-ga-mapping

グループ・アドレスから機能アドレスへの (およびその逆の) マッピングを使

用不能にします。特定の環境では、グループ・アドレスと機能アドレス間のマッピングを広範囲で使用不能にしたい場合もあります。

例: disable fa-ga-mapping

ibm8209_spanning_tree
ブリッジが IBM 8209 ブリッジとのスパンニング・ツリー・プロトコルに参加しないように除去します。

例 : disable ibm8209_spanning_tree

spanning-tree-explorer *port#*
ソース・ルーティングが使用可能になっている場合に、ポートがスパンニング・ツリー探索フレームを伝送できないようにします。このコマンドが使用されるのは、ポートで透過ブリッジングが使用可能になっていない場合に限られます。その場合には、透過スパンニング・ツリーに適合して自動的に知らされます。

例: disable spanning-tree-explorer 2

source-routing *port#*
所定のポートでソース・ルーティングを使用不能にします。このコマンドは、すでに参加しているブリッジ・インターフェースにソース・ルーティングを中断させます。

例: disable source-routing 2

sr-tb-conversion
ソース・ルーティングされたフレームから透過フレームへの変換およびその逆の変換を使用不能にします。

例: disable sr-tb-conversion

stp ブリッジでのスパンニング・ツリー・プロトコルを使用不能にします。省略時値は使用可能です。

例: disable stp

transparent *port#*
特定のポートでの透過ブリッジング機能を使用不能にします。このコマンドは、ソース・ルーティングなどの代替通信方式が必要な場合に役立ちます。

注: このコマンドは正しく使用しないと、不合理な構成を生じさせることがあります。例えば、このコマンドをイーサネット・インターフェースで使用すると、そのインターフェースに関してブリッジング機能が使用不能になる結果を招きます。このコマンドは、SRB および SR-TB ブリッジ機能をもたらすために使用するものです。

例: disable transparent 2

tree *port#*
ポートごとにブリッジへの STP の参加を使用不能にします。

例: disable tree 1

注: ポートごとに STP を使用不能にすると、並列ブリッジが存在しているため、ネットワーク・ループが発生することがあります。

ub-encapsulation

XNS フレームの Ungermann-Bass OUI カプセル化を使用不能にします。XNS フレームは、すべてゼロの OUI をもつ SNAP カプセル化を使用してイーサネットとトークンリングの両方に転送されます。

例: `disable ub-encapsulation`

Enable

以下のブリッジング機能を使用可能にするには、**enable** コマンドを使用します。

- ブリッジング
- 重複フレーム
- グループ・アドレスと機能アドレス間のマップ
- スパンニング・ツリー探索フレームの伝送
- 特定のポートでのソース・ルーティング
- SR-TB 変換
- 特定のポートでの透過 (スパンニング・ツリー) ブリッジング機能
- 重複 MAC アドレス・フィーチャー
- 重複 MAC 負荷平衡
- DLSw

IPトンネル・フィーチャーでは、**enable** コマンドは IP インターネットワークにまたがるエンド・ステーション間のトンネルを使用可能にします。

構文:

enable bridge . . .
dls
duplicate
dmac-addr
dmac-load-balance
ethertype-ibmrt-pc
fa-ga-mapping
ibm8209_spanning_tree
spanning-tree-explorer . . .
source-routing . . .
sr-tb-conversion
stp
transparent . . .
tree
ub-encapsulation

ASRT 構成コマンド (Talk 6)

bridge

ブリッジング・ルーターで構成されたすべての LAN 装置（インターフェース) の透過ブリッジング機能を使用可能にします。ポート番号は、各インターフェースに直前のインターフェース番号プラス 1 として割り当てられます。例えば、インターフェース 1 が LAN 装置である場合には、そのポート番号は 1 になります。

例: enable bridge

dls ブリッジ上での DLSw の操作を使用可能にします。DLSw を実行するルーターは、エンド・ステーションにはブリッジから見えます。詳しくは、493ページの『第25章 DLSw フィーチャーの使用』を参照してください。

例: enable dls

duplicate *frame-type*

重複する STE (スパンニング・ツリー探索) フレームまたは TSF (透過スパンニング・フレーム) フレームの生成を使用可能にします。このコマンドは、**disable duplicate** コマンドを補うために使用できます。省略時解釈では重複フレーム生成が使用可能になります。**enable duplicate** コマンドの後にフレーム・タイプ **TSF** または **STE** を続けて入力すると、それらのフレーム・タイプの 1 つを特に使用可能にすることができ、フレーム・タイプ **BOTH** を続けて入力すると、このパラメーターにフレーム・タイプを指定しない場合と同じ行動を生じます。

例: enable duplicate STE

```
Port Number [1]?
```

dmac-addr

重複 MAC アドレス・フィーチャーを使用不能にします。重複 MAC アドレス・フィーチャーの詳細については、59ページの『SR-TB 重複 MAC アドレス・フィーチャー』を参照してください。

負荷平衡がある場合の例:

```
ASRT config>enable dmac-addr

ASRT config>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05

ASRT config>enable dmac-load-balance

ASRT config>li dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

例 (負荷平衡なしの場合) :

```
ASRT config>enable dmac-addr

ASRT config>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

dmac-load-balance

重複 MAC アドレス・フィーチャーについて重複 MAC 負荷平衡を使用不能にします。重複 MAC 負荷平衡の説明については、59ページの『SR-TB 重複 MAC アドレス・フィーチャー』の記述を参照してください。

例:

```
ASRT config>enable dmac-addr

ASRT config>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05

ASRT config>enable dmac-load-balance

ASRT config>li dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is    ENABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

ethertype-ibmrt-pc

OS/2 EE で稼働する IBM PC RT によって使用されるように SNA フレームのイーサネット・タイプ 2 への変換を使用可能にします。これにより、SNA フレームはイーサネット上のホストにとって未知の 802.3/802.2 形式および IBM-RT 形式の両方に複写されます。

例: enable ethertype-ibmrt-pc

```
            Port Number  [4]?
```

fa-ga-mapping

グループ・アドレスから機能アドレスへの (およびその逆の) マッピングを使用可能にします。このマッピングは、フレームがトークンリングと他の媒体 (シリアル回線を除く) の間を転送されるときに行われます。トークンリング領域では、ハードウェアの制約のため、ローカルに割り当てられたグループ・アドレスですが、機能アドレスの方が一般的です。その他の媒体では、グループ・アドレスが広く使用されます。通常の環境では、グループ・アドレスから機能アドレスへのマッピングが必ず行われます。

マップ・アドレスが追加されていれば、省略時解釈でマップが使用可能にされます。追加したマップ・レコードの削除に関しては、マップを使用可能/使用不能にすることによりユーザーが選択することができます。

例: enable fa-ga-mapping

ibm8209_spanning_tree

ブリッジが IBM 8209 ブリッジを使ったスパニング・ツリー・プロトコルに参加することができます。

例 : enable ibm8209_spanning_tree

spanning-tree-explorer *port#*

ソース・ルーティングが使用可能になっている場合には、ポートを使用可能にしてスパニング・ツリー探索フレームを伝送できるようにします。このコマンドはトークンリングと WAN のポートでのみ有効です。ポートでソース・ルーティングが構成されているときには、省略時解釈でこのフィーチャーが使用可能になります。

例: enable spanning-tree-explorer 2

source-routing *port# segment# [bridge#]*

所定のポートについてソース・ルーティングを使用可能にします。ブリッジの部分でソース・ルーティングが必要な場合は、このコマンドが一般に使用されます。ソース・ルーティングが必要な唯一のフィーチャーである場合には、インターフェースでの透過ブリッジングは使用不能にする必要があります。コマンドの最初のインスタンスでは、ブリッジ番号を入力する必要があります。その後は、この入力は必要でありません。

port# ブリッジ構成に参加する有効なポート

有効値: X'0' ～ X'FFF'

省略時値: 1

segment#

媒体が接続される LAN/WAN を表す 12 ビットの番号。この LAN/WAN に接続された他のブリッジ上のすべての媒体は同じ値を使用して構成する必要があります。ソース・ルーティング機能が正しく働くためには、この LAN/WAN に接続されたすべてのブリッジが LAN/WAN 識別値の同じ外見をもつことが非常に重要です。

bridge#

同じ LAN/WAN に接続されたすべてのブリッジの間で固有の 4 ビットの値。最初のインターフェースでソース・ルーティングが使用可能になっているときには、この値が必須です。それより後のインターフェースでは、この入力は任意です。bridge# はセグメントで固有なものにしてください。

有効値: X'0' ～ X'F'

省略時値: 1

注: 構成が、2 つのセグメントがすでに構成されている (つまり、1:N SRB 構成) 状態である場合には、追加の*virtual-segment#* パラメーターを入力するようプロンプト指示されます。

例: enable source-routing 2 1 1

sr-tb-conversion

このオプションを選択すると、ソース・ルーティング・フレームから透過ブリッジング・フレームへの形式変換またはその逆の変換が使用可能になります。この場合、ソース・ルーティング・ドメインと透過ブリッジング・ドメイン間の互換性が許されます。このフィーチャーが使用可能になっているときは、RIF フィールドをストリップし、透過フレームに変換することにより、ブリッジがソース・ルーティングされたフレームを透過ドメインに受け入れられるようにします。

またブリッジは、通過するソース・ルーティング・フレームからソース・ルーティング・ステーションに関するルーティング情報を収集します。これは RIF から入手されます。次にこの RIF 情報を使用して、透過フレームからソース・ルーティング・フレームに変換します。ステーションで RIF が入手できない場合には、フレームはスパンニング・ツリー探索フレームとしてソース・ルーティング・ドメインに送信されます。

変換機能が正しく働くようにするために、透過ブリッジング・ドメインにセグメント番号を与える必要があります。このドメインに接続されるすべての SR-TB ブリッジも、同じセグメント番号を使って構成する必要があります。

TB ドメイン・セグメント番号の有効値: X'1' ～ X'FFF'

TB ドメイン・セグメント番号の省略時値: 1

最大伝送単位 (MTU) は、所定の物理ネットワークを介して伝送できるデータの、フレームあたりのオクテット数です。IP データグラムが 1 つのホストから別のホストに送信される場合、異なる物理ネットワークを経て送信できます。一部の物理ネットワークではこの MTU が設定されており、物理フレーム上では長い IP データグラムを入れられない場合があります。その物理ネットワークが扱えないほど大きなフレームを送信使用とすると、断片化が発生します。

TB ドメイン MTU の有効値: 576 ～ 18000 バイト

TB ドメイン MTU の省略時値: 2048

例: enable sr-tb-conversion

```
TB-Domain Segment Number in hex(1 - FFF) [1]? 2
Bridge Virtual Segment Number in hex[1 - FFF]? aa
TB-Domain's MTU [1470]? 1455
TB-Domain's MTU is adjusted to 1350
```

stp ブリッジでスパンニング・ツリー・プロトコルを使用可能にします。 これが省略時値です。

例: enable stp

transparent *port#*

特定のポートで透過ブリッジング機能を使用可能にします。通常の状況では、このコマンドは必要ありません。

例 : enable transparent

```
Port Number [1]?
```

tree *port#*

ポートごとにブリッジへの STP の参加を使用可能にします。

例: enable tree 1

ub-encapsulation

SNAP ヘッダー内の Ungermann-Bass OUI を使用して、XNS イーサネット・タイプ 2 のフレームをトークンリング・フレームに変換させます。UB OUI ヘッダーを含むトークンリング・フレームは、802.3/802.2 フレームとしてではなく、タイプ 0x0600 のイーサネット・タイプ 2 フレームとしてイーサネットに転送されます。

例: enable ub-encapsulation

List

全体のブリッジ構成についての情報を表示するか、選択された構成パラメーターについての情報を表示するには、**list** コマンドを使用してください。

構文:

list

address

bridge

dmac

filtering . . .

mapping . . .

multiaccess

permanent . . .

port . . .

prot-filter . . .

protocol

range . . .

address *addr value*

永続データベースからアドレス項目を読み取ります。この addr 値は、必要な項目の MAC アドレスです。これは、個別アドレス、マルチキャスト・アドレス、または同報通信アドレスになりえます。 永続データベースは、電源オフ/オンのプロセスによって破壊されることはなく、経過時間の設定値によって影響されません。永続項目が、動的項目によって取って代わられることはありません。

有効値: X'0000 0000 0000' ～ X'FFFF FFFF FFFF'

省略時値: なし

例: list address 000000123456

```
0000-00-12-34-56    PERMANENT  Input Port:  1
                               Output ports: 1, 2
                               Input port:  2
                               Output ports:  3
ASRT config>
```

Address

12 桁の 16 進形式のアドレス項目

Entry Type

Permanent
本質的に永続項目であり、電源オン/オフまたはシステム・リセットの後も存続することを示します。

Reserved
IEEE 802.1d 委員会による将来の使用に備えた予約済み項目であることを示します。予約済みアドレスあてのフレームは廃棄されます。

Registered
ブリッジ自体用の項目であることを示します。

SAF 発信元アドレス・フィルターが構成される場合に、項目タイプの後に現れます。

Input Port
そのアドレス項目に関連する入力ポートの番号を表示します。

Output Port
そのアドレス項目に関連する出力ポートの番号を表示します。アドレス項目に関連するポートが選択されていないので、あて先アドレス・フィルターが適用されることを示すために 『NONE/DAF』 を表示します。

bridge

ブリッジに関するすべての一般情報をリストします。

例: list bridge

```
Source Routing Transparent Bridge Configuration
===============================================

Bridge:  ENABLED                        Bridge Behavior: ADAPTIVE SRT
                  +----------------------------+
-----------------| SOURCE ROUTING INFORMATION |---------------------------
                  +----------------------------+
Bridge Number:          0A                Segments:          2
Max ARE Hop Cnt:        14                Max STE Hop cnt:  14
1:N SRB:                Active           Internal Segment:  0xFF6
LF-bit interpret:       Extended
                  +--------------------+
-----------------| SR-TB INFORMATION |-----------------------------------
                  +--------------------+
SR-TB Conversion:        Enabled
TB-Virtual Segment:      0x107               MTU of TB-Domain:   1470
                  +-------------------------------------+
-----------------| SPANNING TREE PROTOCOL INFORMATION |------------------
                  +-------------------------------------+
Bridge Address:         00-00-00-00-00-06    Bridge Priority:   32768/0x8000

STP Participation:      IEEE802.1d and IBM-8209
                  +--------------------------+
-----------------| TRANSLATION INFORMATION |-----------------------------
                  +--------------------------+
FA<=>GA Conversion:     Enabled                UB-Encapsulation:  Disabled
DLS for the bridge:     Enabled
                  +------------------+
-----------------| PORT INFORMATION |-----------------------------------
                  +------------------+
Number of ports added:  3
Port:   1      Interface:     0      Behavior:   STB only    STB:  Enabled
VPI:   0      VCI:          48
Port:   2      Interface:     1      Behavior:   STB & SRB   STB:  Enabled
Port:   3      Interface:     2      Behavior:   STB & SRB   STB:  Enabled
Port:   4      Interface:     0      Behavior:   STB only    STP: Enabled
Dest ATM Address: 39.11.22.33.44.55.66.77.88.99.00.11.22.33.44.55.66.77.88.99
```

Bridge
ブリッジの現行の状態を示します。値は ENABLED (使用可能) または DISABLED (使用不能) です。

Bridge Behavior
そのブリッジで使用されているブリッジングの方式を示します。値には、透過ブリッジングの場合は STB が、ソース・ルーティングの場合は SRB が、ソース・ルーティング透過変換ブリッジングの場合は ADAPTIVE がそれぞれ含まれます。

Bridge address
ユーザーによって指定されるブリッジ・アドレス (設定されている場合)。

Bridge priority
ブリッジ識別子内にある上位の 2 オクテットのブリッジ・アドレス。最小番号のポートから入手された MAC アドレスまたは Set Bridge コマンドによって設定されたアドレスのいずれか。

Source Routing Bridge Number
ブリッジを識別する固有の番号。 同じ 2 つのリングを接続する複数のブリッジを区別するために使用されます。

Number of Source Routing Segments
ソース・ルーティング・ドメイン用に構成されたソース・ルーティング・ブリッジ・セグメントの数を示します。

SRB: Max ARE/STE Hop cnt
ブリッジから、ソース・ルーティング・ブリッジングに関連する所定のインターフェースへと伝送されるフレームの最大ホップ・カウント

SR-TB Conversion
ソース・ルーティング/透過型ブリッジ・フレーム変換機能が使用可能になっているか、使用不能になっているかを示します。

TB-Virtual Segment
透過ブリッジング・ドメインのセグメント番号を示します。

MTU for TB-Domain
透過ブリッジングが送受信できる最大フレーム・サイズ (最大伝送単位) を指定します。

1:N Source Routing
1:N ソース・ルーティングの現行の状態が ACTIVE (アクティブ) であるか NOT ACTIVE (非アクティブ) であるかを示します。

Internal Virtual Segment
1:N SRB ブリッジング用に構成されたバーチャル・セグメント番号を表示します。

SRB LF-bit interpretation
このブリッジでソース・ルーティングが使用可能になっている場合には、最大フレーム (LF) ビット・コード化変換処理モードを示します。これは BASIC (基本) または EXTENDED (拡張) としてリストされます。

FA-GA conversion
FA-GA 変換が使用可能になっているか、使用不能になっているかを示します。

Spanning Tree Protocol Participation
ブリッジが参加するスパンニング・ツリー・プロトコルのタイプを表示します。

DLS for the bridge
ブリッジでデータ・リンク・スイッチ・プロトコルが使用可能になっているか、使用不能になっているかを示します。

Number of ports added
ブリッジング構成に追加されるブリッジ・ポートの数

Port Number
Add Port コマンドによってインターフェースに割り当てられたユーザー定義の番号

Interface Number
ブリッジを通じてネットワーク・セグメントに接続された装置を識別します。 ブリッジに参加するには、少なくとも 2 つのインターフェースを追加する必要があります。 ブリッジには 255 のインターフェース番号が使用されます。

Port Behavior
そのブリッジで使用されているブリッジングの方式を示します。透過ブリッジングの 場合には STB、ソース・ルート・ブリッジングの場合は SRB です。

VPI ATM ポートと関連付けられた VPI を指定します。

VCI ATM ポートと関連付けられた VCI を指定します。

dmac 重複 MAC アドレス・フィーチャーの構成済みのオプションを表示します。

例 : `list dmac`

```
Duplicate MAC address feature is    ENABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

filtering *datagroup-option*
list filtering コマンドのもとで、以下の一般データ・グループが表示できます。

All すべてのフィルター・データベース項目を表示します。

Ethertype
イーサネット・プロトコル・タイプのフィルター・データベース項目を表示します。

SAP SAP プロトコルのフィルター・データベース項目を表示します。

SNAP SNAP プロトコル ID のフィルター・データベース項目を表示します。

以下の例は、**list filtering** 表示オプションのそれぞれを例示するものです。

例 1: list filtering all

```
Ethernet type 0800 is routed on ports 1
IEEE 802.2 destination SAP 42 is routed on ports 1
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

パケットがどのように通信されるかを説明するのに使用される記述子には次のものが含まれます。

Routed
転送するためにルーティングの転送側に渡されるパケットを記述します。

Filtered
ユーザーが設定する、管理上フィルターされた設定プロトコル・フィルターであるパケットを記述します。

Bridged and routed
システム内に転送側ではないプロトコル・エンティティーがあるプロトコル ID を記述します。例えば、リンク・レベルのエコー・プロトコルです。このプロトコルからのユニキャスト・パケットは、登録済みアドレスに送信される場合にはブリッジされるか、ローカルに処理されます。 マルチキャスト・パケットは、登録済みマルチキャスト・アドレスの場合は、転送されるか、ローカルに処理されます。

上記の記述子はすべて、Ethertype による ARP パケットにも適用されます。

例 2: list filtering ethertype

```
Ethernet type (in hexadecimal), 0 for all [0]? 0800
Ethernet type 0800 is routed on ports 1
```

例 3: list filtering sap

```
SAP (in hexadecimal), 100 for all [100]? 42
IEEE 802.2 destination SAP 42 is routed on ports 1
```

例 4: list filtering snap

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

mapping *add-type type-field*
所定のプロトコルについての特定アドレス・マップをリストします。

例: list mapping SNAP

```
PROTOCOL TYPE          GROUP ADDRESS          FUNCTIONAL ADDRESS
=============          =============          ==================
123456-7890            12-34-56-78-90-12      12:34:56:78:90:12
```

add-type
DSAP、Ether (イーサネット)、または SNAP のいずれかの選択

type-field
プロトコル・タイプ・フィールド:

- あて先サービス・アクセス・ポイント (DSAP) のプロトコル・タイプは、1 ～ FE (16 進数) の範囲で入力します。
- イーサネット(Ether)のプロトコル・タイプは、5DD ～ FFFF (16 進数) の範囲で入力します。
- サブネットワーク・アクセス・プロトコル (SNAP) のプロトコル・タイプは、10 桁の 16 進形式で入力します。

multiaccess

マルチアクセス・データベース内の項目の経過時間が表示され、マルチアクセス・ブリッジ・ポートが表示されます。ブリッジ・ポート・パラメーターの記述については、**list port** コマンドの出力を参照してください。

例 : `list multiaccess`

```
Aging time (in seconds): 300

Port ID (dec)    : 238:02, (hex): 80-02
Port State       : Enabled
STP Participation: Disabled
Port Supports    : Source Route Bridging Only
SRB: Segment Number: 0x003       MTU:  2040     STE: Enabled
Assoc Interface  : 1
Path Cost        : 0
```

permanent

ブリッジの永続データベース内の項目の数を表示します。

例: `list permanent`

```
            Number of Entries in Permanent Database:  17
```

port *port#*

すでに構成済みのポートに関連するポート情報を表示します。 Port# では、リストしたいポートを選択します。番号を指定しない場合は、すべてのポートを選択したことになります。

例: `list port`

```
Port Id (dec)    : 128: 5, (hex): 80-05
Port State       : Enabled
STP Participation: Enabled
Port Supports    : NO Bridging
Assoc Interface  : 1
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port Id (dec)    : 128: 6, (hex): 80-06
Port State       : FORWARDING
STP Participation: Enabled
Port Supports: Source Routing Bridging Only
SRB: Segment Number:  0x116     MTU:  1979
STE Forwarding:  Auto
Assoc Interface #/name : 1/FR/0   Circuit number 16
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port Id (dec)    : 128: 7, (hex): 80-07
Port State       : FORWARDING
STP Participation: Enabled
Port Supports: Source Routing Bridging Only
SRB: Segment Number:  0x117     MTU:  1979
STE Forwarding:  Auto
Assoc Interface #/name : 1/FR/0   Circuit number 17
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port ID (dec)    : 128: 2, (hex): 80-02
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 0  VPI  0  VCI:    78
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port ID (dec)    : 128: 3, (hex): 80-03
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 2
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

```
Port ID (dec)    : 128: 1, (hex): 80-01
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 0  VPI:   0  VCI:   795
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port ID (dec)    : 128: 4, (hex): 80-04
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 0  Dest ATM Addr: 391122334455667788990011223344
                                                              5566778899
Path Cost        : 0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Port ID

この ID はポート優先度とポート番号の 2 つの部分から構成されます。例では、128 が優先度で、1、2、および 3 はポート番号です。16 進形式では、下位バイトはポート番号を示し、上位バイトは優先度を示します。

Port state

指定されたポートの現行の状態を表示します。これは ENABLED (使用可能) または DISABLED (使用不能) のいずれかです。

Port supports

そのポートによってサポートされるブリッジング方式 (例えば、透過ブリッジング、ソース・ルーティング・ブリッジング) を表示します。

SRB SRB が使用可能になっているときだけ表示され、ソース・ルーティング・ブリッジング情報をリストします。これには、SRB セグメント番号 (16 進数)、最大伝送単位サイズ、およびスパンニング・ツリー探索フレームの使用可能または使用不能状態が含まれています。

Duplicate Frames Allowed

許容されている重複フレームのタイプの内訳およびカウントを表示します。

Assoc interface

表示されたポートと関連付けられたインターフェース番号を表示します。ポートが ATM インターフェース上に存在する場合には、VPI/VCI または宛先 ATM アドレスも表示します。

Path Cost

可能なルート・パス・コストに使用されるポートに関連するコスト。範囲は 1 ～ 65535 です。

prot-filter *port#*

フィルター・プロトコル・タイプの現行のリストを読み取ります。フィルターはポート別に選択的にリストできますし、あるいはすべてのポートを一度に表示することもできます。Port# (ポート番号) ではリストしたいブリッジ・ポートを選択します。

例: `list prot-filter 1`

```
PORT 1
Protocol Class   :  DSAP
Protocol Type    :  01
Protocol State:  :  Filtered
Port Map         :  1, 2, 3
```

Port Number
すべてのポートを表示するよう選択する場合には、各ポートごとにポート番号が表示されます。

Protocol Class
表示・クラス (SNAP、Ether、または DSAP) を表示します。

Protocol Type
プロトコル ID を 16 進形式で表示します。

Protocol State
プロトコルが選択されたポート用にフィルターされていることを示します。

Port Map
このタイプのプロトコル・フィルターがあるポートの番号を表示します。

プロトコル (protocol)
スパンニング・ツリー・プロトコルに関連するブリッジ情報を表示します。

例: `list protocol`

```
IEEE 802.1d Spanning Tree Configuration:
 Bridge Identifier                : 32768/000000000000 (using port address)
 Bridge-Max-Age (in seconds)      : 20
 Bridge-Hello-Time (in seconds)   : 2
 Bridge-Forward-Delay (in seconds): 15

SRB Spanning Tree Configuration:
 Bridge Identifier                : 32768/000000000000 (using port address)
 Bridge-Max-Age (in seconds)      : 20
 Bridge-Hello-Time (in seconds)   : 2
 Bridge-Forward-Delay (in seconds): 15
```

注: これらのブリッジに関連するパラメーターのそれぞれについては、前の章でも詳しく説明しています。

Bridge Identifier
ASCII 形式の 8 バイトの値。この情報の表示に先立ってブリッジ・アドレスが設定されていない場合は、下位の 6 バイトがゼロとして表示され、ポートの省略時の MAC アドレスが使用されていることを示します。ブリッジがルート・ブリッジとして選択されていたときには、ブリッジの最大経過時間およびブリッジのハロー時間がルート・ブリッジから HELLO BPDU を介してネットワーク内のすべてのブリッジに伝送されます。

Bridge-Max-Age
スパンニング・ツリー・プロトコルに関連する情報のタイムアウトに使用される最大経過時間

Bridge-Hello-Timer
HELLO BPDU 間の時間間隔

Bridge-Forward-Delay
(このブリッジがルートになる場合に) 別の状態に変更される前に使用する時間間隔

range *start-index stop-index*
永続データベースからのアドレス項目の範囲を読み取ります。これを指定す

るには、**list permanent** コマンドを使用してまずデータベースのサイズを判別してください。この値からユーザーの項目範囲の 『開始索引』値を判別することができます。開始索引は 1 からデータベースのサイズまでの範囲にあります。次に、限定された数の項目を表示するために『停止索引』を選択することができます。この入力は任意です。停止索引が指定されない場合、省略時値はデータベースのサイズです。

アドレス項目には次の情報が含まれています。

例: `list range`

```
Start-Index [1]? 1
Stop-index [17]? 6
ADDRESS                 ENTRY TYPE      PORT MAP

=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF
01-80-C2-00-00-02       RESERVED        NONE/DAF
01-80-C2-00-00-03       RESERVED        NONE/DAF
01-80-C2-00-00-04       RESERVED        NONE/DAF
01-80-C2-00-00-05       RESERVED        NONE/DAF
```

Address

項目の 6 バイトの MAC アドレス

Type of Entry

以下のタイプのうち 1 つを指定します。

- Reserved - IEEE 802.1d 委員会によって予約済みの項目
- Registered - 項目は、ボックスに接続された専有通信ハードウェアに属するユニキャスト・アドレスまたはプロトコル転送側によって使用可能にされるマルチキャスト・アドレスから構成されます。
- Permanent - 構成プロセスでユーザーによって入力される項目で、電源オン/オフまたはシステム・リセットが行われても残るもの
- Static - 監視プロセスでユーザーが入力する項目で、電源オン/オフまたはシステム・リセットが行われると残らず、経過時間をもたないもの
- Dynamic - ブリッジにより『動的に』『学習される』項目で、電源オン/オフまたはシステム・リセットが行われると残らず、項目に関連する『経過時間』をもつもの。
- Free - データベースのうち、空でアドレス項目を入れられるロケーション

Port Map

すべての着信ポートについての発信ポート・マップを表示します。

NetBIOS

NetBIOS 構成プロンプトを表示します。`ASRT config>` プロンプトで **netbios** を入力すると、NetBIOS 構成プロンプトが表示されます。NetBIOS 構成コマンドのそれぞれに関する説明については、174ページの『NetBIOS コマンド』を参照してください。

構文:

netbios

例: **netbios**

```
NetBIOS Support User Configuration
NetBIOS config>
```

注: NetBIOS フィルター・フィーチャーを未購入の場合は、 このコマンドを使用すると、次のメッセージが表示されます。

```
NetBIOS Filtering is not available in this load.
```

Set

ブリッジ構成に関連した特定の値、機能、およびパラメーターを設定するには、**set** コマンドを使用してください。これらには次のものが含まれています。

- フィルター・データベース内の動的アドレス項目用の経過時間
- ブリッジ・アドレス
- ソース・ルーティングの最大フレーム (LF) ビット・コード化変換処理
- MAC サービス・データ単位 (MSDU) サイズ
- スパンニング・ツリー・プロトコル・ブリッジおよびポートのパラメーター
- ルート記述子 (RD) の限度
- ブリッジ・フィルター・データベースのサイズ
- 重複 MAC アドレスと関連付けられた RIF の経過時間
- マルチアクセス・データベース内の項目の経過時間

構文:

set
- age
- bridge
- dmac-age
- filtering
- lf-bit-interpretation . . .
- maximum-packet-size . . .
- multiaccess-age . . .
- port
- protocol bridge
- protocol port . . .
- route-descriptor-limit . . .

age *seconds resolution*

項目をもつポートが転送状態にあるときに、フィルター・データベース内の動的項目が経時タイムアウトする時間を設定します。この経過時間は、SR-TB ブリッジ固有性の場合に RIF テーブル内の RIF 項目の経過時間設定にも使用されます。

各プロンプトに必要な値を入力し、**Return** を押してください。

経過時間の有効値: 10 ～ 1000000

経過時間の省略時値: 30

レゾリューションの値は、フィルター・データベース内の動的項目が経時タイマーによって設定されたそれぞれの経過時間制限を超えていないかどうかを判別するのに項目を走査しなければならない回数を指定します。

レゾリューションの有効値: 1 ～ 60 秒

レゾリューションの省略時値: 5 秒

例: set age

```
seconds [300]  ?  400
resolution [5] ?  6
```

bridge *bridge-address*

ブリッジ・アドレスを設定します。これはブリッジ識別子内の下位の 6 オクテットのブリッジ・アドレスです。 省略時解釈では、bridge-addr-value は初期設定時に最小番号が付いていたポートの媒体アクセス制御 (MAC) アドレスに設定されます。 このコマンドを使用して、省略時アドレスを取り消し、ユーザー独自の固有なアドレスを入力することができます。

注: ネットワーク内の各ブリッジは固有のアドレスをもっている必要があります。

重要: シリアル回線インターフェース (またはトンネル) が最小番号のポートである場合には、再始動されたときにブリッジが固有なアドレスをもつようにこのコマンドを使用することが必須です。シリアル回線はそれ自体の MAC アドレスをもっていないため、このプロセスが必要です。

プロンプトに、12 桁 の 16 進形式のブリッジ・アドレスを入力し、**Return** を押してください。

アドレスを誤った形式で入力すると、`Illegal Address (アドレスが正しくない)` というメッセージが出ます。プロンプトでアドレスを入力しなかった場合は、`Zero length address supplied (ゼロの長さのアドレスが指定された)` というメッセージが出され、ブリッジは前の値を維持します。ブリッジ・アドレスを省略時値に戻すためには、すべてゼロのアドレスを入力してください。

有効値: 12 個の 16 進数字

各オクテットを分離するのにダッシュまたはコロンは使用しないでください。ネットワーク内の各ブリッジは固有のアドレスをもっている必要があります。

省略時値: 000000000000

例: set bridge

```
Bridge Address (in 12-digit hex)[]?
```

dmac-age *seconds*

重複 MAC アドレスの RIF テーブル内の RIF 項目が経過タイムアウトする

時間を設定します。この値は、学習済みの重複 MAC アドレスについてのみ使用されます。その他のすべてのアドレスについては、**set age** コマンドからの値が経時に使用されます。

各プロンプトに必要な値を入力し、**Return** を押してください。

DMAC 経過時間の有効値: 10 ～ 1000000

DMAC 経過時間の省略時値: 300

例 : set dmac-age

```
seconds [300]? 200
ASRT config>list dmac
Duplicate MAC address feature is   DISABLED
Load balance feature is   DISABLED
Age value for Duplicate MAC address :000000C8
Duplicate MAC ADDRESSES CONFIGURED
================================
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

filtering *database-size*

ブリッジ・フィルター・データベース内に保持できる項目の数を設定します。

省略時値: ブリッジ・ポートの数の 1024 倍

詳細については、**list filtering** コマンド (109) を参照してください。

例: set filtering

```
database-size [2048]?
```

lf-bit-interpretation *encode-mode*

このブリッジでソース・ルーティングが使用可能になる場合に、最大フレーム (LF) ビット・コード化変換処理を設定します。

例: set lf-bit-interpretation basic

Encode-mode

basic (基本) または **extended (拡張)** を入力します。basic モードでは、3 ビットだけのルーティング制御フィールドが使用されます。今日存在するソース・ルーティング・ブリッジではこれが通例です。extended モードでは、ブリッジがサポートする最大データ単位を表すのに、 6 ビットのルーティング制御フィールドが使用されます。省略時値は **extended** です。Extended ノードと Basic ノードは互換性があります。

maximum-packet-size *port# msdu-size*

このポートでソース・ルーティングが使用可能になっている場合は、ポートについての最大 MAC サービス・データ単位 (MSDU) を設定します。MSDU 値の設定は、従来の透過媒体では含意をもちません。ルーター内で構成されたパケット・サイズより大きい MSDU 値はエラーとして扱われます。

このパラメーターが設定されない場合、使用される省略時値は、そのインターフェース用のパケット・サイズとして構成されたサイズになります。

有効値: 16 ～ 65535 の範囲内の整数を指定します。

省略時値: ポートについて設定されたパケット・サイズ

例: set maximum-packet-size 1 4399

multiaccess-age *seconds*

マルチアクセス・データベース内の項目を経時処理する時間を設定します。データベースのスキャンは、**set age** コマンドの *resolution* パラメーターで設定された速度で行われます。

有効値 : 1 ～ 1 000 000

省略時値 : 300

例 :
```
set multiaccess-age
seconds [300]? 500
```

port *block* **または** *disable*

スパンニング・ツリー・プロトコルへのそのポートの参加を開始します。これは、状況値 『block』 を入力することによって行われます。これにより、ポートは当初 『ブロックされた』 状況におかれます。ポートの実際の状態は、後でスパンニング・ツリー・プロトコルがそのトポロジーを決定したときに、決定されます。状況値 『disable』 を入力すると、ポートはスパンニング・ツリーへの参加から除去されます。

例: set port block

```
Port Number [1]?
```

protocol *bridge* **or** *port*

スパンニング・ツリー・プロトコル・ブリッジまたはポートのパラメーターを新しい構成用に修正するか、あるいは構成パラメーターを調整して特定のトポロジーに合うようにします。

ブリッジ・パラメーターを修正するには、オプションとして 『bridge』 を入力してください。このコマンドを使用して修正できるブリッジ関連のパラメーターは以下のとおりです。

ソース・ルーティング・ブリッジ (srb) または透過型ブリッジ (tb) スパンニング・ツリー・プロトコル・パラメーターが影響を受けるかどうか指定するには、**srb** または **tb** を入力します。

これらの値を設定するときは、パラメーター間に次の関係が存在することを確認してください。さもないと、入力は拒否されます。

2 X (ブリッジの転送遅延 - 1 秒) ≥ ブリッジの最大経過時間
ブリッジの最大経過時間 ≥ 2 X (ブリッジのハロー時間 + 1 秒)

例: set protocol bridge tb

```
Bridge Max-Age [20] 25
Bridge Hello Time [2] 3
Bridge Forward Delay [15] 20
Bridge Priority [32768] 1
```

Bridge Maximum Age

スパンニング・ツリー・プロトコルに関連する情報のタイムアウトに使用される最大経過時間

このブリッジング・ルーターがスパンニング・ツリー内のルート・ブリッジとして選択されると、このパラメーターの値は、他のブリッジが受信する構成ブリッジ・プロトコル・データ単位 (BPDU) を格納しておく時間の長さを指定します。 BPDU が交換なしでその最大

経過時間制限に達すると、ネットワーク内のアクティブなブリッジは、それを廃棄し、ルート・ブリッジが失敗したとみなします。その後、新しいルート・ブリッジが選択されます。

依存関係

このパラメーターの設定は、Bridge Hello Time パラメーターの設定による影響を受けます。また、このパラメーターの設定は、Bridge Forward Delay パラメーターの設定に影響します。

有効値: 6 ～ 40 秒

省略時値: 20 秒

Bridge Hello Timer

HELLO BPDU 間の時間間隔

このブリッジング・ルーターがスパンニング・ツリー内のルート・ブリッジとして選択されると、このパラメーターは、このブリッジがどのくらい頻繁に構成ブリッジ・プロトコル・データ単位 (BPDU) を送信するかを指定します。BPDU には、スパンニング・ツリーのトポロジーに関する情報が含まれており、このトポロジーに対する変更が反映されます。

依存関係

このパラメーターの設定は、Max age パラメーターの設定に影響します。

有効値: 1 ～ 10 秒

省略時値: 2 秒

Bridge Forward Delay

(このブリッジがルートになる場合に) 別の状態に変更される前に使用する時間間隔

このブリッジング・ルーターがスパンニング・ツリー内のルート・ブリッジとして選択されると、このパラメーターの値は、すべてのブリッジ内のアクティブなポートが *listening state (待機状態)* になっている時間の長さを指定します。forward delay time (転送遅延時間) が満了すると、待機状態のポートは *forwarding state (転送状態)* になります。アクティブなブリッジが失敗したとか、遮断されたときなど、スパンニング・ツリー内のトポロジーに変更があると、状態が変更します。

ルート・ブリッジはこの値をすべてのブリッジに伝達します。このプロセスにより、変更の前後ですべてのブリッジが一貫したものとなります。

依存関係

このパラメーターの設定は、SRB Bridge Max Age パラメーターの設定による影響を受けます。

有効値: 4 ～ 30 秒

省略時値: 15

Bridge Priority

ブリッジ識別子内にある上位の 2 オクテットのブリッジ・アドレス。最小番号のポートから入手された MAC アドレスまたは **Set Bridge** コマンドによって設定されたアドレスのいずれか。

bridge priority (ブリッジ優先度) は、このブリッジがスパンニング・ツリーのルート・ブリッジとなる可能性を示すものです。bridge priority パラメーターの数値が小さければ小さいほど、そのブリッジの優先度は高くなり、それが選ばれる可能性が高くなります。スパンニング・ツリー・アルゴリズムは、このパラメーターの値として最小の数値をもつブリッジをルート・ブリッジとして選択します。

有効値: 0 ～ 65535

省略時値: 32768

スパンニング・ツリー・プロトコルのポートを修正するには、オプションとして **port** を入力してください。各プロンプトに必要な値を入力し、**Return** を押してください。

例: `set protocol port`

```
Port Number [1]?
Port Path-Cost (0 for default) [0] ?   1
Port Priority [128] ?   1
```

Port Number

ブリッジのポート番号。パス・コストおよびポート優先度を変更するポートを選択します。

Path Cost

可能なルート・パス・コストに使用されるポートに関連するコスト。

各ポート・インターフェースには関連するパス・コストがあります。これは、ブリッジされたネットワーク内でポートを使用してルート・ブリッジに到達するまでの相対値です。スパンニング・ツリー・アルゴリズムはこのパス・コストを使用して、ネットワーク・トポロジーにおいてルート・ブリッジから他のすべてのブリッジへのコストを最小化するパスを計算します。

このブリッジング・ルーターがルート・ブリッジになると、このパラメーターは、このポート・インターフェースを通るフレームと関連するコストを指定します。任意の 2 つのステーション間のスパンニング・ツリー・ルートを判別する際には、この値を計算に入れてください。 0 という値は、ブリッジング・ルーターがその固有の数式を使用してこのポートのパス・コストを自動的に計算するよう指示します。

有効値: 1 ～ 65535

省略時値: 0 (コストが自動的に計算されることを意味します)

Port Priority

指定されたポートのポート優先度を識別します。これは、ポートを選択する (どのポートがルート・ブリッジに最低コス

ト・パスを提供するか) ための比較や、ブロック化決定を行う際にスパンニング・ツリー・アルゴリズムが使用します。

有効値: 0 ～ 255

省略時値: 128

route-descriptor-limit *limit-type*

ソース・ルーティングが使用可能になっている場合には、ユーザーは最大のルート記述子 (RD) の長さを、ブリッジによって転送される全ルート探索 (ARE) フレームまたはスパンニング・ツリー探索 (STE) フレームと関連付けることができます。

例 : `set route-descriptor-limit ARE`

Limit-type

RD 限界値が全ルート探索 (ARE) フレームまたはスパンニング・ツリー探索 (STE) フレームのどちらに適用されるかに応じて、ARE または STE として入力されます。それから、RD 限界値を入力するようプロンプト指示されます。

RD-limit-value

RD 限界タイプによって指定されたフレーム・タイプのルーティング情報フィールド (RIF) に含まれる RD の最大数を指定します。

各フレームのホップ・カウントは、フレームがここまで達するのに通ってきたブリッジの数です。フレームが1 つのブリッジを通るたびにルーティング情報フィールドに RD が 1 つ加算されます。したがって、RD の数は、ホップの数と同じです。RD (ホップ) の数がこのパラメーターによって許されているホップの数を超えると、フレームは廃棄されます。

有効値: 0 ～ 14

省略時値: 14

Tunnel

tunnelコマンドは、トンネル構成プロンプトにアクセスするのに使用します。トンネル構成コマンドはこのプロンプトで入力します。これらのコマンドのそれぞれの説明については、123ページの『トンネル構成コマンド』を参照してください。

構文:

tunnel

BAN 構成コマンド

この節では、すべての BAN (境界アクセス・ノード) 構成コマンドについて説明します。これらのコマンドでは、BAN を ASRT ブリッジングまたは DLSw の追加フィーチャーとして構成できます。

ASRT BAN 構成コマンド (Talk 6)

構成コマンドは BAN config> プロンプトで入力します。このプロンプトにアクセスするには、ASRT config> プロンプトまたは DLSw config プロンプトで ban コマンドを入力します。表5 は BAN 構成コマンドを示しています。

表5. BAN 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	BAN ポートを追加します。
Delete	BAN ポートを削除します。
List	BAN ポートに関するすべての情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

BAN 構成に BAN ポートを追加するには **add** コマンドを使用してください。ポート番号をコマンドとともに提供しない場合には、ポート番号を入力するようプロンプト指示されます。

構文:

add *port#*

例: add

```
Port Number [0]? 3.
Enter the BAN DLCI MAC Address []? 400012345678
Enter the Boundary Node Identifier MAC Address [4FFF00000000]?
Do you want the traffic bridged (b) or DLSw terminated (t) (b/t) [b]
```

Delete

BAN 構成から BAN ポートを削除するには、**delete** コマンドを使用してください。ポート番号をコマンドとともに提供しない場合には、ポート番号を入力するようプロンプト指示されます。

構文:

delete *port#*

例: delete 3

List

すべての BAN ポートについての情報をリストするには、**list** コマンドを使用してください。表示される情報には、BAN ポート番号 や BAN DLCI 用の MAC アドレスのほか、ポートによってハンドルされるフレームがブリッジされているか、または LLC が DLSw によって終端されているかが含まれています。

構文: list

例: list

```
bridge    BAN                  Boundary              bridged or
port      DLCI MAC Address     Node Identifier       DLSw terminated
2       40:00:11:22:33:44  4F:FF:00:00:00:00  bridged
3       40:00:55:66:77:88  4F:FF:00:00:00:00  bridged
```

トンネル構成コマンド

この節では、トンネル構成コマンドについて説明します。トンネル構成コマンドは、IP を介してブリッジング・フレームを伝送するトンネルのネットワーク・パラメーターを指定できるようにします。

トンネルの構成コマンドは、TNL config> プロンプトに入力します。このプロンプトにアクセスするには、ASRT config> プロンプトに **tunnel** コマンドを入力します。 表 6 はトンネル構成コマンドを示しています。

表 6. トンネル構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	IP を通じてブリッジするために IP のユニキャストまたはマルチキャストのアドレス指定構成に参加する宛先ブリッジの IP アドレスを追加します。
Delete	IP を通じてブリッジするために IP のユニキャストまたはマルチキャストのアドレス指定構成に参加する宛先ブリッジの IP アドレスを削除します。
Join	ルーターを 1 つまたは複数のマルチキャスト・グループのメンバーとして構成します。
Leave	ルーターをマルチキャスト・グループのメンバーから除去します。
List	IP を通じてブリッジするために IP のユニキャストまたはマルチキャストのアドレス指定構成に参加するエンド・ステーションの IP アドレスを表示します。IP トンネルを通じてルートされるブリッジ・パケットのサイズ (バイト数) およびマルチキャスト・アドレス指定が使用可能か使用不能かも表示します。
Set	ルーターのマルチキャスト・トンネル用の基本マルチキャスト IP アドレスを設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

トンネルおよびマルチキャスト・パケット

ブリッジング・トンネルは、ユニキャスト・トンネルまたはマルチキャスト・トンネルとして定義できます。ユニキャスト・トンネルを定義するためには、**add** コマンドを使用して、そのトンネルの端点の IP アドレスを設定してください。マルチキャスト・トンネルを定義するためには、**set** および **join** コマンドを使用します。マルチキャスト・パケットが関係するトンネル構成の場合、マルチキャスト・パケットの発信元アドレスは、インターネット・グループ管理プロトコル (IGMP) が使用可能なネットワーク・セグメントになければなりません。

IGMP は、ATM、X.25、およびフレーム・リレー など、一部のインターフェースでは定義されません。つまり、ルーターでマルチキャスト・トンネル (例えば、MOSPF トンネル) を定義する場合に、次の状態のいずれかが存在することを確認する必要があります。

- 発信元が LAN セグメント・アドレスの 1 つであること
- 発信元が内部 IP アドレスであること

最初の条件は、IP の **set router-id** 構成コマンドを使用して確保することができます。2 番目の条件は、IP の **set internal-ip-address** 構成コマンドを使用して確保することができます。

すべての場合に、2 番目のオプションの方が優先され、最初のオプションが使用されるのは、ネットワーク内のルーターの一部がホスト・アドレスを好まない場合 (これは、混合ベンダー・ネットワークの場合に起こることがあります) に限られます。

Add

add コマンドは、ユニキャスト IP アドレス指定構成に参加するエンド・ステーションの IP アドレスを追加するのに使用します。

IP ユニキャスト・アドレス指定の場合、トンネル構成ではあて先ブリッジの IP アドレスを提供する必要があります。このレコードは、ルーター・ ソフトウェアが、ソース・ルーティング・フレーム内のルーティング情報フィールド (RIF) 内のセグメント番号をあて先ブリッジの対応する IP アドレスに変換するのに使用します。透過ブリッジング・フレームの場合は、トンネルの反対側の端点を識別します。

構文 : add

address *IP アドレス*

有効値: 有効な IP アドレス

省略時値: なし

例: add address 128.185.144.37

Delete

delete コマンドは、ユニキャストまたはマルチキャストの IP アドレス指定構成に参加するブリッジの IP アドレスを削除するのに使用します。

構文:

delete address *IP-address*

有効値: 有効な IP アドレス

省略時値: なし

例: delete address 128.185.144.37

Join

join コマンドは、ルーターを 1 つまたは複数のマルチキャスト・グループのメンバーとして確立するのに使用します。トンネル・グループは次の 3 つのタイプ、つまり、対等、クライアント、またはサーバーのうちの 1 つにすることができます。トン

ネル・グループは整数のタグで定義されます。ブリッジは各タグごとに 1 つのグループ・タイプにだけ属することができます。例えば、ブリッジは対等グループ *1* とサーバー・グループ *1* の両方に属することはできません。

構文:

join client-group *group-number*
peer-group *group-number*
server-group *group-number*

client-group *group-number*
所定のグループ番号をもつクライアント・グループを結合します。

有効値: 0 ～ 64

省略時値: 0

例: join client-group 3

peer-group *group-number*
所定のグループ番号をもつ対等グループを結合します。

有効値: 0 ～ 64

省略時値: 0

例: join peer-group 5

server-group *group-number*
所定のグループ番号をもつサーバー・グループを結合します。

有効値: 0 ～ 64

省略時値: 0

例: join server-group 7

Leave

leave コマンドは、ルーターをマルチキャストのメンバーから除去するのに使用します。

構文:

leave server-group *group-number*
client-group *group-number*
peer-group *group-number*

server-group *group-number*
所定のグループ番号をサーバー・グループから除去します。

有効値: 0 ～ 64

省略時値: 0

例: leave server-group 7

client-group *group-number*
所定のグループ番号をクライアント・グループから除去します。

有効値: 0 ～ 64

省略時値: 0

例: `leave client-group 3`

peer-group *group-number*
所定のグループ番号を対等グループから除去します。

有効値: 0 ～ 64

省略時値: 0

例: `leave peer-group 5`

List

list トンネル・コマンドは、IP を介してトンネル伝送するための IP のユニキャストまたはマルチキャストのアドレス指定構成に参加するブリッジの IP アドレスを表示するのに使用します。このコマンドは、トンネルを通じて送信される IP パケットのサイズを表示するために使用することもでき、IP が使用可能か使用不能かを表示します。

構文:

list address
all

address
IP を介するトンネルの IP のユニキャストまたはマルチキャストのアドレス指定構成に参加するブリッジの IP アドレスをリストします。

例: `list address`

```
IP Tunnel Addresses
128.185.179.51      128.185.170.51      128.185.142.39
128.185.143.39       224.0.0.5
```

all ユニキャスト IP アドレス、構成されたマルチキャスト・アドレス、およびトンネル・パケット・サイズをすべてリストします。

例: `list all`

```
IP Tunnel Addresses
128.185.179.51      128.185.170.51      128.185.142.39
128.185.143.39       224.0.0.5
Frame size for the tunnel 2120
```

Set

set コマンドは、ルーターの基本マルチキャスト・アドレスを設定するのに使用します。

IP マルチキャスト・アドレス指定の場合、トンネル構成では、IP マルチキャスト・アドレスのみをトンネル用に予約しておく必要があります。カプセル化には、3 つのグループの IP マルチキャスト・アドレスを使用します。第 1 のグループは全ルート探索 (ARE) フレームを送信するためのもので、第 2 のグループはスパンニング・ツリー探索 (STE) フレームを送信するためのもので、第 3 のグループは特定ルーティング・フレーム (SRF) 用です。

構文:

set base-multicast-address

base-multicast-address

マルチキャスト・トンネル用の基本マルチキャスト IP アドレスを設定します。

有効値: 任意の有効なクラス D IP アドレスで、最後の 2 バイトが 0 に設定されているもの。

省略時値: 224.186.0.0

例: set base-multicast-address 224.10.0.0

フレーム・リレー・コマンド

フレーム・リレー・インターフェースを介してブリッジングを使用可能にする場合は、DLCI 番号 (サーキット番号とも呼ばれる) をブリッジ・ポートに対応付ける必要があります。これは、フレーム・リレー・ポイント・ポイント・ブリッジ・ポートと呼ばれています。また、フレーム・リレー・インターフェース自体に対応付けたマルチアクセス・ブリッジ・ポートを定義することもできます。詳しくは、61ページの『マルチアクセス・ブリッジ・ポートの構成』 を参照してください。

ブリッジ・ポートが構成されると、プロトコル・フィルターやアドレス・フィルターも含めて、ブリッジ・ポートに関連する機能がすべて使用可能になります。

各フレーム・リレー・ポイント・ポイント・ブリッジ・ポートごとに、それぞれ PVC と SVC のどちらかを指定する必要があります。PVC サポートの場合は、対応する DLCI 番号を指定する必要があります。SVC サポートの場合は、 SVC サーキット名を指定する必要があります。

`ASRT config>` プロンプトで、次のようなコマンドを使用して、フレーム・リレー・サーキットのブリッジングを使用可能にします。

add port *interface# port# circuit# circuit-name*

interface#
フレーム・リレー・インターフェースのインターフェース番号

port# サーキットに対応する固有のブリッジ特定番号

有効範囲: 1 ～ 254

省略時値: なし

Use PVC?
No の場合には、SVC が追加されます。

有効値: Yes または No

省略時値: No

circuit#
ブリッジングが使用可能にされる PVC に関する DLCI 番号

circuit-name
ブリッジングが使用可能にされる SVC のサーキット名

ASRT フレーム・リレー・コマンド (Talk 6)

このコマンドでは、*circuit number* で識別されているフレーム・リレー PVC にポート番号を対応付け、そのサーキットが透過ブリッジングに参加できるようにします。

ATM コマンド

ATM インターフェースを介したブリッジングを使用可能にするためには、VCC をブリッジ・ポートと関連付ける必要があります。

ブリッジ・ポートが構成されると、プロトコル・フィルターおよびアドレス・フィルターを含めて、ブリッジ・ポートに関連する機能がすべて使用可能になります。

PVC または SVC サポートを指定する必要があります。PVC サポートの場合、その PVC の VPI および VCI を指定する必要があります。SVC サポートの場合には、リモート ATM アドレスおよびローカル・セレクター・バイトを与える必要があります。

`ASRT config>` プロンプトで、以下のコマンドを使用して、ATM インターフェース上のブリッジングを使用可能にしてください。

add port *interface# port# VPI VCI destaddr selector*

interface#
ATM インターフェースのインターフェース番号

port# VCC と関連付けられた固有のブリッジ特定番号

有効範囲: 1 ～ 254

省略時値: なし

ポートが ATM インターフェース上で追加されていれば、ポート番号は、ATM ARP クライアントおよびそのポートと関連付けられた VCC に対してそのポートを識別します。

ATM ARP クライアント構成情報については、593ページの『第27章 ARP の使用』 を参照してください。

Use PVC?
No の場合には、SVC が追加されます。

有効値: Yes または No

省略時値: No

VPI ブリッジングが使用可能になっている PVC の VPI。

VPI の有効値: 0 ～ 255

VPI の省略時値: 0

VCI ブリッジングが使用可能になっている PVC の VCI。

VCI の有効値: 0 ～ 65535

VCI の省略時値: 0

Destaddr
SVC のあて先 ATM アドレス

宛先 ATM アドレスの有効値: 任意の有効な 20 バイト ATM アドレス

宛先 ATM アドレスの省略時値: なし

Selector

SVC のあて先 ATM アドレスのセレクター

セレクターの有効値: X'00' ～ X'FF'

セレクターの省略時値: X'00'

例 : ATM インターフェース (PVC) 上でのポートの追加

```
ASRT config> add port
Interface number [0]?
Port number [1]?
Use PVC? [Yes]:
VPI, Range 0..255 [0]? 0
VCI, Range 0..65535 [0]? 795
```

例 : ATM インターフェース (SVC) 上でのポートの追加

```
ASRT config> add port
Interface number [0]?
Port number [2]?
Use PVC? [Yes]:No
Destination ATM Address []? 39112233445566778899001122334455667788 99
Selector, Range 00..FF [00]? 0A
ASRT config>
```

例 : フレーム・リレー・インターフェース (PVC) 上でのポートの追加

```
ASRT config> add port
Interface Number [0]? 5
Port Number [7]? 7
Use FR PVC? [Yes]: yes
Frame Relay Circuit number [16]? 17
```

例 : フレーム・リレー・インターフェース (SVC) 上でのポートの追加

```
ASRT config> add port
Interface Number [0]? 5
Port Number [8]? 8
Use FR PVC? [Yes]: no
Frame Relay SVC Circuit Name []? 05svc020
```

ASRT 監視環境へのアクセス

ASRT 監視環境にアクセスするためには、+ (GWCON) プロンプトで **protocol asrt** コマンドを入力します。

```
+protocol asrt
ASRT>
```

ASRT 監視コマンド

この節では、ASRT 監視コマンドについて説明します。これらのコマンドは、アクティブな監視からパラメーターを見て、修正することができます。監視コマンドを使って修正する情報は、ブリッジング・ルーターを再始動すると SRAM 構成にリセットされます。

ASRT 監視コマンド (Talk 5)

これらのコマンドを使用すると、ブリッジ・メモリー内の構成情報を失わずに構成を一時的に修正することができます。ASRT> プロンプトは、すべての ASRT 監視コマンドについて表示されます。

NetBIOS の監視コマンドは、NetBIOS> 監視プロンプトに入力します。NetBIOS プロンプトは、主要 ASRT コマンドのサブセットであり、この章で後述する ASRT **netbios** コマンドを入力することによってアクセスできます。

NetBIOS の監視コマンドは、NetBIOS> 監視プロンプトに入力します。NetBIOS フィルター・プロンプトは、主要 ASRT コマンドのサブセットです。

注: MAC アドレスを入力するよう要求するコマンドでは、アドレスは次の形式で入力できます。

IEEE 802 標準ビット配列
00-00-00-12-34-56

IEEE 802 標準ビット配列 (簡略形式)
000000123456

IBM トークンリング固有ビット配列 (非標準)
00:00:00:12:34:56

表7 は、ASRT 監視コマンドを示しています。

表 7. ASRT 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。xxxiiiページの『ヘルプの入手』 を参照してください。
Add	ブリッジ・ルーターの永続データベースに永続 (静的) アドレス項目を追加します。
BAN	特定の BAN 監視コマンド を入力するために境界アクセス・ノード (BAN) にアクセスできるようにします。詳細については、148ページの表8を参照してください。
Cache	指定したポートについてのキャッシュ項目を表示します。
Delete	ブリッジング・ルーターのデータベースから MAC アドレスを削除します。
Flip	MAC アドレスを標準から 802.5 (非標準または IBM) ビット配列に切り替えます。
List	全体のブリッジ構成について、または選択された構成オプションについての情報を表示します。
NetBIOS	NetBIOS 監視プロンプトを表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、ブリッジング・ルーターのデータベースに静的アドレス項目および あて先アドレス・フィルターを追加するのに使用します。データベースに対するこれらの追加は、ルーターを再始動すると失われます。

構文:

add destination-address-filter

static-entry

destination-address-filter *mac_address*

ブリッジング・ルーターの永続データベースにあて先アドレス・フィルターを追加します。コマンドの後に項目の MAC アドレスを入力してください。

例: add destination-address-filter

```
Destination MAC address [00-00-00-00-00-00]?
```

static-entry *mac_address input_port [output_ports]*

ブリッジング・ルーターの永続データベースに静的アドレス項目を追加します。コマンドの後に静的項目の MAC アドレスおよび入力ポート番号 (任意選択の出力ポート番号も入力できます) を入力してください。複数のポート・マップ (入力ポートごとに 1 つずつ) をもつ静的項目を作成するには、このコマンドを何度か使用してください。

例: add static-entry

```
MAC address [00-00-00-00-00-00]? 400000012345
Input port, 0 for all [0]? 2
Output port, 0 for none [0]? 3
Output port, 0 to end [0]?
```

BAN

ban コマンドは、BAN (境界アクセス・ノード) 監視プロンプトにアクセスするのに使用します。ASRT> プロンプトから **ban** コマンドを入力してください。

構文: ban

例 ASRT>**ban**

```
BAN>
```

BAN 監視プロンプトにアクセスすると、特定の監視コマンドの入力が開始できます。随時 ASRT> プロンプトに戻るには、**exit** コマンドを入力します。

Cache

cache コマンドは、選択したブリッジ・ポートのルーティング・キャッシュの内容を表示するのに使用します。ポートがキャッシュを所有していない場合には、Port X does not have a cache というメッセージが表示されます。

構文:

cache *port#*

例: cache

```
Port number [1]? 3

MAC Address    MC*  Entry Type       Age  Port(s)

00-00-93-00-C0-D0   PERMANENT          0  3 (TKR/1)
00-00-00-11-22-33   STATIC             0  3 (TKR/1)
```

MAC Address

項目の 6 バイトの MAC アドレス

Entry Type

次のアドレス項目タイプの 1 つを指定します。

Reserved - IEEE 802.1D 標準によって予約済みの項目

Registered - 項目は、ボックスに接続された専有通信ハードウェアに属するユニキャスト・アドレスまたはプロトコル転送側によって使用可能にされるマルチキャスト・アドレスから構成されます。

Permanent - 構成プロセスにユーザーによって入力される項目で、電源オン/オフまたはシステム・リセットが行われても残るもの。

Static - 監視プロセスでユーザーが入力する項目で、電源オン/オフまたはシステム・リセットが行われると残らず、経過時間タイマーの影響を受けないもの。

Dynamic - ブリッジにより『動的に』『学習される』項目で、電源オン/オフまたはシステム・リセットが行われると残らず、項目に関連する『経過時間』をもつもの。

Free - データベースのうち、空でアドレス項目を入れられるロケーション

Unknown - ブリッジに知られていない項目タイプ。バグまたは違法アドレスあるいはその両方である可能性があります。

Age 各動的項目の秒数で表された経過時間。経過時間は各レゾリューション時間間隔ごとに減少します。

port(s)

その項目に関連するポート番号を指定し、インターフェース名 (これは常に、キャッシュをもつインターフェースの名前になります) を表示します。

Delete

delete コマンドは、ルーターの永続データベースからステーション (MAC を含む) アドレス項目を削除するのに使用します。

構文:

delete *mac-address*

例: `delete 00-00-93-10-04-15`

Flip

flip コマンドは、アドレス・ビット順を 『切り替える』 ことで特定の MAC アドレスを標準形式および非標準形式で表示するのに使用します。このコマンドは、典型的な非標準形式の IEEE 802.5 アドレスをブリッジ監視および ELS により一般に使用される標準形式に変換する (およびその逆の変換を行う) のに便利です。

構文:

flip *MAC-address*

例: `flip`

```
MAC address [00-00-00-00-00-00]? 00-00-00-33-44-55
IEEE 802 canonical bit order:    00-00-00-33-44-55
IBM Token-Ring native bit order: 00:00:00:CC:22:AA
```

List

list コマンドは、ブリッジング・ルーターの構成についての情報を表示するか、選択された構成またはブリッジ・オプションについての情報を表示するのに使用します。

構文:

list

- adaptive . . .
- bridge . . .
- conversion . . .
- database . . .
- dmac
- filtering . . .
- multiaccess-database . . .
- port
- source-routing . . .
- spanning-tree-protocol . . .
- transparent . . .
- tunnel . . .

adaptive *datagroup-option [sub-option]*

ブリッジのタイプを変換する SR-TB ブリッジに関する一般情報をすべてリストします。多数の一般データ・グループ・オプションが **list adaptive** の下に表示される場合があります。これらには次のものが含まれます。

- Config - SR-TB ブリッジに関する一般情報を表示します。
- Counters - すべての SR-TB ブリッジ・カウンターを表示します。
- Database - SR-TB ブリッジの RIF データベースの内容を表示します。

例 : list adaptive config

```
Adaptive bridge:            Enabled
Translation database size:  0
Aging time:                 320 seconds
Aging granularity           5 seconds

Port  Segment  Interface   State     MTU
   1  001      TKR/1       Enabled   2052
   -  002      Adaptive    Enabled   1470
```

Adaptive bridge

SR-TB 最適ブリッジの現在の状態を示します。 この値は Enabled または Disabled のいずれかで表示されます。

Translation database size
SR-TB データベースの現行のサイズを表示します。このデータベースには、ソース・ルーティング・ドメイン用の MAC アドレスおよび関連する RIF が含まれます。

Aging time
経過時間タイマーの設定値を秒単位で表示します。この時間制限を超える SR-TB RIF データベース項目はすべて廃棄されます。

Aging granularity
経過時間タイマーによる満了を探すために項目がどれだけ頻繁に走査されるかを表示します。

Port 変換ブリッジングに関連するポートの番号を表示します。

Segment
変換ブリッジングに関連するポートに割り当てられたソース・ルーティング・セグメント番号を表示します。

Interface
変換ブリッジ・ネットワーク・セグメントに接続される装置を識別します。

State 変換ブリッジ・ポートの現行の状態を示します。

MTU 変換ブリッジが送受信できる最大フレーム・サイズ (RIF の終わりから FCS の初めまで) を指定します。

例 :

```
list adaptive counters
          Hash collision count: 28
          Adaptive database entry count: 0
          Adaptive database overflow  count: 0
```

Hash Collision Count
ハッシュ・テーブルの同じ場所に保管された (ハッシュされた) アドレスの数を表示します。この数は累積数であり、発生したハッシュ衝突事象の総数を表します。この数が増える場合は、テーブルのサイズに問題があることを示します。

Adaptive Database Entry
最適ブリッジ・データベース内に現在保管されている項目の数を表示します。

Adaptive Database Overflow
変換データベース・テーブル用のテーブル・スペースが足りなくなったためにアドレスが上書きされた回数を表示します。

list adaptive コマンドの *database* オプションを選択すると、最適ブリッジ RIF データベースの特定の部分を選択して表示させることができます。これは、データベースがとりうるサイズによります。表示オプションには次のものが含まれています。

- Address - その特定の MAC アドレスに関連する変換ブリッジ・データベースを表示します。
- All - データベース全体を表示します。
- Port - 特定のポートのすべての変換ブリッジ項目を表示します。

- Segment - 指定されたセグメント番号をもつポートに関連するすべての変換ブリッジ項目を表示します。

以下に **list adaptive database** コマンド・オプションのそれぞれを示す例が挙げてあります。

注: これらは、最適ブリッジングが使用可能になっている場合にのみ表示されます。

例 : `list adaptive database address` *`mac-address`*

例 : `list adaptive database all`

例 : `list adaptive database port` *`segment#`*

例 : `list adaptive database segment` *`segment#`*

各項目は 2 行で表示され、次にブランク行がきます。 次の情報は各項目について表示されます。

Canonical address
この項目に対応するノードの MAC アドレスをリストします。これは IEEE 802 の標準 (16 進) 形式で表示されます。

Interface
この項目を学習したネットワーク・インターフェースの名前を表示します。

Port このアドレス項目を学習したポートのポート番号を表示します。

Seg このアドレスを学習したセグメントの番号を表示します。

Age 項目の経過時間を秒単位で表示します。

RIF Type
RIF タイプを SRF、STE、または ARE として表示します。

RIF Direction
RIF の方向を Forward または Reverse として表示します。

RIF Length
RIF の長さをバイト単位で表示します。

RIF LF
RIF にコード化された最大フレーム値を表示します。

IBM MAC Address
この項目に対応するノードの MAC アドレスを示します。 これは、『IBM』 の非標準ビット配列で表示されます。このビット配列は一般に 802.5 インターフェースでラベル付けされ、IP/ARP、IPX、および NetBIOS プロトコルに使用されます。

RIF このノードから学習されたルーティング情報フィールドを表示します。

adaptive database duplicate
すべての重複 MAC アドレスのデータベース項目をリストします。各重複 MAC アドレスの 1 次および 2 次 RIF を表示します。

例 : list adaptive database duplicate

```
Canonical Address  Interface  Port  Seg    Age  RIF: Type Direct   Length  LF IBM MAC Address    RIF

08-00-5a-ee-ee-ee  TKR/0         3  001    180       SRF  Forward  14  1470 90:00:5a:77:77:77  0e10fef0dcab001b960395029001  PRI. RIF(3)

                   TKR/2         5  003    185       SRF  Reverse  14  1470                    0c9070087109003bdcabfef00000  SEC. RIF(3)
```

bridge

ブリッジング・ルーター構成に関する一般情報をすべてリストします。

例: list bridge

```
Bridge ID (prio/add):  32768/10-00-5A-63-01-00
Bridge state:               Enabled
UB-Encapsulation:      Disabled
Bridge type:           STB
Bridge capability:     ASRT
Number of ports:       2
STP Participation:       IEEE802.1d

最大
Port  Interface      State  MAC Address         Modes   MSDU   Segment

   1  Eth/1            Up   10-00-5A-63-01-00       T    1514
   2  FR/0:16        Down   00-00-00-00-00-00               0
   2  ATM/0:0:48     Down   00-00-00-00-00-00 SR    0     121   RD


SR bridge number:      7
SR virtual segment:    001
Adaptive segment:      000
```

Bridge ID
スパンニング・ツリー・アルゴリズムがスパンニング・ツリーを判別するために使用する固有な ID。ネットワーク内の各ブリッジには、固有のブリッジ識別子が割り当てられます。ブリッジ優先度は 10 進数で表示され、その後に 16 進アドレスが続きます。

Bridge State
ブリッジングが使用可能か使用不能かを示します。

Bridge Type
構成済みのブリッジ・タイプを表示します。これは、NONE、SRB、TB、SRT、ADAPT、A/SRB、A/TB、または ASRT として表示されます。

Number of Ports
そのブリッジ用に構成されたポートの数を表示します。

Port Add Port コマンドによってインターフェースに割り当てられたユーザー定義の番号を指定します。

Interface
ブリッジを通じてネットワーク・セグメントに接続された装置を識別します。

State ポートの現行の状態を示します。これは UP または DOWN として表示されます。

MAC address
そのポートに関連する MAC アドレスを標準ビット配列で表示します。

Modes
そのポートのブリッジ・モードを表示します。T は透過ブリッジングを示します。SR はソース・ルーティングを示します。A は最適ブリッジングを示します。

MSDU ブリッジがこのインターフェースで送受信できる最大フレーム (データ単位) サイズ (MAC ヘッダーは含むが、FCS フィールドは含まない) を指定します。

Segment
そのポート (ある場合) に割り当てられたソース・ルーティング・ブリッジ・セグメント番号を表示します。

SR bridge number
ユーザーに割り当てられたソース・ルーティング・ブリッジ番号を表示します。

SR virtual segment
ソース・ルーティング・ブリッジのバーチャル・セグメント番号 (ある場合) を表示します。

Adaptive segment
(変換を介して) 透過ドメインにルートするためにソース・ルーティング・ドメインで使用されるセグメントの番号を表示します。

conversion *datagroup-option*

- フレーム・タイプに基づきフレーム形式を変換するためのブリッジの規則に関する一般情報を表示します。**list conversion** コマンドのもとで表示できる一般データ・グループはいくつかあります。これらには次のものが含まれます。
  - All - すべての規則を表示します。
  - Ethertype - すべてのイーサネット・タイプまたは特定のイーサネット・タイプについての規則を表示します。
  - SAP - すべての SAP プロトコル識別子または特定の 802.2 SAP タイプについての規則を表示します。
  - SNAP - すべての SNAP プロトコル識別子または特定の 802.2 SNAP タイプについての規則を表示します。

  以下の例は、list conversion 表示オプションのそれぞれを分類しています。

  例: `list conversion all`

  例: `list conversion ethertype`

  ```
  Ethernet type (in hexadecimal), 0 for all [0]?
  ```

  例: `list conversion SAP`

  ```
  SAP (in hexadecimal), 100 for all [100]?
  ```

  例: `list conversion SNAP`

  ```
  SNAP Protocol ID, return for all [00-00-00-00-00]?
  ```

database *datagroup-option*
透過フィルター・データベースの内容をリストします。list database コマンド

のもとで表示されるように選択できるデータ・グループはいくつかあります。これらには次のものが含まれます。

- All - 透過ブリッジング・データベース全体を表示します。
- Dynamic - すべての動的 (学習済み) アドレス・データベース項目を表示します。
- Local - すべてのローカル (予約済み) アドレス・データベース項目を表示します。
- Permanent - すべての永続アドレス・データベース項目を表示します。
- Port - 特定のポート用のアドレス項目を表示します。
- Range - 全体の透過ブリッジング・フィルター・アドレス・データベースからのデータベース項目の範囲を表示します。範囲を定義するための開始および終了 MAC アドレスが与えられます。この範囲にあるすべての項目が表示されます。
- Static - アドレス・データベースからの静的項目を表示します。

以下の例は、list database コマンドのオプションを分類しています。最初の例は関連する出力も示します。

例: `list database all`

```
MAC Address    MC*  Entry Type       Age  Port(s)
00-00-00-00-AA-AA   Dynamic          295  4 (Eth/2)
00-00-00-12-34-56   Perm/Source filter    2 (TKR/1)  ->  3-4
                                          1-2
00-00-00-22-33-44   Permanent             1-2
                                          1-2
00-00-00-33-44-55   Perm Dest filter      All
00-00-00-55-66-77   Perm/Source filter    1-2,4

00-00-93-10-04-15   Registered            1 (Eth/1)
00-00-93-10-E4-F9   Dynamic          300  1 (Eth/1)
00-00-93-90-04-A6   Dynamic          300  1 (Eth/1)
00-00-A7-10-68-28   Dynamic          270  1 (Eth/1)
01-80-C2-00-00-00*  Registered            1,3
01-80-C2-00-00-01*  Reserved              All
01-80-C2-00-00-02*  Reserved              All
01-80-C2-00-00-03*  Reserved              All
01-80-C2-00-00-0D*  Reserved              All
01-80-C2-00-00-0E*  Reserved              All
01-80-C2-00-00-0F*  Reserved              All
03-00-00-00-80-00*  Reserved              All
08-00-17-00-35-F9   Dynamic          300  1 (Eth/1)
08-00-17-00-4D-DA   Dynamic          300  1 (Eth/1)
```

注: 以下のフィールドは、**list database** コマンドのオプションのすべてについて表示されます。

MAC Address
アドレス項目を 12 桁の 16 進形式 (標準ビット配列) で指定します。

MC* アドレス項目の次のアスタリスクは、その項目がマルチキャスト・アドレスとしてフラグ付けされていることを示しています。

Entry Type
以下のタイプのうち 1 つを指定します。

Reserved
IEEE802.1D 標準によって予約されている項目

Registered
ブリッジに関与するインターフェースに属するユニキャス

ト・アドレス、またはプロトコル転送側によって使用可能にされたマルチキャスト・アドレスで構成される項目

Permanent
構成プロセスでユーザーによって入力され、電源オン/オフまたはシステム・リセットが行われても消えないで残る項目

Static 監視プロセスでユーザーによって入力され、電源オン/オフまたはシステム・リセットが行われると残らない、経過時間をもたない項目

Dynamic
ブリッジによって『動的に』『学習』され、電源オン/オフまたはシステム・リセットが行われると残存しない項目で、項目に関連する『経過時間』をもちます。

Free このタイプは使用されることがなく、監視とブリッジの間で生じることのある『競争』状態の場合を除いて、通常は見る必要がありません。

Unknown
不明の項目タイプ。ソフトウェアのバグを示す場合があります。16 進数の項目タイプを保守要員に報告してください。

Age 各動的項目の経過時間 (秒単位) を示します。経過時間はレゾリューション時間間隔ごとに減少します。

Port(s)
その項目についての発信ポート番号を指定します。単一ポートの項目については、装置タイプもリストされます。動的項目が IP トンネル上にある場合、ポートは IP トンネル用の 『5』 になります。

例: `list database dynamic`

例: `list database local`

```
MAC Address    MC*  Entry Type       Age  Port(s)

00-00-93-B8-00-48   Registered            1 (TKR/1)
01-80-C2-00-00-00*  Registered            1
03-00-02-00-00-00*  Registered            1
ASRT>
```

例: `list database permanent`

例: `list database port` *`port#`*

例: `list database static`

例: `list database range`

```
First MAC address [00-00-00-00-00-00]? 00-00-93-00-C0-D0
Last MAC address [FF-FF-FF-FF-FF-FF]? 01-80-C2-00-00-00

MAC Address    MC*  Entry Type       Age  Port(s)
00-00-93-10-04-15   Registered            1 (Eth/2)
01-80-C2-00-00-00   Registered            1,3
```

dmac 重複 MAC アドレス・フィーチャーの構成済みのオプションを表示します。

例 : `list dmac`

```
ASRT>list dmac
Duplicate MAC address feature is   ENABLED
Load balance feature is    ENABLED
```

```
Age value for Duplicate MAC address :00000096
Duplicate MAC ADDRESSES CONFIGURED
==================================
10-00-5A-66-66-00
10-00-5A-66-66-01
10-00-5A-66-66-02
10-00-5A-66-66-03
10-00-5A-66-66-04
10-00-5A-66-66-05
```

filtering *datagroup-option*

ブリッジのプロトコル・フィルター・データベースについての一般情報を表示します。**list filtering** コマンドのもとで表示できる一般データ・グループはいくつかあります。これらには次のものが含まれます。

- All - すべてのフィルター・データベース項目を表示します。
- Ethertype - イーサネット・プロトコル・タイプのフィルター・データベース項目を表示します。
- SAP - SAP プロトコルのフィルター・データベース項目を表示します。
- SNAP - SNAP プロトコル識別子のフィルター・データベース項目を表示します。

以下の例は、list filtering 表示オプションのそれぞれを分類したものです。

例: `list filtering all`

```
Ethernet type 0800 is routed on ports 1
IEEE 802.2 destination SAP 42 is routed on ports 1
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

パケットがどのように通信されるかを説明するのに使用される記述子には次のものが含まれます。

- Routed - ルーティング転送側に渡されて転送されるパケットを記述します。
- Filtered - ユーザーが設定するプロトコル・フィルターによって管理上フィルターされるパケットを記述します。
- Bridged and routed - これは、システム内に転送側でないプロトコル・エンティティーがあるプロトコル識別子を記述します。この例としては、リンク・レベル・エコー・プロトコルがあります。このプロトコルからのユニキャスト・パケットは、登録済みアドレスに送信される場合にはブリッジされるか、ローカルに処理されます。マルチキャスト・パケットは、登録済みマルチキャスト・アドレスの場合は、転送されるか、ローカルに処理されます。

上で説明した記述子はすべて、この Ethertype では ARP パケットにも適用されます。

例: `list filtering ethertype`

```
Ethernet type (in hexadecimal), 0 for all [0]? 0800
Ethernet type 0800 is routed on ports 1
```

例: `list filtering SAP`

```
SAP (in hexadecimal), 100 for all [100]? 42
IEEE 802.2 destination SAP 42 is routed on ports 1
```

例: `list filtering SNAP`

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

multiaccess-database [all-ports or port port#]

マルチアクセス・データベースの内容が表示されます。このデータベースでは、ソース・ルーティング・セグメント番号をフレーム・リレー・サーキット番号にマップします。

all-ports

データベース項目すべての表示を指定します。

例 :

```
list multiaccess-database all-ports
Aging Time (in seconds): 300

4 entries used out of 512

Segment  Age    Port  Interface   Circuit
204      100    2     FR/0        16
267      200    3     FR/1        16
375      120    2     FR/0        18
400      220    3     FR/1        18
```

port *port#*

特定のブリッジ・ポートが表示されます。

例 :

```
list multiaccess-database port 2
Aging Time (in seconds): 300

4 entries used out of 512

Segment  Age    Port  Interface   Circuit
204      100    2     FR/0        16
375      120    2     FR/0        18
```

表示されている項目の意味 :

Segment

あて先ソース・ルーティング・セグメント番号

Age 項目の存続時間 (秒数)

Port この項目を作成したマルチアクセス・ブリッジ・ポートのポート番号

Interface

この項目を作成したネットワーク・インターフェースの名前

Circuit

この項目を作成したフレーム・リレー・サーキット番号

port ポート情報が表示されます。

```
Port  Interface      State  MAC Address         Modes   MSDU   Segment

   1  Eth/1            Up   10-00-5A-63-01-00       T    1514
   2  FR/0:16        Down   00-00-00-00-00-00               0
   2  ATM/0:0:48     Down   00-00-00-00-00-00 SR    0     121   RD
```

Port Add Port コマンドによってインターフェースに割り当てられたユーザー定義の番号を指定します。

Interface

ブリッジを通じてネットワーク・セグメントに接続された装置を識別します。

State ポートの現行の状態を示します。これは UP または DOWN として表示されます。

MAC address
そのポートに関連する MAC アドレスを標準ビット配列で表示します。

Modes
そのポートのブリッジ・モードを表示します。T は透過ブリッジングを示します。SR はソース・ルーティングを示します。A は最適ブリッジングを示します。

MSDU ブリッジがこのインターフェースで送受信できる最大フレーム (データ単位) サイズ (MAC ヘッダーは含むが、FCS フィールドは含まない) を指定します。

Segment
そのポート (ある場合) に割り当てられたソース・ルーティング・ブリッジ・セグメント番号を表示します。

source-routing
ソース・ルーティング・ブリッジ構成の情報を表示します。list source-routing コマンドのもとで表示できる一般データ・グループ・オプションはいくつかあります。これらには次のものが含まれます。

- Configuration - SRB ブリッジに関する一般情報を表示します。
- Counters - SRB ブリッジ・カウンターをすべて表示します。
- State - すべての関連する SR-TB ブリッジ・データベースの内容を表示します。

以下の例は、list source-routing 表示オプションのそれぞれを示しています。

例: `list source-routing configuration`

```
Bridge number:              1
Bridge state:               Enabled
Maximum STE hop count       14
Maximum ARE hop count       14
Virtual segment:            003
Port  Segment  Interface   State     MTU    STE Forwarding  LNM
2     001      TKR/1       Enabled   4399   Yes             ENA
3     002      TKR/2       Enabled   4399   Yes
```

Bridge number
このブリッジに割り当てられたブリッジ番号 (16 進値)

Bridge State
ブリッジングが使用可能か使用不能かを示します。

Maximum STE hop count
ブリッジから、ソース・ルーティング・ブリッジングに関連する所定のインターフェースへと伝送されるスパンニング・ツリー探索フレームの最大ホップ・カウント

Maximum ARE hop count
ブリッジから、ソース・ルーティング・ブリッジングに関連する所定のインターフェースへと伝送される全ルート探索フレームの最大ホップ・カウント

Virtual segment
1:N ブリッジングに割り当てられたバーチャル・セグメント番号

Port ソース・ルーティング・ブリッジングに関連するポートの番号

Segment
ソース・ルーティング・ブリッジングに関連するネットワークに割り当てられたセグメント番号

Interface
関連付けられたインターフェース名。SR-TB フィーチャーに参加するインターフェースおよび ATM の VPI/VCI については 『Adaptive』がリストされます。FR については DLCI です。

State 現行のポート状態 (Enabled または Disabled)

MTU そのポート用に設定された MTU サイズ

STE Forwarding
このポートで受信されるスパンニング・ツリー探索が転送されるか (Yes)、また他のポートからの STE がこのポートから出ていくかを示します。

LNM LAN ネットワーク管理プログラム (LNM) エージェントが、その特定のポートで使用可能 (ENA) か使用不能 (DIS) かを示します。

カウンター・オプションにはさらに情報のサブグループがありますが、これらは list source-routing コマンドを使用して表示することができます。これらには次のものが含まれます。

- All-ports - すべてのポートについてのカウンターを表示します。
- Port - 特定のポートについてのカウンターを表示します。
- Segment - 特定のセグメントに対応するポートについてのカウンターを表示します。

以下の例は、list source-routing 表示オプションのそれぞれを示しています。

例: `list source-routing counters all-ports`

```
ASRT>list source counters all-ports
Counters for port 2, segment 001, interface TKR/1
SRF frames received:          0    sent:          0
STE frames received:          0    sent:          0
ARE frames received:        648    sent:          0
SR frames sent as TB:                             0
TB frames sent as SR:                          2057
Dropped, input queue overflow:                    0
Dropped, source address filtering:                0
Dropped, dest address filtering:                  0
Dropped, invalid RIF length:                      0
Dropped, duplicate segment:                    2594
Dropped, segment mismatch:                        0
Dropped, Duplicate LAN ID or tree error:          0
Dropped, STE hop count exceeded:                  0
Dropped, ARE hop count exceeded:                  0
Dropped, no buffer available to copy:             0
Dropped, MTU exceeded:                            0


Counters for port 3, segment 002, interface TKR/2:
SRF frames received:          0    sent:          0
STE frames received:          0    sent:          0
ARE frames received:        825    sent:          0
SR frames sent as TB:                             0
TB frames sent as SR:                          2041
Dropped, input queue overflow:                    0
Dropped, source address filtering:                0
Dropped, dest address filtering:                  0
Dropped, invalid RIF length:                      0
Dropped, duplicate segment:                    3300
Dropped, segment mismatch:                        0
Dropped, Duplicate LAN ID or tree error:          0
Dropped, STE hop count exceeded:                  0
Dropped, ARE hop count exceeded:                  0
Dropped, no buffer available to copy:             0
Dropped, MTU exceeded:                            0
```

Port ソース・ルーティング・ブリッジングに関連するポートの番号をリストします。

Segment
16 進数で示したソース・ルーティング・セグメント番号をリストします。

Interface
ネットワーク・インターフェースの名前をリストします。ATM については VPI/VCI。FR については DLCI です。

SRF Frames Received/Sent
このブリッジで受信または送信される特定ルーティング・フレームの数をリストします。

STE Frames Received/Sent
このブリッジで受信または送信されるスパンニング・ツリー探索フレームの数をリストします。

ARE Frames Received/Sent
このブリッジで受信または送信される全ルート探索フレームの数をリストします。

SR Frames Sent as TB
このインターフェースで受信され、透過型ブリッジ・フレームとして送信された、ソース・ルーティング・フレームの数をリストします。

TB Frames Sent as SR
このインターフェースで受信され、ソース・ルーティング・フレームとして送信された、透過型ブリッジ・フレームの数をリストします。

Dropped, input queue
このインターフェースに到着するフレームのうち、フロー制御の理由からブリッジされなかったものの数をリストします。転送側への入力待ち行列はオーバーフローしました。

Dropped, source address filtering
このインターフェースに到着するフレームのうち、この発信元アドレスがフィルター・データベース内の発信元アドレス・フィルターに一致したためにブリッジされなかったものの数をリストします。

Dropped, destination address filtering
このインターフェースに到着するフレームのうち、この宛先アドレスがフィルター・データベース内のあて先アドレス・フィルターに一致したためにブリッジされなかったものの数をリストします。

Dropped, protocol filtering
このインターフェースに到着するフレームのうち、そのプロトコル識別子が管理上フィルターされているプロトコル識別子であったためブリッジされなかったものの数をリストします。

Dropped, invalid RIF length
このインターフェースに到着するフレームのうち、RIF の長さが 2 より小さいか 30 を超えるために除去されたものの数をリストします。

Dropped, duplicate segment
このインターフェースに到着するフレームのうち、RIF 内に重複するセグメントがあったために除去されたものの数をリストします。これは ARE フレームでは正常です。

Dropped, segment mismatch
このインターフェースに到着するフレームのうち、発信セグメント番号がこのブリッジ内のどのセグメント番号にも一致しないために除去されたものの数をリストします。

Dropped, Duplicate LAN ID or tree error:
重複する LAN ID またはツリー・エラーの数。これは、旧式の IBM ソース・ルーティング・ブリッジを含むネットワーク内での問題を検出するのに役立ちます。

Dropped, STE hop count exceeded:
ルーティング情報フィールドが最大のルート記述子の長さを超えたためにこのポートから廃棄された探索フレームの数

Dropped, ARE hop count exceeded:
ルーティング情報フィールドが最大のルート記述子の長さを超えたためにこのポートから廃棄された探索フレームの数

Dropped, no buffer available to copy:
フレームを複写するために使用可能なバッファー資源がなかったために、フレームがインターフェースから転送されなかった回数。(マルチキャストのあて先または不明のあて先へのフレームは、すべての活動ポートで送信するのに複写する必要があります。)

Dropped, MTU exceeded:
サイズが大きすぎるためにこのポートから廃棄されたフレームの数。

例: `list source-routing counters port 3`

```
Counters for port 3, segment 002, interface TKR/1:
SRF frames received:          0    sent:           0
STE frames received:          0    sent:           0
ARE frames received:       1140    sent:           0
SR frames sent as TB:                                0
TB frames sent as SR:                             2931
Dropped, input queue overflow:                       0
Dropped, source address filtering:                   0
Dropped, dest address filtering:                     0

Dropped, invalid RIF length:                         0
Dropped, duplicate segment:                       4560
Dropped, segment mismatch:                           0
Dropped, Duplicate LAN ID or tree error:             0
Dropped, STE hop count exceeded:                     0
Dropped, ARE hop count exceeded:                     0
Dropped, no buffer available to copy:                0
Dropped, MTU exceeded:                               0
Dropped, dest address filtering:                     0
Dropped, protocol filtering:                         0
```

例: `list source-routing counters segment 2`

```
Counters for port 3, segment 002, interface TKR/2:
SRF frames received:          0    sent:          0
STE frames received:          0    sent:          0
ARE frames received:       1249    sent:          0
SR frames sent as TB:                               0
TB frames sent as SR:                            3200
Dropped, input queue overflow:                      0
Dropped, source address filtering:                  0
Dropped, dest address filtering:                    0
Dropped, protocol filtering:                        0
Dropped, invalid RI length:                         0
Dropped, duplicate segment:                      4996
Dropped, segment mismatch:                          0
```

```
Dropped, Duplicate LAN ID or tree error:         0
Dropped, STE hop count exceeded:                 0
Dropped, ARE hop count exceeded:                 0
Dropped, no buffer available to copy:            0
Dropped, MTU exceeded:                           0
```

spanning-tree protocol

- スパンニング・ツリー・プロトコル情報を表示します。スパンニング・ツリー・プロトコルは、透過型ブリッジがループのないトポロジーを形成するために使用します。 **list spanning-tree-protocol** コマンドのもとで表示できる一般データ・グループ・オプションはいくつかあります。これらには次のものが含まれます。
  - Configuration - スパンニング・ツリー・プロトコルに関する情報を表示します。
  - Counters - スパンニング・ツリー・プロトコルのカウンターを表示します。
  - State - 現行のスパンニング・ツリー・プロトコルの状態情報を表示します。
  - Tree - ポート、インターフェース、およびコストの情報を含む現行のスパンニング・ツリー情報を表示します。

  以下の例は、list spanning-tree-protocol 表示オプションのそれぞれを示しています。

例: list spanning-tree-protocol configuration

```
Bridge ID (prio/add):  32768/0000-93-00-84-EA
Bridge state:          Enabled
Maximum age:           20 seconds
Hello time:            2 seconds
Forward delay:         15 seconds
Hold time:             1 seconds
Filtering age:         320 seconds
Filtering resolution:  5 seconds

Port  Interface  Priority  Cost   State
  4   Eth/1      128    100     Enabled
128   Tunnel     128    65535   Enabled
```

例: list spanning-tree-protocol counters

```
  Time since topology change (seconds)         0
  Topology changes:                            1
  BPDUs received:                              0
  BPDUs sent:                              14170

Port  Interface  BPDUs received  BDPU input overflow  Forward transitions

  1  TKR/1             0              0              1
```

例: list spanning-tree-protocol state

```
Designated root (prio/add):    32768/00-00-93-00-84-EA
Root cost:                     0
Root port:                     Self
Current (root) maximum age:    20 seconds
Current (root) hello time:     2 seconds
Current (root) Forward delay:  15 seconds
Topology change detected:      FALSE
Topology change:               FALSE

Port  Interface   State
  4  Eth/1       Forwarding
128  Tunnel      Forwarding
```

例: list spanning-tree-protocol tree

```
Port                 Designated   Desig.         Designated   Des.
No.  Interface            Root     Cost             Bridge   Port

1  TKR/1  32768/12-34-56-78-90-12    0 32768/12-34-56-78-90-12 90-01
```

tunnel *bridges* **または** *config*

トンネル構成情報を表示します。list tunnel コマンドのもとで表示される場合のある一般データ・グループ・オプションはいくつかあります。これらには次のものが含まれています。

- Bridges - トンネル・ブリッジ情報を表示します。
- Config - トンネル構成に関する情報を表示します。

以下の例は、list tunnel 表示オプションのそれぞれを示しています。

例: `list tunnel bridges`

例: `list tunnel config`

NetBIOS

netbios コマンドは、NetBIOS> プロンプトにアクセスするのに使用します。NetBIOS 監視コマンドは、NetBIOS> プロンプトで入力できます。

NetBIOS 監視コマンドについては、174ページの『NetBIOS コマンド』を参照してください。

構文:

netbios

注: ブリッジング・ルーター・ソフトウェア・ロード用として NetBIOS フィルター・フィーチャーを購入していない場合は、このコマンドを使用しようとすると、次のメッセージを受け取ります。

```
NetBIOS Filtering is not available in this load.
```

BAN 監視プロンプトへのアクセス

BAN コマンドにアクセスするには、ASRT> または DLSw> 監視プロンプトから **ban** コマンドを使用してください。

BAN 監視プロンプトにアクセスするには、ASRT 監視プロンプトまたは DLSw 監視プロンプトから **ban** コマンドを入力します。例えば、次のように入力してください。

```
ASRT> ban
BAN>
```

または

```
DLSw> ban
BAN>
```

BAN 監視プロンプトにアクセスすると、特定の監視コマンドの入力が開始できます。元の監視プロンプトに戻る場合は、**exit** コマンドを入力します。

BAN 監視コマンド

この節では、BAN 監視コマンドについて説明します。コマンドは、BAN> コマンドに入力します。

表 8. BAN 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
List	BAN ポートに関するすべての情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

List

すべての BAN ポートについての情報をリストするには、**list** コマンドを使用してください。表示される情報には、BAN ポート番号、BAN DLCI 用の MAC アドレスのほか、ポートによってハンドルされるフレームがブリッジされているか、または LLC が DLSw で終端されているか、およびポートの状況が含まれています。

ポートの状況は次の 3 つの値のうち 1 つをとります。

- Init Fail - 構成の問題が存在することを示します。
- Up - フレーム・リレー DLCI がアクティブで稼働中であることを示します。
- Down - DLCI がアクティブでないことを示します。

構文:

list

例: `list`

```
bridge  BAN                Boundary             bridged or
port    DLCI MAC Address   Node Identifier      DLSw terminated  Status
2       40:00:12:34:56:78  4F:FF:00:00:00:00    bridged          Up
```

第7章 NetBIOS の使用

この章では、IBM が実施した、ブリッジされたネットワークおよび DLSw ネットワークにおける NetBIOS について説明します。この章には次のトピックが含まれます。

- 『NetBIOS について』
- 151ページの『NetBIOS トラフィックの削減』
- 152ページの『フレーム・タイプ・フィルター』
- 165ページの『NetBIOS のホスト名フィルターおよびバイト・フィルターの構成手順』

NetBIOS について

NetBIOS プロトコルは、トークンリング LAN で使用するように設計されたものです。ルーティング可能なプロトコルではないが、ブリッジすることができ、DLSw を使用して交換することができます。NetBIOS トラフィックを取り扱うこれらの方式が両方ともサポートされます。

NetBIOS は、データ転送以外の機能のほとんどで同報通信フレームを使用します。そのため、LAN 環境では問題を生じることはありませんが、制御が行われないと、WAN 環境では問題を生じやすくなります。

以下の各項では、NetBIOS 名とさまざまなタイプの NetBIOS 同報通信について説明します。

NetBIOS 名

NetBIOS ステーション間の通信で重要なのは NetBIOS 名です。各 NetBIOS エンティティーには、NetBIOS 名が割り当てられます。他の NetBIOS エンティティーと通信するためには、その NetBIOS 名が分かっている必要があります。同報通信 NetBIOS フレームでは NetBIOS 名を使用して、そのフレームの発信元 NetBIOS エンティティー、およびそのフレームを受信させたい着信先 NetBIOS エンティティーを示します。

NetBIOS フレーム内で使用する NetBIOS 名は、すべて ASCII 文字 16 字です。NetBIOS 名には、次の 2 つのタイプがあります。

個別 (つまり固有)

単一の NetBIOS クライアントまたはサーバーを表します。個別名はその NetBIOS ネットワーク内で固有であることが必要です。

特定の NetBIOS エンティティーと通信する場合は、この名前を使用します。

グループ

NetBIOS ステーションのグループ (例えば、OS/2 の LAN サーバー・ドメイン) を表します。この名前は、ネットワーク内の個別 NetBIOS 名のいずれとも同じであることはできません。

この名前を使用すると、NetBIOS エンティティーのグループ間での通信ができます。

NetBIOS の使用

1 つ NetBIOS ステーション (単一 MAC アドレス) が、複数の個別名またはグループ名、あるいはその両方をもっていても構いません。これらの名前は、NetBIOS ステーションでネットワーク管理担当者によって構成された 1 つまたは複数の名前に基づいて、NetBIOS アプリケーションによって生成されます。

NetBIOS 名の競合解消

NetBIOS エンティティーは、ある個別 NetBIOS 名をそれ自体の独自の個別名として使用する準備段階で、ネットワーク内に同じ名前をすでに使用している NetBIOS ステーションが他にないかどうか調べます。

同じ NetBIOS 名の有無を調べるには、すべての NetBIOS ステーションを対象に特定の NetBIOS UI フレーム の同報通信を繰り返し行います。どのステーションからも応答がなければ、その名前を固有であるものとみなし、使用することができます。別のステーションから応答があった場合は、新規ステーションで該当の名前の使用を試みることはできません。

NetBIOS セッションのセットアップ手順

データ転送タイプの操作を行うために NetBIOS セッションを確立するには、まず、NetBIOS クライアントが NetBIOS サーバーの MAC アドレス、および NetBIOS サーバーに至る LLC ルートを決定します。

このためには、すべての NetBIOS ステーションを対象に特定の NetBIOS UI フレーム の同報通信を繰り返し行います。このフレームには、クライアントがセッションを確立したい相手先のサーバーの NetBIOS 名が入っています。自らの NetBIOS 名が入っているこのフレームを受信したサーバーは、対応する同報通信 NetBIOS UI フレームを用いて、クライアントに応答します。こうしてクライアントが受信した応答フレームには、NetBIOS サーバーの MAC アドレス、および NetBIOS サーバーに至るルートが入っています。

NetBIOS アプリケーションによっては、NetBIOS サーバーを見つけるプロセスが複数のステップになるものがあります。例えば、使用するドメイン・サーバーをクライアントに知らせるドメイン制御装置を見つけるのが、最初のステップになる場合があります。その後で、クライアントがこのドメイン・サーバーを見つけます。

NetBIOS サーバーの MAC アドレスおよび NetBIOS サーバーに至るルートが見つかると、NetBIOS クライアントは次のいずれかのアクションをとることができます。

- I フレームの使用によるサーバーとの通信を行うために、 NetBIOS サーバーとの LLC2 接続を確立する。
- 特定ルーティング NetBIOS UI フレームの使用による NetBIOS サーバーとの通信を開始する。

NetBIOS 同報通信のデータ流れ

NetBIOS アプリケーションによっては、データ・フレームの同報通信を定期的に行うのが普通の場合があります。これが行われるのは、あるステーションが別の NetBIOS ステーションに単一フレーム分のデータを送信したいような場合です。この場合

は、すべての NetBIOS ステーションを対象に特定の NetBIOS UI フレーム (着信先 NetBIOS ステーションの名前がフレームに入っている) の同報通信を行うことができます。

もう 1 つの場合として、グループ (つまり、ドメイン) 内の NetBIOS ステーションが相互に通信する必要がある場合があります。この場合は、すべての NetBIOS ステーションを対象に特定の NetBIOS UI フレーム (着信先 NetBIOS グループ名がフレームに入っている) の同報通信を行うことができます。通常行われるのは、こちらです。

NetBIOS の状況の流れ

普通あまり使用されることはありませんが、NetBIOS には 任意の NetBIOS ステーションから状況を入手できる機能があります。この場合は、すべての NetBIOS ステーションを対象に特定の NetBIOS フレーム (着信先 NetBIOS ステーションの名前がフレームに入っている) の同報通信を行うことができます。このフレームを受信した着信先 NetBIOS ステーションは、対応する同報通信 NetBIOS 応答フレームを用いて応答します。

NetBIOS の全ステーション同報通信フレーム

NetBIOS 機能にはめったに使用されることのない 2 つのタイプがあります。これらの機能はともに、すべての NetBIOS ステーションを対象とする NetBIOS フレームの同報通信を伴います。フレームに着信先 NetBIOS 名を入れることはありません。これら 2 つの機能とは、次のようなものです。

- NetBIOS 一般同報通信。ネットワーク上のすべての NetBIOS ステーションにデータ・フレームを送信します。
- NetBIOS トレース終端機能。この機能を使用すると、ネットワーク管理担当者は、ネットワーク上のすべての NetBIOS ステーションの NetBIOS トレース機能を単一の地点で終端することができます。ネットワーク上のすべての NetBIOS ステーションを対象に特定の NetBIOS フレームの同報通信が行われます。

NetBIOS トラフィックの削減

ネットワークを安定化するには、ゴールはブリッジ・ネットワークまたは DLSw 交換ネットワークを通じて転送される同報通信 NetBIOS トラフィックの量を減らすことです。これは次の 2 つの方法で行うことができます。

- できるだけ多くの同報通信 NetBIOS フレームをブリッジングまたは DLSw 交換の前にフィルターする。
- フィルターされていない NetBIOS UI フレームを転送するブリッジ・ポートまたは DLSw TCP セッションをできるだけ少なくする。

表9 に IBM で用意しているフィルターをリストしてあります。

表 9. NetBIOS フィルター

フィルター・タイプ	フィルター
MAC アドレス	発信元とあて先のいずれかの MAC アドレスによりフレームをフィルターする。
バイト	フレーム内のバイト・オフセットおよびフィールド長によりフレームをフィルターする。
名前	NetBIOS 発信元名およびあて先名によりフレームをフィルターする。
重複フレーム	重複フレームをフィルターする。
応答	ルーターが NetBIOS 同報通信フレームを転送しなかった応答をフィルターする。

ルーターがフレームをフィルターすると、NetBIOS 名リスト、NetBIOS 名前キャッシュ、およびルート・キャッシュは、残りのフレームの転送方法を制御します。バイト・フィルターおよび名前フィルターについては、54ページの『NetBIOS バイト・フィルター』および 53ページの『NetBIOS ホスト名フィルター』で、それぞれ説明します。MAC アドレス・フィルターについては、 *ソフトウェア使用者の手引き*で説明しています。

ホスト名フィルターおよびバイト・フィルターの紹介は、52ページの『NetBIOS の名前フィルターとバイト・フィルター』で扱っています。

以下の各項では、フレーム・タイプ、重複フレーム、および応答フレーム、NetBIOS 名前リスト、NetBIOS 名前キャッシュ、およびルート・キャッシュについて説明します。

フレーム・タイプ・フィルター

フレーム・タイプ・フィルターでは、DLSw トラフィックまたはブリッジ・トラフィック、あるいは DLSw トラフィックとブリッジ・トラフィックの両方に備えて、特定のカテゴリーの NetBIOS フレームをすべてフィルターすることができます。

フィルターできるのは、次の 3 つのカテゴリーの NetBIOS フレームです。

- 名前競合解消フレーム

  使用する NetBIOS 名がネットワーク内で固有であることを学習するのに使用する同報通信 NetBIOS フレームです。

  NetBIOS ネットワークでは、NetBIOS セッションを確立する相手先のステーション (通常は NetBIOS サーバー) の NetBIOS 名が固有であることが必須です。また、通常は、同一グループ (つまり、ドメイン) 内ではステーションの個別 NetBIOS 名が固有であることも必須です。ただし、NetBIOS セッションのセットアップ元のステーション (通常は NetBIOS クライアント) の NetBIOS 名が固有であることは、特にドメイン間にまたがる場合を始めとして、必須ではないことがしばしばあります。

  したがって、サーバー名の制御が十分に行われているネットワークでは、名前競合解消フレームをフィルターすることによる利点が得られます。特に DLSw 交換ネットワークがこの場合に該当します。

NetBIOS 名前競合解消フレームには、名前追加照会 (Add-Name-Query)、グループ名追加照会 (Add-Group-Name-Query)、および名前追加応答 (Add-Name-Response) があります。

- 一般同報通信フレーム

  ネットワーク内のすべての NetBIOS ステーションにデータを送信する場合に使用する同報通信 NetBIOS フレームです。このフレームはめったに使用されず、通常はフィルターすることができます。

  NetBIOS 一般同報通信フレームはデータグラム同報通信 (Datagram-Broadcast) です。

- トレース終端フレーム

  ネットワーク内のすべての NetBIOS ステーションで NetBIOS トレースを終端する場合に使用する同報通信 NetBIOS フレームです。これらのフレームはめったに使用されず、通常はフィルターすることができます。

  NetBIOS トレース終端フレームはトレース終端 (Terminate-Trace) です。

ブリッジされた NetBIOS トラフィックの場合は、上記のフレーム・タイプのいずれもフィルターしないのが省略時値であり、DLSw 交換 NetBIOS トラフィックの場合は、上記のフレーム・タイプをすべてフィルターするのが省略時値です。ただし、NetBIOS トラフィックを WAN リンク上でブリッジする場合は、上記のフレーム・タイプをフィルターする方が有利です。

ブリッジングの場合は、**set filters bridge** を入力して、フレーム・タイプ・フィルターをオンまたはオフにします。DLSw の場合は、**set filters dlsw** を入力して、フレーム・タイプ・フィルターをオンまたはオフにします。

例えば、次のようにします。

```
NetBIOS config>set filters bridge

Filter Name Conflict frames? [Yes]:

Name conflict filtering is              ON

Filter General Broadcast frames? [Yes]:

General broadcast filtering is          ON

Filter Trace Control frames? [Yes]:

Trace control filtering is              ON
```

重複フレーム・フィルター

応答を生じる可能性のある NetBIOS フレームは、起点 NetBIOS ステーションによって、一定の間隔 (省略時値は 1/2 秒間隔) で一定の回数 (省略時値は 6 回) だけ送信されます。以下の説明では、これらのフレームを *NetBIOS コマンド・フレーム*と呼び、可能な応答フレームを *NetBIOS 応答フレーム*と呼びます。

NetBIOS コマンド・フレームには、次に挙げるものがあります。

- 名前競合解消フレーム - 名前追加照会およびグループ名追加照会
- NetBIOS セッション・セットアップ・フレーム - 名前照会
- NetBIOS 状況フレーム - 状況照会

コマンド・フレームは、伝送が正常に行われる確率を高めるため、複数回送信されます (これらのフレームは無接続フレームです)。各応答フレームは、受信した各コマンド・フレームごとに、それに対する応答として一回だけ送信されます。

DLSw 交換ネットワークでは、WAN セッション間をまたがって行う再試行ごとの転送は、非常にコスト高になる可能性があります。したがって、最初のコマンド・フレームを受信した時点で、該当する近隣 DLSw およびブリッジ・ポートに転送し、コピーを保管します。 構成可能な時間枠内に受信した同一の NetBIOS コマンド・フレームの再試行は、すべて廃棄されます。

ブリッジ・ネットワークに関する構成可能な時間枠が 1 つ、DLSw ネットワークに関する構成可能な時間枠が 1 つあります。

ブリッジ・ネットワークに関する構成可能な時間枠は、次の 2 つのコマンドによって制御されます。

- **enable duplicate-filtering / disable duplicate-filtering**。重複 NetBIOS コマンド・フレームがブリッジ・ネットワーク上でフィルターされるかどうかを制御します。
- **set general** (『Duplicate frame filter timeout value in seconds』 パラメーター)

  重複フレーム・フィルターがブリッジ・ネットワークで使用可能にされている場合、この値で指定するのは、NetBIOS コマンド・フレームがブリッジされた後で重複 NetBIOS コマンド・フレームを廃棄する期間です。

  このタイムアウトの満了後に重複 NetBIOS コマンド・フレームが受信された場合は、そのフレームはブリッジ・ネットワークに転送されます。

DLSw ネットワークに関する構成可能な時間枠は、単一のパラメーターによって制御されます。

- **set cache-parms** (『Reduced search timeout value in seconds』 パラメーター)

  この値で指定するのは、NetBIOS コマンド・フレームが DLSw ネットワークに転送された後、重複 NetBIOS コマンド・フレームを廃棄する期間です。

  このタイムアウトの満了後に重複 NetBIOS コマンド・フレームが受信された場合は、そのフレームは DLSw ネットワークに転送されます。

  注: DLSw ネットワークの場合は、重複 NetBIOS コマンド・フレームのフィルターは常に使用可能にされています。

NetBIOS コマンド・フレームが DLSw 近隣で受信されると、そのフレームはブリッジ・ネットワークに転送され、コピーが保管されます。構成可能な間隔 (省略時値は 1/2 秒) で構成可能な回数 (省略時値は 6 回)だけ、近隣 DLSw 機能はそのコマンド・フレームの再試行をブリッジ機能に転送します。ブリッジ機能は、構成済み重複フレーム・ブリッジ・パラメーターに基づいて、コマンド・フレームを処理します。

構成可能な再試行回数および間隔は、次のコマンドおよびパラメーターによって制御されます。

- **set general** (『Command frame retry count』 パラメーターおよび 『Command frame retry timeout value in seconds』 パラメーター)

最後に、上記のブリッジ・ネットワーク転送および DLSw ネットワーク転送を実行するために、コマンド・フレームを保管する期間を制御するパラメーターが 1 つあります。

- **set general** ("Duplicate frame detect timeout value in seconds" パラメーター)

  このパラメーターで指定するのは、受信した NetBIOS コマンド・フレームを重複フレームおよび応答フレームの処理に備えて保管する期間です。タイムアウトの満了後、コマンド・フレームは削除され、重複フレーム・フィルター・タイマーおよびそれに関連する限定探索タイマーは取り消されます。タイムアウト期間の後に受信された最初の重複コマンド・フレームは、受信された最初のコマンド・フレームとして取り扱われます。タイムアウト期間後に受信した応答フレームは、すべて廃棄されます。

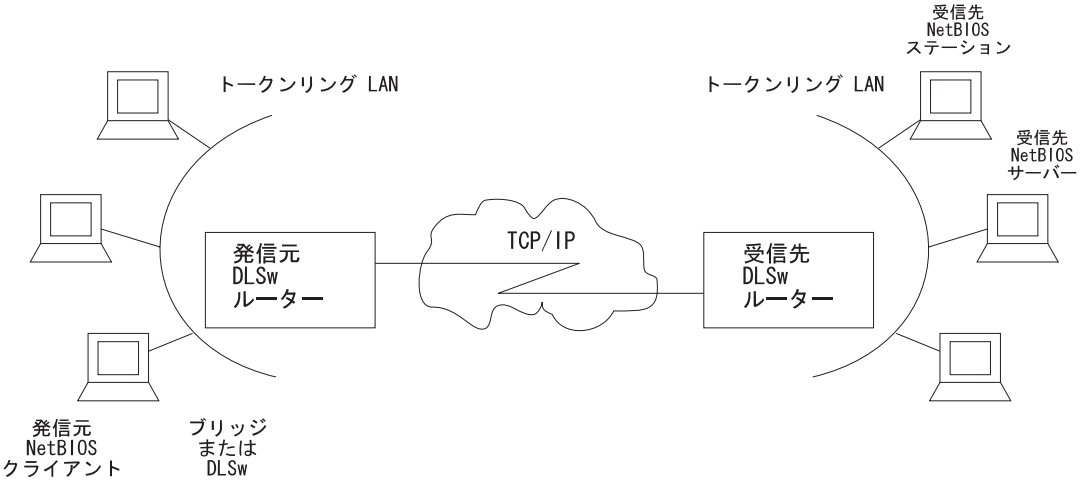
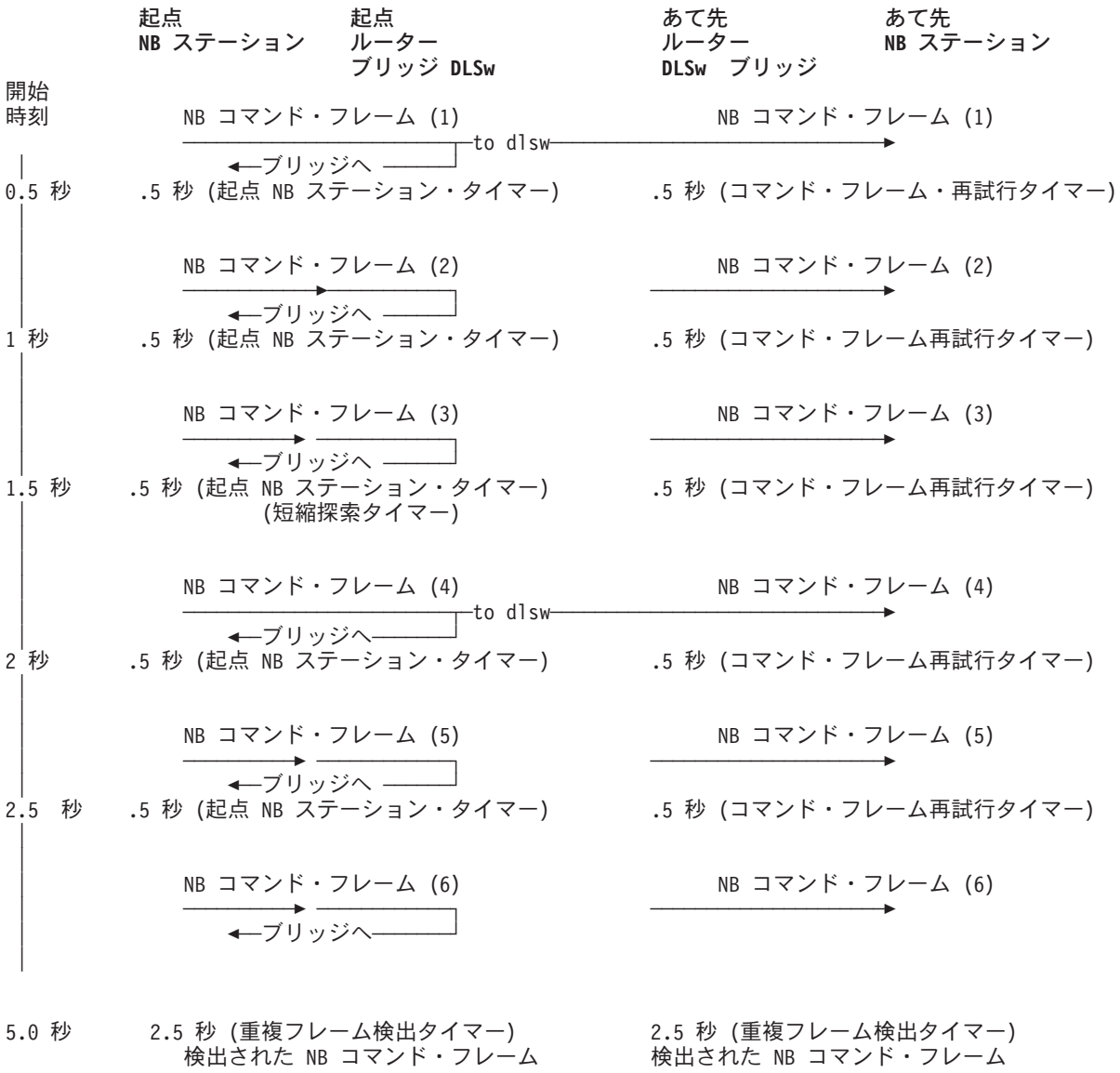


図 24. DLSw 上における NetBIOS セッションのセットアップ. 重複フィルターにより、DLSw WAN 上を転送される同報通信フレーム数が削減されます。

図24 には、次に説明する事象の順序ともども、このプロセスの働き方が示してあります。単純化のため、応答フレームの受信はないものと想定しています。

NetBIOS の使用



事象の順序は次のとおりです。

1. 最初の NetBIOS コマンド・フレームが、起点 DLSw ルーターのブリッジ・ポートで受信されます。この NetBIOS コマンド・フレームのコピーが保管されます。ブリッジングが使用可能にされているので、フレームはブリッジ・ネットワークに転送されます。 ブリッジ・ネットワーク上の重複フィルターが省略時値として使用不能にされているので、重複フレーム・フィルター・タイマーは開始されません。DLSw NetBIOS が使用可能にされているので、フレームは DLSw ネットワークに転送され、限定探索タイマーが開始されます (省略時値 1-1/2 秒)。重複フレーム検出タイマー (省略時値 5 秒) も開始されます。
2. 着信先ルーター DLSw 機能が最初の NetBIOS コマンド・フレームを受信します。この NetBIOS コマンド・フレームのコピーが保管されます。ブリッジングが使用可能にされているので、フレームはブリッジ・ネットワークに転送されます。 ブリッジ・ネットワーク上の重複フィルターが省略時値として使用不能にされているので、重複フレーム・フィルター・タイマーは開始されません。コマンド再試行タイマー (省略時値 1/2 秒) および重複フレーム検出タイマー (省略時値 5 秒) が開始されます。

3. 起点ルーターで、2 回目の NetBIOS コマンド・フレーム (最初の再試行) が受信されます。ブリッジ・ネットワーク上の重複フィルターが省略時値として使用不能にされているので、このフレームはブリッジ・ネットワークに転送されます。限定探索タイムアウトが満了していないので、フレームは DLSw ネットワークには転送されません。
4. 着信先ルーターで、DLSw 機能が NetBIOS コマンド・フレームの最初の再試行 (ローカルで生成された) をブリッジ機能に転送します。ブリッジ・ネットワーク上の重複フィルターが省略時値として使用不能にされているので、このフレームはブリッジ・ネットワークに転送されます。 コマンド再試行タイマー (省略時値 1/2 秒) が開始されます。
5. 起点ルーターで、3 回目の NetBIOS コマンド・フレーム (2 回目の再試行) が、2 回目の NetBIOS コマンド・フレームの場合と同様に処理されます。
6. 着信先ルーターで、NetBIOS コマンド・フレームの 2 回目の再試行が最初の再試行の場合と同様に処理されます。
7. 起点ルーターで、4 回目の NetBIOS コマンド・フレーム (3 回目の再試行) が受信されます。ブリッジ・ネットワーク上の重複フィルターが省略時値として使用不能にされているので、このフレームはブリッジ・ネットワークに転送されます。限定探索タイムアウトが今度は満了しているので、フレームは DLSw ネットワークに転送されます。限定探索タイマーが再始動します。
8. 着信先ルーターで、DLSw 機能が NetBIOS コマンド・フレームの 3 回目の再試行 (ローカルで生成された) をブリッジ機能に転送します。ブリッジ・ネットワーク上の重複フィルターが省略時値として使用不能にされているので、このフレームはブリッジ・ネットワークに転送されます。コマンド再試行タイマー (省略時値 1/2 秒) が開始されます。着信先ルーターでは、起点ルーターから転送された NetBIOS コマンド・フレームも受信しますが、これは重複として廃棄します。
9. 起点ルーターで、5 回目の NetBIOS コマンド・フレーム (4 回目の再試行) が、2 回目の NetBIOS コマンド・フレームの場合と同様に処理されます。
10. 着信先ルーターで、NetBIOS コマンド・フレームの 4 回目の再試行が最初の再試行の場合と同様に処理されます。
11. 起点ルーターで、6 回目の NetBIOS コマンド・フレーム (5 回目の再試行) が受信されます。ブリッジ・ネットワーク上の重複フィルターが省略時値として使用不能にされているので、このフレームはブリッジ・ネットワークに転送されます。限定探索タイムアウトが満了していないので、フレームは DLSw ネットワークには転送されません。
12. 着信先ルーターで、DLSw 機能が NetBIOS コマンド・フレームの 5 回目の再試行 (ローカルで生成された) をブリッジ機能に転送します。ブリッジ・ネットワーク上の重複フィルターが省略時値として使用不能にされているので、このフレームはブリッジ・ネットワークに転送されます。再試行カウントがこれで終わりに達したので、コマンド再試行タイマーは再始動されません。
13. さらに 2-1/2 秒後、起点ルーターで、重複フレーム検出タイマーが満了し、保管されていた NetBIOS コマンド・フレームが削除されます。
14. さらに 2-1/2 秒後、着信先ルーターで、重複フレーム検出タイマーが満了し、保管されていた NetBIOS コマンド・フレームが削除されます。

応答フレーム・フィルター

NetBIOS セッション・セットアップ・コマンド・フレームおよび NetBIOS 状況コマンド・フレームには、それぞれ対応する NetBIOS 応答フレームがあるものと予測されます。応答フレームを受信しなかった場合は、上記の例の場合と同じようにコマンド・フレームが再試行されます。

最初の NetBIOS 応答フレームがブリッジ・ネットワークの着信先ルーターで受信されると、それは起点ルーターに返送され、保管されていた NetBIOS コマンド・フレームが削除されます。それ以降に着信先ルーターで受信される応答フレームがあっても、対応する NetBIOS コマンド・フレームが見つからないため、いずれも廃棄されます。

起点ルーターでは、受信された応答フレームがブリッジ・ネットワークに転送され、保管されていた NetBIOS コマンド・フレームは廃棄されます。それ以降に起点ルーターで受信される (DLSw ネットワークまたはブリッジ・ネットワークから) 応答フレームがあっても、すべて廃棄されます。

NetBIOS 名前競合解消フレームの場合は、対応する NetBIOS 応答フレームが生じることもありますが、それが必要なわけではありません。さらに、受信された応答フレームについては、すべてが使用されます (複数の競合の有無を判別するため)。

したがって、受信された NetBIOS 名前競合フレームはすべてが転送されますが、重複フレーム検出タイマーが満了するまでは、NetBIOS コマンド・フレームが削除されることはありません。

NetBIOS 名前リスト

NetBIOS 名前リストは、NetBIOS UI フレームが転送される先の DLSw パートナーの数を制限する DLSw 専用の媒体です。

ローカル NetBIOS 名前リストは各ルーターで構成することができます。この名前リストは、DLSw パートナーによってアクセスすることができる、ルーターのローカル・ブリッジ・ネットワークに接続された NetBIOS 名をすべて表します。ルーターはすべての DLSw パートナーにローカル NetBIOS 名前リストを送信します。これらのパートナーはリストを使用して、パートナーがこのルーターに送信する NetBIOS トラフィックを制限します。

NetBIOS 名前リストは、NetBIOS 名に対する良好な制御がある環境では有用です。特に DLSw を通じてリモートからアクセスする必要がある環境では有用です。

ローカル NetBIOS 名前リストの構成

NetBIOS 名前リストは NetBIOS 名前リスト項目のセットです。ローカル NetBIOS 名前リストの構成には次のことが含まれます。

- 最大 30 までの項目を名前リストに追加する
- このリストが、ルーターの DLSw パートナーによって到達可能なすべての NetBIOS 名を表すかどうかを構成する

NetBIOS config> プロンプトで *add name-list* コマンドを使って名前リスト項目を構成します。各項目は次の情報から構成されます。

name qualifier

名前修飾子は 1 つまたは複数の NetBIOS 名を表します。各名前修飾子は最大 16 文字にすることができます。複数の NetBIOS 名は、名前内でワイルドカード (組み込みの ? または後書きの *) を使用して表すことができます。

? (疑問符) は、NetBIOS 名内でその位置にある文字が任意の値をもつことができることを意味します。

名前の最後の文字としての * (アスタリスク) は、NetBIOS 名内の残りのすべての文字が任意の値をもつことができることを意味します。

注: クライアント/サーバー NetBIOS アプリケーションの大部分では、名前リストで必要とされる名前はサーバーまたはドメインの名前です。個別のクライアント名は名前リスト内に構成する必要はありません。

name qualifier type

NetBIOS 名は個別の名前またはグループ名にすることができます。各名前修飾子は、個別の NetBIOS 名のセットまたはグループ NetBIOS 名のセットです。名前修飾子タイプは、どのタイプの NetBIOS 名 (個別またはグループ) が対応する名前修飾子を表すかを指定します。

一般的規則として、ドメイン名はグループ名であり、クライアント名またはサーバー名は個別の名前です。

名前リスト自体は、NetBIOS config> プロンプトで SET NAME-LIST コマンドを使用して構成される属性をもっています。その属性は *name list exclusivity* です。

属性は、名前リスト項目のセットが、このルーターの DLSw パートナーが到達することができるすべての NetBIOS 名を表すか (排他的) 、またはこのルーターの DLSw パートナーが到達できる一部だか必ずしもすべてではない NetBIOS 名を表す (非排他的) ことを示します。

排他的名前リストは、ネットワーク上の NetBIOS DLSw トラフィックを制限する最適のジョブを行います。ルーターの排他的名前リストによって表される NetBIOS 名に宛てられるフレームだけがそのルーターに転送されます。

非排他的名前リストは、ネットワーク上の NetBIOS DLSw トラフィックを制限するのに役立ちますが、排他的名前リストほどよくは働きません。ルーターの非排他的名前リストによって表される NetBIOS 名に宛てられたフレームは、そのルーターに最初に転送されます。

ルーターが、任意のルーターの名前リストによって表されていない NetBIOS 名に宛てられたフレームを受信する場合、そのルーターはフレームを非排他的名前リストをもつすべてのルーターに転送します。

特定のルーターがそのローカル NetBIOS 名前リスト、およびその DLSw パートナーから受信した名前リストを、次のパラメーターを使用して制御することが可能です。

use local NetBIOS name list

この機能は、NetBIOS config> プロンプトで **enable name-list local** コマンドまたは **disable name-list local** コマンドを使って構成されます。

use local NetBIOS name list を使用可能にする場合、ルーターはそのルーターで構成されたローカル NetBIOS 名前リストをすべての DLSw パートナーに送信します。

use local NetBIOS name list を使用不能にする場合、ルーターはそのルーターで構成されたローカル NetBIOS 名前リストをすべての DLSw パートナーに送信しません。

use remote NetBIOS name lists

この機能は、NetBIOS config> プロンプトで **enable name-list remote** コマンドまたは **disable name-list remote** コマンドを使って構成されます。

use remote NetBIOS name lists を使用可能にする場合、ルーターはそのルーターの DLSw パートナーから受信されたすべての NetBIOS 名前リストを使用して、特定の NetBIOS フレームを転送する方法を判別します。

use remote NetBIOS name lists を使用不能にする場合、ルーターはそのルーターの DLSw パートナーから受信されたすべての NetBIOS 名前リストを無視します。

NetBIOS 名前リスト変更のコミット

すべての NetBIOS 名前リスト・パラメーターは、NetBIOS config> プロンプトで永続的に変更するか、NetBIOS> プロンプトで一時的に変更することができます。

行われる各変更は、ルーターに情報を各 DLSw パートナーに送信することを要求するので、NetBIOS> プロンプトで **set name-list** を入力することにより、名前リストの変更の準備が整っていることを示す必要があります。

NetBIOS 名前リストの使用

ルーターは NetBIOS 名前リストを使用して、次の NetBIOS フレームを転送する方法を判別します。

- NetBIOS セッション・セットアップ・コマンド・フレーム (名前照会)
- NetBIOS 状況コマンド・フレーム (状況照会)
- NetBIOS 無接続データ転送フレーム (データグラム)

排他的 NetBIOS 名前リストの効果的な使用: 可能な場合はいつでも排他的 NetBIOS 名前リストを構成してください。排他的名前リストを構成し、すべての DLSw パートナーに送信する場合には、DLSw パートナーから受信された NetBIOS フレームだけが、あて先名が名前リスト項目の 1 つに一致するフレームになります。

便利な排他的 NetBIOS 名前リストは空の NetBIOS 名前リストです。特定のルーターが、その DLSw パートナーのどれかによりアクセスされる NetBIOS サーバーをもたない場合、空の排他的名前リストを使用する必要があります。

非排他的 NetBIOS 名前リストの使用: ルーターが多くの DLSw パートナーをもち、それらがすべて異なるブリッジ・ネットワーク上にある場合、非排他的名前リストを使用することができます。名前リスト項目は、最も頻繁に使用されるサーバー用

に構成することができるので、これらのサーバーにあてられるトラフィックはこのルーターに最初に進むことになります。名前リストを非排他的として指定することにより、名前リストでサーバーを構成しなくても、トラフィックは最も使用頻度の少ないサーバーに進むことができます。この構成は、NetBIOS 名の厳しい制御のないネットワーク、特に DLSw を通じてリモートからアクセスするサーバーで使用してください。

非排他的 NetBIOS 名前リストのもう 1 つの使用は、ブリッジされたネットワーク間で並列 DLSw パスを含む構成で行われます。2 つのルーターが同じブリッジされたネットワーク上にある場合、1 つのルーターは、ブリッジされたネットワーク上で DLSw を通じてリモートからアクセスされる 1 セットのサーバーを表す NetBIOS 名前リストを構成することができ、もう 1 つのルーターは異なるセットのサーバーを表す NetBIOS 名前リストを構成することができます。両方のルーターがアクティブである場合、NetBIOS トラフィックは 2 つのルーター間で配布されます。1 つのルーターが非アクティブである場合、すべての NetBIOS トラフィックは他方のルーターを通じて進みます。それが非排他的リストをもっているからです。

省略時の名前リストは空の非排他的 NetBIOS 名前リストです。これは、ルーターがその DLSw パートナーにすべての転送不能 NetBIOS トラフィックをルーターに送信してもらいたいことを示します。

NetBIOS 名前キャッシュおよびルート・キャッシュ

NetBIOS 名前キャッシュはルーター内の機能で、NetBIOS 名のタイプおよび NetBIOS 名に到達するのに必要な情報を分類するものです。この情報を使用して、フィルターされていない NetBIOS フレームをできるだけ少ない DLSw 近隣およびブリッジ・ポートに転送する方法の最善の判別を行います。NetBIOS 名のタイプおよびそのそれぞれについて保管される情報としては、次のものが考えられます。

Individual remote
: 特定の DLSw TCP セッションを介してリモートに到達可能と分かっている NetBIOS 名です。最適の TCP セッションが保管されます。

Individual local
: ブリッジ・ネットワークを介してローカルに到達可能と分かっている NetBIOS 名です。この名前に関連する MAC アドレスが保管されます。ルート・キャッシュが使用可能にされている場合は、ルーターと NetBIOS ステーションの間の最適の LLC ルートも保管されます。

グループ
: グループ名であることが分かっている NetBIOS 名です。ローカルまたはリモート (あるいはその両方) に到達可能で、複数の NetBIOS ステーションを表すことができます。他の情報は保管されません。

Unknown
: NetBIOS 名についての情報がまだ不明であり、名前の探索が不完全であることを示します。他の情報は保管されません。

NetBIOS セッション・セットアップ・フレームまたは無接続データ転送フレームが受信された場合は、常に名前キャッシュを使用してそのフレームの転送方法を判別します。これらのフレームの 1 つをブリッジ・ネットワーク上のルーターで受信した場合は、次のアクションのいずれかがとられます。

- NetBIOS フレーム内のあて先名がルーターの NetBIOS 名前キャッシュ内にない場合、すべての DLSw パートナーの名前リストを探索して一致がないか調べる。

  グループ名修飾子との一致が見つかった場合、NetBIOS 名前キャッシュ項目が名前タイプ *group* を指定して作成される。フレームはすべてのブリッジ・ポート上で、一致する名前リスト項目をもつ非排他的名前リストまたは排他的名前リストをもつすべての DLSw パートナーに転送されます。

  個別の名前修飾子との一致が見つかると、NetBIOS 名前キャッシュ項目が *individual remote* を指定して作成されます。フレームは、一致する名前リスト項目をもつ各 DLSw パートナーに転送されます。

  一致が見つからない場合、NetBIOS 名前キャッシュ項目は名前タイプ *unknown* を指定して作成されます。フレームはすべてのブリッジ・ポート上で、非排他的名前リストをもつすべての DLSw パートナーに転送されます。
- NetBIOS フレームの中のあて先名がルーターの NetBIOS 名前キャッシュの中にあり、個別リモートに分類されている場合は、フレームは学習された最適の DLSw TCP セッションに転送されます。

  複数の同等に最適の TCP セッションが学習されている場合は、それぞれ異なる NetBIOS セッション・セットアップ・フレームで交互に使用されます。
- NetBIOS フレームの中のあて先名がルーターの NetBIOS 名前キャッシュの中にあり、個別ローカルに分類されている場合は、保管されている MAC アドレスによって NetBIOS フレームの MAC アドレスが置き換えられます。

  ルート・キャッシュが使用不能になっている場合は、NetBIOS フレームのルーティング情報は放置され、フレームはすべてのブリッジ・ポートに転送されます。

  ルート・キャッシュが使用可能にされている場合は、NetBIOS フレームのルーティング情報は保管されているルーティング情報によって更新され、フレームは適正なブリッジ・ポート (MAC アドレスおよびルートによって判別される) に転送されます。
- NetBIOS フレームの中のあて先名が NetBIOS 名前キャッシュの中にあり、グループまたは不明に分類されている場合は、フレームはすべてのブリッジ・ポートおよびすべての DLSw 近隣に転送されます。

NetBIOS 名を学習する

NetBIOS 名は、NetBIOS セッション・セットアップ・フレーム (名前照会および名前認識 (Name-Recognized)) の中の情報から、学習されて分類されます。

NetBIOS 名前キャッシュ項目の構成

個別リモート NetBIOS 名を構成し、特定の DLSw TCP セッションに関連付けることが可能です。そうすれば、探索オーバーヘッドを大幅に節減することができます。パフォーマンスの向上を図るには、ルーターのローカル・ブリッジ・ネットワーク内の NetBIOS クライアントが普通にアクセスするリモート NetBIOS サーバーを構成することをお勧めします。

個別ローカル NetBIOS 名を構成し、特定の MAC アドレスおよびルートに関連付けることは不可能です。

NetBIOS 名前キャッシュ項目には 3 つのタイプがあります。

- 永続項目。NetBIOS 構成プロンプト (NetBIOS config>) で追加される項目です。ルーターは、ルーターの再始動時に、その構成内に永続項目を保管します。

  永続項目を追加する場合は、NetBIOS config> プロンプトで **add cache-entry** を入力します。NetBIOS 名および対応する IP アドレスの入力を指示するプロンプトが出されます。
- 静的項目。NetBIOS 監視プロンプト (NetBIOS> コンソール) で追加される項目です。ルーターは、ルーターの再始動時に静的項目を保管しません。

  静的項目を追加する場合は、NetBIOS> コンソール・プロンプトで **add cache-entry** を入力します。NetBIOS 名および対応する IP アドレスの入力を指示するプロンプトが出されます。
- 動的項目。NetBIOS 構成または監視プロンプトで追加されることは**ない** が、NetBIOS セッション・セットアップ・フレームから動的に学習される項目です。ルーターは、ルーターの再始動時に動的項目を保管しません。

名前キャッシュ・パラメーターの構成

名前キャッシュ全体が 1 つのタイプの NetBIOS 名でいっぱいになるのを防ぐために、構成可能な NetBIOS 名前キャッシュには 2 つの限界が設けられています。

- ローカル名前キャッシュ項目の最大数では、一度にキャッシュできる個別ローカル NetBIOS 名前キャッシュ項目の最大数を指定します。使用された時期が最も以前の項目は、新しい項目で上書きされます。
- リモート名前キャッシュ項目の最大数では、一度にキャッシュできる個別リモート、グループ、および不明 NetBIOS 名前キャッシュ項目を組み合わせた最大数を指定します。使用された時期が最も以前の項目は、新しい項目で上書きされます。

構成可能なタイムアウト期間中参照されなかった項目は、自動的に削除されます。このタイムアウト期間が項目非参照タイムアウト値です。

TCP セッションまたは MAC アドレスおよびルートのいずれかへの NetBIOS 名の関連付けは、1 つの経時インスタンスで行われます。ネットワークは変わり、NetBIOS 名への最適パスも変わる場合があるので、NetBIOS 名と TCP セッションまたは MAC アドレスおよびルートの間の関連は、構成可能な期間のみに限って保管されます。この期間の後は、新しい最適パス関連が学習されます。この構成可能な期間を制御するパラメーターが最適パス経時タイムアウト値です。

もう 1 つの有用な構成パラメーターは限定探索タイムアウト値です。これは、重複コマンド・フレームを DLSw ネットワークに対してフィルターする期間を制御するだけでなく、NetBIOS 名の探索を拡張する前に待機する期間も制御します。NetBIOS セッション・セットアップ・フレームが受信され、あて先 NetBIOS 名がルーターの NetBIOS 名前キャッシュ内に個別リモート・フレームとしてある場合は、フレームは対応する TCP セッションに転送されます。このフレームに対する応答を受信しなかった場合は、名前がこのパスを経由してアクセスできなくなっていることが原因である可能性があります。限定探索タイマーの満了後最初に受信した重複 NetBIOS セッション・セットアップ・フレームは、すべての DLSw TCP セッションに転送されるので、探索が拡張されてより適切なパスを探索します。

NetBIOS の使用

最後のパラメーター (名前の中の有効文字数) では、NetBIOS 名の 16 文字の中で、固有の NetBIOS 名であるとみなすのに必要な文字数を制御します。NetBIOS アプリケーションによっては、NetBIOS 名の 16 番目の文字を使用して、単一の NetBIOS 名に関連する特定のエンティティー間の区別を行うものがあります (例えば、プリント・サーバーおよびファイル・サーバー)。このような場合は、名前の中の有効文字数を 15 に指定するのが最善です。こうすると、あて先 NetBIOS 名の最初の 15 文字がルーターの NetBIOS 名前キャッシュ項目の最初の 15 文字に一致するフレームが、名前キャッシュ項目情報に応じて転送されます。したがって、複数の NetBIOS 名を単一の NetBIOS 名前キャッシュ項目で表すことができます。

上記の NetBIOS 名前キャッシュ関連パラメーターはすべて、**set cache-parms** コマンドを使用して、次のように構成することができます。

```
NetBIOS config>set cache-parms

Significant characters in name [15]?
Best path aging timeout value in seconds [60.0]?
Reduced search timeout value in seconds [1.5]?
Unreferenced entry timeout value in minutes [5000]?
Max nbr local name cache entries [500]?
Max nbr remote name cache entries [100]?

Cache parameters set
```

set cache-parms コマンドの詳細については、174ページの『NetBIOS コマンド』を参照してください。

キャッシュ項目の表示

ルーターには次のコマンドが用意されていますから、それを使用すれば、キャッシュ項目を表示することができます。 NetBIOS 構成プロンプトでは、表10 の **list cache** コマンドを使用することができます。

表 10. NetBIOS List Cache 構成コマンド

コマンド	表示内容. .
list cache all	すべての永続項目。静的および動的項目を示しません。
list cache entry-number	その項目番号に従っての永続キャッシュ項目
list cache NetBIOS-name	特定の NetBIOS 名についての永続キャッシュ項目
list cache ip-address	特定の IP アドレスについての永続キャッシュ項目

NetBIOS 監視プロンプトでは、表11 の list cache コマンドを使用することができます。

表 11. NetBIOS List Cache 監視コマンド

コマンド	表示内容. .
list cache active	ルーターの名前キャッシュ内のすべての活動項目 (永続項目、静的項目、および動的項目を含む)。
list cache config	静的項目および永続項目。 動的項目は表示しません。
list cache group	NetBIOS グループ名に関して存在している項目
list cache local	ローカル・キャッシュ項目。ローカル・キャッシュ項目とは、ルーターがブリッジ・ネットワーク上で学習するキャッシュ項目です。
list cache name	特定の NetBIOS 名に関するキャッシュ項目
list cache remote	リモート・キャッシュ項目。 これらは、ルーターが DLSw WAN を通じて学習する項目です。

表 11. NetBIOS List Cache 監視コマンド (続き)

コマンド	表示内容. .
list cache unknown	NetBIOS 項目のタイプが不明の項目。ルーターは、項目のタイプを学習するまで、すべての項目を不明とみなします。

NetBIOS のホスト名フィルターおよびバイト・フィルターの構成手順

以下の各項では、NetBIOS フィルターをセットアップする方法の例を示します。最初の例ではホスト名フィルターの作成方法について説明します。2 番目の例ではバイト・フィルターの構成方法を示します。これらの例で使用するコマンドの詳細については、 174ページの『NetBIOS コマンド』を参照してください。

ホスト名フィルターを作成する場合は、NetBIOS Filter config> プロンプトでコマンドを入力します。

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>NetBIOS

NetBIOS Support User Configuration

NetBIOS config>set filter name
NetBIOS Filtering configuration
NetBIOS Filter config>
```

ホスト名フィルターの作成

ホスト名フィルターを作成するには、以下の手順を使用します。

1. 空の名前フィルター・リストを作成する。

   ```
   NetBIOS Filter config>create name-filter-list
   Handle for Name Filter List []? boston
   ```

2. 名前フィルター・リストにフィルター項目を追加する。

   update を入力して、フィルター・リストに関するプロンプトにアクセスします。このプロンプトからフィルター・リストにフィルター項目を追加することができます。

   ```
   NetBIOS Filter config>update
   Handle for Filter List []? boston
   Name Filter List Configuration
   NetBIOS Name boston config>
   ```

3. **add** コマンドを用いて、フィルター・リストにフィルター項目を追加する。フィルター項目を構成する方法により、どの NetBIOS パケットがブリッジされるのか除去されるのかが決まります。ホスト名フィルター項目は、この順序で入力される次のパラメーターを使用して構成されます。

   - *Inclusive* (ブリッジされる) または *Exclusive* (除去される)
   - *ASCII* または *HEX* - ホスト名を表す方法
   - *host name* - ASCII または 16 進数のストリングで表される実際のホスト名 (構文については、174ページの『NetBIOS コマンド』を参照してください)

     注: この項目は大文字と小文字を区別します。

   - <*LAST-hex-number*> - 16 文字未満の ASCII ストリングと併用する任意指定パラメーター。

次の例では、ホスト名フィルター・リスト **boston** にフィルター項目を追加します。これにより、ホスト名 **westboro** (ASCII ストリング) を含むパケットをブリッジする (*inclusive* (組み込み) として構成する) ことができます。 この項目については、*<LAST-hex-number>* パラメーターは構成されていません。

```
NetBIOS Name boston config>add inclusive ascii
Hostname []? westboro
Special 16th character in ASCII hex (<CR> for no special char) []?
```

プロンプトによる指示を望まない場合は、すべてのパラメーターを 1 つのストリングとしてコマンド行に入力することができます。各パラメーターの間には必ずスペースを 1 つ入れてください。

4. フィルター項目の入力を検証する。

   list と入力して、入力を検証します。

```
NetBIOS Name boston config>list

NAME Filter List Name: boston
NAME Filter List Default: Inclusive

 Item #   Type    Inc/Ex    Hostname         Last Char

   1      ASCII    Inc      westboro
```

5. フィルター・リストに追加のフィルター項目を追加する。

   フィルター・リストに追加のフィルター項目を追加するには、上記の最初の 4 つのステップを繰り返します。フィルター項目を入力する順序は、ルーターがパケットにフィルター項目を適用する方法がそれによって決まるため、重要です。最初の一致によってフィルター項目の適用が停止し、フィルター項目が組み込みか排除かに応じて、ルーターはパケットを転送または除去します。

   ソフトウェアはリストの始めで突き合わせを行う可能性が高いので、最も普通のフィルター項目を最初に入力すると、フィルター・プロセスの効率を高めることになります。

   パケットがフィルター項目のいずれとも一致しない場合は、ルーターはフィルター・リストの省略時条件 (組み込みまたは排除) を使用します。フィルター・リスト構成プロンプトで、**default inclusive** または **default exclusive** を入力することによって、フィルター・リストの省略時条件を変更することができます。例えば、次のようにします。

```
NetBIOS Name boston config> default exclusive
```

6. フィルター・リストにフィルター項目を追加し終えたら、**exit** を入力して、NetBIOS Filter config> プロンプトに戻ります。

```
NetBIOS Name boston config>exit
NetBIOS Filter config>
```

7. ユーザーの構成にフィルターを追加する。

   これで、フィルター項目が入っているフィルター・リストを、フィルターとしてブリッジング・ルーター構成に追加することができます。これを行うには **filter-on** コマンドを使用してください。ホスト名フィルターは、次のパラメーター (この順序で入力する) を使用して構成します。

   - *Input* (そのポートで受信されたすべての NetBIOS パケットをフィルターする) または output (そのポートで送信されたすべての NetBIOS パケットをフィルターする)
   - *Port#* (ルーター上の必要な構成済みブリッジ・ポート番号)

- *Filter-list* (このフィルターに組み込みたいフィルター・リスト (フィルター項目が入っている) の名前)
- すべて大文字で AND または OR のいずれかとして入力される任意指定の演算子。演算子がある場合は、演算子の後にフィルター・リスト名を入力する必要があります。複数のフィルター・リストをもつフィルターは複合フィルターと呼ばれます。

次の例では、ポート #3 で入力されたパケットに影響を及ぼすホスト名フィルターを追加します。これは、ホスト名フィルター・リスト **boston** で構成されます。ポート #3 で入力されたパケットはすべて、フィルター・リスト **boston** に入っているフィルター項目によって提供される規則に従って評価されます。つまり、ポート #3 で入力され、ホスト名 **westboro** を含むパケットは、すべてブリッジされることを意味します。

```
NetBIOS Filter config>filter-on input
Port Number [1]? 3
Filter List []? boston
```

8. 新規に作成されたフィルターを検証する。

   list を入力して、入力を検証します。

```
NetBIOS Filter config>list

NetBIOS Filtering: Disabled

NetBIOS Filter Lists
--------------------

    Handle           Type
    nlist            Name
    newyork          Name
    HELLO            Byte
    boston           Name

NetBIOS フィルター
---------------

    Port #      Direction      Filter List Handle(s)
       3          Output       nlist
       1          Input        newyork OR HELLO
       3          Input        boston
```

9. NetBIOS フィルターをグローバルに使用可能にする。

   ルーター上で NetBIOS フィルターをグローバルに使用可能にするには、**enable** コマンドを使用します。

```
NetBIOS Filter config>enable NetBIOS-filtering
```

10. ルーターを再始動して、NetBIOS フィルター構成の変更をすべて活動化する。

    exit に続けて **Ctrl-P** を入力して、* プロンプトに戻ります。このプロンプトから **restart** を入力して、NetBIOS フィルター構成プロセスの過程で加えられたソフトウェア変更をすべて活動化します。

```
NetBIOS Filter config>exit
ASRT config>exit
Config> Ctrl-P
* restart
```

バイト・フィルターの作成

バイト・フィルターを作成する場合は、以下の手順を指針として使用します。コマンドはすべて、NetBIOS filtering config> プロンプトで入力します。

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>NetBIOS
```

```
NetBIOS Support User Configuration

NetBIOS config> set filter byte
NetBIOS Filtering configuration
NetBIOS Filter config>
```

1. **create byte-filter-list** コマンドを使用して、空のフィルター・リストを作成する。

```
NetBIOS Filter config>create byte-filter-list
Handle for Byte Filter List []? westport
```

2. バイト・フィルター・リストにフィルター項目を追加する。

   update を入力して、フィルター・リストに関するプロンプトにアクセスします。このプロンプトからフィルター・リストにフィルター項目を追加することができます。

```
NetBIOS Filter config>update
Handle for Filter List []? westport
Byte Filter List Configuration
NetBIOS Byte westport config>
```

   add コマンドを使用して、フィルター・リストへのフィルター項目の追加を開始します。フィルター項目を構成する方法により、どの NetBIOS パケットがブリッジされるのか除去されるのかが決まります。バイト・フィルター項目は次のパラメーター (この順序で入力されます) を使って構成されます。

   - Inclusive (ブリッジされる) または Exclusive (除去される)
   - Byte Offset - フィルターされるパケットにオフセットするバイト数 (10 進数)。これはパケットの NetBIOS ヘッダーから始まります。ゼロでは、ルーターがパケット内のすべてのバイトを調べることを指定します。
   - Hex pattern - NetBIOS ヘッダーのバイト・オフセットから始まるバイト数と比較するのに使用する 16 進数。構文規則については、174ページの『NetBIOS コマンド』を参照してください。
   - Hex mask - (ある場合) hex pattern と同じ長さであることが必要であり、オフセットから始まるパケット内のバイト数を用いて AND (論理積) をとってから、結果が hex pattern と等しいかどうか比較されます。*hex-mask* 引き数が省略されている場合は、すべて 2 進数の 1 であるとみなされます。

   次の例では、バイト・フィルター・リスト **westboro** に、バイト・オフセット 0 で hex pattern が 0x12345678 のパケットをブリッジする (inclusive として構成する) ことができるフィルター項目を追加します。hex mask はありません。

```
NetBIOS Byte westport config>add inclusive
Byte Offset [0]? 0
Hex Pattern []? 12345678
Hex Mask (<CR> for no mask) []?
```

3. **list** コマンドを用いてフィルター項目の入力を検証する。

```
NetBIOS Byte westport config>list

BYTE Filter List Name: westport
BYTE Filter List Default: Inclusive

 Item #   Inc/Ex   Offset  Pattern        Mask

   1       Inc        0    0x12345678     0xFFFFFFFF
```

4. フィルター・リストに追加のフィルター項目を追加する。

   フィルター・リストに追加のフィルター項目を追加するには、上記の最初の 3 つのステップを繰り返します。

5. フィルター・リストにフィルター項目を追加し終えたら、**exit** を入力して、NetBIOS Filter config> プロンプトに戻ります。

```
NetBIOS Byte westport config>exit
NetBIOS Filter config>
```

フィルター項目を入力する順序は、ルーターがパケットにフィルターを適用する方法がそれによって決まるため、重要です。最初の一致によってフィルター項目の適用が停止し、フィルター項目が組み込みか排除かに応じて、ルーターはパケットを転送または除去します。

ソフトウェアは、リスト全体を調べてから突き合わせを行うのではなく、リストの始めで突き合わせを行う可能性の方が高いので、最も普通のフィルター項目を最初に入力すると、フィルター・プロセスの効率を高めることになります。

パケットがフィルター項目のいずれとも一致しない場合は、ルーターはフィルター・リストの省略時条件 (組み込みまたは排除) を使用します。フィルター・リスト構成プロンプトで、**default inclusive** または **default exclusive** を入力することによって、フィルター・リストの省略時条件を変更することができます。例えば、次のようにします。

```
NetBIOS Byte westport config> default exclusive
```

6. ユーザーの構成にフィルターを追加する。

これで、フィルター項目が入っているフィルター・リストを、フィルターとしてブリッジング・ルーター構成に追加することができます。これを行うには **filter-on** コマンドを使用してください。ホスト名フィルターは、次のパラメーター (この順序で入力する) を使用して構成します。

- *Input* (そのポートで受信されたすべてのパケットをフィルターする) または output (そのポートで送信されたすべてのパケットをフィルターする)
- *Port#* - 構成されたブリッジ・ポート番号
- *Filter-list* - このフィルターに組み込みたいフィルター・リスト (フィルター項目が入っている) の名前
- すべて大文字で AND または OR のいずれかとして入力される任意指定の演算子。演算子がある場合は、演算子の後にフィルター・リスト名を入力する必要があります。複数のフィルター・リストをもつフィルターは複合フィルターと呼ばれます。これらについては、171ページの『NetBIOS 構成コマンドおよび監視コマンド』で詳細に説明します。

次の例では、ポート #3 で出力されたパケットに影響を及ぼすホスト名フィルターを追加します。これは、バイト・フィルター・リスト **westboro** で構成されます。ポート #3 で出力されるすべてのパケットは、フィルター・リスト **westboro** に含まれるフィルター項目によって提供される規則に従って評価されます。

```
NetBIOS Filter config>filter-on output
Port Number [1]? 3
Filter List []? westboro
```

7. 新規に作成されたフィルターを検証する。

list を入力して、入力を検証します。

```
NetBIOS Filter config>list

NetBIOS Filtering: Disabled

NetBIOS Filter Lists
--------------------
```

```
    Handle          Type
    nlist           Name
    newyork         Name
    HELLO           Byte
    westboro        Byte

NetBIOS フィルター
---------------

    Port #      Direction      Filter List Handle(s)
       3          Output       nlist
       1          Input        newyork OR HELLO
       3          Output       westboro
```

8. NetBIOS フィルターをグローバルに使用可能にする。

   ブリッジング・ルーター上で NetBIOS フィルターをグローバルに使用可能にするには、**enable** を入力します。

```
NetBIOS Filter config>enable NetBIOS-filtering
```

9. ルーターを再始動して、NetBIOS フィルター構成の変更をすべて活動化する。

   exit に続けて **Ctrl-P** を入力して、* プロンプトに戻ります。**restart** を入力します。

```
NetBIOS Filter config>exit
ASRT config>exit
Config> Ctrl-P
* restart
```

第8章 NetBIOS の構成と監視

この章では、IBM が行うブリッジされたネットワークおよび DLSw ネットワークにおける NetBIOS の構成と監視について説明します。 この章には次のトピックが含まれます。

- 『NetBIOS 構成コマンドおよび監視コマンド』
- 174ページの『NetBIOS コマンド』

NetBIOS 構成コマンドおよび監視コマンド

NetBIOS 構成コマンドは ASRT/DLSW config> プロンプトで使用可能です。ルーターの構成に加えた変更は、即時有効にはなりません。このような変更は、ルーターの構成メモリーを再始動した時点で、その一部になります。ここでは構成変更を永続変更と呼びます。

NetBIOS 監視コマンドは、ASRT/DLSW> プロンプトで使用可能です。監視コマンドは即時有効になりますが、ルーターの不揮発性構成メモリーには保管されません。したがって、監視コマンドを使用すると、ルーターの構成にリアルタイムで変更を加えることができますが、このような変更は一時的なものです。ルーターが再始動すると、これらの変更はルーターの構成メモリーによって上書きされます。ここでは、監視プロンプトで加える変更は静的変更と呼びます。

NetBIOS 構成環境へのアクセス

NetBIOS config> プロンプトは、ASRT 構成環境と DLSw 構成環境のどちらからでも表示できます。NetBIOS config> プロンプトで加えた変更は、ブリッジングと DLSw の両方に影響します。

NetBIOS config> プロンプトを ASRT 構成環境から表示する場合は、次のようにします。

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>NetBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

NetBIOS config> プロンプトを DLSw 構成環境から表示する場合は、次のようにします。

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>NetBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

NetBIOS 監視環境へのアクセス

NetBIOS> プロンプトは、ASRT 監視環境と DLSw 監視環境のどちらからでも表示できます。

NetBIOS> 監視プロンプトで行った変更は、ブリッジングと DLSw の両方に影響します。

NetBIOS> 監視プロンプトを ASRT 監視環境から表示する場合は、次のようにします。

```
+protocol asrt
 ASRT>NetBIOS

  NetBIOS Support User Console

  NetBIOS>
```

NetBIOS> プロンプトを DLSw 監視環境から表示する場合は、次のようにします。

```
  + protocol dls
 DLSw>NetBIOS

  NetBIOS Support User Console

  NetBIOS>
```

DLSw 用 NetBIOS の構成

DLSw で NetBIOS トラフィック を送信する場合は、DLSw config> プロンプトで次の手順を使用してください。

- NetBIOS SAP のオープン
- SNA セッションおよび NetBIOS セッションに関する優先順位の設定
- 最大 NetBIOS フレーム・サイズの設定
- NetBIOS UI フレームに関して割り振るバイト数の設定

NetBIOS SAP のオープン

リンクの両側で NetBIOS SAP をオープンして、DLSw が NetBIOS フレームを伝送できるようにします。

```
DLSw config> open-sap
Interface # [0]?
Enter SAP in hex(range 0-F0),'SNA', or 'NB'[4]? nb
SAP F0 opened on interface 0
```

SNA セッションおよび NetBIOS セッションに関する優先順位の設定

SNA トラフィックおよび NetBIOS トラフィックの優先順位づけを行えば、ネットワーク輻輳時に 1 つのタイプのセッションが使用可能な帯域幅の多くを使用し過ぎることがないようにすることができます。そのためには、**priority** を入力して、SNA セッションおよび NetBIOS セッションの優先順位を設定します。また、セッションの優先順位に対応するメッセージ割り振りも設定することができます。

set priority コマンドは、次の例に示すように使用します:

```
DLSw config> set priority
Default priority for SNA DLSw session traffic (C/H/M/L) [M]?  C
Default priority for NetBIOS DLSw session traffic (C/H/M/L) [M]? L
```

```
Default priority for SNA DLSw explorer traffic (C/H/M/L) [M]?  H
Default priority for NetBIOS DLSw explorer traffic (C/H/M/L) [M]? M
Message allocation by C/H/M/L priority (4 digits) [4/3/2/1]?
Maximum NetBIOS frame size (516, 1470, 2052, or 4399) [2052]? 516
```

省略時メッセージ割り振り 4/3/2/1 では、セッションに次のような割り振りがなされます。

4 - 重大

3 - 上位

2 - 中位

1 - 下位

ルーターは優先順位およびメッセージ割り振りを使用して、特定のタイプのトラフィックのバースト長を選択的に制限します。例えば、次のようにします。

- SNA トラフィックに優先順位「重大」を割り当て、「重大」セッションがメッセージ割り振り 4 で、

  しかも

- NetBIOS トラフィックに「中位」優先順位を割り当て、「中位」セッションがメッセージ割り振り 2 である場合は、

ルーターは 4 つの SNA フレームを処理してから 2 つの NetBIOS フレームを処理します。ルーターは 2 つの NetBIOS フレームを処理すると、さらに 4 つの SNA フレームを処理し、以後についても同様です。

この例では、ルーターは使用可能な帯域幅の 3 分の 2 を SNA トラフィックの専用にしています (4 対 2 の比率)。ユーザーが割り当てた優先順位に応じて帯域幅を割り振る際に、ルーターがカウントするのはバイト数ではなく、フレーム数であることに注意してください。

セッションに関するメッセージ割り振りは、省略時値 4/3/2/1 から変更することができます。ただし、9 から 1 の範囲で、4 つの数字を降順に入力することが必要です。例えば、SNA トラフィックの優先順位が「重大」で、NetBIOS トラフィックの優先順位が「中位」で、メッセージ割り振りを 8/7/6/5 に変更した場合は、ルーターは 8 つの SNA フレームを処理してから、6 つの NetBIOS フレームを処理します。

最大 NetBIOS フレーム・サイズの設定

DLSw **set priority** コマンドを使用すれば、最大 NetBIOS フレーム・サイズを変更することもできます。省略時値は 2052 です。このパラメーターは、必要になると考えられる最大のフレーム・サイズに設定し、それより大きい値に設定することがないようにします。必要以上に大きいフレーム・サイズを設定すると、使用可能なバッファーの数が減少します。

NetBIOS UI フレームに関するメモリー割り振りの設定

DLSw **set memory** コマンドを使用して、NetBIOS UI フレーム用のバッファーとしてルーターが割り振るバイト数を設定します。TCP 転送バッファーがいっぱいになった場合は、ルーターは NetBIOS UI フレーム用としてこのバッファーを使用します。

NetBIOS に関して割り振られるバイト数はグローバルであり、セッション別ではないことに注意してください。

```
DLSw config> set memory
Number of bytes to allocate for DLSw (at least 26368) [141056]?
Number of bytes to allocate per LLC session [8192]?
Number of bytes to allocate per SDLC session [4096]?
Number of bytes to allocate for NetBIOS UI-frames [40960]?
```

NetBIOS コマンド

表12 に NetBIOS 構成コマンドおよび監視コマンドをリストしてあります。

表 12. NetBIOS 構成コマンドおよび監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	ルーターの名前キャッシュにキャッシュ項目を追加し、ルーターのローカル名前リストに名前リスト項目を追加します。
Delete	**add** コマンドを使用して追加したキャッシュ項目または名前リスト項目を削除します。
Disable	重複フレーム・フィルター、ルート・キャッシュ、およびローカルとリモートの NetBIOS 名前リストの使用を使用不能にします。
Enable	重複フレーム・フィルター、ルート・キャッシュ、およびローカルとリモートの NetBIOS 名前リストの使用を使用可能にします。
List	構成プロンプトまたは監視プロンプトのどちらにいるかによって、さまざまな NetBIOS 名前キャッシュおよび名前リストの構成情報を表示します。
Set	名前キャッシュ、重複フレーム・フィルター、フレーム・タイプ・フィルター、および名前リストに関するパラメーターを構成します。 `NetBIOS Filter config>` プロンプトも表示します。
Test	このコマンドは監視プロンプトでのみ使用可能であり、特定の NetBIOS 名を現行の NetBIOS 名前キャッシュおよび名前リストと突き合わせてテストします。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

ルーターの永続または静的構成に新しい名前キャッシュ項目を追加するか、リモート・ステーションがローカル DLSw にアクセスするのに使用される NetBIOS 名前リスト項目を追加します。追加できる名前キャッシュ項目は、DLSw 近隣用の項目だけです。ASRT トラフィック用に項目を追加しても、ルーターはこれを無視します。

構文 :

add cache-entry

name-list

cache-entry

ルーターの名前キャッシュに新しい項目を追加します。

- 構成プロンプトからの場合は、永続項目を追加します。
- 監視プロンプトからの場合は、一時項目を追加します。

set cache-parms によって、NetBIOS 名で 16 文字が有効であることを示した場合は、16 番目の文字を 16 進数でのみ入力するように指示するプロンプトが、ルーターによって出されます。

異なる IP アドレスをもつ複数の項目が、単一の NetBIOS 名に関して追加される場合があります。この場合は、複数の DLSw 近隣を介してその名前にアクセスすることができます。

注: NetBIOS 名は大文字と小文字を区別し、ネットワーク NetBIOS 名の大/小文字に一致することが必要です。

例 : add cache-entry

```
Enter up to 15 characters of NetBIOS name (no wild cards)
Enter NetBIOS name[]? Accounting
Enter last character of NetBIOS name in hex [0]? 01
Enter IP Address [0.0.0.0]? 20.2.1.3
Name cache entry has been created
```

name-list

ルーターのローカル名前リストに新しい項目を追加します。

構成プロンプトからの場合は、永続名前リスト項目を追加します。変更が有効になるのは、ルーターが再始動されるか、変更が NetBIOS> プロンプトから **set name-list** コマンドを使用してコミットされてからです。

監視プロンプトからの場合は、一時名前リスト項目を追加します。変更が有効になるのは、変更が NetBIOS> プロンプトから **set name-list** コマンドを使用してコミットされてからです。ルーターを再始動すると、変更は失われます。

NetBIOS 名前修飾子は、DLSw を通じて他のルーターに到達可能にされる、ルーターのローカルにブリッジされたネットワークに到達可能な 1 つまたは複数の NetBIOS 名を表します。

NetBIOS 名前修飾子は、次の 2 つのタイプのワイルドカード文字を含むことができます。

? (疑問符)
実際の NetBIOS 名の中の単一の文字が任意の値をとりうることを示します。

*** (アスタリスク)**
名前修飾子の末尾に付け、実際の NetBIOS 名の中の残りの文字が任意の値をとりうることを示します。

注:

1. アスタリスクが名前修飾子の末尾に表示されない場合は、名前修飾子の残りの部分は最大 16 文字までヌル (16 進数のゼロ) で埋め込まれます。
2. NetBIOS 名前修飾子は大文字と小文字を区別し、ネットワーク NetBIOS 名の大文字/小文字に一致することが必要です。

例 : add name-list

```
Enter up to 16 characters of NetBIOS name qualifier (wild cards OK).
  Enter name qualifier []? NY_SERV*
NetBIOS name qualifier type (I=individual, G=group) [I]?
```

```
Name list entry has been created

For the new entry to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

Delete

名前キャッシュ項目または NetBIOS 名前リスト項目を削除します。

構文 :

delete cache-entry

name-list

cache-entry

構成プロンプトからの場合は、ルーターの永続構成から名前キャッシュ項目を削除します。ルーターはプロンプトを出して、レコード番号 (削除したい項目の番号) の入力を指示します。項目番号のリストを表示するには、**list cache all** を入力します。

監視プロンプトからの場合は、ルーターの静的構成または活動キャッシュから名前キャッシュ項目を削除します。ルーターはプロンプトを出して、キャッシュ項目名の入力を指示します。項目のリストを表示するには、**list cache conf**、または **list cache active** を入力します。

注: NetBIOS 名は大文字と小文字を区別します。

構成の場合の例: delete cache-entry

```
Enter name cache record number [1]? 2

Name cache entry has been deleted
```

監視の場合の例: delete cache-entry

```
Enter up to 15 characters of NetBIOS name (no wild cards)
  Enter NetBIOS name []? ADMIN

Name cache entry NOT found in Active list for name entered
Name cache entry has NOT been deleted from Active list

Static name cache entry deleted from Config list
```

name-list

ルーターのローカル名前リストから項目を削除します。

構成プロンプトからの場合は、永続名前リスト項目を削除します。ルーターはプロンプトを出して、レコード番号 (削除したい項目の番号) の入力を指示します。項目番号のリストを表示するには、**list name-list all** コマンドを入力します。変更が有効になるのは、ルーターが再始動されるか、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。

監視プロンプトからの場合は、名前リスト項目を一時的に削除します。ルーターはプロンプトを出して、レコード番号 (削除したい項目の番号) の入力を指示します。項目番号のリストを表示するには、**list name-list config** コマンドを入力します。変更が有効になるのは、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。ルーターを再始動すると、変更は失われます。

例 : delete name-list

```
Enter name list record number [1]? 1

Name list entry NY_SERV*         / INDIVIDUAL has been deleted.

For the deletion to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

Disable

重複フレーム・フィルター、NetBIOS 名前リストの使用、またはルート・キャッシュを使用不能にします。

構文 :

disable duplicate-filtering
name-list local
name-list remote
route-caching

duplicate-filtering

ブリッジングに関して重複フレーム・フィルターを使用不能にします。DLSw トラフィックに関して重複フレーム・フィルターを使用不能にすることはできません。

例 : disable duplicate-filtering

```
Duplicate frame filtering is          OFF
```

name-list local

ローカル名前リストを使用不能にします。ローカル名前リスト項目は DLSw パートナーには送信されません。

構成プロンプトからの場合、ローカル名前リストの使用を永続的に使用不能にします。変更が有効になるのは、ルーターが再始動されるか、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。

監視プロンプトからの場合は、ローカル名前リストを一時的に使用不能にします。変更が有効になるのは、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。 ルーターを再始動すると、変更は失われます。

例 : disable name-list local

```
Use of local NetBIOS name list is  DISABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

name-list remote

リモート名前リストを使用不能にします。DLSw パートナーから受信された NetBIOS 名前リストは使用されません。

構成プロンプトからの場合、リモート名前リストを永続的に使用不能にします。変更が有効になるのは、ルーターが再始動されるか、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。

監視プロンプトからの場合は、リモート名前リストを一時的に使用不能にします。変更が有効になるのは、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。ルーターを再始動すると、変更は失われます。

例 : disable name-list remote

```
Use of remote NetBIOS name list is  DISABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

route-caching

ブリッジングおよび DLSw に関してルート・キャッシュを使用不能にします。ルート・キャッシュは、NetBIOS 名前キャッシュ内の項目を使用して、同報通信フレームを特定ルーティング・フレーム (SRF) に変換するプロセスです。

例 : disable route-caching

```
Route caching is                    OFF
```

Enable

重複フレーム・フィルター、NetBIOS 名前リスト、またはルート・キャッシュを使用可能にします。

構文 :

enable duplicate-filtering
name-list local
name-list remote
route-caching

duplicate-filtering

ブリッジングに関して重複フレーム・フィルターを使用可能にします。DLSw に関しては、重複フレーム・フィルターは常に使用可能になっています。したがって、使用可能および使用不能にすることはできません。

例 : enable duplicate-filtering

```
Duplicate frame filtering is          ON
```

name-list local

ローカル名前リストの使用を使用可能にします。ローカル名前リスト項目はすべての DLSw パートナーに送信されます。

構成プロンプトからの場合、ローカル名前リストの使用を永続的に使用可能にします。変更が有効になるのは、ルーターが再始動されるか、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。

監視プロンプトからの場合は、ローカル名前リストの使用を一時的に使用可能にします。変更が有効になるのは、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。ルーターを再始動すると、変更は失われます。

例 : enable name_list local

```
Use of local NetBIOS name list is   ENABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

name-list remote

リモート名前リストの使用を使用可能にします。DLSw パートナーから受信されたすべての NetBIOS 名前リストが使用されます。

構成プロンプトからの場合、リモート名前リストの使用を永続的に使用可能にします。 変更が有効になるのは、ルーターが再始動されるか、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。

監視プロンプトからの場合は、リモート名前リストの使用を一時的に使用可能にします。変更が有効になるのは、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。ルーターを再始動すると、変更は失われます。

例 : enable name_list remote

```
Use of remote NetBIOS name list is   ENABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET NAME-LIST'.
```

route-caching

ブリッジングおよび DLSw に関してルート・キャッシュを使用可能にします。ルート・キャッシュは、NetBIOS 名前キャッシュ内の項目を使用して、同報通信フレームを特定ルーティング・フレーム (SRF) に変換するプロセスです。

例 : enable route-caching

```
Route caching is                    ON
```

List (構成)

すべてのキャッシュ項目を表示するか、項目のタイプ別にキャッシュ項目を表示します。フィルター構成情報または一般構成情報を表示します。ローカル NetBIOS 名前リスト項目を表示します。

構文 :

list

cache all

cache entry-number

cache name

cache ip-address

filters all

filters bridge

filters dlsw

general

name-list all

name-list *entry-number*

cache all

ルーターの名前キャッシュ内のすべての永続項目を表示します。静的項目や動的項目は表示しません。

例: list cache all

```
Entry  Name                IP Address
-----  ------------------  ---------------

    1  ACCOUNTING     <00>  20.2.1.3
    2  NOTES          <00>  20.2.3.4
```

cache entry-number *record#*

キャッシュ項目をその項目番号に応じて表示します。 項目番号のリストを表示するには、**list cache all** を入力します。

例 : list cache entry-number

```
Enter name cache record number [1]? 1

Entry  Name                IP Address
-----  ------------------  ---------------
    1  ACCOUNTING     <00>  20.2.1.3
```

cache name *name*

特定の NetBIOS 名に関するキャッシュ項目を表示します。次に挙げるワイルドカードを使用して探索を単純化することができます。

***** (アスタリスク) では、0 回または 1 回以上現れる任意の文字を表します。例えば、San* は次のいずれにも該当します。

- San Francisco
- Santa Fe
- San Juan

? (疑問符) では、任意の 1 文字を表します。

$ (ドル記号) が有効なのは、NetBIOS 名の有効文字数が 16 でない場合、および探索引き数がアスタリスク (*) で始まっていない場合だけです。

ワイルドカードは、NetBIOS 名内の最大文字数 (構成に応じて 15文字または 16 文字) 以下であれば、いくつでも好きなだけ使用することができます。

注: NetBIOS 名は大文字と小文字を区別します。

例 : list cache name

```
Enter up to 15 characters of NetBIOS name (wild cards ok) []? Acc*

Entry  Name                IP Address
-----  ------------------  ---------------
    1  Accounting     <00>  20.2.1.3
```

cache ip-address

特定の IP アドレスをもつ項目をすべて表示することができます。

例 : list cache ip-address

```
Enter IP Address [0.0.0.0]? 20.2.1.3

Entry  Name                IP Address
-----  ------------------  ---------------
    1  Accounting     <00>  20.2.1.3
```

filters all

ブリッジングおよび DLSw の両方に関して、フレーム・タイプ・フィルター

がオンまたはオフであるかないかを表示します。これらのフィルターをオンまたはオフにするには、**set filters bridge** コマンドを使用します。

例 : list filters all

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF

DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON
```

filters bridge

ブリッジングに関して、フレーム・タイプ・フィルターがオンまたはオフであるかないかを表示します。これらのフィルターをオンまたはオフにするには、**set filters bridge** を使用します。

例 : list filters bridge

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF
```

filters dlsw

ブリッジングに関して、フレーム・タイプ・フィルターがオンまたはオフであるかないかを表示します。これらのフィルターをオンまたはオフにするには、**set filters dlsw** を使用します。

例:

```
list filters dlsw
DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON
```

general

現行の NetBIOS キャッシュおよびフィルター構成を表示します。

例:

```
list general
Bridge-only Information:

Bridge duplicate filtering is          OFF
Bridge duplicate frame filter t/o      1.5 seconds

DLS-only Information:
DLS command frame retry count            5
DLS max remote name cache entries      100
DLS command frame retry timeout        0.5 seconds
DLS type of local name list  NON-EXCLUSIVE
DLS use of local name list is     DISABLED
DLS use of remote name list is     ENABLED
```

name-list all

永続的に構成されたすべてのローカル NetBIOS 名前リスト項目を表示します。静的項目は表示しません。

例:

```
list name-list all
Entry  Name Qualifier    Type
-----  ----------------  ----------
  1    NY_SERV*          INDIVIDUAL
  2    NY_DOMAIN*             GROUP
```

name-list *entry-number*

永続的に構成された特定のローカル NetBIOS 名前リスト項目を表示します。

例:

```
list name-list entry-number
Enter name list record number [1]? 1

Entry  Name Qualifier    Type
-----  ----------------  ----------
  1    NY_SERV*          INDIVIDUAL
```

List (監視)

さまざまなタイプのキャッシュ項目、フィルター構成、一般構成情報、NetBIOS 名前リスト、またはその他の事柄に関する統計を表示します。

構文 :

list

cache active
cache config
cache group
cache local
cache name
cache remote
cache unknown
filters all
filters bridge
filters dlsw
general
name-list all
name-list config
name-list local
name-list remote
statistics cache
statistics frames bridge
statistics frames dlsw
statistics general bridge
statistics general dlsw

cache active

ルーターの名前キャッシュ内のすべての活動項目を表示します。

かぎ括弧内の数は NetBIOS 名の 16 番目の文字です。この文字は、キャッシュ項目を作成する場合に、16 進数で入力できるもので、特殊な目的で NetBIOS アプリケーションによって使用されます。

「Name Type」フィールドに LOCAL の指定がない場合は、リモート項目です。

例 : `list cache active`

```
Cnt  NetBIOS Name         Name Type          Entry Type
---  -------------------  -----------------  ----------
  1  HYPERION       <01>  INDIVIDUAL LOCAL   DYNAMIC
  2  LANGROUP       <00>  UNKNOWN            STATIC
  3  ACCOUNTING     <00>  GROUP              PERMANENT
```

cache config

静的および永続名前キャッシュ項目をすべて表示します。動的項目は表示しません。

かぎ括弧内の数は NetBIOS 名の 16 番目の文字です。この文字は、キャッシュ項目を作成する場合に、16 進数で入力できるもので、特殊な目的で NetBIOS アプリケーションによって使用されます。

例 : list cache config

```
Name                IP Address      Source     Last Mod
------------------  --------------  ---------  ---------
Admin         <00>  20.3.120.8      STATIC     ADDED
Finance       <01>  20.4.96.8       PERMANENT  MODIFIED
Notes         <00>  20.8.210.3      PERMANENT  UNCHANGED
```

cache group

NetBIOS グループ名に関して存在しているキャッシュ項目を表示します。

例 : list cache group

```
Cnt  NetBIOS Name         Entry Type  Loc Path State  Rem Path State
---  -------------------  ----------  --------------  --------------
  2  HYPERION       <01>  DYNAMIC     UNKNOWN         GROUP
  3  EXCEL          <00>  DYNAMIC     GROUP           GROUP
```

cache local

ローカル・キャッシュ項目を表示します。ローカル・キャッシュ項目とは、ルーターがローカル・ブリッジ・ネットワークを介して学習するキャッシュ項目のことです。

NetBIOS クライアントの場合は、「Local Path State」は常に UNKNOWN であり、「MAC Address」フィールドおよび「Routing Information」フィールドは常に空です。

例 : list cache local

```
Cnt  NetBIOS Name     Loc Path State  MAC Address  Routing Information
---  ---------------  --------------  -----------  -------------------
  2  HYPERION   <01>  UNKNOWN
```

Cnt キャッシュ項目の番号

NetBIOS Name
項目の NetBIOS 名

Loc Path State
ローカル・パス状態

MAC Address
項目がサーバーの場合は、そのサーバーの MAC アドレスを表示します。

Routing Information
標準 RIF 情報を表示します。

cache name *name*

特定の NetBIOS 名に関するキャッシュ項目を表示します。 次に挙げるワイルドカードを使用して探索を単純化することができます。

***** (アスタリスク) では、0 回または 1 回以上現れる任意の文字を表します。例えば、San* は次のいずれにも該当します。

- San Francisco
- Santa Fe
- San Juan

? (疑問符) では、任意の 1 文字を表します。

$ (ドル記号) が有効なのは、NetBIOS 名の有効文字数が 16 でない場合、および探索引き数がアスタリスク (*) で始まっていない場合だけです

ワイルドカードは、NetBIOS 名内の最大文字数 (構成に応じて 15文字または 16 文字) 以下であれば、いくつでも好きなだけ使用することができます。

注: NetBIOS 名は大文字と小文字を区別します。

例 : list cache name

```
     NetBIOS Name         Name Type          Entry Type
     -------------------  -----------------  ----------
     HYPERION       <01>  INDIVIDUAL REMOTE  DYNAMIC

Count of name cache entry hits ............................. 20

Age of name cache entry ..................................... 689
Age of name cache last reference ............................ 85

Local path information:

  Loc Path State  Timestamp  MAC Address    LFS   Routing Information
  --------------  ---------  ------------  -----  -------------------
  UNKNOWN         689

Remote path information:

  Rem Path State  Timestamp   LFS   IP Address(es)
  --------------  ---------  -----  --------------
  BEST FOUND      85         2052   20.3.120.8
```

cache remote

ルーターが DLSw WAN 上で学習するキャッシュ項目を表示します。

例 : list cache remote

```
Cnt  NetBIOS Name         Entry Type  Rem Path State  IP Address(es)
---  -------------------  ----------  --------------  --------------
  2  HYPERION       <01>  STATIC      BEST FOUND      20.3.120.8
  3  EXCEL          <00>  DYNAMIC     SEARCH ALL
```

Cnt キャッシュ項目の番号

NetBIOS Name
項目の NetBIOS 名

Rem Path State
リモート・パス状態。 考えられる状態は、次のものです。

Best Found
ルーターがこのステーションへの最適ルートを見つけました。

Unknown
ルーターはこのステーションへの最適ルートをまだ見つけていません。

Group ルーターはグループ名に関して最適ルートを探索しません。

Search Limited
ルーターはこの NetBIOS 名に関して限定探索を行っています。 限定探索の詳細については、**set cache-parms** コマンドを参照してください。

Search All
ルーターは全探索を行っています。**set cache-parms** コマンドの限定探索タイマーが満了すると、ルーターは全探索を行います。

IP Address(es)
最適パスが見つかった場合は、NetBIOS ステーションに到達することができる近隣 DLSw に関連する IP アドレス (複数の場合もある) が表示されます。

cache unknown
NetBIOS 名のタイプが不明のキャッシュ項目を表示します。ルーターは、名前のタイプを学習するまで、動的項目すべてを UNKNOWN として入力します。学習後に項目をローカル、リモート、またはグループとしてマーク付けします。

例 : `list cache unknown`

```
Cnt  NetBIOS Name         Entry Type  Loc Path State  Rem Path State
---  ---------------  --------------  --------------  --------------
  2  HYPERION   <01>  STATIC          UNKNOWN          UNKNOWN
  3  EXCEL      <00>  STATIC          UNKNOWN          UNKNOWN
```

filters all

ブリッジングと DLSw の両方に関して、フレーム・タイプ・フィルターがオンまたはオフであるかないかを表示します。

これらのフィルターをオンまたはオフにするには、**set filters bridge** コマンドおよび **set filters dlsw** コマンドを使用します。

例 : `list filters all`

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF

DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON
```

filters bridge
ブリッジングに関して、フレーム・タイプ・フィルターがオンまたはオフであるかないかを表示します。これらのフィルターをオンまたはオフにするには、**set filters bridge** コマンドを使用します。

例 : `list filters bridge`

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF
```

filters dlsw
DLSw に関して、フレーム・タイプ・フィルターがオンまたはオフであるかないかを表示します。これらのフィルターをオンまたはオフにするには、**set filters dlsw** コマンドを使用します。

例 : list filters dlsw

```
DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON
```

general

現行の NetBIOS キャッシュおよびフィルター構成を表示します。

例 : list general

```
Bridge-only Information:

Bridge duplicate filtering is          OFF
Bridge duplicate frame filter t/o      1.5 seconds

DLS-only Information:


DLS command frame retry count            5
DLS max remote name cache entries      100
DLS command frame retry timeout        0.5 seconds
DLS type of local name list  NON-EXCLUSIVE
DLS use of local name list is     DISABLED
DLS use of remote name list is     ENABLED

DLS-Bridge Common Information:

Route caching is                       OFF
Significant characters in name          15
Max local name cache entries           500
Duplicate frame detect timeout         5.0 seconds
Best path aging timeout               60.0 seconds
Reduced search timeout                 1.5 seconds
Unreferenced entry timeout            5000 minutes
```

name-list all

現在アクティブなすべての NetBIOS 名前リストをローカルおよびリモートの両方について表示します。ローカル名前リスト項目がコミットされていないか、ローカル名前リストの使用が使用不能にされている場合、ローカル名前リスト項目はリストに表示されません。リモート名前リストが使用不能にされている場合、リモート名前リスト項目はリストに表示されません。

例 : list name-list all

```
Name Qualifier    Type        IP Address
----------------  ----------  ---------------
LA_DOMAIN*             GROUP  20.2.1.3
LA_SERV*          INDIVIDUAL  20.2.1.3
NY_DOMAIN*             GROUP  Local
NY_SERV*          INDIVIDUAL  Local
SF_DOMAIN*             GROUP  20.2.3.4
SF_SERV*          INDIVIDUAL  20.2.3.4
TEMP_DOMAIN            GROUP  Local
TEMP_SERV01       INDIVIDUAL  Local
```

name-list config

永続的および一時的に構成されたすべてのローカル NetBIOS 名前リスト項目を表示します。

送信元フィールドは次の値のいずれかをもつことができます。

PERMANENT
永続的に構成された項目

STATIC
一時的に構成された項目

LastMod フィールドは次の値のいずれかをもつことができます。

ADDED
ローカル名前リスト項目が追加されましたが、変更がコミットされていません。

DELETED
ローカル名前リスト項目が削除されましたが、変更がコミットされていません。

UNCHANGED
ローカル名前リスト項目が追加され、変更がコミットされました。

例 : list name-list config

```
Entry  Name Qualifier    Type        Source     LastMod
-----  ----------------  ----------  ---------  ---------
  1    NY_SERV*          INDIVIDUAL  PERMANENT  UNCHANGED
  2    NY_DOMAIN*             GROUP  PERMANENT  UNCHANGED
  3    TEMP_SERV01       INDIVIDUAL  STATIC     ADDED
  4    TEMP_DOMAIN            GROUP  STATIC     ADDED
```

name-list local

現在アクティブなすべてのローカル NetBIOS 名前リスト項目を表示します。ローカル名前リスト項目がコミットされていないか、ローカル名前リストの使用が使用不能にされている場合は、ローカル名前リスト項目はリストに表示されません。

例 : list name-list local

```
LOCAL Name List
Type of Name List (active) .......     EXCLUSIVE
Type of Name List (pending) ...... NON-EXCLUSIVE

Name Qualifier    Type
----------------  ----------
NY_DOMAIN*             GROUP
NY_SERV*          INDIVIDUAL
TEMP_DOMAIN            GROUP
TEMP_SERV01       INDIVIDUAL
```

name-list remote

現在アクティブなすべてのリモート NetBIOS 名前リスト項目を特定の DLSw パートナーについて表示します。リモート名前リストの使用が使用不能にされている場合、項目は表示されません。

例 : list name-list remote

```
Enter IP Address [0.0.0.0]? 20.2.1.3

Partner IP Address ........... 20.2.1.3

Type of Name List .............     EXCLUSIVE
    Use of remote name lists ..... ENABLED

Name Qualifier    Type
----------------  ----------
LA_DOMAIN*             GROUP
LA_SERV*          INDIVIDUAL
```

statistics cache

次の名前キャッシュ統計をリストします。

例 : list statistics cache

```
Local name cache entries                1
Remote name cache entries               1
Local individual names                  1
Remote individual names                 0
Group names                             0
Unknown names                           1
Name cache hits                      2194
Name cache misses                       2
```

statistics frames bridge

ブリッジングに関する次の名前キャッシュ統計をリストします。

例 : list statistics frames bridge

```
Frames in cache                         0
Name query frames                       0
Status query frames                     0
Add name frames                         0
Add group name frames                   0
Name in conflict frames                 0
Frames not filtered as duplicates       0
```

statistics frames dlsw

DLSw に関する次の名前キャッシュ統計をリストします。

例 : list statistics frames dlsw

```
Name query frames                       0
Status query frames                     0
Add name frames                         0
Add group name frames                   0
Name in conflict frames                 0
Frames not filtered as duplicates       0
```

statistics general bridge

ブリッジングに関するフレーム・カウントを表示します。

例 : list statistics general bridge

```
Frames received                      1339
Frames discarded                        0
Frames forwarded to bridge           1339
Frames forwarded to DLS              1339
```

statistics general dlsw

DLSw に関するフレーム・カウントを表示します。

例 : list statistics general dlsw

```
Frames received                      1339
Frames discarded                        0
Frames forwarded to bridge           1339
```

Set

名前キャッシュ・パラメーターを設定し、ブリッジングまたは DLSw のいずれかに関してフレーム・タイプ・フィルターをオンまたはオフにし、重複フレーム・フィルター・タイマーおよびフレーム再試行タイマーを調整し、NetBIOS 名前リスト・パラメーターを設定します。 また、NetBIOS の名前およびバイト・フィルター・プロンプトも表示します。

構文 :

set cache-parms
filters bridge
filters byte
filters dlsw
filters name
general
name-list

cache-parms

ブリッジングまたは交換に適用される名前キャッシュ・パラメーターを設定します。

例 : set cache-parms

```
   Significant characters in name [15]?
   Best path aging timeout value in seconds [60.0]?
   Reduced search timeout value in seconds [1.5]?
   Unreferenced entry timeout value in minutes [5000]?
   Max nbr local name cache entries [500]?
   Max nbr remote name cache entries [100]?

Cache parameters set
```

Significant characters in name

ルーターが NetBIOS 名を調べる際に 15 文字と 16 文字のどちらを考慮するかを決めます。 15 を入力した場合は、ルーターは 16 番目の文字を無視します。 16 を選択した場合は、ルーターは、キャッシュ項目を調べる際に、 16 番目の文字を含めます。

省略時値は 15 です。

Best path aging timeout

ルーターがある名前キャッシュ項目のアドレスおよびルートをそのステーションへの最適パスであるとみなす時間。 このタイマーが満了すると、ルーターはその名前キャッシュ項目を削除し、 NetBIOS 名に関して新しい最適パスを見つける試みを行います。

最適パスの判別にあたっては、ルーターは、最大フレーム・サイズだけでなく、ノードを接続する可能性のあるすべてのルートでのノード間伝送時間についても考慮します。 パスを通って伝送される可能性のある最大 NetBIOS フレームに対処できないパスについては、ルーターはそのパスを適切とはみなしません。

省略時値は 60 秒です。 範囲は 1.0 秒から 100000.0 秒までです。

Reduced search timeout

ルーターは、タイムアウト期間中に名前照会、状況照会、またはデータグラムを受信すると、現行 NetBIOS 名前キャッシュ情報に基づいて、探索を実行します。

このタイマーの満了後にルーターが重複フレームを受信した場合は、ルーターは、前のルートは無効になっているものと想定し、探索を拡大します。ルーターは、その重複フレームをブリッジと DLS の両方に転送します。 DLS は、可能性のあるすべての DLS パートナーに対して、対応する SSP メッセージの同報通信を行います。

省略時値は 1.5 秒です。 範囲は 1.0 秒から 100.0 秒までです。

Unreferenced entry timeout

参照されていない名前については、ルーターは、それを削除する前にこの時間だけそのキャッシュ内に保持します。 ただし、キャッシュがいっぱいになった場合は、ルーターはそれ以前でも項目を除去します。

省略時値は 5000 分です。 範囲は 1 ～ 100000 です。

Max nbr local name cache entries

ルーターが名前キャッシュに保管するローカル学習した項目の最大数。

省略時値は 500 です。範囲は 100 ～ 30000 です。この値を小さくすると、ルーター・メモリーを節約することができます。メモリー使用率、プロセッサー使用率、および同報通信トラフィックの量を

最適化するには、ローカル名前キャッシュ項目の数を、このルーターのローカル・ブリッジ・ネットワークでアクティブな NetBIOS ステーション (サーバーおよびクライアント) の合計数にできるだけ近く設定してください。

Max nbr remote name cache entries

ルーターが名前キャッシュに保管するリモート学習した項目、グループ名項目、および不明項目の最大数。

省略時値は 100 です。範囲は 100 ～ 30000 です。この値を小さくすると、ルーター・メモリーを節約することができます。メモリー使用率、プロセッサー使用率、および同報通信トラフィックの量を最適化するには、リモート名前キャッシュ項目の数を、このルーターのローカル・ブリッジ・ネットワーク上で NetBIOS クライアントによってアクセスされるリモート NetBIOS サーバーの数に約 25 % を加えた数に設定してください。

filters bridge

ブリッジングに関するフレーム・タイプ・フィルターをオンまたはオフにします。

例 : set filters bridge

```
Filter Name Conflict frames? [No]: y
Name conflict filtering is              ON
Filter General Broadcast frames? [No]:
General broadcast filtering is          OFF
Filter Trace Control frames? [No]:
Trace control filtering is              OFF
```

filters byte

NetBIOS config> プロンプトからの場合は、NetBIOS フィルター構成プロンプト (NetBIOS Filter config>) を表示します。NetBIOS フィルターの構成については、195ページの『第9章 NetBIOS フィルターの構成と監視』で説明します。

NetBIOS > 監視プロンプトからの場合は、NetBIOS フィルター監視プロンプト (NetBIOS Filter>) を表示します。NetBIOS フィルターの監視については、205ページの『NetBIOS フィルターの監視』で説明します。

このパラメーターを使用すると、NetBIOS バイト・フィルターにアクセスすることができます。

例 : set filters byte

```
NetBIOS Filtering configuration
NetBIOS Filter config>
```

filters dlsw

DLSw トラフィックに関してフレーム・タイプ・フィルターを設定します。

例 : set filters dlsw

```
Filter Name Conflict frames? [Yes]:
Name conflict filtering is              ON
Filter General Broadcast frames? [Yes]:
General broadcast filtering is          ON
Filter Trace Control frames? [Yes]:
Trace control filtering is              ON
```

filters name

NetBIOS config> プロンプトからの場合は、NetBIOS フィルター構成プロン

プト (NetBIOS Filter config>) を表示します。NetBIOS フィルターの構成については、195ページの『第9章 NetBIOS フィルターの構成と監視』で説明します。

NetBIOS > 監視プロンプトからの場合は、NetBIOS フィルター監視プロンプト (NetBIOS Filter>) を表示します。NetBIOS フィルターの監視については、205ページの『NetBIOS フィルターの監視』で説明します。

このパラメーターを使用すると、NetBIOS 名前フィルターにアクセスすることができます。

例 : set filters name

```
NetBIOS Filtering configuration
NetBIOS Filter config>
```

general

重複フレーム・タイムアウト、重複フレーム検出タイムアウト、およびコマンド・フレーム再試行カウントおよびタイムアウトを設定します。重複フレームの動作の詳細については、153ページの『重複フレーム・フィルター』を参照してください。

例 : set general

```
ATTENTION! Setting Duplicate Frame Filter Timeout to zero...
disables duplicate frame checking!
Duplicate frame filter timeout value in seconds [1.5]?
Duplicate frame detect timeout value in seconds [5.0]?
General parameters set
```

DLSw が使用可能にされている場合は、ソフトウェアがプロンプトを出して次の入力も指示します。

```
Command frame retry count [5]?
Command frame retry timeout value in seconds
[0.5]?
```

Duplicate frame filter timeout

重複フィルターが使用可能にされている場合に、ブリッジされたトラフィックにのみ適用されます。このタイムアウト期間中、ルーターは受信する重複フレームをすべてフィルターします。

範囲は 0.0 秒から 100.0 秒までです。ゼロは重複フレーム検査を使用不能にします。省略時値は 1.5 秒です。

Duplicate frame-detect timeout

ブリッジされたトラフィックと DLSw トラフィックの両方に適用されます。ルーターがその重複フレーム・フィルター・データベースに項目を保管する時間。このタイマーが満了すると、ルーターは受信する新しいフレームに関する新しい項目を作成します。

範囲は 0.0 秒から 100.0 秒までです。省略時値は 5 秒です。

Command frame retry count

DLSw トラフィックにのみ適用されます。

着信先 DLSw ルーターがそのローカル接続 LAN に送信する重複 NetBIOS UI フレームの数。これらのフレームは、コマンド・フレーム再試行タイムアウトで指定された間隔で送信されます。

範囲は 0 から 10 までです。省略時値は 5 です。

Command frame retry timeout

DLSw トラフィックにのみ適用されます。近隣 DLSw ルーターがそのローカル・ブリッジ・ネットワークへの重複 NetBIOS UI フレームの送信を再試行する間隔です。

範囲は 0.0 秒から 10.0 秒までです。省略時値は 0.5 秒です。

name-list

ローカル NetBIOS 名前リストに関連するパラメーターを設定します。現在、ローカル NetBIOS 名前リストに関連するパラメーターは local NetBIOS name list exclusivity だけです。

構成プロンプトからの場合、ローカル NetBIOS 名前リスト・パラメーターを永続的に設定します。変更が有効になるのは、ルーターが再始動されるか、変更が監視プロンプトから **set name-list** コマンドを使用してコミットされてからです。

監視プロンプトからの場合は、このコマンドはローカル NetBIOS 名前リスト・パラメーターを一時的に設定します。このコマンドは、構成プロンプトまたは監視プロンプトから行われたどの NetBIOS 名前リストの変更もコミットします。

Test (監視のみ)

実際の NetBIOS 名を現行の NetBIOS キャッシュまたは NetBIOS 名前リストと突き合わせてテストすることができます。

構文 :

test cache

name-list

test cache

所定の NetBIOS あて先名をもつ DLSw フレームが転送される先の DLSw パートナーのリスト、およびフレームがどのように転送されるかを表示します。

例 (対応する NetBIOS キャッシュ項目はありません): test cache ABC

```
Destination NetBIOS name being tested .... ABC           <20>

Name cache entry NOT found.

How frame destined for this NetBIOS name is forwarded to DLSw partners .....
  Send to all partners.
```

例 (対応する NetBIOS キャッシュ項目): test cache LA_SERV01

```
Destination NetBIOS name being tested .... LA_SERV01     <00>

Name cache entry found:
  Name type = INDIVIDUAL REMOTE;   Entry type = DYNAMIC

How frame destined for this NetBIOS name is forwarded to DLSw partners .....
  Send to all name list learned and dynamically learned partners.

List of DLSw partners to which frame destined for this name is forwarded .....

  Send via TCP           to 20.2.1.3 ( Name list, Learned )
```

test name-list

所定の NetBIOS 名に一致する NetBIOS 名前リスト項目 (ローカルまたはリモート) のリストを表示します。

例 : test name-list

```
Enter up to 15 characters of NetBIOS name (no wild cards).
  Enter NetBIOS name []? LA_SERV01
Enter last character of NetBIOS name in hex [0]?

Name Qualifier    Type        IP Address
---------------  ----------  ---------------
LA_SERV*          INDIVIDUAL  20.2.1.3
```

第9章 NetBIOS フィルターの構成と監視

この章では、NetBIOS フィルター構成コマンドについて説明します。これらのコマンドでは、NetBIOS フィルターを ASRT ブリッジの追加フィーチャーとして構成できます。構成コマンドは、NetBIOS config> プロンプトからアクセスできます。

この章には次の節が含まれます。

- 『ASRT および DLSW 構成環境へのアクセス』
- 『NetBIOS フィルター構成コマンド』

ASRT および DLSW 構成環境へのアクセス

ASRT 環境から NetBIOS フィルター・プロンプトを表示するには、次の例に示すようにコマンドを入力します。

```
Config> protocol asrt
Adaptive Source Routing Transparent Bridge user configuration

ASRT config> netbios
NetBIOS Support User Configuration

NetBIOS config> set filters name or byte
NetBIOS filtering configuration

NetBIOS filter config>
```

NetBIOS config> プロンプトを DLSw 構成環境から表示する場合は、次のようにします。

```
Config> protocol dls
DLSw protocol user configuration

DLSw config> netbios
NetBIOS Support User Configuration

NetBIOS config> set filters name or byte
NetBIOS filtering configuration

NetBIOS filter config>
```

表13 は NetBIOS フィルター構成コマンドを示しています。

NetBIOS フィルター構成コマンド

表 13. NetBIOS フィルター構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Create	NetBIOS フィルター用のバイト・フィルターおよびホスト名フィルターのリストを作成します。
Delete	NetBIOS フィルター用のバイト・フィルターおよびホスト名フィルターのリストを削除します。
Disable	ブリッジング・ルーター上での NetBIOS フィルターを使用不能にします。
Enable	ブリッジング・ルーター上での NetBIOS フィルターを使用可能にします。

表 13. NetBIOS フィルター構成コマンド (続き)

コマンド	機能
Filter-on	作成されたフィルターを特定のポートに割り当てます。これは、フィルター・リストを、所定のポートで入力**または**出力されるすべての NetBIOS パケットに適用する必要があることを示しています。
List	作成されたフィルターに関するすべての情報を表示します。
Update	ホスト名フィルター・リストまたはバイト・フィルター・リストに対して情報を追加または削除します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Create

create コマンドは、バイト・フィルター・リストまたはホスト名フィルター・リストを作成するのに使用します。

構文 :

create byte-filter-list *filter-list*

name-filter-list *filter-list*

byte-filter-list *filter-list*

NetBIOS フィルター用にバイト・フィルター・リスト名を作成します。作成されるリストを識別するのに、最大 16 文字まで使用することができます。*Filter-list* は、以前 **create byte-filter-list** コマンドまたは **create name-filter-list** コマンドで使用したことのない固有の名前であることが必要です。

例: `create byte-filter-list newyork`

name-filter-list *filter-list*

NetBIOS フィルター用にホスト名フィルター・リスト名を作成します。作成される名前フィルター・リストを識別するのに、最大 16 文字まで使用することができます。 *Filter-list* は、以前 **create byte-filter-list** コマンドまたは **create name-filter-list** コマンドで使用したことのない固有の名前であることが必要です。

例: `create name-filter-list atlanta`

Delete

バイト・フィルター・リスト、ホスト名フィルター・リスト、および**filter-on input** コマンドまたは **filter-on output** コマンドを使用して作成されたフィルターを削除するには、**delete** コマンドを使用してください。このコマンドは、バイト・フィルター・リストおよびホスト名フィルター・リストに関連するすべての情報を除去します。また、このコマンドは、ユーザー定義のストリングを新しいフィルター・リスト用の名前として解放もします。

構文 :

delete byte-filter-list *filter-list*

name-filter-list *filter-list*

filter input *port#*

filter output *port#*

byte-filter-list *filter-list*

NetBIOS フィルター用に作成されたバイト・フィルター・リストを削除します。*filter-list*は、削除されるバイト・フィルター・リストを識別するために使用されるユーザー定義のストリングです。

例: delete byte-filter-list newyork

name-filter-list *filter-list*

NetBIOS フィルター用に作成されたホスト名フィルター・リストを削除します。*filter-list*は、削除される名前フィルター・リストを識別するために使用されるユーザー定義のストリングです。

例: delete name-filter-list atlanta

filter input *port#*

filter-on input 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。このコマンドはフィルターに関連するすべての情報を除去し、結果的にフィルター番号に生じたギャップがあれば、それをすべて埋めます。

例: delete filter input 2

filter output *port#*

filter-on output 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。このコマンドはフィルターに関連するすべての情報を除去し、結果的にフィルター番号に生じたギャップがあれば、それをすべて埋めます。

例: delete filter output 2

Disable

disable コマンドは、ルーター上で NetBIOS 名前フィルターおよびバイト・フィルターをグローバルに使用不能にするのに使用します。

構文 :

disable netbios-filtering

例: disable netbios-filtering

Enable

ルーター上で NetBIOS 名前フィルターおよびバイト・フィルターをグローバルに使用可能にする場合は、**enable** コマンドを使用します。

構文 :

enable netbios-filtering

例: enable netbios-filtering

Filter-on

このコマンドは、以前に構成された 1 つまたは複数のフィルター・リストを特定のポートの入力または出力に割り当てます。

構文 :

filter-on input *port# filter-list <operator filter-list . . . >*

output *port# filter-list <operator filter-list . . . >*

input *port# filter-list <operator filter-list . . . >*

このコマンドでは、特定のポート上で着信パケットに 1 つまたは複数のフィルター・リストを割り当てます。その結果得られるフィルターは、指定されたポートのすべての NetBIOS パケットの入力に適用されます。

port# は、ルーター上で構成されたブリッジ・ポート番号です。そのポート番号がこのフィルターを識別します。ポート番号のリスト見る場合は、**list** を入力します。filter-list は、**create** コマンドを介して以前に入力されたストリングです。このポートに追加のフィルター・リストを追加する場合は、すべて大文字で AND または OR を入力し、その後に続けてフィルター・リスト名を入力します。

注: 複数の演算子を使用して複合フィルターを作成することができます。複数の演算子を入力する場合は、すべてを同一のコマンド行に同時に入力する必要があります。

このコマンドによって作成されたフィルターは、指定されたポート上のすべての着信 NetBIOS パケットに適用されます。コマンド行の各フィルター・リストは、演算子があればそれも一緒に、左から右へと評価されます。フィルター・リストの組み込み評価は、True (真) の条件に相当し、排除評価は False (偽) の条件に相当します。フィルター・リストの評価の結果が真である場合は、パケットがブリッジされます。そうでない場合は、パケットがフィルターされます (除去されます)。

パケットが NetBIOS フィルターによってサポートされるタイプの 1 つでない場合には、このフィルターについてのすべてのホスト名フィルター・リストが 『Inclusive (組み込み)』 (True (真)) となります。指定したポート番号について入力フィルターがすでに存在する場合は、エラー・メッセージが表示されます。

例: `filter-on input 2 newyork AND boston`

output *port# filter-list <operator filter-list . . . >*

このコマンドでは、ポート上で発信パケットに 1 つまたは複数のフィルターを割り当てます。このフィルターはその後、そのポート上のすべての NetBIOS パケットの出力に適用されます。

port# は、ルーター上で構成されたブリッジ・ポート番号です。そのポート番号がこのフィルターを識別します。ポート番号のリスト見る場合は、**list** を入力します。 Filter-list は、create コマンドを介して以前に入力されたストリングです。任意選択の演算子は、すべて大文字の AND または OR として入力

します。演算子がある場合は、演算子の後にフィルター・リスト名を入力する必要があります。そのポート番号を使用してこのフィルターを識別します。

注: 複数の演算子を使用できます。これにより複合フィルターが作成されます。 1 つまたは複数の演算子がある場合には、すべて同一のコマンド行に同時に入力する必要があります。

このコマンドによって作成されたフィルターは、指定したポート番号のすべての NetBIOS パケットの出力に適用されます。コマンド行の各フィルター・リストは、演算子があればそれも一緒に、左から右へと評価されます。フィルター・リストの組み込み評価は、True (真) の条件に相当し、排除評価は False (偽) の条件に相当します。フィルター・リストの評価の結果が True (真) である場合は、パケットがブリッジされます。そうでない場合は、パケットがフィルターされます (除去されます)。

パケットが NetBIOS フィルターによってサポートされるタイプの 1 つでない場合には、このフィルターについてのすべてのホスト名フィルター・リストが 『Inclusive (組み込み)』 (True (真)) となります。指定したポート番号に出力フィルターがすでに存在する場合、エラー・メッセージが表示されます。

例: filter-on output 2 newyork OR boston

List

作成されたフィルターに関するすべての情報を表示するには、**list** NetBIOS フィルター・コマンドを使用してください。

構文 :

list

例: list

```
NetBIOS Filtering: Disabled

NetBIOS Filter Lists
--------------------

Handle           Type

nlist            Name
newyork          Byte

NetBIOS Filters
---------------

Port #      Direction      Filter List Handle(s)

3           Output         nlist
```

NetBIOS Filtering:
NetBIOS フィルターが使用可能か使用不能かを表示します。

NetBIOS Filter Lists
構成済みのフィルター・リストのユーザー定義の名前 (handle) を表示します。タイプについては、『Name』 はホスト名フィルター・リストを示し、『Byte』 はバイト・フィルター・リストを示します。

NetBIOS Filters

各フィルターの割り当てられたポート番号および方向 (入力または出力) を表示します。Filter List Handles はフィルターを構成するフィルター・リストの名前を表示します。

Update

ホスト名フィルター・リストまたはバイト・フィルター・リストに情報を追加または削除するには、**update** コマンドを使用してください。filter-list は、create byte (または name) filter-list プロンプトを使用して以前に入力されたストリングです。このコマンドを実行すると、`NetBIOS Byte (または Name) filter-list Config>` プロンプトが表示されるので、指定したフィルター・リストに対する更新タスクを実行することができます。このプロンプトでは、バイト・フィルター・リストまたはホスト名フィルター・リストに対してフィルター項目の追加、削除、リスト、または移動を行うことができます。このプロンプトでは、各フィルター・リストの省略時値を組み込みまたは排除に設定することもできます。

add サブコマンドを使用すると、フィルター・リスト内にフィルター項目が作成されます。作成された最初のフィルター項目には番号 1 が割り当てられ、次のフィルター項目には番号 2 が割り当てられ、以下同様です。正常な add サブコマンドが入力された後、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。

注: フィルター・リストに追加のフィルター項目を追加すると、処理時間が (リスト内の各フィルター項目を評価するのに要する時間のため) 増加して、 NetBIOS トラフィックが多い場合にパフォーマンスに影響を及ぼす可能性があります。

特定のフィルター・リストに関してフィルター項目を指定する順序は重要です。この順序によって、パケットに対するフィルター項目の適用のされ方が決まるからです。最初に生じた一致によってフィルター項目の適用が停止し、フィルター・リストは組み込みか排除のいずれかとして評価されます (一致したフィルター項目が組み込み指定か排除指定かに応じて)。フィルター・リストのフィルター項目がどれも一致しない場合には、フィルター・リストの省略時条件 (組み込みまたは排除) が戻されます。

delete サブコマンドは、フィルター・リストから削除すべきフィルター項目の番号を指定します。delete サブコマンドを与えると、リスト内に生じた穴は埋め込まれます。例えば、フィルター項目 1、2、3、および 4 が存在していて、フィルター項目 3 が削除された場合は、フィルター項目 4 の番号が 3 に付け直されます。

default サブコマンドにより、フィルター・リストの省略時の設定値を組み込みまたは排除のいずれかに変更することができます。フィルター・リストが組み込みと評価されると、パケットはブリッジされます。そうでない場合は、パケットはフィルターされます。

フィルター・リスト内のフィルター項目の番号を付け直すには、move サブコマンドが使用できます。move サブコマンドに対する最初の引き数は、移動されるフィルター・リストの番号です。move サブコマンドに対する 2 番目の引き数は、最初のフィルター・リストをその後に移動されるフィルター・リストの番号です。

構文 :

update byte-filter-list . . .

name-filter-list . . .

byte-filter-list *filter-list*

バイト・フィルター・リストに属する情報を更新します。filter-list パラメーターは、**create byte-filter-list** コマンドを介して以前に入力されたストリングです。このコマンドにより、次の NetBIOS BYTE filter-list Config> コマンド・レベルに入ります (例を参照してください)。このレベルで、指定されたフィルター・リストに対する更新タスクを実行できます。

例: update byte-filter-list newyork

```
NetBIOS Byte newyork Config>
```

このプロンプト・レベルで、いくつかのコマンドを実行できます。使用可能な各コマンドは、後述する 『**Update Byte-Filter** コマンド・オプション』の項にリストされています。

name-filter-list *filter-list*

名前フィルター・リストに属する情報を更新します。このコマンドは、バイト・フィルター・リストではなく名前フィルター・リストを指定することを除き、byte-filter-list コマンドと同様です。filter-list パラメーターは、create name-filter-list プロンプトを使用して以前に入力されたストリングです。このコマンドにより、次の NetBIOS Name filter-list Config> コマンド・レベルに入ります (例を参照してください)。このレベルで、指定されたフィルター・リストに対する更新タスクを実行できます。

例: update name-filter-list accounting

```
NetBIOS Name accounting Config>
```

このプロンプト・レベルで、いくつかのコマンドを実行できます。使用可能な各コマンドは、後述する 『**Update Name-Filter** コマンド・オプション』の項にリストされています。

Update Byte-Filter-List (コマンド・オプション)

この項では、**update byte-filter-list** コマンド用に使用できるコマンド・オプションをリストします。

add inclusive *byte-offset hex-pattern <hex mask>*

バイト・フィルター・リストにフィルター項目を追加します。追加されたバイト・フィルター項目が NetBIOS パケットと合致した場合、それが属するフィルター・リストは組み込み (TRUE) と評価されます。

- byte-offset ではフィルターされるパケットでオフセットすべきバイトの数 (10 進数) を指定します。これはパケットの NetBIOS ヘッダーから始まります。
- hex-pattern は、NetBIOS ヘッダーの byte-offset から開始したバイト数と比較するために使用される 16 進数です。hex-pattern の構文規則には、0x が前にないこと、最大 32 の数字、および偶数個の 16 進数であることが含まれます。
- hex-mask がある場合には、これは hex-pattern と同じ長さでなければならず、byte-offset で開始するパケット内のバイトと AND (論理積) をとられ

てから結果が hex-pattern と等しいか比較されます。hex-mask 引き数が省略される場合には、その引き数はすべて 2 進数の 1 と見なされます。

バイト・フィルター項目のオフセットおよびパターンが NetBIOS パケットに存在しないバイト数を表す場合 (つまり、byte-filter list をセットアップしたときに予定されていたよりパケットが短くなる場合) には、フィルター項目はそのパケットに適用されず、パケットはフィルターされません。単一の NetBIOS フィルター・リストをセットアップするのに一連のバイト・フィルター項目が使用される場合には、NetBIOS フィルター・リスト内のバイト・フィルター項目のいずれかが NetBIOS パケット内に存在しないバイト数を表していると、パケットはフィルターについてテストされません。

例: add inclusive

```
Byte Offset  [0] ?
Hex Pattern  [] ?
Hex Mask  (<CR> for no mask)  [] ?
```

add exclusive *byte-offset hex-pattern <hex mask>*

バイト・フィルター・リストにフィルター項目を追加します。このコマンドは add inclusive 上のコマンドと同様ですが、異なる点は、フィルター項目と NetBIOS パケットの間の比較の結果、一致が生じる場合にはフィルター・リストは排除 (FALSE) に評価されることです。データグラム同報通信パケットは、バイト・オフセットを 4 に、バイト・パターンを 09 に指定してこのコマンドを使用することにより廃棄されるよう指定することができます。

- byte-offset ではフィルターされるパケットでオフセットすべきバイトの数 (10 進数) を指定します。これはパケットの NetBIOS ヘッダーから始まります。
- hex-pattern は NetBIOS ヘッダーの byte-offset オフセットで開始されるバイト数と比較される 16 進数です。hex-pattern の構文規則には、0x が前にないこと、最大 32 の数字、および偶数個の 16 進数であることが含まれます。
- hex-mask がある場合には、これは hex-pattern と同じ長さでなければならず、byte-offset で開始するパケット内のバイトと AND (論理積) をとられてから結果が hex-pattern と等しいか比較されます。hex-mask 引き数が省略される場合には、その引き数はすべて 2 進数の 1 と見なされます。

バイト・フィルター項目のオフセットおよびパターンが NetBIOS パケットに存在しないバイト数を表す場合 (つまり、byte-filter list をセットアップしたときに予定されていたよりパケットが短くなる場合) には、フィルター項目はそのパケットに適用されず、パケットはフィルターされません。単一の NetBIOS フィルター・リストをセットアップするのに一連のバイト・フィルター項目が使用される場合には、NetBIOS フィルター・リスト内のバイト・フィルター項目のいずれかが NetBIOS パケット内に存在しないバイト数を表していると、パケットはフィルターについてテストされません。

例: add exclusive

```
Byte Offset  [0] ?
Hex Pattern  [] ?
Hex Mask  (<CR> for no mask)  [] ?
```

default include

フィルター・リストの省略時の設定値を『inclusive (組み込み)』に変更します。このコマンドは、フィルター・リストのフィルター項目がフィルターに

ついて考慮されているパケットの内容に一致しない場合には、フィルター・リストが組み込みとして評価されることを示しています。これは省略時の設定値です。

default exclude
フィルター・リストの省略時の設定値を『exclusive (排除)』に変更します。このコマンドは、フィルター・リストのフィルター項目がフィルターについて考慮されるパケットの内容と一致しない場合には、フィルター・リストは排除として評価されることを示してします。

delete *filter-item*
フィルター・リストからフィルター項目を削除します。

filter-item は以前に add コマンドによって作成されたフィルター項目を表す 10 進数です。

list 指定されたフィルター・リスト内のフィルター項目に関連する情報を表示します。

```
BYTE Filter List Name:     Engineering
BYTE Filter List Default:  Exclusive
Filter Item # Inc/Ex     Byte Offset  Pattern      Mask
1             Inclusive     14        0x123456    0xFFFF00
2             Exclusive      0        0x9876      0xFFFF
3             Exclusive     28        0x1000000   0xFF00FF00
```

move *filter-item1 filter-item2*
フィルター・リスト内のフィルター項目の順序を変えます。番号が filter-item1 によって指定されているフィルター項目を filter-item2 の直後になるように移動して、番号を付け直します。

exit 終了して、前のコマンド・プロンプト・レベルになります。

Update Name-Filter-List (コマンド・オプション)

次の項では、update name-filter-list コマンドについて使用できるコマンド・オプションをリストします。

add inclusive *ASCII host-name <LAST-hex number>*
ホスト名フィルター・リストにフィルター項目を追加します。このコマンドでは、NetBIOS パケットのホスト名フィールドがこのコマンドで与えられているホスト名と比較されます。次のリストはこれらの比較がどのように行われるかを示しています。

- ADD_GROUP_NAME_QUERY: 発信元 NetBIOS 名前フィールドが検査されます
- ADD_NAME_QUERY: 発信元 NetBIOS 名前フィールドが検査されます
- DATAGRAM: あて先 NetBIOS 名前フィールドが検査されます
- NAME: あて先 NetBIOS 名前フィールドが検査されます

(このコマンドでのワイルドカード指定を考慮に入れて) 一致がある場合には、フィルター・リストは組み込みとして評価されます。そうでない場合は、フィルターのフィルター・リスト (ある場合) の次のフィルター項目がパケットに適用されます。パケットが NetBIOS 名前フィルターによってサポートされる 4 つのタイプの 1 つでない場合には、パケットはブリッジされます。

- host-name は最大 16 文字までの長さの ASCII ストリングです。単一文字のワイルドカードを示すには、ホスト名で疑問符 (?) を使用することがで

きます。ホスト名の残りの部分についてワイルドカードを示す場合、ホスト名の最終文字としてアスタリスク (*) を使用することができます。ホスト名の文字数が 15 文字未満の場合は、15 番目の文字に達するまで ASCII スペースが埋め込まれます。ホスト名は次のものを除く任意の文字を含むことができます。

. / \ [ ] : | < > + = ; , <space>

注: ホスト名は大文字と小文字を区別します。

- LAST-hex-number は、host-name が含む文字が 16 文字より少ない場合に使用することができます。これは 16 進数 (前に 0x が付いていないもの) で、最後の文字の代わりに使用すべき値を示しています。16 文字より少ないホスト名で LAST 引き数が指定されていない場合には、『?』 の ワイルドカードが 16 番目の文字の代わりに与えられます。

add inclusive HEX *hexstring*

ホスト名フィルター・リストにフィルター項目を追加します。このコマンドは、機能的には add inclusive ASCII コマンドと同じです。ただし、ホスト名の表示が異なります。このコマンドでは、ホスト名を一連の 16 進数 (0x が前にないもの) として示します。

- hexstring は偶数の 16 進数で構成しなければなりません。全部で 32 の 16 進数を提供しない場合は、ASCII ブランクが 29 番目と 30 番目の数字に埋め込まれ、ワイルドカードが 31 番目と 32 番目の数字 (16 番目のバイト) として埋め込まれます。単一バイト用のワイルドカードは、**??** で指定できます。

add exclusive ASCII *host-name <LAST-hex-number>*

ホスト名フィルター・リストにフィルター項目を追加します。このコマンドは add inclusive ASCII コマンドと同様ですが、異なる点は、このフィルター項目と突き合わせされるパケットがフィルター・リストについて排除結果を生じさせることです。

- host-name は最大 16 文字までの長さの ASCII ストリングです。単一文字のワイルドカードを示すには、ホスト名で疑問符 (?) を使用することができます。ホスト名の残りの部分についてワイルドカードを示す場合、ホスト名の最終文字としてアスタリスク (*) を使用することができます。ホスト名の文字数が 15 文字未満の場合は、15 番目の文字に達するまで ASCII スペースが埋め込まれます。ホスト名は次のものを除く任意の文字を含むことができます。

  . / \ [ ] : | < > + = ; , <space>

- LAST-hex-number は、host-name が含む文字が 16 文字より少ない場合に使用することができます。これは 16 進数 (前に 0x が付いていないもの) で、最後の文字の代わりに使用すべき値を示しています。16 文字より少ないホスト名で LAST 引き数が指定されていない場合には、**?** のワイルドカードが 16 番目の文字の代わりに与えられます。

add exclusive HEX *hexstring*

名前フィルター・リストにフィルター項目を追加します。このコマンドは、機能的には add inclusive hex コマンドと同じですが、異なる点は、このフィルター項目と突き合わせされるパケットがフィルター・リストについて排除結果を生じることです。

- hexstring は偶数の 16 進数で構成しなければなりません。全部で 32 の 16 進数を提供しない場合は、ASCII ブランクが 29 番目と 30 番目の数字に埋め込まれ、ワイルドカードが 31 番目と 32 番目の数字 (16 番目のバイト) として埋め込まれます。単一バイト用のワイルドカードは、**??** で指定できます。

default include
フィルター・リストの省略時の設定値を『inclusive (組み込み)』に変更します。このコマンドは、フィルター・リストのフィルター項目がフィルターについて考察されるパケットの内容と一致しない場合には、フィルター・リストが組み込みと評価されることを示しています。これは省略時の設定値です。

default exclude
フィルター・リストの省略時の設定値を『exclusive (排除)』に変更します。このコマンドは、フィルター・リストのフィルター項目がフィルターについて考察されるパケットの内容と一致しない場合には、フィルター・リストは排除と評価されることを示しています。

delete *filter-item*
フィルター・リストからフィルター項目を削除します。

- filter-item は以前に add コマンドによって作成されたフィルター項目を表す 10 進数です。

list 指定されたフィルター・リスト内のフィルター項目に関連する情報を表示します。

```
NAME Filter List Name: nlist
NAME Filter List Default: Exclusive

Filter Item #   Type    Inc/Ex        Hostname       Last Char

      1         ASCII   Inclusive     EROS
      2         ASCII   Inclusive     ATHENA
      3         ASCII   Exclusive     FOOBAR
```

move *filter-item1 filter-item2*
フィルター・リスト内のフィルター項目の順序を変えます。番号が filter-item1 によって指定されているフィルター項目は filter-item2 の直後になるように移動され、番号を付け直されます。

exit 終了して、前のコマンド・プロンプト・レベルになります。

NetBIOS フィルターの監視

この節では、NetBIOS フィルター監視コマンドについて説明します。これらのコマンドでは、NetBIOS フィルター情報を ASRT ブリッジングの追加フィーチャーとして監視し表示できます。監視コマンドは、NetBIOS > 監視プロンプトで入力します。

NetBIOS> 監視プロンプトで行った変更は、ブリッジングと DLSw の両方に影響します。

ASRT および DLSw NetBIOS フィルター監視環境へのアクセス

NetBIOS> 監視プロンプトを ASRT 監視環境から表示するためには、ASRT> プロンプトに **netbios** コマンドを入力してください。

NetBIOS フィルター監視コマンド (Talk 5)

```
+ protocol asrt

ASRT> netbios
NetBIOS Support User monitoring

NetBIOS monitoring> set filters name or byte

NetBIOS filter>
```

NetBIOS> 監視プロンプトを DLSw 監視環境から表示する場合は、次のようにします。

```
+ protocol dls
DLSw> netbios
NetBIOS Support User monitoring

NetBIOS Console> set filters name or byte
NetBIOS filtering

NetBIOS filter>
```

NetBIOS フィルター監視コマンド

表14 は、NetBIOS フィルター・コマンドを示しています。

表 14. NetBIOS フィルター監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
List	作成されたフィルターに関するすべての情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

List

作成されたフィルターに関するすべての情報を表示させる場合は、 **list** NetBIOS フィルター・コマンドを使用します。

構文 :

list byte-filter-lists

filters

name-filter-lists

byte-filter-lists

指定した byte-filter-list 内のフィルター項目に関連する情報を表示します。

例: `list byte-filter-lists`

```
BYTE Filter-List Name:  Engineering
BYTE Filter-List Default:  Exclusive

Filter Item # Inc/Ex     Byte Offset  Pattern      Mask

1             Inclusive     14        0x123456    0xFFFF00
2             Exclusive      0        0x9876      0xFFFF
3             Exclusive     28        0x1000000   0xFF00FF00
```

Filter Item#

フィルター項目のフィルター項目番号を指定します。フィルター・リストの Inclusive/Exclusive 状況を判別するときに、フィルター項目は数値順に評価されます。

Inc/Ex フィルター項目の省略時の状況を指定します。

Byte-offset
フィルターされるパケットのオフセットのバイト数 (10 進数) を指定します。これはパケットの NetBIOS ヘッダーから始まります。

Pattern
NetBIOS ヘッダーの byte-offset から開始したバイト数と比較するために使用される 16 進数。hex-pattern の構文規則には、0x が前にないこと、最大 32 の数字、および偶数個の 16 進数であることが含まれます。

Mask マスクがある場合には、これは hex-pattern と同じ長さでなければならず、byte-offset で開始されるパケット内のバイト数と AND (論理積) をとられてから、結果が hex_pattern と等しいか比較されます。hex-mask 引き数が省略される場合には、その引き数はすべて 2 進数の 1 と見なされます。

filters すべての構成済みフィルターに関する情報を表示します。

例: `list filters`

```
NetBIOS Filtering: Enabled

    Port #      Direction      Filter List Handle(s)   Pkts Filtered

       1          Input        valencia                      0
       2          Output       raleigh                       0
```

name-filter-lists
指定した name-filter-list 内のフィルター項目に関連する情報を表示します。

例: `list name-filter-lists`

```
NAME Filter List Name: nlist
NAME Filter List Default: Exclusive


Filter Item #   Type    Inc/Ex     Hostname   Last Char

 1              ASCII   Inclusive  EROS       <0x03>
 2              ASCII   Inclusive  ATHENA
 3              ASCII   Exclusive  FOOBAR
```

Filter Item#
フィルター項目のフィルター項目番号を指定します。フィルター・リストの Inclusive/Exclusive 状況を判別するときに、フィルター項目は数値順に評価されます。

Inc/Ex フィルター項目の省略時の状況を指定します。

Type 『ASCII』 は、ASCII 文字として追加されたホスト名フィルター項目を示します。『Hex』 は、16 進数として追加されたホスト名フィルター項目を示します。

Host-name
最大 16 文字の長さの ASCII ストリング。単一文字のワイルドカードを示すには、ホスト名で疑問符 (?) を使用することができます。ホスト名の残りの部分についてワイルドカードを示す場合、ホスト名の最終文字としてアスタリスク (*) を使用することができます。ホスト名に含まれる文字が 15 文字より少ない場合、15 番目の文字まで ASCII スペースが埋め込まれます。ホスト名は次のものを除く任意の文字を含むことができます。

. / \ [ ] : | < > + = ; , <space>

Last char

ホスト名に含まれる文字が 16 文字より少ない場合に使用されます。これは 16 進数 (前に 0x が付いていないもの) で、最後の文字の代わりに使用すべき値を示しています。16 文字より少ないホスト名で LAST 引き数が指定されていない場合には、『?』 の ワイルドカードが 16 番目の文字の代わりに与えられます。

第10章 LAN ネットワーク管理プログラム (LNM) の使用

この章では、IBM の ASRT LAN ネットワーク管理プログラム (LNM) について説明します。この章には次の節が含まれています。

- 『LNM について』
- 『LNM エージェントと機能』
- 212ページの『LNM の構成制限』

LNM について

LNM は、ソース・ルート・ブリッジによって相互接続されたトークンリング・ネットワークを管理するために使用します。リング、ブリッジ、および個別のリング・ステーションの動作を監視することができます。

ブリッジ上でソフトウェア・エージェントによって収集された情報は LNM 管理ステーションで使用可能です。さらに明確に言えば、LNM エージェントは、 LAN 報告機構 (LRM) と呼ばれる別のエージェント (IBM が所有権を主張できるプロトコル) を介して、収集された情報を転送します。情報の転送は、LAN ネットワーク管理プログラム・ステーションとの LLC2 接続を介して行われます。

LNM エージェントと機能

LNM エージェントおよびその機能には、以下に挙げるようなものがあります。

- 構成報告書サーバー (CRS) - LNM にリング・トポロジーの変更およびリング・ステーションの状況を報告します。
- リング・パラメーター・サーバー (RPS) - リング・ステーションからのリング・パラメーター情報 (リング番号、ソフト・エラー報告書タイマー値、および物理ロケーションを含む) に対する要求に対処します。
- リング・エラー・モニター (REM) - リング・ステーションからのエラー報告書を収集し分析します。しきい値を超えている場合は、REM は LNM にエラー情報を転送します。
- LAN 報告機構 (LRM) - LNM ステーションからブリッジ・エージェントへの報告リンクの確立を制御します。これらのリンクを通して他のエージェントとの間で行われる情報の転送についても管理します。

210ページの図25 は、IBM ブリッジ、LNM エージェント、および IBM LNM ステーション間の接続を示しています。

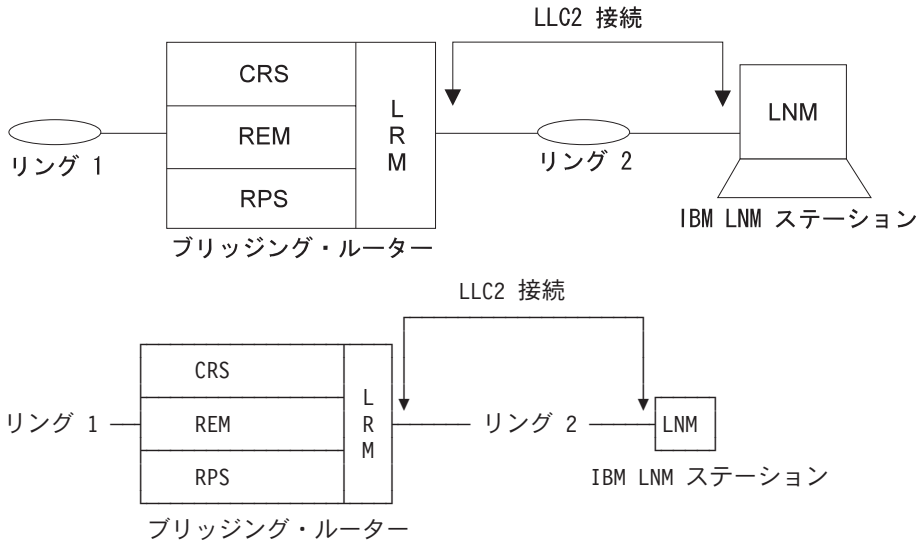


図 25. LNM ステーションおよびエージェント

以下の各項で各 LNM エージェントについて詳細に説明します。

構成報告書サーバー

LNM の要求に応じて、CRS はリング・ステーションの状況を入手し、それを LNM に転送します。また、CRS を使用して、リング・ステーション・パラメーターの設定およびリングからのステーションの除去も行うことができます。

リング・ステーションによって生成された構成情報が LNM に転送されます。LNM がリング・ステーションの状況を要求すると、CRS は MAC フレームを作成し、情報を入手するためにリング・ステーションに MAC フレームを送信します。そのときに CRS がリング・ステーションに送信するのは以下のフレームです。

- リング・ステーション・アドレス要求 MAC フレーム
- リング・ステーション状態要求 MAC フレーム
- リング・ステーション接続機構要求 MAC フレーム

リング・ステーションが応答すると、CRS は適正に形式設定された LLC2 フレームに情報を入れて、LNM に転送します。

CRS は、LNM の要求に応じて、リングからリング・ステーションを除去することもできます。リング・ステーションを除去する場合は、CRS はステーション除去 MAC フレームをリングに送信します。CRS は、また、除去が正常に行われたか行われなかったかを示す応答をも LNM に送ります。

CRS は新規活動モニター報告 MAC フレームを受信すると、LNM に情報を転送します。NAUN (次近隣活動アップストリーム) 変更報告 MAC フレームを受信すると、この情報も報告します。CRS エージェントには独自の機能アドレスがあり、リング・ステーション MAC レイヤーはこれを使用して、CRS に MAC フレームを転送することができます。

リング・パラメーター・サーバー

RPS はリングにリング・ステーションを挿入します。リング・ステーションがリングに新たに挿入されると、次のことが行われます。

- 新規リング・ステーションは、そのリングに関して初期設定要求 MAC フレームを RPS に送信します。この MAC フレームには、リング・ステーションについての情報が含まれています。
- RPS はリング・ステーション初期設定 MAC フレームによって応答しますが、これにはリング番号、およびソフト・エラー報告 MAC フレームの送信間に待機する時間の間隔が入っています。初期設定要求フレームから収集された情報は、LNM でリング上のすべてのリング・ステーションのデータベースを維持できるように、LNM に渡されます。
- RPS は、LNM からの状況に関する要求にも応答します。リング番号、RPS のバージョン情報、およびソフト・エラー報告書タイマー値が LNM に戻されます。

RPS 機能には、他のリング・ステーションから送信される MAC フレームを受信するための関連機能アドレスがあります。

重要: ステーションはリングへ入り込もうとするときに、そのリングのリング・パラメーター・サーバー (RPS) に初期化要求 MAC フレームを送信します。このフレームが RPS により正常にコピーされると、ステーションは、リング・ステーション初期化 MAC フレームを RPS から受信するものと予期します。そのようなフレームを受信しない場合、ステーションはリングに入り込めません。

ステーションは、装置が LNM 用に構成されていない場合はリングに入り込めず、リング・パラメーター・サーバーになり、リング・パラメーター初期化 MAC フレームを送信できない輻輳 (ふくそう) した状態になります。この問題を解決するには、影響を受けるポート上の RPS を使用不能にすることです。RPS が使用可能でなく、サーバーが初期化要求フレームをコピーしない場合には、送信側のステーションは、応答を予期せず、リングに入り込みます。

リング・エラー・モニター

REM は、ハード・エラーおよびソフト・エラーを検出することによって、接続されたトークンリングの動作を監視します。その上で、これらのエラーを LRM に報告し、エラーの原因の分離を援助します。ハード・エラーの検出時には次のことが行われます。

- ビーコン MAC フレームの受信によって、ハード・エラーがリング上で検出されます。
- 障害ドメイン内のステーションは、それ自体をリングから除去することによって、問題の訂正を試みます。
- REM は、ハード・エラーが訂正されたかどうかを判別してから、LNM に結果を報告します。

REM によるソフト・エラーの監視は、次のようにして行われます。

- ソフト・エラー MAC フレームがリング・ステーションによって定期的に REM に送信されて、さまざまな断続障害 (例えば、CRC エラーおよび周波数エラー) が発生する回数を REM に通知します。
- あるステーションに関するソフト・エラーの数が特定のしきい値を超えると、REM は LNM にこの条件を報告します。
- REM は、受信側輻輳 (ふくそう) 条件についてもソフト・エラー報告 MAC フレームを監視します。受信側輻輳 (ふくそう) では、リング・ステーションが受信バッファーの不足を理由にフレームを廃棄したことが示されます。
- あるステーションが受信側輻輳 (ふくそう) を報告する回数が特定のしきい値を超えた場合は、REM は LNM にこれを報告します。受信側輻輳 (ふくそう) 条件が正常に戻ると、受信側輻輳 (ふくそう) 条件が終了した旨が LNM に通知されます。

LAN 報告機構

LRM は、エージェントへの LNM の接続を制御します。LRM は、それ自体と接続されている各 LNM との間に報告リンクを確立します。*報告リンク* とは、LNM と LRM の間の LLC2 接続のことです。

LNM とエージェントの間の通信は、すべて報告リンクを経由して行われます。LRM は、該当するエージェントとの間でやりとりする管理データを報告リンクに渡します。報告リンクは最大 4 つまでサポートされます。そのうち 1 つは*制御リンク* に指定され、他の 3 つは*監視リンク* に指定されます。

制御リンクを介して接続された LNM は、使用可能な操作をすべて行うことができます。監視リンクによって接続された LNM は、使用可能な操作のうち限定された一部しか実行できません。

LNM の構成制限

IBM 2210 は、マルチポート・トークンリング構成および 2 トークンリング構成をサポートします。

LNM エージェントと LNM ステーションでは、メッセージは 2 パーティー・モデル上で渡されることを常に想定しています。ただし、LNM は、既存の構成との整合性をもつように、ブリッジ・ポートごとに使用可能にされます。

マルチポート構成では、LNM は、任意のソース・ルーティング・トークンリング・ブリッジ・ポートで使用可能にすることができます。LNM が使用可能にされる各ポートごとに、 LNM のインスタンスを作成することができます。

2 トークンリング構成では、もう一方のポートは、常に、疑似アドレスによって指定されます。これは、マルチポート・ブリッジと呼ばれます。バーチャル ・リングまたはシリアル回線インターフェースに対応することができます。

IBM 2210 ブリッジが 2 つのソース・ルーティング・トークンリング・ポートをもっている場合のみ、2 ポート・モデルのもう一方のポート・ブリッジが実アドレスをもつトークンリングです。

LNM 管理プログラムを構成するのに必要な MAC アドレスを入手するには、ASRT> プロンプトで **list lnm ports** を入力します。

LAN ブリッジ・サーバー (LBS) は、管理プログラム・ステーションによって要求されたときは、パケット転送およびパケット廃棄パフォーマンス・データ統計を報告することができます。管理プログラム・ステーションからのリモート構成更新はサポートされません。

論理リンク制御クラス 2 サポート

LAN では、データ・リンク・レイヤーは 2 つのサブレイヤーで構成されています。つまり、媒体アクセス制御 (MAC) サブレイヤーとリンク・レイヤー制御 (LLC) サブレイヤーです。LLC には次の 2 つのタイプのサービスがあります。

- LLC1 (タイプ 1) - 無応答コネクションレス・サービス
- LLC2 (タイプ 2) - 一組のコネクション型サービス

LAN ネットワーク管理プログラム (LNM) は LLC2 コネクション型サービスを必要とします。LLC2 では、次のことに関する機能が提供されます。

- 新しいデータ・リンク接続の開始
- データ・リンク接続の管理
- データの順次 (順序保証) 交換
- 確立された接続でのあるレベルのフロー制御の実行
- サービス・ユーザーからの要求時または回復不能リンク・エラー発生時のリンク接続の終結

LLC サブレイヤーは IEEE 802.5 標準に準拠しています。

第11章 LAN ネットワーク管理プログラム (LNM) の構成と監視

この章では、IBM が実施した ASRT の LAN ネットワーク管理プログラム (LNM) について説明します。この章には次の節が含まれています。

LNM の構成

この節では、ブリッジング・ルーター上での LNM フィーチャーの基本構成用の手順を要約します。

1. ネットワーク管理プログラム・ソフトウェアで必要な MAC アドレスを入手する。

   ネットワーク管理ステーションで稼働するネットワーク管理プログラム・ソフトウェアで必要とされる MAC アドレスを入手するには、ASRT> プロンプトで **list lnm ports** コマンドを入力します。例えば、次のようにします。

   ```
   ASRT> list lnm ports
   Port Number [1]? 1
   Port 1
   LNM Agents Enabled: RPS CRS REM
   Reporting Link          State          LNM Station Address
   0                       ACTIVE         10:00:5A: F1:02:37
   1                       AVAILABLE
   2                       AVAILABLE
   3                       AVAILABLE
   MAC Addresses to use when configuring LNM Manager:
   00:00:C9:08:35:47
   40:00:D9:08:35:47
   LNM not enabled on port 4
   LNM not enabled on port 5
   ```

   表示された MAC アドレス (例では太字で示されている) がネットワーク管理プログラムによって使用されて、ルーターに存在している LNM エージェントに対してそれを構成します。

   注: これらのアドレスは出力に表示されているとおり正確に入力する必要があります。そうしないと、LNM は正しく構成しません。

2. ルーター上の LNM エージェントを使用可能にする。ブリッジング・ルーターの必要なポート上の LNM エージェントを使用可能にするには、LNM config> プロンプトで **enable lnm** を入力します。例えば、次のようにします。

   ```
   LNM config>enable lnm
   Port Number [1]? 1
   ```

   省略時設定値では、LNM エージェントがすべて使用可能にされます。

3. 使用可能にされた LNM エージェントを表示することによって構成を検査する。構成済みのポートで使用可能にされている LNM エージェントを表示するには、LNM config> プロンプトで **list port** を入力します。例えば、次のようにします。

   ```
   LNM config>list port
   Port Number [1]? 1
   LNM Agents Enabled: RPS CRS REM
   ```

LNM コマンド

この節では、LNM 構成コマンドおよび監視コマンドについて説明します。これらのコマンドを使用すると、LNM に関するネットワーク・パラメーターを構成と監視することができます。

構成コマンドは LNM config> プロンプトで入力します。このプロンプトへのアクセスは、次のようにして行います。

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>lnm
LNM configuration
LNM config>
```

監視コマンドは LNM> プロンプトで入力します。このプロンプトを表示するには、次のようにします。

```
+protocol asrt
ASRT>lnm
LNM>
```

表15 に LNM コマンドをリストします。

表 15. LNM コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Disable	指定されたポート上のすべての LNM エージェント、または指定されたポート上の指定された LNM エージェント (RPS、CRS、または REM) を使用不能にします。 ブリッジにリンクされたリモート LNM アプリケーションから特定の LNM パラメーターの設定値を使用不能にします。ブリッジ内の LNM のすべてのインスタンスにグローバルに適用されます。 このコマンドは構成でのみ使用します。
Enable	指定されたポート上のすべての LNM エージェント、または指定されたポート上の指定された LNM エージェント (RPS、CRS、または REM) を使用可能にします。 ブリッジにリンクされたリモート LNM アプリケーションから特定の LNM パラメーターの設定値を使用可能にします。ブリッジ内の LNM のすべてのインスタンスにグローバルに適用されます。 このコマンドは構成でのみ使用します。
List	指定されたポートに関して使用可能にされている LNM エージェントを表示します。ブリッジに関して構成されたパスワードを表示します。 このコマンドは構成と監視の両方で使用します。
Set	指定された報告リンク番号に関するパスワードを設定します。 このコマンドは構成でのみ使用します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Disable

指定されたポート上のすべての LNM エージェント (RPS、CRS、または REM) を使用不能にするには、**disable** コマンドを使用します。

このコマンドでは、ブリッジにリンクされたリモート LNM アプリケーションからも報告リンク・パスワードの設定値を使用不能にします。

構文 :

disable *agent port#*
lnm . . .
configuration-remote-change

agent *port#*
指定されたポート上の指定された LNM エージェント (RPS、CRS、または REM) を使用不能にします。ポートが構成されていない場合は、`LNM not configured for port XX` というメッセージが表示され、コマンドは無効です。

例 : `disable REM 1`

lnm 指定されたポート上の LNM を使用不能にします。ポートが構成されていない場合は、`LNM not configured for port XX` というメッセージが表示され、コマンドは無効です。

例 : `disable lnm`

```
Port number [1]? 1
LNM not configured for Port 1
```

configuration-remote-change
ブリッジにリンクされたリモート LNM アプリケーションから報告リンク・パスワードの設定値を使用不能にします。このコマンドは、ブリッジ内の LNM のすべてのインスタンスにグローバルに適用されます。

例 : `disable configuration-remote-change`

```
CONFIGURATION-REMOTE-CHANGE: disabled
```

Enable

指定されたポート上のすべての LNM エージェントを使用可能にするか、または指定されたポート上の指定された LNM エージェント (RPS、CRS、または REM) を使用可能にします。

インターフェースがトークンリングでない場合は、`Port number XX is not token-ring` というメッセージが表示され、コマンドは無効です。

ポートが構成されていない場合は、`Port number XX does not exist` というメッセージが表示され、コマンドは無効です。

指定されたエージェントが指定されたポートですでに使用可能にされている場合は、`Already enabled` というメッセージが表示されます。

このコマンドでは、ブリッジにリンクされたリモート LNM アプリケーションからも報告リンク・パスワードの設定値を使用可能にします。

構文 :

enable *agent port#*

lnm . . .

configuration-remote-change

agent *port#*

指定されたポート上の指定された LNM エージェント (RPS、CRS、または REM) を使用可能にします。

例 : **enable CRS 1**

lnm *port#*

指定されたポート上の LNM エージェントをすべて使用可能にします。

例 : **enable lnm**

```
Port Number [1]? 1
```

configuration-remote-change

ブリッジにリンクされたリモート LNM アプリケーションから報告リンク・パスワードの設定値を使用可能にします。省略時設定値では、LNM 構成パラメーターの設定値をリモートで使用不能にします。

このコマンドは、ブリッジ内の LNM のすべてのインスタンスにグローバルに適用されます。

例: **enable configuration-remote-change**

```
CONFIGURATION-REMOTE-CHANGE: Enabled
```

List (構成コマンド)

指定されたポートに関して使用可能にされた LNM エージェントを表示し、さらにブリッジに関して構成されているパスワードも表示します。コマンドは、ASRT> プロンプトに入力します。

構文 :

list password

port . . .

password

ブリッジの報告リンクに関して構成されているパスワードを表示します。パスワードがリモート LNM アプリケーションによって変更される場合があるかどうかを表示します。

例 : **list password**

```
Reporting Link     Password
0             87654321
1             MADRAS
2             ABC1234
3             123ABC
CONFIGURATION-REMOTE-CHANGE: Disabled
```

port *port#*

指定されたポートがソース・ルーティング・ブリッジングをサポートするトークンリング・ポートである場合は、指定されたポートに関して使用可能にされた LNM エージェントを表示します。

例 : list port

```
Port Number [1]? 1
LNM Agents Enabled: RPS CRS REM
```

List (監視コマンド)

LNM 構成の状況に関する情報を表示します。コマンドは、ASRT> プロンプトに入力します。

構文 :

list bridge
lnm ports
source-routing configuration

bridge

LNM が特定のポート上で使用可能にされるかどうかを表示します。

例 : list bridge

```
Bridge ID (prio/add):  32768/00-00-00-00-00-38
Bridge state:               Enabled
UB-Encapsulation:      Disabled
Bridge type:           SR-TB
Bridge capability:     ASRT
Number of ports:       5
STP Participation:     IEEE802.1d on TB ports and IBM-8209 on SR ports
最大
Port  Interface State MAC Address      Modes   MSDU  Segment  Flags
2  TKR/0       Up  00-00-93-90-4C-F7    T    2096           RD
3  TKR/1     Down  00-00-00-00-00-00 SR         0 223        RD,LE
5  Eth/0     Down  AA-00-04-00-26-14            0            RD
Flags: RE =IBMRT PC behaviour Enabled, RD = IBMRT PC behaviour Disabled
LE = LNM Enabled, LD = LNM Disabled, LF = LNM Failed
SR bridge number:      8
SR virtual segment:    812
Adaptive segment:
214
```

lnm ports

ブリッジング・ルーター上で使用可能にされた LNM の構成についての情報を表示します。

例 : list LNM ports

```
LNM not enabled on port 1
LNM not enabled on port 2
Port 3
LNM Agents Enabled: RPS CRS REM
Reporting Link          State          LNM Station
Address
0                 AVAILABLE
1                 AVAILABLE
2                 AVAILABLE
3                 AVAILABLE
MAC Addresses to use when configuring LNM Manager:
00:00:00:00:00:00
00:00:00:00:00:00
LNM not enabled on port 4
LNM not enabled on port 5
```

source-routing configuration

LNM が特定のポート上で使用可能にされるかどうかを表示します。

例 : list source-routing configuration

```
Bridge number:              8
Bridge state:               Enabled
Maximum STE hop count       14
Maximum ARE hop count       14
Virtual segment:            812
Port  Segment  Interface  State    MTU   STE Forwarding   LNM
   3  223      TKR/1      Enabled  4399  Auto             ENA
   -  214      Adaptive   Enabled  1470  Yes
```

Set

指定された報告リンク番号に関するパスワードを設定します。リンク番号は 0、1、2、または 3 とすることができます。リンク 0 は制御リンクに使用されます。リンク 1、2、および 3 は監視リンクに使用されます。

このパスワードは、6 ～ 8 文字で構成する必要があり、LNM がブリッジとの報告リンクを確立するとき使用するパスワードに一致する必要があります。リンクに関して設定されるのでなければ、パスワードは省略時値であるストリング 00000000 になります。

構文 :

set password *link# password*

例: **set password**

例 : **set password**

```
Link Number [0]? 1
Enter new password :  [ABCDEFGH]? guesswho
```

第12章 TCP/IP ホスト・サービスの構成と監視

この章では、TCP/IP ホスト・サービス (TCP/IP Host) プロトコルを構成する方法および TCP/IP ホスト構成コマンドを使用する方法について説明します。この章には次の節が含まれています。

- 『基本構成手順』
- 222ページの『TCP/IP ホスト構成環境へのアクセス』
- 222ページの『TCP/IP ホスト構成コマンド』
- 225ページの『TCP/IP ホスト監視環境へのアクセス』
- 225ページの『TCP/IP ホスト監視コマンド』

TCP/IP ホスト・サービスを使用する理由の詳細を知りたい場合は、51ページの『TCP/IP ホスト・サービス (ブリッジ専用管理)』を参照してください。

IP ソース用のルーターを構成する場合は、この章を使用しないで、237ページの『第14章 IP の使用』を参照してください。

注: ホスト・サービスを構成する場合、インターフェースで構成された IP アドレスは入手できません。ルーターは IP 用のルーターとして構成することはできません。ホスト・サービスはブリッジング専用です。

基本構成手順

以下の項では、ユーザーの 2210 で TCP/IP ホスト・サービスを使用可能にするための基本構成手順について説明します。

IP アドレスの設定

TCP/IP ホスト・サービスを最小限に構成するには、**set ip-host** コマンドを使用して 2210 に IP アドレスを割り当ててください。この IP アドレスは、単一のインターフェースに関連しているのではなく、2210 全体に関連しています。

省略時ゲートウェイの追加

2210 では、2210 が直接接続されているブリッジされたネットワーク上にないホストおよびゲートウェイとの通信には、省略時ゲートウェイを使用します。 2210 は、ICMP ルーター発見 (この章の **enable router-discovery** コマンドを参照) か、または RIP (この章の **enable rip-listening** コマンドを参照) かどちらかを使用して、省略時ゲートウェイを動的に学習することができます。また、**add default gateway** コマンドを使用して、1 つまたは複数の省略時ゲートウェイを静的に指定することもできます。2210 では省略時ゲートウェイは一度に 1 つしか使用しません。追加の省略時ゲートウェイはバックアップで使用します。

割り当てられた IP アドレスおよび省略時ゲートウェイ情報を保管するには、TCP/IP-Host config> プロンプトから Config> に出て、**restart** コマンドを使用してください。2210 を再始動した後、TCP/IP-Host config> プロンプトに戻ってください。

TCP/IP ホスト・サービスを使用可能にする

2210 の IP アドレスおよび省略時ゲートウェイ情報を割り当てて保管した後、TCP/IP ホスト・サービスを使用可能にするには、**enable services** コマンドを使用してください。

TCP/IP ホスト構成環境へのアクセス

TCP/IP ホスト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てください。

```
Config> protocol hst
TCP/IP-Host Services user configuration
TCP/IP-Host Config>
```

TCP/IP ホスト構成コマンド

この節では、TCP/IP ホスト構成コマンドについて説明します。TCP/IP ホスト構成コマンドを使うと、TCP/IP ホスト・ブリッジについてネットワーク・パラメーターを指定することができます。構成コマンドを活動化するためには、ルーターを再始動します。 TCP/IP-Host config> プロンプトで TCP/IP ホスト構成コマンドを入力してください。表16 はコマンドを示しています。

表 16. TCP/IP ホスト構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	省略時ゲートウェイを追加します。
Delete	省略時ゲートウェイを削除します。
Disable	TCP/IP ホスト・サービス、ルーター発見プロセス、および RIP listen を使用不能にします。
Enable	TCP/IP ホスト・サービス、ルーター発見プロセス、および RIP listen を使用可能にします。
List	現行の TCP/IP ホスト構成をリストします。
Set	2210 の IP アドレスを設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

構成に省略時ゲートウェイ (つまり、ルーター) を追加するには、**add** コマンドを使用します。

ローカル接続から外れている IP あて先にパケットを送信しようとするときは、省略時ゲートウェイが使用されます。その場合、ルーティング・テーブルはあて先変更

処理を通じて作成されます。消えたルーターを検出するための試行が行われます。2210 がネットワークを通じて (TFTP/BootP を介して) ブートされた場合、省略時ゲートウェイはブート・プロセスからの情報を使用して構成されます。

構文:

add default-gateway *def-gateway-IP-address*

例: add default-gateway

```
Default-Gateway address [0.0.0.0]? 123.45.67.89
```

Delete

ユーザーの 2210 構成から省略時ゲートウェイを削除する場合は、**delete** コマンドを使用してください。**delete** コマンドの後に、除去したい省略時ゲートウェイの IP アドレスを入力してください。

構文:

delete default-gateway *def-gateway-IP-address*

例: delete default-gateway

```
Enter address to be deleted [0.0.0.0]? 123.45.67.89
```

Disable

次の TCP/IP 機能を使用不能にするには、**disable** コマンドを使用してください。

- TCP/IP ホスト・サービス
- ルーター発見プロセス
- RIP listen

構文:

disable rip-listening

router-discovery

services

rip-listening

RIP プロトコルを listen することにより収集されたルーティング・テーブル項目の作成を使用不能にします。省略時では、RIP listen が使用不能にされます。

例: disable rip-listening

router-discovery

ICMP ルーター発見メッセージを受信することにより省略時ゲートウェイを学習する能力を使用不能にします。省略時では、ルーター発見は使用可能にされます。

例: disable router-discovery

services

TCP/IP ホスト・サービス・プロトコルを全く使用不能にします。 IP ルートが使用可能にされていない場合、TCP/IP ホスト・サービスが省略時解釈により使用可能にされます。

例: `disable services`

Enable

次の TCP/IP 機能を使用可能にするには、**enable** コマンドを使用してください。

- TCP/IP ホスト・サービス
- ルーター発見プロセス
- RIP listen

構文:

enable	rip-listening
	router-discovery
	services

rip-listening

RIP プロトコルのブリッジ 『listen』 によって収集されたルーティング・テーブル項目の作成を使用可能にします。省略時では RIP listen は使用不能にされます。

例: `enable rip-listening`

router-discovery

ICMP ルーター発見メッセージの受信により省略時ゲートウェイの学習を使用可能にします。省略時では、ルーター発見は使用可能にされます。

例: `enable router-discovery`

services

TCP/IP ホスト・サービス・プロトコルを使用可能にします。 IP ルートが使用可能にされていない場合、TCP/IP ホスト・サービスが省略時解釈により使用可能にされます。

例: `enable services`

List

現行の TCP/IP ホスト構成についての情報を表示するには、**list** コマンドを使用してください。

構文:

list	all

例: `list all`

```
IP-Host IP address : 128.185.142.1
Address mask : 255.255.255.0

Default Gateway IP-address(es)
128.185.142.47
```

```
TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.
```

IP-Host IP address	現行の IP ホストの IP アドレスを表示します。
Address mask	現行の IP ホストの IP サブネット・アドレス・マスクを表示します。
Default Gateway IP-address(es)	現行の省略時ゲートウェイの IP アドレスを表示します。
TCP/IP Host Services	TCP/IP ホスト・サービスが使用可能か使用不能かを表示します。
RIP-LISTENING	RIP-LISTENING が使用可能か使用不能かを表示します。
Router Discovery	ルーター発見が使用可能か使用不能かを表示します。

Set

set コマンドは、2210 の IP アドレスを設定するのに使用します。TCP/IP ホスト・サービスを使用可能にする前に、2210 に IP アドレスを割り当てる必要があります。

注: IP アドレスがまだ構成されていない場合は、ブート情報を使用して設定されます (省略時)。このプロセスは、2210 が IP ホストとして稼働しているネットワーク・ホストである場合にのみ、適用されます。

構文:

set ip-host address *IP-host-address*

例: set ip 123.45.67.89

```
Address mask [255.255.0.0]?
IP-Host Address set.
```

TCP/IP ホスト・サービスの監視

この節では、IBM 2210 で TCP/IP ホスト・サービスを監視する方法を説明します。

TCP/IP ホスト監視環境へのアクセス

TCP/IP ホスト監視環境にアクセスするには、+ (GWCON) プロンプトで次のコマンドを入力してください。

```
+ protocol hst
TCP/IP-Host>
```

TCP/IP ホスト監視コマンド

この節では、TCP/IP ホスト監視コマンドについて説明します。 これらのコマンドを使用すると、活動端末からパラメーターを見たり、情報要求を入力することができます。これらのコマンドは、 TCP/IP-Host> プロンプトで入力します。 226ページの表17 はコマンドを示しています。

表 17. TCP/IP ホスト監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Dump	現行の IP ルーティング・テーブルを表示します。各あて先につき 1 行が印刷されます。
Interface	IBM 2210’ の IP アドレスを表示します。
Ping	所定のあて先を継続的に PING し、受信した各応答ごとに 1 行を印刷します。
Traceroute	所定のあて先までのホップ単位のルートを表示します。
Routers	2210 が認識しているすべての IP ルーターのリストを表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Dump

現行の IP ルーティング・テーブルを表示する場合は、**dump** コマンドを使用してください。各あて先につき 1 行が印刷されます。表示された項目の多くは、ICMP あて先変更の結果です。

構文:

dump

例:

```
TCP/IP Host> dump
Type   Dest net         Mask      Cost     Age       Next hop(s)

Stat   0.0.0.0          00000000  0        51        128.185.142.47
 Dir*  128.185.142.0    FFFFFF00  1        50        BDG/0

Default gateway in use.
Type Cost     Age       Next hop
Stat 0        51        128.185.142.47

Routing table size: 768 nets (52224 bytes), 2 nets known
                    0 nets hidden, 0 nets deleted, 0 nets inactive
                    0 routes used internally, 766 routes free
```

Type
: ルートがどのように派生したかを示すルート・タイプ

  RIP - ルートは RIP プロトコルを介して学習されました。

  Stat - 静的に構成されたルート

  Dir - 直接接続されたネットワークまたはサブネット

Dest net
: あて先ネットワーク/サブネットの IP アドレスを表示します。

Mask
: IP アドレス・マスクを表示します。

Cost
: Route Cost (ルート・コスト) を表示します。

Age
: RIP ルートの場合は、ルートの更新後の経過時間を秒数で表示します。その他のタイプのルーターの場合には、そのルーターがインストールされてからの経過時間を秒数で表示します。

Next Hop
: あて先ホストに向かってのパス上の次のルーターの IP アドレスを表示します。送信側ルーターがパケットを転送するのに使用するインターフェース・タイプも表示されます。

Default gateway
: 省略時のゲートウェイの IP アドレスを、その項目に関連するルート・タイプ、コスト、経過時間、および次のホップの情報とともに表示します。

Routing table size
: 現行のテーブルの現行のサイズ (ネットワーク数およびバイト数) を表示します。ホストが認識しているネットワーク (ネット) の数も表示します。

Interface

IBM 2210 の IP アドレスを表示するには、**interface** コマンドを使用してください。TCP/IPホスト・サービスがブリッジを介して実行されているときは、端末上に単一のアドレスが Bridge/0 として表示されます。

構文:

interface

例:

```
TCP/IP Host> interface
Interface  IP Address(es)   Mask(s)
  BDG/0    128.185.142.16   255.255.255.0
```

Interface	インターフェースのタイプを表示します。 TCP/IP ホスト・サービスの場合、これは、常に、BDG/0 で、ブリッジを指します。
IP Address	TCP/IP ホスト・サービス・インターフェースの IP アドレスを表示します。
Mask	IP アドレスのサブネット・マスクを表示します。

Ping

ping コマンドは、ルーターが所定のあて先に 1 秒間に 1 回 ICMP エコー要求を送信し (『PING』)、応答を観察するようにさせるのに使用します。このコマンドは、インターネットワーク環境での問題を分離するのに使用できます。

このプロセスは継続的に行われ、パケットが 1 つ追加されるごとに ICMP シーケンス番号が増えます。合致する受信された ICMP エコー応答が、そのシーケンス番号および往復時間とともに報告されます。往復時間の細分性 (時間レゾリューション) はプラットフォームに固有であり、通常は約 20 ミリ秒です。

PING プロセスを停止するには、端末で任意の文字を入力してください。そうすると、パケット喪失、往復時間、および到達不能な ICMP あて先の数の要約が表示されます。

マルチキャスト・アドレスがあて先として与えられている場合、各グループ・メンバーについて 1 つずつ送信される各パケットについて複数の応答が印刷されることがあります。戻された各応答は応答側の発信元アドレスとともに表示されます。

PING のサイズ (ICMP メッセージから ICMP ヘッダーを除いたもののデータ・バイト数)、TTL 値、および PING の頻度はすべてユーザーが構成可能です。省略時値は、56 バイトのサイズ、64 の TTL、および 1 秒に 1 回の PING の率です。

構文:

ping *destination source size ttl rate*

例:

```
TCP/IP Host> ping
Destination IP address [0.0.0.0]? 128.185.142.11
Source IP address [128.185.142.16]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
PING 128.185.142.16 -> 128.185.142.11: 56 data bytes, ttl=64, ... every 1 sec.
56 data bytes from 128.185.142.11: icmp_seq=0. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=1. ttl=254. time=0. ms
```

```
56 data bytes from 128.185.142.11: icmp_seq=2. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=3. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=4. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=5. ttl=254. time=0. ms

----128.185.142.11 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

Traceroute

所定のあて先へのパス全体をホップ単位で表示する場合は、**traceroute** コマンドを使用してください。各継続ホップごとに、traceroute コマンドは 3 つのプローブを送信し、応答側の IP アドレスを、応答に関連する往復時間とともに印刷します。特定のプローブが応答を受信しない場合は、アスタリスク (*) が印刷されます。画面の各行は、この 3 つのプローブの組み合わせに関連しており、一番左の数はコマンドを実行するルーターからの距離 (ルーター・ホップ数) を示しています。

あて先に到達するか、ICMP あて先到達不能メッセージが受信されるか、パスの長さが 32 のルーター・ホップに達すると、traceroute は完了します。

構文:

traceroute *destination source size probes wait ttl*

例:

```
TCP/IP Host>
traceroute
Destination IP address [0.0.0.0]? 128.185.144.239
Source IP address [128.185.142.16]?
Data size in bytes [56]?
         Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
TRACEROUTE 128.185.142.16 -> 128.185.144.239: 56 data bytes
 1 128.185.142.11 16 ms 0 ms 0 ms
 2 128.185.143.33 16 ms 0 ms 0 ms
 3 128.185.144.239 16 ms 0 ms 0 ms
```

表示パネルでは、次のようになります。

TRACEROUTE	あて先区域アドレスおよびそのアドレスに送信されるパケットのサイズを表示します。
1	あて先の NSAP およびパケットがあて先に到達して戻るに要した往復時間を示す最初のトレース。パケットは 3 度トレースされます。
Destination unreachable	あて先へのルートがないことを示します。
1 * * * 2 * * *	ルーターがあて先から何らかの形の応答を予期していますが、あて先が応答しないことを示します。

プローブが予期しない結果 (前の出力例を参照) を受信すると、いくつかの標識が印刷されます。これらの標識については以下の表で説明します。

!N	ICMP Destination Unreachable (ネット到達不能) が受信されたことを示します。
!H	ICMP Destination Unreachable (ホスト到達不能) が受信されたことを示します。
!P	ICMP Destination Unreachable (プロトコル到達不能) が受信されたことを示します。

! あて先に到達したが、あて先から送信された応答が 1 の TTL とともに受信されたことを示します。これは通常は、UNIX のいくつかのバージョンでよく起きる、あて先のエラーを示します。この場合、あて先はその応答にプローブの TTL を挿入しています。運悪くこれが生じると、あて先へ最後に到達する前に、アスタリスクのみから構成される行がいくつも印刷されることになります。

Routers

IBM 2210 に知られているすべての IP ルーターのリストを表示する場合は、**routers** コマンドを使用してください。ルーターは次のものを通じて学習することができます。

- 静的構成 (222ページの『Add』 ページで説明している **add default-gateway** コマンドを使用する)。
- 受信された ICMP あて先変更
- ICMP ルーター発見メッセージ (構成されている場合)
- RIP 更新 (構成されている場合)

各ルーターは、その起点、その優先順位 (省略時ルートを選択するときに使用されます)、およびその存続時間 (ルーターが、通信が途絶えていて無効と宣言される前の秒数) とともにリストされます。

構文:

routers

例: `routers`

第2部 ルーター・プロトコルの構成と監視

第13章 ATM を介したルーティングの概要

注: この章で使用されている省略形および用語の定義については、用語集を参照してください。この章では、固有の ATM を介したルーティングについて説明します。

ルーティングの概要

LAN エミュレーション (LE)、クラシカル IP (CIP)、およびサポートされているルーティング・プロトコルの関係が単純であるため、この節では、ルーティングの概要を簡単に記載しています。 ルーターは、 図26 および 図27 に示されているとおりに、IP および IPX ルーティングをサポートしています。

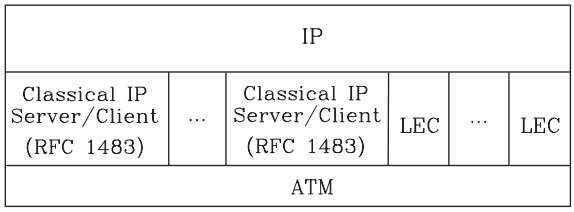


図 26. IP ルーティング

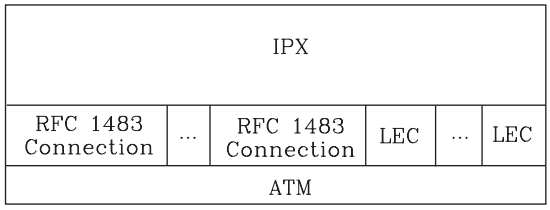


図 27. IPX ルーティング

IP ルーティングは、クラシカル IP (CIP) と LAN エミュレーション (LE) サブネットの任意の組み合わせでサポートされています。これらのサブネットでは、他のルーターへのエミュレートされた LAN インターフェースおよび RFC 1483 [1]接続を介してサポートされます。これらのプロトコルは、LAN エミュレーション (LE) クライアントによって実装されたエミュレートされたインターフェースを、実際のイーサネットおよびトークンリング・インターフェースと同様に扱います。LE クライアントは作成されると、固有のインターフェース番号が割り当てられます。

1. J. Heinanen 発表の “ATM アダプテーション・レイヤー 5 を介したマルチプロトコルのカプセル化” RFC 1483、Telecom Finland、1993 年 7 月。

RFC 1483 サポートの概要

RFC 1483 (ATM アダプテーション・レイヤー 5 を介したマルチプロトコルのカプセル化) は、ブリッジされたフレームおよびルーター・フレームのマルチプロトコルに関する詳細を提供します。IP および IPX トラフィックのルーティングがサポートされます。ソフトウェアにより全範囲のブリッジング機能も提供されるため、ブリッジされたトラフィックが ATM を介して固有に伝送できます。

RFC 1483 は、ATM を介してマルチプロトコル・トラフィックを搬送するために LLC/SNAP のカプセル化を指定します。SNAP ヘッダーが存在することを示すために、0xAA-AA-03 という LLC 値が指定されます。SNAP ヘッダーの OUI 部分は、ルーティングされたプロトコルの場合は 0x00-00-00、ブリッジされたプロトコルの場合は 0x00-80-C2 です。

ルーティングのための RFC 1483 サポートの概要

クラシカル IP は、RFC 1483 で定義されたルーティング済みプロトコルのために LLC/SNAP 形式を使用します。ルーターは、LLC/SNAP カプセル化を使用する IPX ルーターへの接続もサポートします。この IPX サポートは、クラシカル IP 手法を手本にしています。

IPX ルーティングのための RFC 1483 サポート

IPX ルーターは、ルーティング情報プロトコル (RIP) およびサービス公示プロトコル (SAP) を使用して、ルーティングおよび装置情報テーブルを伝えます。LAN またはエミュレート済みの LAN 上では、これらのプロトコルは、同報通信フレームを使用して、関心を寄せているユーザーに情報を伝えます。ルーターは、他の IPX ルーターとのすべての RFC 1483 接続との間でも、ルーティングおよび装置情報をやり取りします。

ATM 上での RFC 1483 LLC/SNAP カプセル化をサポートする他のルーターは、手動で構成された RFC 1483 接続を介して全体または部分的なメッシュで相互に接続することができます。

完全メッシュ・ネットワークでは、各ルーターは、他のすべてのルーターに直接に接続しています。*部分メッシュ・ネットワーク*では、すべてのルーターが他のルーターと直接に接続しているわけではありません。ただし、どのルーターでも、直接または他のルーターを介して別のルーターに接続できるだけの接続が存在します。部分メッシュ・ネットワークでは、いくつかのルーターが中間ルーティングを実行する必要があります。中間ルーターは、互いに直接に接続されていないルーター間を接続します。

パーマネント・バーチャル・サーキット (PVC) および構成済みスイッチド・バーチャル・サーキット (SVC) の両方がサポートされます。ただし、IPX ルーターへのバーチャル・チャネル・コネクション (VCC) は IPX 専用にする必要があります。それらは、IP などの他のプロトコルと共用することはできません。

クラシカル IP の場合と同様に、サービス品質特性は、ピーク速度および保持速度などの VCC トラフィック・パラメーターを構成することによって指定することができ、複数のサーキットを単一の ATM インターフェース上で構成することができます。

ルーター は、ATM インターフェースごとに単一の IPX ネットワークをサポートします。これは、IPX を明示的に構成する必要のある各インターフェースごとに単一の ATM ARP クライアントを意味します。したがって、ATM インターフェース上の相互に接続されたすべてのルーターは同じ IPX ネットワークの部分である必要があります。

IPX ATM アドレスは、RFC 1483 カプセル化 (これには、クラシカル IP 構成要素が含まれています) を使用するすべての構成要素の間で固有である必要があります。IPX ATM アドレスのエンド・システム識別子 (ESI) およびセレクターの部分は、クラシカル IP の ATM アドレスと同様に構成されます。 ルーターが SVC を開始しない場合、呼び出しルーターで構成することのできる固定アドレスを提供するためには、現行の構成で少なくともセレクターが明示的に指定されている必要があります。

IPX プロトコル・アドレスには、4 バイトのネットワーク番号と 6 バイトのホスト番号 (またはホスト ID) という 2 つの部分があります。ネットワーク番号は IPX ルーティング・ドメイン内で固有である必要があり、ホスト番号は与えられたネットワーク内で固有である必要があります。ルーターは、IPX ホスト番号を、関連する ATM アドレスの ESI 構成要素に設定します。ESI を明示的に構成しない場合は、必ず、ATM インターフェース・ハードウェアに組み込まれた MAC アドレスが省略時値として解釈されます。

あて先 IPX ホスト番号は VCC 構成中に指定することができますが、InATMARP を使用して動的に学習することもできます。InATMARP をサポートしていないあて先ルーターの IPX ホスト番号は手動で構成する必要があります。ルーターは、また、InATMARP を定期的に使用して、パートナー・ルーターの IPX ホスト番号についての知識を更新します。

部分メッシュで相互接続され、同じ ATM インターフェース上で中間ルーティングを提供するルーターは、ATM インターフェース上で IPX 水平分割を使用不能にする必要があります。これを行うと、RIP および SAP は、相互接続されたルーターに使用可能なすべてのルートとおよびサービスについて必ず知らせるようになります。全部のメッシュで相互接続されたルーターは、水平分割を使用不能にする必要はありません。

ルーターが IPX ルーティングのための RFC 1483 サポートを実装するためには、最小構成が必要です。必要な情報は、IPX ネットワーク番号と IPX ホスト番号 (IPX ATM ARP クライアント) だけです。リモート IPX ルーターへの接続をオープンする必要がある場合は、必要な接続 (VCC) を追加して構成する必要があります。RFC 1483 のカプセル化および InATMARP の組み合わせはまだ標準化されていませんが、この組み合わせはフレーム・リレーを介した IPX については RFC 1490 [2]で規定されています。

2. T. Bradley、C. Brown、および A. Malis 発表の “フレーム・リレーを介したマルチプロトコル相互接続” RFC 1490、Wellfleet Communications Inc. および Ascom Timeplex Inc.、1993 年 7 月。

第14章 IP の使用

この章では、インターネットワーク・プロトコル (IP) を構成する方法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。

- 『基本構成手順』
- 256ページの『BOOTP/DHCP 転送プロセスを構成する』
- 258ページの『UDP 転送を構成する』
- 258ページの『バーチャル・ルーター冗長プロトコル (VRRP) を構成する』
- 261ページの『冗長省略時 IP ゲートウェイを構成する』
- 262ページの『IP マルチキャスト・サポート』

基本構成手順

この節では、IP プロトコルを立ち上がらせ、稼働させるのに必要な最初の手順を概説します。さらに構成変更を行う場合について詳しくは、この章の他の節に記載されています。個別の構成コマンドについては、この章のコマンドの節で詳しく説明しています。次のリストは、IP をルーターで起動するための初期の構成作業の概要です。これらの作業を完了したら、ルーターを再始動して、新しい構成を有効にする必要があります。

1. IP 構成環境にアクセスする。(265ページの『IP 構成環境にアクセスする』を参照してください。)
2. ネットワーク・インターフェースに IP アドレスを割り当てる。(『ネットワーク・インターフェースへ IP アドレスを割り当てる』を参照してください。)
3. 動的ルーティングを使用可能にする。(241ページの『動的ルーティングを使用可能にする』を参照してください。)
4. 静的ルーティング情報を追加する (必要な場合)。(243ページの『静的ルーティング情報を追加する』を参照してください。)
5. ARP サブネット・ルーティングを使用可能にする (必要な場合)。(246ページの『ARP サブネット・ルーティングを使用可能にする』を参照してください。)
6. ARP パラメーターをセットアップする (必要な場合)。(246ページの『ARP 構成のセットアップ』を参照してください。)
7. IP 構成プロセスを終了する。
8. ルーターを再始動し、構成変更を活動化する。

以下の項では、各構成作業をさらに詳しく説明します。

ネットワーク・インターフェースへ IP アドレスを割り当てる

ネットワーク・インターフェースに IP アドレスを割り当てるには、IP 構成 **add address** コマンドを使用してください。このコマンド用の引き数には、インターフェ

ース番号 (Config> **list devices** コマンドから入手できます) および IP アドレスおよびそれに関連するアドレス・マスクが組み込まれます。

次の例では、ネットワーク・インターフェース 2 にアドレス 128.185.123.22 が関連するアドレス・マスク 255.255.255.0 とともに (サブネット用の第 3 のバイトを使用して) 割り当てられています。

```
IP config> add address 2 128.185.123.22 255.255.255.0
```

複数の IP アドレスを、単一のネットワーク・インターフェースに割り当てることができます。

省略時解釈では、ネットワーク・インターフェースに割り当てられた IP アドレスは、それぞれ、別のネットワークまたはサブネット内になければなりません。この制限は、**enable same-subnet** コマンドにより取り除くことができます。

IP では、回線に実 IP アドレスを割り当てることなく、IP トラフィックにシリアル回線インターフェースを使用することができます。ただし、各シリアル回線に擬似 IP アドレスを割り当てることは必要です。このアドレスはルーターがインターフェースを参照するために使用しますが、外部から使用されることは決してありません。**add address** コマンドを使用して、シリアル回線に 0.0.0.*n* の形式のアドレスを割り当てます。ここで、*n* はハードウェア・インターフェース番号 (これも Config> **list devices** コマンドから入手されます)。このアドレス形式は、ルーターに問題のインターフェースが*無番号のシリアル回線* であることを示します。

インターフェースに IP アドレスを割り当てることなく、シリアル回線インターフェース番号 2 で IP を使用可能にするには、次のコマンドを使用してください。

```
IP config> add address 2 0.0.0.2
```

ブリッジ・ネットワーク・インターフェースへ IP アドレスを割り当てる

2210 は、IP アドレスが割り当てられているネットワーク・インターフェース (*ルーティング・インターフェース*) 上で IP パケットをルートし、ブリッジングが構成されているが、IP アドレスは割り当てられていないネットワーク・インターフェース (*ブリッジング・インターフェース*) 上で IP パケットをブリッジします。2210 は、ブリッジング・インターフェースとの間で IP データグラムの送受信し、ブリッジング・インターフェースとルーティング・インターフェースとの間で IP パケットをルートすることができます。ブリッジ・ネットワーク・インターフェースに 1 つまたは複数の IP アドレスを追加することにより、2210 上でこれらの機能を使用可能にできます。ブリッジ・ネットワーク・インターフェースは、2210 の接続先である、ブリッジされたネットワークに IP を接続する論理インターフェースです。

ブリッジ・ネットワーク・インターフェースに IP アドレスを追加するには、次のように、**add address** コマンドを使用して、ネットワーク・インターフェースとして **bridge** を指定します。

```
IP config> add address bridge ip-address ip-address-mask
```

このコマンドは、IP アドレスを個々のブリッジング・インターフェースに割り当てるのではなく、ブリッジング・インターフェースのすべてに割り当てます。

ブリッジング・ネットワーク・インターフェースに IP アドレスを割り当てると、2210 上の物理ネットワーク・インターフェース (物理ポート) の 1 つを空けることができます。これを理解するには、まず最初に、図28 を考慮してください。この図には、別個の装置でルーターおよびブリッジ機能を実行している IP インターネットワークが示されています。LAN 2 と LAN 3 はブリッジで接続され、ブリッジされたネットワークを作成します。したがって、ルーターにとって、このブリッジされたネットワークは、IP アドレス 9.67.5.1 およびマスク 255.255.255.0 によって定義された単一の IP サブネットです。

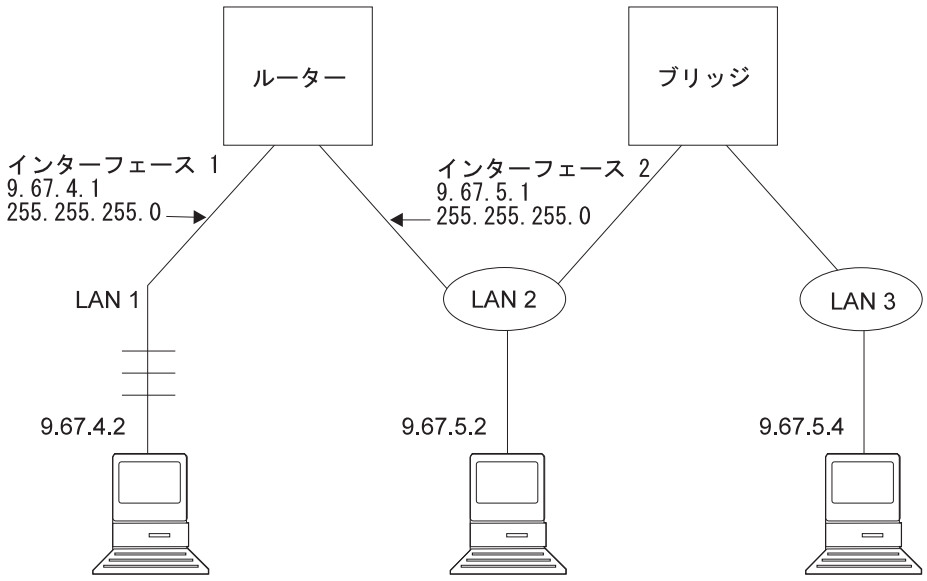


図 28. ブリッジされたネットワークまでのルーティング - 代案 1

240ページの図29 は、前図と同じインターネットワークですが、ルーターとブリッジの機能が単一の装置に組み込まれたものを示します。この図では、ルーターは、まだ、ブリッジされたネットワークにつながっている独自の物理ネットワーク・インターフェース (インターフェース 2) をもっています。

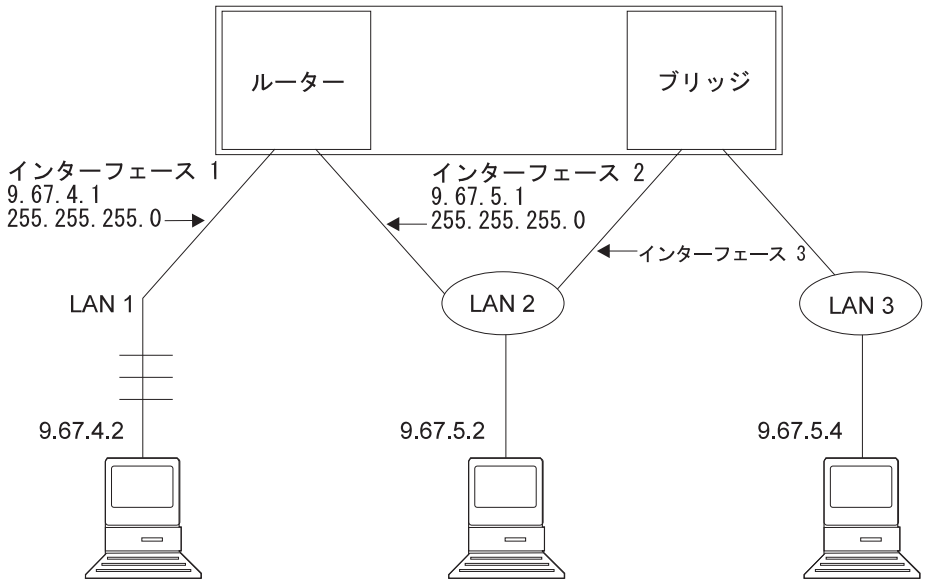


図 29. ブリッジされたネットワークまでのルーティング - 代案 2

最後に、図30 では、ブリッジされたネットワークにつながっているルーターの物理ネットワーク・インターフェースは、ブリッジ・ネットワーク・インターフェース (内部インターフェース) で置き換えられています。これは、図28 および 図29 に示されているインターネットワークと同じものですが、ルーターには、ブリッジされたネットワークにつながっている独自の物理ネットワークは必要なくなっています。

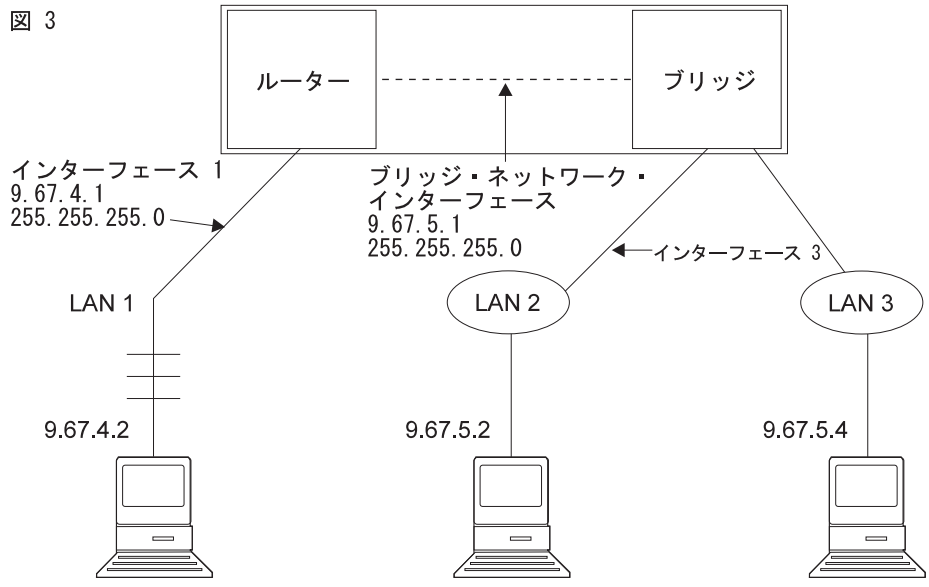


図 30. ブリッジされたネットワークまでのルーティング - 代案 3

注: ブリッジ・ネットワーク・インターフェース上に IP アドレスを構成する場合は、ソース・ルート・ブリッジングが構成されているトークンリング・インターフェース上に IP アドレスは構成できません。

内部 IP アドレスを設定する

これは、どのインターフェースの状態からも独立し、どのインターフェースも参照せずに設定された IP アドレスです。IP 構成によっては、これが必要です。詳細については、310 ページのコマンド **set internal-IP-address** を参照してください。

動的ルーティングを使用可能にする

ルーターで動的ルーティングを使用可能にするには、次の手順を使用してください。ルーター・ソフトウェアは、内部ゲートウェイ・プロトコル (IGP) のほか、外部ゲートウェイ・プロトコルである BGP について、OSPF、RIPv1、および RIPv2 をサポートします。

すべてのルーティング・プロトコルは同時に稼働することができます。ただし、ほとんどのルーターは、単一のルーティング・プロトコル (IGP の 1 つ) だけを実行します。OSPF プロトコルを使用するようお勧めします。これは、頑丈であることと、それがサポートする追加 IP フィーチャー (等コスト・マルチパスや可変長サブネットなど) であるためです。

ルーティング・テーブル・サイズを設定する

ルーティング・テーブル・サイズは、動的ルーティング・プロトコルおよび静的ルートを含む、すべての発信元からのルーティング・テーブル内の項目の数を決定します。省略時のサイズは 768 項目です。

ルーティング・テーブルのサイズを変更するには、**set routing table-size** 構成コマンドを使用してください。ルーティング・テーブル・サイズを小さく設定しすぎると、ルートが廃棄されることになります。それを大きく設定しすぎると、メモリー資源を効率的に使用できなくなります。操作の後、**dump** コマンドを使用してテーブルの内容を表示させてから、必要に応じてサイズを調整し、拡張のためいくらか余裕があるようにしてください。

OSPF プロトコルを使用可能にする

OSPF 構成はそれ自体の構成コンソールを介して行われます (`Config>` **protocol ospf** コマンドを介して入力されます)。OSPF を使用可能にするには、次のコマンドを使用してください。

```
OSPF Config> enable OSPF
```

OSPF プロトコルを使用可能にした後、OSPF リンク状態データベースのサイズの推定値を入力するようプロンプト指示されます。これにより、ルーターは OSPF 用にどれだけのメモリーを予約しておくべきか予測できます。OSPF リンク状態データベースのサイズを推定するのに使用される次の 2 つの値を提供する必要があります。

- OSPF ルーティング・ドメインにインポートされた外部ルートの総数
- ルーティング・ドメインでの OSPF ルーターの総数

次のプロンプトでこれらの値を入力してください (サンプル値を示してあります)。

```
OSPF Config> enable ospf
Estimated # external routes[0]? 200
Estimated # OSPF routers [50]? 60
Maximum LSA size [2048]?
```

次に、OSPF ルーティングに参加する各 IP インターフェースを構成してください。OSPF 用の IP インターフェースを構成するには、次のコマンドを使用します。

```
OSPF Config> set interface
```

一連の操作パラメーターを入力するようプロンプト指示されます。各インターフェースには、コストならびに他の OSPF 操作パラメーターが割り当てられます。

OSPF 以外の他の IP ルーティング・プロトコルを稼働するときに、OSPF と他のプロトコルの間でルートを交換したい場合があります。これを行うには、次のコマンドを使用してください。

```
OSPF Config> enable AS-boundary-routing
```

OSPF 構成プロセスについて詳しくは、333ページの『第16章 OSPF の使用』を参照してください。

RIP プロトコルを使用可能にする

この項では、初期に RIP プロトコルを構成する方法を説明します。RIP プロトコルを構成するときは、ルーターが各 IP インターフェースでどの組み合わせのルートを公示または受け入れあるいはその両方を行うかを指定できます。

RIP は、X.25 やネイティブ ATM (RFC 1577) のネットワーク・インターフェース上ではサポートされません。これらのタイプのインターフェースの場合は、内部ゲートウェイ・プロトコル (IGP) について、RIP ではなく、OSPF を使用してください。RIP がサポートされるのは、ATM LAN エミュレーション・ネットワーク・インターフェースの場合です。

最初に、次のコマンドを使って、RIP プロトコルを使用可能にします。

```
IP config> enable RIP
```

RIP が使用可能にされる場合は、次の省略時行動が確立されます。

- ルーターは、その構成された各 IP インターフェースから送信される RIP 更新内にすべてのネットワークおよびサブネットのルートを含んでいます。 省略時ルートおよび静的ルートは含まれません。
- ルーターは、その構成された IP インターフェースのそれぞれで受信されるすべての RIP 更新を処理します。
- RIP は省略時ルートおよび静的ルートを上書きしません。

省略時の送信/受信行動のいずれかを変更するには、各 IP インターフェースごとに定義される、以下の IP 構成コマンドを使用してください。

```
IP config> enable/disable sending net-routes
IP config> enable/disable sending subnet-routes
IP config> enable/disable sending static-routes
IP config> enable/disable sending host-routes
IP config> enable/disable sending default-routes
IP config> enable/disable receiving rip
IP config> enable/disable receiving dynamic nets
IP config> enable/disable receiving dynamic subnets
IP config> enable/disable receiving host-routes
```

```
IP config> enable/disable override default
IP config> enable/disable override static-routes
IP config> set originate-rip-default
```

BGP プロトコルを使用可能にする

BGP プロトコルは、その独自の構成プロンプト BGP Config> から使用可能にします。BGP の構成について詳しくは、 *プロトコルの構成と監視 解説書 第 2 巻* に記載されている BGP4 の使用と構成についての説明を参照してください。

静的ルーティング情報を追加する

この手順が必要なのは、上記の動的ルーティング・プロトコルのどれからも入手できない情報のルートを指定する場合だけです。静的ルーティング情報は停電があっても残ります。決して変化しないか、あるいは動的に学習することのできないルートに使用されます。

静的ルートのあて先は、IP アドレス (*dest-addr*) および IP アドレス・マスク (*dest-mask*) によって記述されます。マスクは、ルートが適用される IP アドレスの範囲を示します。例えば、IP アドレス 10.0.0.0 とマスク 255.0.0.0 をもつルートは、10.0.0.0 ～ 10.255.255.255 までの IP アドレスに適用されます。あて先までのルートは、次のホップ・ルーターの IP アドレス (*next-hop*) と、このルート上でのパケットの転送コスト (*cost*) によって記述されます。

静的ルートを作成、修正、または削除するには、以下のコマンドを使用してください。

```
IP config> add route dest-addr dest-mask
next-hop  cost
IP config> change route dest-addr  dest-mask next-hop cost
IP config> delete route dest-addr  dest-mask
```

これらのコマンドを使用すると、1 つの IP あて先に対して最大 4 つの静的ルートを定義し、そのルートのうちの 1 つまたは複数に障害が発生した場合には代替ルートを用意できます。これらのコマンドは即時に有効になるので、ルーターをリブートする必要はありません。

最長一致規則

ルートのあて先には IP アドレス・マスクが組み込まれているため、複数のルートが特定の IP アドレスに一致することはあり得ます。例えば、IP アドレス 10.1.2.3 の場合、IP アドレス 10.0.0.0 とマスク 255.0.0.0 をもつルートと、IP アドレス 10.1.0.0 とマスク 255.255.0.0 をもつルートは、一致します。どちらのルートを使用するかを決定するために、最長一致規則が適用されます。最大マスクをもつルートが使用されます (この場合、IP アドレス 10.1.0.0 とマスク 255.255.0.0 をもつルート)。

省略時ルート、ネットワーク・ルート、サブネット・ルート、およびホスト・ルート

ルートは、それぞれのあて先 IP アドレスとマスクに応じて、*省略時*、ネットワーク、サブネット、またはホスト に分類できます。

省略時 ルートは、0.0.0.0/0.0.0.0 という IP アドレス/マスクをもっています。このルートは、すべてのあて先 IP アドレスに一致しますが、最長一致規則により、他に一致ルートがない場合に限り使用されます。静的省略時ルートは、以下のコマンドによって作成します。

```
IP config> add route
IP destination [ ]? 0.0.0.0
Address mask [255.0.0.0]? 0.0.0.0
Via gateway 1 at [ ]? 192.9.1.4
Cost [1]? 5
Via gateway 2 at [ ]?
IP config>
```

静的省略時ルートは、 **set default network-gateway** コマンドによっても設定できますが、このコマンドは、即時に有効にはならないため、省略時静的ルートを 1 つしか定義できません。以下の例では、上記の **add route** コマンドと同じ静的省略時ルートを作成します。

```
IP config> set default network-gateway
Default gateway [ ]? 192.9.1.4
gateway's cost [1]? 5
IP config>
```

ネットワーク・ルート はマスクがありますが、このマスクは、RFC-791 で定義されている IP アドレス・クラスによって指定されたとおりのルートのあて先 IP アドレスの値に左右されます。

IP アドレス・クラス	IP アドレスの範囲	ネットワーク・マスク
A	0.0.0.0 ～ 127.255.255.255	255.0.0.0
B	128.0.0.0 ～ 191.255.255.255	255.255.0.0
C	192.0.0.0 ～ 223.255.255.255	255.255.255.0

コマンド **add route**、**change route**、および **delete route** はあて先 IP アドレスに対応するネットワーク・マスクを省略時のマスク値として使用します。静的ネットワーク・ルートは、以下のコマンドによって作成します。

```
IP config> add route 172.16.0.0
Address mask [255.255.0.0]?
Via gateway 1 at [ ]? 192.9.1.4
Cost [1]? 5
Via gateway 2 at [ ]?
IP config>
```

静的ネットワーク・ルートは、 **set default subnet-gateway** コマンドによっても設定できますが、このコマンドは、即時に有効にはならないため、1 つのあて先について静的ルートを 1 つしか定義できません。以下の例では、上記の **add route** コマンドと同じ静的ネットワーク・ルートを作成します。

```
IP config> set default subnet-gateway
For which subnetted network [ ]? 172.16.0.0
Default gateway [ ]? 192.9.1.4
gateway's cost [1]? 5
IP config>
```

サブネット・ルート は、ルートのあて先 IP アドレスのネットワーク・マスクよりも大きなマスクをもっています。静的サブネット・ルートは、以下のコマンドによって作成します。

```
IP config> add route 172.16.1.0
Address mask [255.255.0.0]? 255.255.255.0
Via gateway 1 at [ ]? 192.9.1.4
Cost [1]? 5
Via gateway 2 at [ ]?
IP config>
```

ホスト・ルート は、特定の IP アドレスまでのルートで、255.255.255.255 というマスクをもっています。静的ホスト・ルートは、以下のコマンドによって作成します。

```
IP config> add route 172.16.1.2
Address mask [255.255.0.0]? 255.255.255.255
Via gateway 1 at [ ]? 192.9.1.4
Cost [1]? 5
Via gateway 2 at [ ]?
IP config>
```

静的ルーティングと動的ルーティングとの間の対話

OSPF プロトコルおよび RIP プロトコルを通じて動的に学習されたルートは、静的ルートを指定変更できます。RIP プロトコルの場合は、この指定変更を使用不能にできます。**enable/disable override static-routes** コマンドについては、この章の RIP の節を参照してください。

これらの動的プロトコルが使用可能にされているインターフェースを通じて構成された静的ルートを公示するには、OSPF および RIP の両方を構成することができます。

静的ルートを公示するよう RIP を構成するには、IP config> プロンプトで次のコマンドを入力してください。

```
IP config> enable sending static-routes ip-interface-address
```

静的ルートを公示するよう OSPF を構成するには、OSPF Config> プロンプトで次のコマンドを入力してください。

```
OSPF Config> enable as boundary
Import static routes? yes
```

ネクスト・ホップ認識

ネクスト・ホップ認識により、ルーターは、近隣ルーターが起動しているかどうかを検知することができます。このオプションが選択されていると、ルーターは、近隣ルーターをそのネクスト・ホップとして使用する静的ルートが機能するかどうかを、より正確に判別することができます。ルーターは、さらに、静的ルートのネクスト・ホップが複数ネットワーク・インターフェース上で定義されている IP サブネット内にあるときに、そのネクスト・ホップが到達できるネットワーク・インターフェースも判別できます。

特定の IP インターフェース上でネクスト・ホップ認識を使用可能にするには、IP 構成プロンプトで以下のコマンドを入力してください。

```
IP config> enable nexthop-awareness ip-interface-address
```

特定の IP インターフェース上でネクスト・ホップ認識を使用不能にする場合は、IP 構成プロンプトで以下のコマンドを入力してください。

```
IP config> disable nexthop-awareness ip-interface-address
```

ネクスト・ホップは、近隣ルーターが逆 ARP をサポートしているフレーム・リレー・ネットワーク上でのみサポートされます。

ARP 構成のセットアップ

アドレス解決プロトコル (ARP) は、パケットがルーターによって転送される前にプロトコル・アドレスをハードウェア・アドレスにマップするために使用されます。ARP はルーター上で常にアクティブであるため、その省略時の特性を指定してそれを使用可能にするのに追加の構成を行う必要はありません。ただし、ARP 構成パラメーター (省略時の最新表示タイマーを変更する **enable auto-refresh** または **set refresh-timer** など) を更新する必要がある場合、または永続アドレス・マッピングを追加、変更、または削除する必要がある場合は、593ページの『第27章 ARP の使用』を参照してください。

LAN エミュレーションがインターフェースで構成される場合は、省略時値が適用されます。ARP プロトコルは変更なしに効率的に使用することができます。 RFC 1577 (ATM を介したクラシカル IP および ARP) を使用する場合は、ATM インターフェース上に構成されているそれぞれの IP アドレスごとに、ARP クライアントと ARP サーバーの追加構成が必要です (615ページの『ATM を介した ARP の構成コマンド』に説明してあるように)。

ARP サブネット・ルーティングを使用可能にする

接続されたサブネット・ネットワーク上にサブネットをサポートしないホストがある場合は、アドレス解決プロトコル (ARP) サブネット・ルーティング (RFC 1027 に記述されています) を使用してください。ルーターが ARP サブネット・ルーティング用に構成されている場合は、ルーターは代わりにあて先の ARP 要求に応答します (つまり、ルーター自体があて先への最適のルートであり、あて先が発信元と同じ自然ネットワーク内にある場合、LAN を離れます)。正しい操作のためには、サブネットを知らないホストを含む LAN に接続されたすべてのルーターは、ARP サブネット・ルーティング用に構成する必要があります。

ARP サブネット・ルーティングを使用可能にするには、次のコマンドを使用してください。

```
IP config> enable arp-subnet-routing
```

ARP ネットワーク・ルーティングを使用可能にする

一部の IP ホストは、ARP をすべてのあて先へ (あて先が発信元と同じ自然ネットワーク内にあるかどうかには無関係に) ルートします。これらのホストにとっては、ARP サブネット・ルーティングは十分ではありません。あて先がルーターを通じて到達可能であり、あて先が発信元と同じローカル・ネットワーク・セグメント上にない限り、ルーターは代わりにどの ARP 要求にも応答するよう構成することができます。

ARP ネットワーク・ルーティングを使用可能にするには、次のコマンドを使用してください。

```
IP config> enable arp-network-routing
```

IP フィルター

フィルターすることにより、ルーターがパケット転送に使用する特定の基準を指定できます。ユーザーがセキュリティーと管理目標を達成する上で役立つよう、主に次の 2 つのタイプのフィルターが提供されます。

- アクセス制御
- ルート・フィルター

アクセス制御

アクセス制御により、IP ルーターは、以下のパラメーターに基づいて個々のパケットの処理を制御できます。

- IP 発信元アドレス
- IP あて先アドレス
- IP プロトコル番号
- TCP または UDP 発信元ポート番号
- TCP または UDP あて先ポート番号
- TCP SYN および ACK ビット
- ICMP タイプおよびコード
- 優先順位とサービス・タイプ (TOS) フィルター

アクセス制御は、互いに通信するための IP ホストおよびサービスの特定の集合の能力を制限することができます。

アクセス制御リストを構成することにより、アクセス制御を定義することができます。インターフェースごとに 1 つのグローバル・リストおよび 2 つのリストを指定することができます。グローバル・リストはルーター全体に適用されます。インターフェース・リスト (パケット・フィルターとも言います) は、割り当てられた名前で、指定されたインターフェースにのみ適用されます。各インターフェースごとに、1 つのリストが着信パケットに適用され、他方が発信パケットに適用されます。これらのリストは互いに独立して適用されます。パケットは着信インターフェース・リストを*通過*し、グローバル・リストによって*除去される* 場合があります。

図31 は、パケットが転送される前に通過しなければならない一連のアクセス制御リストを示しています。

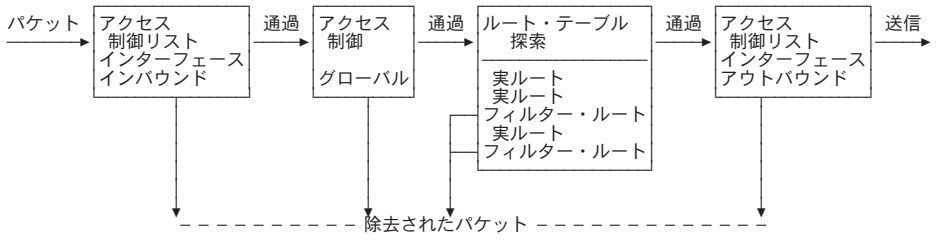


図 31. パケット転送パス内のアクセス制御リスト

アクセス制御規則

各アクセス制御リストは、フィルター基準を設定する 1 つまたは複数のアクセス制御規則から構成されます。 ルーター上のインターフェースすべてに影響するグローバル・フィルターを定義するアクセス制御規則もあれば、インターフェース固有のアクセス制御リスト (パケット・フィルターとも呼ばれます) を定義するものもあります。 グローバル・アクセス制御規則は、IP config> プロンプトで **add access** コマンドを使用して構成します。 パケット・フィルターは、IP config> プロンプトで次の 2 つのコマンドを使用して設定します。つまり、フィルターを定義する場合は **add packet-filter** コマンドを、また、フィルターを構成する場合は **update packet-filter** コマンドを使用します。

IP パケットがルーターを通じて流れるときに、IP パケット・フィールドがアクセス制御規則と比較されます。 規則の指定された各フィールドがパケット内の対応するフィールドに一致する場合、パケットは規則に一致します。 パケットが規則に一致し、その規則フィルター・タイプが inclusive (組み込み) であれば、パケットは *通過*します。 規則フィルター・タイプが exclusive (排除) である場合、パケットは *除去*され、ルーターはそれ以上の処理を行いません。 リスト全体を通過した後でどの規則も一致しない場合も、パケットは除去されます。

アクセス制御リストでレコードを定義する際には、以下の情報を忘れないでください。

- リスト内のレコードの配列は重要です。リスト内のレコードの配列を変更するために、構成コマンドが提供されています。
- アクセス制御規則が少なくとも 1 つ含まれているリストの場合は、そのアクセス制御規則のどれにも適合しないパケットがリストを通過するためには、それぞれ inclusive (組み込み) 規則が存在する必要があります。指定されている規則のどれにも適合しないパケットがすべて通過できるようにするには、次のようなワイルドカード規則を最後の規則としてリスト内に組み込む方法があります。

```
IP config> add access-control
Enter type [E]? i
Internet source [0.0.0.0]?
Source mask [0.0.0.0]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter starting DESTINATION port number ([0] for all ports) [0]?
Enter starting SOURCE port number ([0] for all ports) [0]?
Filter on ICMP Type ([-1] for all types) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]? CD
TOS/Precedence start value (00-FF) [0]?
TOS/Precedence end value [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]? FA
New TOS/Precedence value (00-FF) [0]?
Use policy-based routing? [No]: yes
Next hop gateway address [ ]? 8.8.8.2
Use default route if next hop gateway unreachable? [Yes]:
Enable Logging (Yes or [No]):
```

アクセス制御を使用可能にする

IP アクセス制御 (グローバル・アクセス制御およびインターフェース・アクセス制御を含む) を使用可能にするには **set access-control on** コマンドを、また、使用不能にするには **set access-control off** コマンドを使用します。 IP アクセス制御が

使用可能になっているときに特定のパケット・フィルターを使用可能にするには **enable packet-filter** コマンドを、また、使用不能にするには **disable packet-filter** コマンドを使用します。

IP アクセス制御が使用可能になっている場合は、ルーターが発信し、受信するパケットに注意する必要があります。 ルーターによって送信または受信する RIP パケットまたは OSPF パケットをフィルターしないように注意してください。 これを行う最も簡単な方法は、アクセス制御リストの最後にワイルドカードの組み込み規則を追加することです。 別の方法として、RIP および OSPF について特定の規則を、場合によっては制限的なアドレスおよびマスクを指定して、追加できます。 一部の OSPF パケットはクラス D のマルチキャスト・アドレス 224.0.0.5 および 224.0.0.6 に送信されることに注意してください。このことは、アドレス検査をルーティング・プロトコルに対して行っている場合には重要です。 アクセス制御について詳しくは、**add** コマンドを参照してください。

グローバル・アクセス制御リストを定義する

グローバル・アクセス制御リストは、IP config> プロンプトで規則を追加するときに定義します。

```
IP config> add access-control...
```

グローバル・アクセス制御規則は、**list**、**move**、または **delete** コマンドを使用して、それぞれ、リスト、移動、または削除することができます。 詳しくはこれらのコマンドを参照してください。

パケット・フィルターの定義

インターフェース固有のパケット・フィルターを定義するには、IP config> プロンプトで **add packet-filter** コマンドを使用します。 ルーターはプロンプトを出してフィルターの名前、フィルターの方向 (入力または出力)、およびフィルターが適用されるインターフェース番号を入力するよう指示してきます。

```
IP config> add packet filter
Packet-filter name [ ]? test
Filter incoming or outgoing traffic? [IN]? in
Which interface is this filter for [0]? 1
```

ルーターで構成されたインターフェースに固有のすべてのアクセス制御リストをリストするには、**list packet-filter** コマンドを使用することができます。

パケット・フィルターについてのアクセス制御規則の設定

定義された各リスト (パケット・フィルター) についてアクセス制御レコードを定義する必要があります。そうしないと、定義されたパケット・フィルターは、着信または発信するトラフィックに何の効果ももちません。 IP config> プロンプトで **update packet-filter** コマンドを使用して、アクセス制御規則を定義してください。 ルーターはプロンプトを出して、更新したいフィルターの名前を入力するよう指示してきます。 次に、IP config> プロンプトは Packet-filter 'name' Config> に変わります。ここで、‘name’ は、ユーザーが提供するリスト名です。

```
IP config>  update packet-filter
Packet-filter name [ ]?  test
Packet-filter 'test' Config>
```

このプロンプトから、**add**、**list**、 **move**、および **delete** コマンドを出すことができます。これらのコマンドは、グローバル・アクセス制御リストを修正するのに使用されるコマンドに似ています。

アクセス制御規則のパラメーター

アクセス制御規則は、複数のパラメーターで構成されます。 すべてのアクセス制御規則に指定できるパラメーターもあれば、パケット・フィルターの規則にしか指定できないものもあります。 次のパラメーターは、すべてのアクセス制御規則に指定できます。

- Type (inclusive, exclusive)
- IP source address and mask
- IP destination address and mask
- IP protocol number range
- TCP/UDP destination port number range
- TCP/UDP source port number range
- TCP SYN filtering
- ICMP message type and code
- Precedence and TOS filtering support
- Policy-based routing (ネクスト・ホップ・ゲートウェイの選択)
- Security logging options

次のパラメーターは、パケット・フィルターにのみ指定できます。

- Packet filter name
- Source address verification
- Additional types: IP security (IPsec) and network address translation (NAT)
- IPsec tunnel ID

Type

アクセス制御規則のタイプにより、その規則に一致するパケットに対して規則が行うことを定義します。*exclusive* (E) 規則はパケットを廃棄します。 *inclusive* (I) 規則では、パケットをルーターがさらに処理することができます。 *network address translation* つまり NAT (N) 規則は、アドレス変換を行うためにパケットを NAT に引き渡します。出力パケット・フィルター内に *IP security* つまり IPsec (S) 規則があると、パケットは、IPsec トンネル内でのカプセル化および場合によって暗号化を行うために IPsec に引き渡され、入力パケット・フィルター内に IPsec 規則があると、パケットが正しい IPsec トンネルを通じて受信されたか確認されます。NAT および IPsec 規則は、パケット・フィルターでのみ、しかも inclusive (組み込み) (IN または IS) と組み合わせて指定された場合にのみ有効です。構成プログラムでは、Inclusive を指定してから、NAT および IPsec を指定する必要があります。

また、NAT と IPsec を、同じ規則 (INS) 内に指定することができます。出力パケット・フィルター内に INS 規則があると、一致するパケットは、最初に NAT によって処理され、次に IPsec によって処理されます。入力パケット・フィルター内に INS

規則があると、一致するパケットが正しい IPsec トンネルを通じて受信されたかどうかが最初に検査され、次に、それらのパケットは NAT によって処理されます。

IP Source and Destination Addresses

各規則は、IP 発信元とあて先の両方の IP アドレスについて IP アドレスとマスクのペアをもっています。IP パケットがアクセス制御規則と比較される場合、パケット内の IP アドレスは規則内のマスクと AND を取られ、結果が規則内のアドレスと比較されます。例えば、アクセス制御規則内の発信元アドレス 26.0.0.0 (マスクが 255.0.0.0) は、最初のバイトが 26 である任意の IP 発信元アドレスに一致します。192.67.67.20 のあて先アドレスおよび 255.255.255.255 のマスクは、IP あて先ホスト・アドレス 192.67.67.20 にのみ一致します。マスクが 0.0.0.0 で 0.0.0.0 のアドレスはワイルドカードであり、任意の IP アドレスに一致します。

IP Protocol Number

各レコードは IP プロトコル番号の範囲ももつことができます。この範囲は IP ヘッダー内のプロトコル・バイトと比較されます。アクセス制御規則によって指定された範囲内のプロトコル値が一致します (範囲の最初と最後の番号を含む)。0 〜 255 の範囲を指定する場合、どのプロトコルも一致します。一般的に使用されるプロトコル番号は 1 (ICMP)、6 (TCP)、17 (UDP)、および 89 (OSPF) です。

TCP/UDP Source and Destination Port Numbers

IP プロトコル番号の範囲に 6 (TCP) または 17 (UDP) が含まれていれば、発信元およびあて先の両方のポートについて、TCP/UDP ポート番号の範囲もアクセス制御規則に指定できます。 これらの範囲は、IP パケットの TCP または UDP ヘッダー内のポート番号フィールドと比較されます。指定された範囲 (最初と最後の番号を含む) 内のポート番号値が一致します。 TCP または UDP パケットでない IP パケットの場合、これらのフィールドは無視されます。 0 〜 65535 の範囲を指定する場合は、どのポート番号も一致します。 一般的に使用されるポート番号は 21 (FTP)、23 (Telnet)、25 (SMTP)、513 (rlogin) および 520 (RIP) です。 IP プロトコルおよびポート番号については、RFC 1700 (割り当てられた番号) を参照してください。

TCP Connection Establishment (SYN) Filtering

プロトコル番号の範囲に 6 (TCP の場合) が含まれており、フィルター・タイプが exclusive (排除) である場合は、TCP 接続確立フィルターを設定できます。TCP 接続確立フィルターが使用可能になっていると、アクセス制御規則は、そのパケットが TCP 接続を確立した場合にのみ TCP パケットに適用されます。 (これらは、TCP SYN ビットが 1 で、ACK ビットが 0 になっているパケットです。)

ICMP Message Type and Code

プロトコル番号の範囲に 1 (ICMP を表す) が含まれていれば、 ICMP message type and code が指定できます。省略時解釈では、すべての ICMP message types and code にアクセス制御規則が適用されます。

Precedence and TOS Filtering Support

TOS をサポートするルーターでは、要求されたレベルのサービスを提供する特定のルートが識別されています。ルーターは、ルートの TOS ビットの設定に応じて、これらのルートを通してパケットを送信します。

IP 内の TOS は、特定のサービス・タイプを保証するものではなく、ルーターに対して要求されたタイプのサービスの提供を要求するものです。例えば、 TOS フィールドで最大スループットを要求しているパケットの場合は、帯域幅が異なる幾つかのホップを通して送信できます。TOS をサポートしないルーターの管理下にあるホップを通過する必要がある場合は、特殊な扱いではなく、通常のサービスを得ることになります。これらのパラメーターの説明については、 266 ページの **add access-controls** コマンドを参照してください。

また、帯域幅予約システム (BRS) フィーチャーを使用して、フィルターを設定し、TOS に基づく QOS を提供することもできます。BRS は、PPP インターフェースとフレーム・リレー・インターフェースで使用されます。 *フィーチャーの使用と構成* の『帯域幅予約と優先待ち行列の使用』 と 『帯域幅の構成と監視』 を参照してください。

TOS に基づくルーティング・サポートに関するパラメーター: ルーターが TOS ビットを変換処理し、それに応じてパケットのルーティングを行えるようにするために、ルーターが TOS パケットを受信して、フィルター処理とサービス・タイプ・ルーティングを行うアクセス制御規則を作成します。こうして作成したアクセス制御規則は、ルーター上のすべてのインターフェースに適用されます。次のパラメーターを使用して、ルーターが比較する TOS ビットを定義します。

- TOS バイトのビットの範囲開始値
- TOS バイトのビットの範囲終了値
- TOS バイト内で範囲に含まれるビットを判別するフィルター・マスク

TOS ビットの変更: ルーターが着信パケットの TOS ビットを変更できるようにするために、ルーターが変更の対象となる TOS パケットを受信するグローバル・アクセス制御規則を作成します。TOS ビットの値の変更は、その変換処理やパケットのルーティングとは別の活動です。変換処理と変更の両方が構成される場合は、変更が行われるのは変換処理の後になります。次のパラメーターを使用して、変更の対象となる TOS ビットを定義します。

- TOS ビットの新しい範囲
- TOS バイト内で変更の対象となるビットを判別する変更マスク

Policy-Based Routing (ネクスト・ホップ・ゲートウェイの選択)

インバウンド・パケットをフィルターして、手動で選択したネクスト・ホップ・ゲートウェイ・アドレスに送信 (ポリシーに基づくルーティングと呼ばれる) できます。この場合は、組み込みインバウンド・アクセス制御規則を、グローバルにルーターに関して作成するか、特定のインターフェースに関して作成し、次のパラメーターを用意します。

- ポリシーに基づくルーティングを使用するかどうか
- ネクスト・ホップ・ゲートウェイの IP アドレス

- ネクスト・ホップが使用不能の場合に、通常のルーティング・テーブルを使用してパケットを送信するかしないか

SysLog Facility Option

SysLog はログ・オプションの 1 つで、リモートのログ・サーバーへ SysLog メッセージを生成します。SysLog が使用可能になっていると、SysLog 機能オプションは、リモート・ログに使用される SysLog 機能を指定します。このオプション (省略時値は *User*) は、SysLog メッセージを格納し、後で分析できるリモート・ログ・ファイルを定義します。 SysLog 機能オプションは、構成プログラムとコマンド行インターフェースの両方で表示されます。

Security Logging Options

セキュリティー・ログを使用可能にすると、以下のログ・オプションをどれでも (またはすべて) 指定できます。

- ELS メッセージ
- SNMP トラップ
- SysLog

ELS メッセージおよび SysLog は、指定された場合、*short* または *long* のどちらかのメッセージ形式を使用できます。SNMP トラップは、*enabled (使用可能)* または *disabled (使用不能)* です。ログ・オプションが指定されない場合、セキュリティー・ログは使用不能です。

SysLog 優先順位も設定できます。*Emergency (非常用)* または *Information (通知)* など、表示されるエラー・メッセージのレベルを指定します。 省略時値は、ルーターのシステム省略時値です。 SysLog 優先順位のレベルは、構成プログラムとコマンド行インターフェースの両方で表示されます。

SysLog メッセージは、リモート・サーバーへ送信され、現行の SysLog 機構オプションの SysLog ファイルに保管されます。

Packet Filter Name

このインターフェース特定パラメーターは、任意の名前で構成できます。長さは最大 16 文字で、ダッシュ (-) および下線 (_) を含めることができます。各パケット・フィルター名に最大 2 つのアクセス制御レコード・リストを設定できます。1 つは発信パケット用で、もう 1 つは着信パケット用です。

Source Address Verification

この入力パケット・フィルター・オプションは、IP ルーティング・テーブルに基づいて、受信されたパケットの送信元 IP アドレスが送信元のインターフェースと矛盾していないか検査します。このオプションを選択すると、自分のものではない発信元 IP アドレスを使用している誤動作 IP ホストからパケットが転送されないようにすることができます。この誤動作は、スプーフィング と呼ばれます。

IPsec Tunnel ID

この数値パラメーターは、IPsec (タイプ S) アクセス制御規則でのみ有効です。出力パケット・フィルター内では、一致するパケットの送信に使用される IPsec トンネルの ID を指示します。入力パケット・フィルター内では、一致するパケットの受信に使用されるはずだった IPsec トンネルの ID を指示します。このトンネルから受信されなかった一致するパケットは廃棄されます。

例

次の例では、どのホストも 192.67.67.20 上の SMTP TCP ソケットにパケットを送信することができます。

```
add access-control inclusive 0.0.0.0 0.0.0.0 192.67.67.20 255.255.255.255 6 6 25 25
```

次の例では、クラス B のネットワーク 150.150.0.0 のサブネット 1 上のどのホストも、クラス B のネットワーク 150.150.0.0 のサブネット 2 上のホストにパケットを送信できません (1 バイトのサブネット・マスクを想定)。

```
add access-control exclusive 150.150.1.0 255.255.255.0 150.150.2.0 255.255.255.0 0 255 0 65535
```

このコマンドでは、ルーターはすべての RIP パケットを送信および受信できます。

```
add access-control inclusive 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 17 17 520 520
```

この例では、グローバル・アクセス制御規則の作成方法を示しています。値を入力して、IP アドレス 9.1.2.3 から到着するパケットの TOS ビットを変換処理し、パケットを送信する前にこれらのビットの値を変更します。TOS フィルターとポリシーに基づくルーティングを作成するパラメーターの意味の説明については、266ページの『Add』 を参照してください。

```
IP config> add access-control
Enter type [E]? i
Internet source [0.0.0.0]? 9.1.2.3
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Enter starting protocol number ([0] for all protocols) [0]?
Enter starting DESTINATION port number ([0] for all ports) [0]?
Enter starting SOURCE port number ([0] for all ports) [0]?
Filter on ICMP Type ([-1] for all types) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]? e0
TOS/Precedence start value (00-FF) [0]?
TOS/Precedence end value [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]? 1f
New TOS/Precedence value (00-FF) [0]? 08
Use policy-based routing? [No]: y
Next hop gateway address [ ]? 9.2.160.1
Use default route if next hop gateway unreachable? [Yes]:
Enable Logging (Yes or [No]):
```

ルート・フィルター

ルート・フィルターは、ルーティング・テーブルの内容に影響を与えることによりパケット転送に影響を及ぼします。 一般に、ルート・フィルターはアクセス制御より効率的ですが、柔軟性は劣ります。あて先 IP アドレス以外のパケット・フィールドに基づくフィルターは、上記のアクセス制御を使用しないと行えません。

このルーターでは、ルーティング・テーブルの内容に影響を与えるのに次の方式が使用されます。

- フィルター・ルート
- RIP 入力フィルター
- ルート・テーブル・フィルター

フィルター・ルートを定義する

ルーティング・テーブルに挿入すべき IP あて先は*フィルター・ルート* として示すことができます。IP パケットはこれらのあて先には転送されず、それらに関するルーティング情報は公示されません。ネットワークで OSPF が使用されているときはフィルター・ルートはお勧め ***しません***。OSPF によって学習された内部ルートが、ルーティング・テーブルでフィルターされたルートを上書きするからです。

フィルター・ルートを構成するには、IP config> プロンプトで次のコマンドを入力してください。

```
IP config>  add filter  dest-IP-address  address-mask
```

IP ルーティング・テーブルを表示するのに **dump** コマンドが使用されるときは、フィルター・ルートが、タイプ *fltr* をもつ項目としてリストされます。

注: より特定のルートが使用可能な場合は、パケットが転送されます。例えば、フィルター・ルートがネットワーク 9.0.0.0 (マスク 255.0.0.0) について定義されているが、ルートがネットワークのサブネット (例えば 9.1.0.0、マスク 255.255.0.0) について学習される場合には、パケットはサブネット 9.1.0.0 には転送されるが、そのネットワークの他のサブネットには転送されません。

RIP 入力フィルターを定義する

RIP が動的ルーティング・プロトコルとして使用される場合、RIP 更新内のルートを無視するために特定のインターフェースを構成することができます。

次のコマンドは、インターフェースで受信されたすべての RIP 更新を無視することになります。

```
IP config>  disable receiving rip  ip-interface-address
```

以下のコマンドは、インターフェースで受信された特定のタイプのルートを無視することになります。

```
IP config> disable receiving dynamic nets ip-interface-address
IP config> disable receiving dynamic subnets ip-interface-address
IP config> disable receiving dynamic host ip-interface-address
```

後者のグループのコマンドが使用される場合、次のコマンドを使用して特定のルートが受け入れられるようにすることができます。

```
IP config> add accept-rip-route ip-network/subnet/host
```

ルート・テーブル・フィルターを定義する

ルート・テーブル・フィルターが使用可能になっており、ルート・フィルターが定義されているときは、ルートを IP ルーティング・テーブルに追加する前に検査が実行されます。追加されるルートが組み込み(inclusive) ルート・フィルターに一致する場合には、IP ルート・テーブルに追加されます。追加されるルートが exclusive (排除)

ルート・フィルターに一致する場合には、IP ルート・テーブルには追加されません。直接および静的ルートは、フィルターされません。

この機能を使用して、ネットワーク管理者がルーティング・プロトコルによって公示されたすべてのルートを使用可能にしたくない場合に、ルートを IP ルート・テーブルに追加しないようにすることができます。この機能をサービス提供者環境で使用して、カスタマーが互いのネットワークにアクセスできないようにすることもできます。

BOOTP/DHCP 転送プロセスを構成する

BOOTP (RFC 951 および RFC 1542 に文書化されています) は、ディスクのないワークステーションがその IP アドレス、そのブート・ファイルのロケーション、およびブート・サーバー名を学習するために使用するブートストラップ・プロトコルです。 RFC 1541 に文書化されている動的ホスト構成プロトコル (DHCP) は、再使用可能なネットワーク・アドレスおよびサーバーからのホスト固有構成パラメーターを割り振るために使用されます。

BOOTP/DHCP 転送プロセスを論じるには、次の用語が役に立ちます。

- クライアント - BOOTP/DHCP サービスを必要とするワークステーション
- サーバー - ブート・ホスト (UNIX デーモンが bootp され、 DOS バージョンは FTP ソフトウェアから使用可能、または OS/2) またはこれらのサービスを提供する他の BOOTP/DHCP サーバー。このルーターはサーバー・サポートを提供しません。
- *BOOTP リレー・エージェント* または *BOOTP 転送者* - クライアントおよびサーバーによって交換される要求/応答を転送する装置。このルーターはリレー・エージェント機能をサポートします。

以下のステップでは、BOOTP 転送プロセスの例を概説します。 (DHCP 交換は同様の方法で進行します):

1. クライアントはそのイーサネット・アドレス (または該当する MAC アドレス) を BOOTP パケットにコピーし、それをローカル LAN に同報通信します。BOOTP は UDP 最上位で稼働します。
2. ローカル BOOTP リレー・エージェントはパケットを受信し、パケットが正しくフォーマットされているかどうか、アプリケーション・ホップの最大数になっていないかを調べます。クライアントの試行が十分に長いかも調べます。

   注: BOOTP エージェントに到達するのに複数のホップが必要な場合は、パケットは正常に、IP を介してルートされます。他のすべてのルーターでは、パケットを調べてそれが BOOTP パケットであるかどうか判別することはしません。
3. ローカル BOOTP エージェントはその構成済みのサーバーのそれぞれに別個の BOOTP 要求を転送します。BOOTP 要求はクライアントが最初に送信した要求と同様ですが、異なる点は、BOOTP 要求の本体にリレー・エージェントの IP アドレスが複写されて新しい IP ヘッダーが付いていることです。
4. サーバーは要求を受信し、そのデータベース内のクライアントのハードウェア (例えば、イーサネット) アドレスを調べます。見つかった場合は、サーバーはクライ

アントの IP アドレス、そのブート・ファイル、およびブート・サーバー名を含む BOOTP 応答をフォーマットします。次に応答が BOOTP リレー・エージェントに送信されます。

5. BOOTP リレー・エージェントは応答を受信し、その ARP テーブルにクライアント用の項目を作成してから、応答をクライアントに転送します。
6. クライアントは次に TFTP を使用し、BOOTP 応答パケット内の情報を使用してブートを継続します。

BOOTP 転送を使用可能/使用不能にする

ルーターで BOOTP 転送を使用可能または使用不能にするには、IP 構成プロンプトで次のコマンドを入力してください。(BOOTP 転送を使用可能にし、ルーターが BOOTP または DHCP あるいはその両方の要求および応答をネットワークの異なるセグメント上にあるクライアントおよびサーバーの間で転送できるようにします。)

```
IP config> enable/disable bootp
```

BOOTP が使用可能になっている場合は、次の値を入力するようプロンプト指示されます。

- BOOTP 要求を到達させるためのアプリケーション・ホップの最大数。これは、パケットを転送できる BOOTP リレー・エージェントの最大数です。これはサーバーへの IP ホップの最大数では***ありません***。このパラメーターの典型的な値は 1 です。
- BOOTP 要求が転送される前にクライアントに再試行させたい秒数。このパラメーターは*普通使用されません*。 このパラメーターの典型的な値は 0 です。

BOOTP 要求を受信した後、ルーターはその BOOTP 要求を各 BOOTP サーバーに転送します。BOOTP 用に構成されたサーバーが複数ある場合、ルーターがパケットを複写します。

BOOTP/DHCP サーバーを構成する

ルーターの構成に BOOTP または DHCP サーバーを追加するには、IP 構成プロンプトで次のコマンドを入力してください。

```
IP config> add bootp-server server-IP-address
```

複数のサーバーを構成できます。さらに、サーバーのネットワーク番号のみが分かっている場合、または複数のサーバーが同じネットワーク・セグメントにある場合は、サーバーに同報アドレスを構成できます。

IP と SNA の統合

TN3270E を使用して IP と SNA を統合できます。TN3270E について詳しくは、 *プロトコルの構成と監視 解説書 第 2 巻* の中の 『APPN の使用』 の章と *プロトコルの構成と監視 解説書 第 2 巻* の中の 『APPN の構成と監視』 の章を参照してください。

UDP 転送を構成する

RFC 768 に文書化されているユーザー・データグラム・プロトコル (UDP) は、インターネット・プロトコル を使用して無接続サービスを提供するトランスポート・レイヤーです。 UDP 転送では、ローカルで送達された UDP パケット (IBM 2210 接続 LAN 上の UDP 同報通信など) が、特定の IP あて先やあて先ネットワークに指定同報通信として転送できます。

例えば、NetBIOS は一部のクライアント/サーバー・アプリケーションで UDP 同報通信を使用して、名前照会パケットを同報通信します。UDP 転送をセットアップしない限り、ルーターはこれらのパケットを除去します。したがって、ルーターはローカル・ネットワークを越えてパケットを転送することはしません。

UDP 転送を構成するには、以下のステップに従ってください。

1. UDP あて先ポート番号および IP アドレスを追加します。ルーターはこの IP アドレスを UDP ポートにマップします。

```
IP config> add udp-destination
UDP port number [-1] 36
Destination IP address [0.0.0.0] 20.1.2.2
```

2. UDP 転送を使用可能にします。

```
IP config>enable udp-forwarding
For which UDP port number [-1] 36
```

上の例で、ルーターはそれが UDP ポート 36 について受信したパケットを IP アドレス 20.1.2.2 に転送します。

UDP 転送構成を表示するには、**list udp-forwarding** を入力します。

UDP 転送を使用可能/使用不能にする

ルーターで UDP 転送を使用可能または使用不能にするには、IP 構成プロンプトで次のコマンドを入力してください。(UDP 転送を使用可能にし、ルーターが各 UDP ポートごとに UDP 同報通信パケットを所定のアドレスに転送できるようにします。)

```
IP config> enable/disable udp-forwarding port-number
```

UDP あて先を追加する

パケットを転送する先の IP アドレスに続けてポート番号を指定することにより、UDP 転送あて先を追加します。UDP あて先を追加するには、IP 構成プロンプトで次のコマンドを入力します。

```
IP config> add udp-destination port-number dest-ip-address
```

バーチャル・ルーター冗長プロトコル (VRRP) を構成する

静的に構成された省略時ルートは、ホスト IP 構成によく使用されます。この場合、構成と処理オーバーヘッドが最小化されるため、事実上すべての IP インプリメンテーションでサポートされます。この操作モードは、通常、エンド・ホスト IP アドレスや省略時ゲートウェイに構成を提供する動的ホスト構成プロトコルが配置されている場合と似ています。しかし、この場合には、単一障害点が作成されます。省略

時ルートがないと、不連続的事象が発生し、使用可能であると考えられる代替パスをまったく検出できないエンド・ホストがすべて分離されます。

バーチャル・ルーター冗長プロトコル (VRRP) は、静的省略時ルーティング環境に固有の単一障害点を除外するよう設計されています。 VRRP は、ルーターの集合が互いにバックアップすることを動的に許可する選定プロトコルを指定します。1 つまたは複数の IP アドレスを制御する VRRP ルーターはマスター・ルーターと呼ばれ、送信されたパケットを、これらの IP アドレスに転送します。マスターが使用不能になった場合には、選定プロセスにより、転送責任における動的フェールオーバーが提供されます。そうすると、バーチャル・ルーター上の IP アドレスはどれも、エンド・ホストが省略時の最初のホップ・ルーターとして使用できます。VRRP を使用することによって得られる利点は、すべてのエンド・ホスト上に動的ルーティングまたはルーター発見プロトコルの構成がなくても省略時パスの可用性が高くなることです。

VRRP の使用や構成を行うためには、まず最初に、VRRP を実行する各 LAN セグメント上でバーチャル・ルーター ID (VRID) を定義する必要があります。各 VRRP について、1 つのルーターが、LAN セグメント上のホスト用に構成された省略時 IP アドレスを所有します。このルーターは、そのアドレスについての ARP 要求に応答し、そのルーターが使用可能である限りパケットを転送します。LAN セグメント上の他のルーターを構成して、その IP アドレスを所有するルーターをバックアップすることができます。VRID は、ユニキャストまたはマルチキャスト MAC アドレスを暗黙指定します。バックアップ・ルーターが引き継ぐときの混乱を最小限に抑えるためには、共通の MAC アドレスが必要です。以下に、非常に単純な VRRP トポロジーの例を示します。

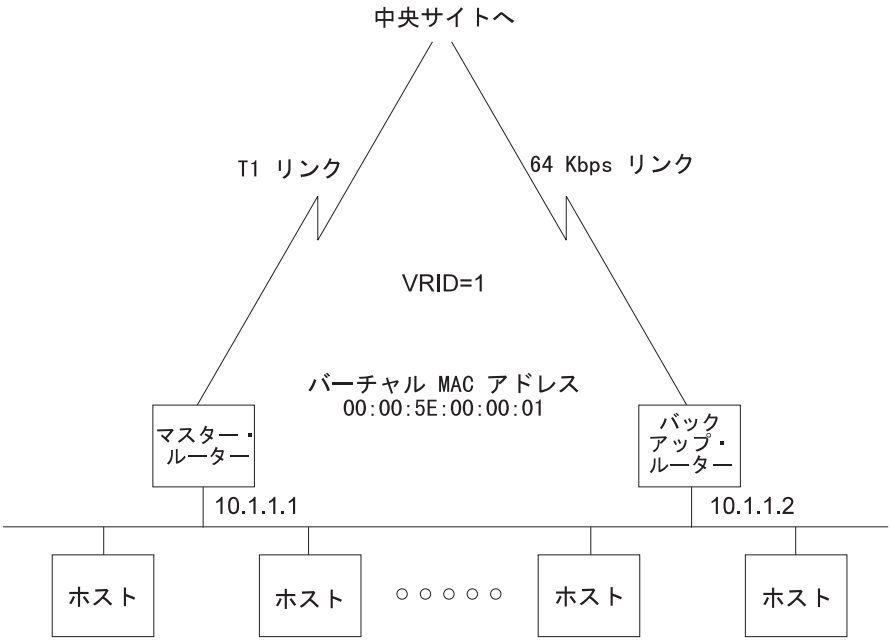


図 32. サブネット 10.1.1.0/255.255.255.0 をもつイーサネット LAN。すべてのホストは、省略時ゲートウェイ 10.1.1.1 で構成されている。

1. すべてのホストは、10.1.1.1 という省略時ゲートウェイで構成されています。

2. マスター・ルーターは、00:00:5E:00:00:01 というバーチャル MAC アドレスをもつ 10.1.1.1 についてのすべての ARP 要求に応答します。
3. マスター・ルーターは、このバーチャル MAC アドレスにアドレス指定されたパケットを転送します。
4. マスター・ルーターが使用可能でない場合、バックアップは、VRRP 公示がないことからこれを判別し、バーチャル MAC アドレスにアドレス指定されたパケットの受信を始めます。バックアップは、10.1.1.1 についての ARP 要求にも応答します。

複数の VRRP ルーターがある場合にはトポロジーが複雑なものとなるため、もう完全なバックアップ機能をもっていないルーター間での負荷の平衡を取る必要があります。この場合、2 つの VRID を定義する必要があり、各ルーターは、一方についてはマスター・ルーターで、他方についてはバックアップ・ルーターとなります。以下に、これを図で示します。

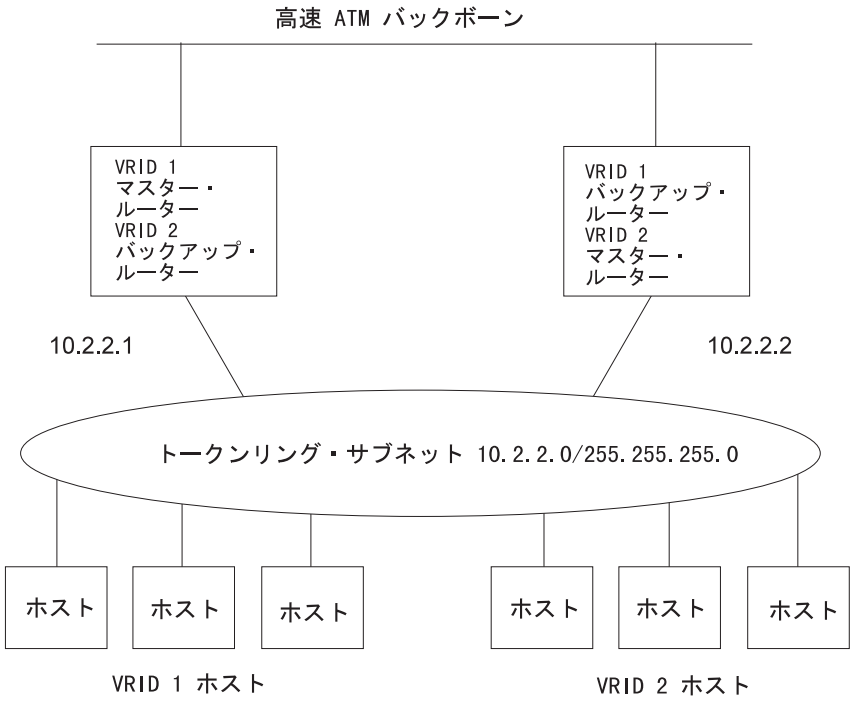


図 33. 複数の VRRP ルーター

1. VRID 1 ホストはすべて、10.2.2.1 という省略時ゲートウェイ・アドレスで構成されます。
2. VRID 2 ホストはすべて、10.2.2.2 という省略時ゲートウェイ・アドレスで構成されます。
3. VRID 1 マスター・ルーターは、バーチャル MAC アドレス C0:00:00:10:00:00 をもつアドレス 10.2.2.1 についての ARP 要求に応答します。このルーターは、バーチャル MAC アドレス C0:00:00:10:00:00 にアドレス指定されたパケットの受信と転送も行います。

4. VRID 2 マスター・ルーターは、バーチャル MAC アドレス C0:00:00:20:00:00 をもつアドレス 10.2.2.2 についての ARP 要求に応答します。このルーターは、バーチャル MAC アドレス C0:00:00:20:00:00 にアドレス指定されたパケットの受信と転送も行います。
5. どちらかのルーターが使用不能になると、もう一方のルーターが引き継ぎます。
6. ルーターが使用不能ではないが、その外側の接続性を失った場合は、ICMP リダイレクトを使ってもう一方のルーターを介してトラフィックを再転送します (この場合、2 つのルーターは、RIP または OSPF などのルーティング・プロトコルによりルートを交換しているものと想定します)。

VRRP は、イーサネット、高速イーサネット、トークンリングでサポートされます。

ソース・ルーティングされた LAN がブリッジされたネットワークの一部であるとき、そのブリッジ・ネットワークではマルチキャスト VRRP はサポートされません。 制限は、ブリッジ・ネットワーク上に IP が構成されている接続形態でしか適用できないことです。

冗長省略時 IP ゲートウェイを構成する

この節では、ELAN 上で冗長省略時 IP ゲートウェイを構成するのに使用されるステップについて概説します。冗長ゲートウェイを構成すると、手動により構成された省略時ゲートウェイをもつエンド・ステーションは、それぞれの 基本ゲートウェイで障害が発生した後で他のサブネットへのトラフィックの引き渡しを続行することができます。

基本ゲートウェイまたはバックアップ・ゲートウェイをもつ装置を構成するためには、次のように行います。

1. エンド・ステーションが省略時ゲートウェイとして使用する IP アドレスを判別します。
2. ELAN 上のどのインターフェースでも使用されていない MAC アドレスを判別します。使用される MAC アドレスの判別については、 *ソフトウェア 使用者の手引き* の「LAN エミュレーション・サービスの監視」の章の「データベース・リスト」の項を参照してください。
3. 基本ゲートウェイをもつ装置を選択します。この装置は、エンド・ステーションの ELAN 上に LEC インターフェースをもっているものでなければなりません。
4. バックアップ・ゲートウェイをもつ装置または装置の集合を選択します。この装置または装置の集合は、エンド・ステーションの ELAN 上に LEC インターフェースをもっているものでなければなりません。
5. IP について 『Add』 オプションを使用して、各装置上に冗長ゲートウェイを構成します。

IP マルチキャスト・サポート

IP マルチキャストは、TCP/IP インターネットへの LAN マルチキャストの拡張です。これは、IP ホストが複数のあて先に送達される単一のデータグラム (IP マルチキャスト・データグラムと呼ばれます) を送信する能力です。IP マルチキャスト・データグラムは、そのあて先がクラス D IP アドレスである (つまり、その最初のバイトが 224 ～ 239 の範囲にある) パケットとして識別されます。各クラス D アドレスごとにマルチキャスト・グループを定義します。

IP ホストが IP マルチキャストに参加するのに必要な拡張は、RFC 1112 (IP マルチキャスト用のホスト拡張) で 指定されます。この文書は、ホストがマルチキャスト・グループを動的に結合し、分離することを使用可能にするプロトコルである、インターネット・グループ管理プロトコル (IGMP) を定義します。このルーターは、IGMP プロトコル機能を実施します。これらの機能は、IGMP ホスト・メンバーシップ照会を送信し、IGMP ホスト・メンバーシップ報告を受信することにより、そのローカル物理 LAN およびそのエミュレートされた LAN 上でルーターが IP グループ・メンバーシップを追跡することを使用可能にします。

また、ルーターは発信元および (複数の) あて先ホストの間で IP マルチキャスト・データグラムをルートすることができることも必要です。このルーターは、RFC 1584 (OSPF のマルチキャスト拡張) に定義されるマルチキャスト最短パス最優先オープン (MOSPF) プロトコル、および距離ベクトル・マルチキャスト・ルーティング・プロトコル (DVMRP) をサポートします。

MOSPF ルーターは、新しいタイプのリンク状態公示であるグループ・メンバーシップ LSA (タイプ 6) を伝送することによって、ルーティング・ドメイン全体にグループ・ロケーション情報を配布します。これにより、MOSPF ルーターはマルチキャスト・データグラムをその複数のあて先に最も効率的に転送することが可能になります。つまり、各ルーターは、マルチキャスト・データグラムのパスを、その根がデータグラム発信元で、その末端の枝がグループ・メンバーを含む LAN であるツリーとして計算します。詳しくは、336ページの『マルチキャスト OSPF』を参照してください。

DVMRP は、ルーティング情報プロトコル (RIP) から引き出されたマルチキャスト・ルーティング・プロトコルです。このルーターは、DVMRP 用のサポートを提供するので、MOSPF をサポートしていない他のルーティング・エンティティーとマルチキャスト・ルーティング情報を交換することができます。また、このルーターの DVMRP 実施により、DVMRP 情報を MOSPF が使えるネットワークを通じてとマルチキャストが使えない IP ネットワークを通じてトンネルすることができます。

また、このルーターでは、ルーター自体を 1 つまたは複数のマルチキャスト・グループのメンバーとして『登録する』 ことができます。マルチキャスト・グループのメンバーとして、ルーターはグループ・アドレスにアドレス指定された 『PING』 および SNMP 照会に応答します (1 つのコマンドを使用して複数のルーターを照会することもできます)。

そのほかに、装置の IP マルチキャスト・サポートを使用して、 DLSw グループを確立し、管理することができます。これにより、DLSw に必要とされる構成の量を減ります。詳細については、493ページの『第25章 DLSw フィーチャーの使用』を参照してください。

ルーターを IP マルチキャスト用に構成する

ルーターが IP マルチキャスト・グループ・メンバーシップを追跡し、マルチキャスト・データグラムを転送することができるようにするには、MOSPF、DVMRP、あるいは MOSPF と DVMRP の両方を使用可能にする必要があります。

DVMRP を使用可能にする

DVMRP を使用可能にするには:

1. ルーター上で DVMRP を使用可能にします。

```
DVMRP config> dvmrp on
```

2. どの LAN インターフェースで DVMRP が稼働するかを確立します。

```
DVMRP config> phyint
interface-address metric threshold
```

DVMRP がインターフェース上の唯一のマルチキャスト・ルーティング・プロトコルである場合、IGMP ポーリング間隔およびタイムアウトが設定され、変更することはできません。これらの値は、それぞれ 125 秒および 270 秒です。

これらのコマンドおよび、ルーター上で DVMRP と MOSPF の両方がアクティブであるときにこれらの間での対話を設定するために使用される他の構成コマンドについては、*プロトコルの構成と監視 解説書 第 2 巻* の『DVMRP の構成』を参照してください。

IP マルチキャスト・グループ内のルーターを登録する

ルーター自体が 1 つまたは複数のマルチキャスト・グループを結合する場合、次の join/leave コマンドが使用されます。

- **join multicast-group-address**
- **leave multicast-group-address**

これらの **join** コマンドおよび **leave** コマンドは、OSPF Config プロンプトおよび OSPF 監視プロンプトからアクセス可能です。これらのコマンドは、DVMRP 監視コンソールでも使用可能です。

これらのコマンドは、ルーターがその IP マルチキャスト転送機能または IGMP グループ追跡機能を実行するためには必要ありません。これらのコマンドは、ルーターをグループに追加して、これらのグループにアドレス指定される『PING』および SNMP 照会に応答できるようにするために使用されます。

第15章 IP の構成と監視

この章では、IP の構成と監視コマンドについて説明します。この章には次の節が含まれています。

- 『IP 構成環境にアクセスする』
- 『IP 構成コマンド』
- 316ページの『IP 監視環境へのアクセス』
- 317ページの『IP 監視コマンド』

IP 構成環境にアクセスする

IP 構成環境へアクセスするには、Config> プロンプトで次のコマンドを入力します。

```
Config> Protocol IP
Internet protocol user configuration
IP config>
```

IP 構成コマンド

この節では、IP 構成コマンドについて説明します。これらのコマンドを使用して、ユーザーの特定の要件に合うように IP プロトコルの動作を修正できます。完全に機能しうる IP ルーターを作成するには、ある程度の構成が必要です。IP 構成コマンドは、IP config> プロンプトに入力します。

表 18. IP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	IP 構成情報に追加します。インターフェース・アドレスをアクセス制御、フィルター、およびパケット・フィルターとともに追加することができます。
Change	**add** コマンドを用いて当初入力した情報を修正します。
Delete	**add** コマンドを用いて入力されていた IP 構成情報を削除します。
Disable	**enable** コマンドによってオンにされた特定の IP フィーチャーを使用不能にします。
Enable	ARP サブネット・ルーティング、UDP 転送、発信省略時値、指定同報通信、BOOTP、ならびに RIP 情報の送信と受信を制御するさまざまな RIP フラグなどの IP フィーチャーを使用可能にします。
List	IP 構成項目を表示します。
Move	アクセス制御レコードの配列を変更します。
Set	アクセス制御の使用や同報通信アドレスの形式など、 IP 構成モードを確立します。また、ルーターによって発信されたパケットの TTL (活動時間)、IP ルーティング・テーブルのサイズ、RIP インターフェース・メトリックなど、IP パラメーターも設定し、IGMP 構成パラメーターも設定もします。
Update	アクセス制御項目を割り当てるのに使用されます。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、構成に IP 情報を追加するのに使用します。

構文:

add

- accept-rip-route . . .
- access-control . . .
- address . . .
- bootp-server
- filter . . .
- packet-filter
- redundant-default-gateway
- route . . .
- route-table-filter
- udp-destination . . .
- vrid . . .
- vr-address . . .

accept-rip-route *IP-network/subnet*

インターフェースで入力 RIP フィルターが使用可能になっている場合に、インターフェースが RIP ルートを受け入れられるようにします。**list rip-routes-accept** コマンドを使用すると、すでに入力済みのネットワーク/サブネットのリストを印刷できます。RIP ルートの入力フィルターは IP インターフェースごとに使用可能にできます。これは、ネットワーク・レベルのルート (例えば、10.0.0.0 へのルート) について、サブネット・レベルのルート (例えば、128.185.0.0 へのルート) について、およびホスト・レベルのルート (例えば、128.185.123.28) について個別に行われます。IP インターフェースでルートの入力フィルターを使用可能にするには、**disable dynamic nets/subnets/host** コマンドを使用してください。

IP network/subnet

有効値: 任意の有効な IP アドレス

省略時値: なし

例:

```
add accept-rip-route 10.0.0.1
```

または

```
add accept-rip-route 10.0.0.1

Network number [0.0.0.0]? 10.0.0.0
```

access-control *type IP-source source-mask IP-dest dest-mask first-protocol last-protocol [first-dest-port last-dest-port first-source-port last-source-port] [tcp-syn] [icmp-type icmp-code]*

[tos-mask tos-range-low tos-range-high tos-mod-mask new-tos-value policy-based-routing next-hop-gateway use-default-route] [ipsec-tunnel-id] [log els snmp-trap syslog syslog-level]

IP config> プロンプトからこのコマンドを使用すると、グローバル・アクセス制御リストの末尾にアクセス制御項目が追加されます。Packet-filter '*packet-filter-name*' Config> プロンプトからこのコマンドを使用すると、パケット・フィルター・アクセス制御リストの末尾にアクセス制御項目が追加されます。アクセス制御により、アクセス制御規則に指定されたパケット値に基づいて、転送、除去、IP セキュリティーによる処理、またはネットワーク・アドレス変換による処理の対象となるパケットのカテゴリーを定義することができます。IP アクセス制御リストの長さおよび配列は、IP パケット転送側のパフォーマンスに影響します。

注: **add access-control** コマンドは、アクセス制御規則を構成しますが、アクセス制御を自動的に使用可能にするものではありません。**set access-control** コマンドおよび **enable packet-filter** コマンドを参照してください。パケット・フィルター用のアクセス制御を構成する場合は、**add packet-filter** コマンドおよび **update packet-filter** コマンドを参照してください。

type アクセス制御規則パラメーターに適合するパケットの扱い方を指示します。

- **E** Exclusive (排除)。適合するパケットは廃棄されます。
- **I** Inclusive (組み込み)。適合するパケットは、ルーターによりさらに処理されます。
- **N** ネットワーク・アドレス変換 (NAT)。適合するパケットは、アドレス変換のために NAT に引き渡されます。このタイプは、inclusive (組み込み) と組み合わせて指定された場合 (例えば、*IN*) に限り有効です。タイプ NAT と IPsec は、同じ規則に指定できます (例えば、*INS*)。このパラメーターは、パケット・フィルター構成コンソール (**update packet-filter** コマンドでアクセスします) でのみ有効です。
- **S** IP セキュリティー (IPsec)。アウトバウンド・パケット・フィルター内で、適合するパケットは、IP 保護 (IPsec) トンネルでのカプセル化 (さらに、場合により暗号化) のために IPsec に引き渡されます。入力パケット・フィルターでは、適合するパケットが正しい IPsec トンネルを通じて受信されたかどうか検査されます。このタイプは、inclusive (組み込み) と組み合わせて指定された場合 (例えば、*IS*) に限り有効です。タイプ NAT と IPsec は、同じ規則に指定できます (例えば、*INS*)。このパラメーターは、パケット・フィルター構成コンソール (**update packet-filter** コマンドでアクセスします) でのみ有効です。

IP-source source-mask

発信元 IP アドレスおよびマスク。発信元マスクは、規則が発信元 IP アドレスの範囲に適合できるように、受信された発信元 IP アドレスとビット AND が取られます。発信元マスクのビットが 0 の場合は、IP 発信元アドレスの対応ビットも 0 でなければなりません。

有効値: 0.0.0.0 ～ 255.255.255.255

省略時値: 0.0.0.0 (発信元 IP アドレスの場合)。発信元マスクに関する省略時値は、構成済み IP 発信元アドレスです。

IP-dest dest-mask

あて先 IP アドレスおよびマスク。あて先マスクは、規則があて先 IP アドレスの範囲に適合できるように、受信されたあて先 IP アドレスとビット AND が取られます。あて先マスクのビットが 0 の場合は、あて先 IP アドレスの対応ビットも 0 でなければなりません。

有効値: 0.0.0.0 ～ 255.255.255.255

省略時値: 0.0.0.0 (あて先 IP アドレスの場合)。あて先マスクに関する省略時値は、構成済み IP あて先アドレスです。

first-protocol last-protocol

IP プロトコル番号の範囲

以下に、一般的な IP プロトコル番号をいくつか示します。

ICMP の場合は 1

TCP の場合は 6

UDP の場合は 17

OSPF の場合は 87

有効値: 0 ～ 255

省略時値: 最初のプロトコルについては 0、最後のプロトコルについては 255

first-dest-port last-dest-port

TCP/UDP あて先ポート番号の範囲。これらのパラメーターが有効なのは、IP プロトコル番号の範囲に 6 (TCP を表す) か 17 (UDP を表す) が含まれている場合だけです。これらのパラメーターは、IP プロトコル番号が 6 または 17 でないパケットについては無視されます。

以下に、一般的に使用されるポート番号をいくつか示します。

FTP の場合は 21

Telnet の場合は 23

SMTP の場合は 25

rlogin の場合は 513

RIP の場合は 520

有効値: 0 ～ 65535

省略時値: 最初のあて先ポートについては 0、最後のあて先ポートについては 65535

first-source-port last-source-port

TCP/UDP 発信元ポート番号の範囲。これらのパラメーターが有効なのは、IP プロトコル番号の範囲に 6 (TCP を表す) か 17 (UDP を表す) が含まれている場合だけです。これらのパラメーターは、IP プロトコル番号が 6 または 17 でないパケットについては無視されま

す。 一般的に使用される TCP/UDP ポート番号については、*first-dest-port last-dest-port* の説明を参照してください。

有効値: 0 ～ 65535

省略時値: 最初の発信元ポートについては 0、最後の発信元ポートについては 65535

tcp-syn

これらのパラメーターは、TCP 接続を確立する TCP パケット (つまり、SYN ビットが 1 で、ACK ビットが 0 の TCP パケット) に適合します。このパラメーターは、IP プロトコル番号の範囲に 6 (TCP の場合) が含まれており、規則タイプが exclusive (排除) の場合に限り有効です。このパラメーターは、タイプ IPsec および NAT (これらは、常に inclusive (組み込み) です) に有効です。このパラメーターは、IP プロトコル番号が 6 でないパケットについては無視されます。

有効値: Yes または No

省略時値: No

icmp-type

このパラメーター (ICMP タイプを定義する) が有効なのは、 IP プロトコル番号の範囲に 1 (ICMP を表す) が含まれている場合だけです。このパラメーターの値は、アクセス規則の ICMP タイプを定義します。 ICMP パケットは、パケットの ICMP タイプがアクセス規則の ICMP タイプに一致する場合に限りアクセス規則に適合できます。省略時値 -1 が指定された場合には、すべての ICMP タイプ値がアクセス規則に適合するものとして扱われます。 このパラメーターは、IP プロトコル番号が 1 でないパケットについては無視されます。

有効値: -1 ～ 255

省略時値: -1 (すべての ICMP タイプ)

icmp-code

このパラメーター (ICMP コードを定義する) が有効なのは、 IP プロトコル番号の範囲に 1 (ICMP を表す) が含まれている場合だけです。このパラメーターの値は、アクセス規則の ICMP コードを定義します。 ICMP パケットは、パケットの ICMP コードがアクセス規則の ICMP コードに一致する場合に限りアクセス規則に適合できます。省略時値 -1 が指定された場合には、すべての ICMP コード値が適合するものとして扱われます。 このパラメーターは、IP プロトコル番号が 1 でないパケットについては無視されます。

有効値: -1 ～ 255

省略時値: -1 (すべての ICMP コード)

tos-mask、tos-range-low、tos-range-high

tos-mask をゼロ以外の値に設定すると、TOS バイト内のビットに応じてフィルター処理ができます。*Tos-mask* では、優先/TOS バイト内でフィルター処理の対象になるビットを識別します。例えば、 *tos-mask*

が X'E0' (B'11100000') であれば、フィルター処理の対象になるのは、TOS バイト内の 3 つの優先ビット (TOS バイトの 3 つの最上位ビット) だけです。

tos-range-low と *tos-range-high* では、選択されたビット内の連続した値の範囲を定義します。優先ビットの 8 つの値 (10 進数 0 ～ 7) すべてをフィルター処理したい場合は、 *tos-range-low* は X'00' (B'00000000') で、 *tos-range-high* は X'e0' (フィルター処理の対象として選択された 3 ビット内の 10 進数 7 を定義する B'11100000') です。フィルター処理したいのが 3 つの優先ビットの 2 進数値 B'000'、B'001'、 B'010'、B'011' (10 進 0 ～ 3) の場合は、 *tos-range-low* は X'00' (B'00000000') で、 *tos-range-high* は X'60' (B'01100000') です。

フィルター処理したいビット・パターンが連続した順序の値でない場合は、フィルター処理したい値の範囲ごとに、それぞれ別のアクセス制御規則を定義する必要があります。例えば、2 つの優先ビット値 B'001' (10 進数 1) と B'011' (10 進数 3) をフィルター処理し、B'010' (10 進数 2) はフィルター処理しない場合は、*tos-mask* は X'e0' に等しく、 *tos-range-low* と *tos-range-high* は両方とも X'20' に等しいとして、最初のアクセス制御規則を定義する必要があります。次に、 *tos-mask* は X'e0' に等しく、*tos-range-low* と *tos-range-high* は両方とも X'60' に等しいとして、2 番目のアクセス制御規則を定義する必要があります。

tos-mask **の有効値**: X'00' ～ X'FF'

省略時値: 0 (なしを表す)

tos-range-low **の有効値**: X'00' ～ X'FF'

省略時値: 0

tos-range-high **の有効値**: X'00' ～ X'FF'

省略時値: 構成済みの *tos-range-low*

new-tos-value、tos-mod-mask

これらのパラメーターを設定すると、TOS バイト内の指定ビットを変更できます。*tos-mod-mask* では、TOS バイト内の変更したいビットを識別します。*new-tos-value* では、選択されたビットの新しい値を定義します。例えば、*tos-mod-mask* が X'1e' で、 *new-tos-value* が X'00' であれば、TOS フィールドの 4 つのビット (バイト内で *tos-mod-mask* 値 X'1e' [B'00011110'] で識別) は、B'0000' に設定されます。 TOS ビットを最大スループットの値 (B'0100') に設定する場合は、*tos-mod-mask* X'1e' と *new-tos-value* X'08' (B'00001000') を使用します。

tos-mod-mask **の有効値**: X'00' ～ X'FF'

省略時値: 0 (なしを表す)

new-tos-value **の有効値**: X'00' ～ X'FF'

省略時値: 0

policy-based-routing、next-hop-gateway、use-default-route

これらのパラメーターでは、フィルター処理後のパケットの送信先

となるネクスト・ホップ・ゲートウェイを指定できる機能である、ポリシーに基づくルーティングができます。*policy-based-routing* パラメーターを Yes に設定すると、フィルター処理後のパケットの送信先を定義済みネクスト・ホップ・ゲートウェイにする計画であることを示します。*Next-hop-gateway* は、このようなパケットの送信先となるネクスト・ホップ・ゲートウェイのアドレスです。

use-default-route を Yes に設定すると、定義済みゲートウェイが使用不能になった場合に、ルーターは通常のルーティング・テーブルを使用して、パケットのルートを指定できます。このパラメーターが No に設定されていると、定義済みゲートウェイが使用不能になった場合は、パケットが廃棄され、 ICMP *到達不能* メッセージが廃棄されたパケットの発信元アドレスに送信されます。

policy-based-routing **の有効値**: Yes または No

省略時値: No

next-hop-gateway **の有効値**: 有効な IP アドレス

省略時値: なし

use-default-route **の有効値**: Yes または No

省略時値: Yes

IPsec-tunnel-ID

このパラメーターは、規則タイプが IPsec の場合にのみ有効です。出力パケット・フィルターでは、このパラメーターは、パケットの送信に使用される IP 保護 (IPsec) トンネルを指定します。入力パケット・フィルターでは、このパラメーターは、パケットの受信に使用される IPsec トンネルを指定します。 このパラメーターは、パケット・フィルター構成コンソール (**update packet-filter** コマンドでアクセスします) でのみ有効です。

有効値 1 ～ 65535

省略時値: 1

log ログを使用可能にします。

有効値: Yes または No

省略時値: No

els ログが使用可能な場合に、このアクセス制御規則について ELS メッセージを使用可能にします。

有効値: No、short、または long

省略時値: No

snmp-trap

ログが使用可能な場合に、このアクセス制御規則について SNMP トラップの送信を使用可能にします。

有効値: Yes または No

省略時値: No

syslog

ログが使用可能な場合に、このアクセス制御規則について SysLog を使用可能にします。 SysLog は、接続されているリモート・ワークステーションにシステム・メッセージを通知します。

有効値: No、short、または long

省略時値: No

syslog-level

SysLog が使用可能な場合に、SysLog メッセージのレベルを指定します。

有効値: Sys Def、Emerg、Alert、Crit、Error、Warn、Notice、Info、または Debug

省略時値: ルーター・システムの省略時値

例:

```
IP config> add access-control
Enter type [E] I
Internet source [0.0.0.0]?
Source mask [0.0.0.0]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Enter starting protocol number ([CR] for all) [-1]?
Enter starting destination port number ([CR] for all) [-1]?
Enter starting source port number ([CR] for all) [-1]?
Enter ICMP Type ([CR] for all) [-1]? 3
Enter ICMP Code ([CR] for all) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]? CD
TOS/Precedence start value (00-FF) [0]?
TOS/Precedence end value [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]? FA
New TOS/Precedence value (00-FF) [0]?
Use policy-based routing? [No]: y
Next hop gateway address [ ]? 8.8.8.2
Use default route if next hop gateway unreachable? [Yes]:
Enable Logging? (Yes or [No]) : y
Enable ELS Messages? (N, S or L ) [N]?
Enable SNMP Trap (Y or N) : [N]? y
Enable SYSLOG (N, S or L) : [N]? l
SYSLOG Level? (Sys Def, Emerg, Alert, Crit, Error, Warn, Notice, Info or Debug): [sys]
IP config>
```

address *interface-number IP-address address-mask*

ルーターのハードウェア・ネットワーク・インターフェースの 1 つに IP アドレスを割り当てます。ハードウェア・ネットワーク・インターフェースは、少なくとも 1 つの IP アドレスをもつまでは、IP パケットを受信または送信しません。IP アドレスはそのサブネット・マスクとともに指定する必要があります。 例えば、アドレスがクラス B のネットワーク上にあり、サブネットに 3 番目のバイトを使用する場合、マスクは 255.255.255.0 となります。 該当するコマンド・インターフェース番号を入手するには、**list devices** コマンドを使用してください。シリアル回線はアドレスを必要としません。そのような回線は無番号と呼ばれます。ただし、**add address** コマンドを使用して、そのような回線を IP トラフィック用に使用可能にする必要はあります。その場合に使用されるアドレスは 0.0.0.*n* です。ここで、*n* は *インターフェース番号* です。

注: IP アドレスを 2210 のブリッジ・ネットワークに割り当てるためには、*interface number* に **bridge** を指定します。詳細については、238ページの『ブリッジ・ネットワーク・インターフェースへ IP アドレスを割り当てる』を参照してください。

IP アドレスはそのサブネット・マスクとともに指定する必要があります。 例えば、アドレスがクラス B のネットワーク上にあり、サブネットに 3 番目のバイトを使用する場合、マスクは 255.255.255.0 となります。 該当するオプション・インターフェース番号を入手するには、**List Devices** オプションを使用してください。

interface-number

有効値: 任意の定義済みインターフェース番号、または **bridge**

省略時値: なし

ip-address

有効値:

クラス A の範囲は、1.0.0.1 〜 126.255.255.254

クラス B の範囲は、128.0.0.1 〜 191.255.255.254

クラス C の範囲は、192.0.0.1 〜 223.255.255.254

無番号のシリアル回線インターフェースの場合は、0.0.0.n (ここで、*n* はインターフェース番号)

省略時値: なし

address mask

有効値: 0.0.0.0 〜 255.255.255.255

省略時値: なし

例: add address 0 128.185.123.22 255.255.255.0

bootp-server *server-IP-address*

BOOTP/DHCP サーバーを、ルーターが BOOTP/DHCP 要求を転送する着信先となるサーバーのリストに追加します。詳細については、256ページの『BOOTP/DHCP 転送プロセスを構成する』を参照してください。

server-IP-address

有効値: 任意の有効な Bootp サーバー IP アドレス

省略時値: なし

例: add bootp-server 128.185.123.22

filter *dest-IP-address address-mask*

フィルターすべき IP あて先を指定します。IP パケットはフィルターされたあて先に転送されることはなく、ルーティング情報がそのようなあて先に関して伝送されることもありません。フィルターされたあて先へのパケットは単に廃棄されます。フィルターされたあて先は、そのサブネット・マスクをもつ IP アドレスとして指定する必要があります。例えば、クラス B のネットワークのサブネットをフィルターする場合、サブネットに 3 番目のバイトを使用すると、マスクは 255.255.255.0 になります。フィルター・メカニズムを使用するのは、柔軟性はありませんが、 IP アクセス制御より効率的です。また、フィルターは、アクセス制御と異なり、IP ルーティング・プロトコルの操作に影響を及ぼします。フィルターされたネットワーク/サブネットは、OSPF ルーティング・プロトコルを使用して学習された場合は、指定変更されます。

このコマンドは即時に有効になります。コマンドを有効にするためにルーターをリブートする必要はありません。

dest-IP-address

有効値: 任意の有効な IP アドレス

省略時値: なし

address mask.

有効値: 0.0.0.0 ～ 255.255.255.255

省略時値: 0.0.0.0

例: add filter 127.0.0.0 255.0.0.0

packet-filter *filter-name type interface-number*

ルーターの構成内でパケット・フィルター・レコードを定義します。

filter-name

有効値: 任意の 16 文字の名前

この名前には、ダッシュ (-) および下線 (_) を含めることができます。

省略時値: なし

type *IN* は、トラフィックが着信するフィルター

OUT は、トラフィックが発信するフィルター

interface-number

有効値: 任意の定義済みインターフェース、あるいはブリッジング・ネットワーク・インターフェースの場合は **bridge**

省略時値: なし

例: add packet-filter

```
Packet-filter name [ ]? filt-1-0
Filter incoming or outgoing traffic? [IN]?
Which interface is this filter for [0]? 1
```

redundant-default-gateway *interface-number gateway-IP-address address-mask MAC-address primary-gateway*

冗長省略時ゲートウェイ IP アドレスを構成に追加します。

interface-number

ELAN 上の LEC インターフェースの正味の数を指定します。

有効値: LEC インターフェースの正味の数

省略時値: なし

gateway-IP-address

エンド・ステーションの省略時ゲートウェイを指定します。

有効値: 省略時ゲートウェイとして使用される IP アドレス

省略時値: 0.0.0.0

address-mask

IP アドレスのマスクを指定します。

有効値: 任意の有効な IP ネットマスク

省略時値: 0.0.0.0

MAC-address

有効値: ELAN 上の他のインターフェースが使用していない任意の有効 MAC アドレス

省略時値: 00.00.00.00.00.00

primary-gateway

ゲートウェイが基本ゲートウェイとして使用されるか、バックアップ・ゲートウェイとして使用されるかを指定します。

この照会は、この装置上のゲートウェイがネットワークの通常の動作時にアクティブとなる基本ゲートウェイであるのか、基本ゲートウェイが組み込まれている LEC インターフェースが作動可能でないときにアクティブとなるバックアップ・ゲートウェイであるのかを尋ねます。**Yes** と応答すると、基本ゲートウェイが構成されます。基本ゲートウェイは、ELAN ごとに 1 つだけです。

有効値 Yes または No

省略時値: No

例: add redundant-default-gateway

```
Which net is this redundant gateway for [0]? 1
IP address of gateway [0.0.0.0]? 9.67.205.1
Address mask [255.255.0.0]? 255.255.240.0
MAC address [00.00.00.00.00.00.]? 00.00.00.00.00.BA
Is this the primary gateway [No]? Yes or No
```

route *dest-addr dest-mask next-hop1 cost1 [next-hop2 cost2 [next-hop3 cost3 [next-hop4 cost4]]]*

1 〜 4 個の静的ルートを装置の IP 構成に追加します。特定のあて先についての動的ルーティング情報が入手できないときは、静的ルートが使用されます。

あて先は IP アドレス (*dest-addr*) およびアドレス・マスク (*dest-mask*) によって指定されます。あて先 IP アドレスがネットワーク・アドレスである場合は、あて先マスクはネットワーク・マスクでなければなりません。あて先 IP アドレスがサブネット・アドレスである場合は、あて先マスクはサブネット・マスクでなければなりません。最後に、あて先 IP アドレスがホスト・アドレスである場合は、あて先マスクはホスト・マスクである必要があります (これは、唯一の有効値が 255.255.255.255 であることを意味します)。あて先マスクは正確でなければなりません。正確でない場合は、その静的ルートは受け入れられません。

あて先へのルートは、次のホップの IP アドレス *(next-hop)*、およびパケットをあて先にルーティングするコスト *(cost)* によって指定されます。次のホップは、ルーターの直接接続されたインターフェースの 1 つと同じ (サブ) ネット上になければなりません。静的ルートは、OSPF を通じて学習されたルートによって常に指定変更されます。省略時には、静的ルートは RIP を通じて学習されたルートによっても指定変更されます。ただし、それは **enable/disable override static-routes** コマンドを使って変更することができます。このコマンドは即時に有効になります。コマンドを有効にするためにルーターをリブートする必要はありません。

dest-addr

有効値: 任意の有効な IP アドレス

省略時値: なし

dest-mask

有効値: 0.0.0.0 ～ 255.255.255.255

省略時値: なし

next-hop1, next-hop2, next-hop3, next-hop4

有効値: 任意の有効な IP アドレス

省略時値: なし

cost1, cost2, cost3, cost4

有効値: 0 ～ 255 の範囲内の任意の整数

省略時値: 1

例 :

```
IP config>
add route
IP destination []? 1.1.0.0
Address mask [255.0.0.0]? 255.255.0.0
Via gateway 1 at []? 10.1.1.1
Cost [1]? 1
Via gateway 2 at []?
IP config> add route 1.1.0.0 255.255.0.0
Via gateway 2 at []? 20.1.1.1
Cost [1]? 2
Via gateway 3 at []? 30.1.1.1
Cost [1]? 3
Via gateway 4 at []?
IP config> add route 2.2.0.0 255.255.0.0 10.2.2.2 1 20.2.2.2 2
IP config> list routes

route to 1.1.0.0        ,255.255.0.0     via 10.1.1.1        cost 1
                                         via 20.1.1.1        cost 2
                                         via 30.1.1.1        cost 3
route to 2.2.0.0        ,255.255.0.0     via 10.2.2.2        cost 1
                                         via 20.2.2.2        cost 2

IP config>
```

route-table-filter *destination mask [both | exact | more-specific] [exclusive | inclusive]*

指定されたルートのルート・テーブル・フィルターを追加します。**route-table-filtering** が使用可能であると、ルート・テーブル・フィルターは、IP ルート・テーブルに追加されるルートと突き合わせられます。ルート・テーブル・フィルターの順序は重要ではありません。指定された順序ではなく、最も明確な一致をもつルート・テーブル・フィルターが選ばれます。一致が見つからない場合、そのルートはルート・テーブルに追加されます。**exact** が指定された場合は、ルートのあて先およびマスクがルート・テーブル・フィルターのあて先およびマスクとまったく同じでないと、一致にはなりません。**more-specific** が指定された場合は、ルートのあて先およびマスクがルート・テーブル・フィルターのあて先およびマスクによって包含されている範囲の一部でなければなりません。**both** を指定すると、both と more-specific のスーパーセットとなります (つまり、一致は、exact と more-specific の両方の一致が見つかった場合に発生します)。ルート・テーブル・フィルターが**組み込み (include)** を指示する場合、ルートは IP ルート・テーブルに追加されます。ルート・テーブル・フィルターが**排除 (exclude)** を指示する場合は、ルートは IP ルート・テーブルに追加されません。静的および直接ルートは、IP ルート・テーブルから排除されません。

destination mask

有効値 任意の有効な IP マスク

省略時値 both exclude

udp-destination *port-number address*

UDP 転送あて先アドレスを追加します。指定されたあて先 UDP ポート番号をもつ受信された UDP データグラムは、指定の IP アドレスへ転送されます。

同報通信またはユニキャスト IP アドレスを入力することができます。

同じ UDP ポートに 2 つ以上の IP アドレスを追加するには、このコマンドを繰り返します。これにより、ルーターは IP アドレスのそれぞれに UDP データグラムを転送します。

port-number

有効値: 0 〜 65535

省略時値: なし

address

有効値: 任意の有効な IP アドレス

省略時値: なし

例:

```
add udp-destination 36 20.1.2.2
```

vrid *interface-ip-address vrid advertisement-interval backup-router backup-ip-address priority functional/group- mode authentication-type authentication-key*

LAN セグメント上の VRRP ルーターについてバーチャル・ルーター ID 定義を追加します。

interface-ip-address

この VRID が定義される IP インターフェースを指示します。

有効値: 任意の構成済み IP インターフェース

省略時値: なし

vrid バーチャル・ルーター識別子。*ip-interface-address* と *vrid* を組み合わせることにより、VRID は一意に定義されます。同じ *vrid* を複数の物理インターフェース上で使用することができます。

有効値: 1 〜 255

省略時値: なし

advertisement-interval

VRRP 公示間の間隔

有効値: 1 〜 255

省略時値: 1

backup-router

このルーターが、この VRID のマスター・ルーターであるか、バックアップ・ルーターであるかを指示します。

有効値: Yes または No

省略時値: No

backup-ip-address

この VRID のバックアップである最初の IP アドレスを指示します。複数のサブネットをサポートする LAN セグメントについて *add vr-address* コマンドを使用することにより、アドレスをさらに追加することができます。*backup-router* について **No** が設定されている場合は、該当しません。

有効値: 任意の有効な IP アドレス

省略時値: なし

priority

バックアップ・ルーターの VRRP 優先順位を指示します。バックアップ・ルーターが基本ルーターを引き継ぐ場合は、その VRRP 公示でこの優先順位を使用します。 *backup-router* について **No** が設定されている場合は、該当しません。 マスター・ルーターは、常に、255 という優先順位を公示します。

有効値: 1 〜 254

省略時値: 100

functional/group-mode

マルチキャスト MAC アドレスを VRID バーチャル MAC アドレスとして使用するかどうかを指示します。この VRID 用に構成されたすべてのルーターがこのパラメーターについて同じ値をもっていないと、VRRP は正しく機能しません。

有効値: Yes または No

省略時値: No

authentication-type

VRRP 公示に使用される認証のタイプを指示します。認証タイプの選択肢としては、1 (単純パスワードを示します) または 0 (認証が使用されないことを示します) があります。

有効値: none、simple

省略時値: なし

authentication-key

この VRID のパスワードを定義するパラメーター。パスワード認証が使用された場合は、正しい認証キーをもつパケットだけが受け入れられます。*authentication type* について *none* が指定されるか、あるいは省略時解釈が行われた場合には、*authentication key* は適用できません。

有効値: 任意の 1 〜 8 文字

省略時値: ヌル・ストリング

例: `add vrid`

```
IP config> add vrid
IP Interface [ ]? 153.2.2.25
VRID (1-255) [0]? 1
Advertisement Interval (1-255) [1]?
```

```
Backup Virtual Router? [No]:
Use Functional/Group Address? [No]:
Authentication Type (0 - None, 1 - Simple) [0]?
VRID 153.2.2.25/1 added successfully
```

vr-address *interface-ip-address vrid ip-address*

LAN セグメント上の VRRP ルーターについてバーチャル・ルーター ID 定義を追加します。構成済みのバーチャル・ルーター ID (VRID) 定義に 2 次アドレスを追加します。 2 次アドレスは、VRID の VRRP 公示に組み込まれます。 2 次アドレスは、複数の IP サブネットをサポートする物理 LAN 上で必要です。各アドレスは、そのサブネットの省略時ゲートウェイ・アドレスを指定します。ルーターがマスター・ルーターの場合、*add vr-address* コマンドを使用して追加されたアドレスが VRID の *ip-interface-address* と共に追加されます。ルーターがバックアップ・ルーターの場合、*add vr-address* コマンドを使用して追加されたアドレスが *backup-ip-address* と共に追加されます。

interface-ip-address

VRID の IP インターフェース

有効値: 任意の構成済み IP インターフェース

省略時値: なし

vrid バーチャル・ルーター識別子。*ip-interface-address* と *vrid* を組み合わせることにより、VRID は一意に定義されます。VRID が構成されていないと、その定義にアドレスを追加することはできません。

有効値: 1 〜 255

省略時値: なし

ip-address

VRID の VRRP 公示に組み込まれる追加の IP アドレス

有効値: 任意の IP アドレス

省略時値: なし

例: add vr-address

```
IP config>add vr-address
IP Interface [ ]? 153.2.2.25
Virtual Router ID (1-255) [0]? 1
Additional IP Address [ ]? 5.1.1.1
VRID 153.2.2.25/1 address 5.1.1.1 added successfully.
```

Change

change コマンドは、以前に **add** コマンドによって導入済みの IP 構成項目を変更するのに使用します。 **add** コマンドで項目を指定したのと同様に、通常、変更したい項目を指定する必要があります。

構文:

change access-control . . .
address . . .
route . . .

access-control *rule-number type IP-source source-mask IP-dest dest-mask first-protocol last-protocol [first-dest-port last-dest-port first-source-port last-source-port] [tcp-syn] [icmp-type*

icmp-code] [tos-mask tos-range-low tos-range-high tos-mod-mask new-tos-value policy-based-routing next-hop-gateway use-default-route] [ipsec-tunnel-id] [log els snmp-trap syslog syslog-level]

既存のグローバル・アクセス制御レコードを修正します。既存のすべてのレコードを表示して規則番号を入手するには、 **list access-control** コマンドを使用します。パラメーターの定義については、talk 6 **Add** コマンドを参照してください。

例 :

```
IP config> change access-control 2
Enter type [E]? i
Internet source [9.1.2.3]?
Source mask [255.255.255.255]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Enter starting protocol number [0]?
Enter starting DESTINATION port number [0]?
Enter starting SOURCE port number [0]?
Filter on ICMP Type [-1]?
TOS/Precedence filter mask [e0]?
TOS/Precedence start value [0]?
TOS/Precedence end value [0]?
TOS/Precedence modification mask [1f]? 1e
New TOS/Precedence value[0]? 08
Use policy-based routing? [Yes]:
Next hop gateway address [9.2.160.1]?
Use default route if next hop gateway unreachable? [Yes]:
Enable Logging [No]:
```

address *old-address new-address new-mask*

ルーターの IP インターフェース・アドレスの 1 つを修正します。各新規アドレスを新規アドレスのサブネット・マスクとともに指定する必要があります。このコマンドは、既存のアドレスのサブネット・マスクを変更するのにも使用できます。

有効な IP アドレスは、次のものです。

- クラス A の範囲は、1.0.0.1 ～ 126.255.255.254
- クラス B の範囲は、128.0.0.1 ～ 191.255.255.254
- クラス C の範囲は、192.0.0.1 ～ 223.255.255.254
- 無番号のシリアル回線インターフェースの場合は、0.0.0.n (ここで、n はインターフェース番号)

old-address

有効値: 現在構成済みの IP インターフェース・アドレス

省略時値: なし

new-address

有効値: 任意の有効な IP アドレス

省略時値: なし

new-mask

有効値: 0.0.0.0 ～ 255.255.255.255

省略時値: なし

例: change address 192.9.1.1 128.185.123.22 255.255.255.0

route *dest-addr dest-mask new-next-hop1 new-cost1 [new-next-hop2 new-cost2 [new-next-hop3 new-cost3 [new-next-hop4 new-cost4]]]*

指定されたあて先までの構成済みの静的ルートと関連付けられたネクスト・

ホップまたはコストのいずれかを修正します。このコマンドは即時に有効になります。コマンドを有効にするためにルーターをリブートする必要はありません。

dest-addr

有効値: 任意の有効な IP アドレス

省略時値: なし

dest-mask

有効値: 0.0.0.0 〜 255.255.255.255

省略時値: なし

new-next-hop1, new-next-hop2, new-next-hop3, new-next-hop4

有効値: 任意の有効な IP アドレス

省略時値: なし

new-cost1, new-cost2, new-cost3, new-cost4

有効値: 0 〜 255 の範囲内の任意の整数

省略時値: 1

例:

```
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.1.1.1        cost 1
                                         via 20.1.1.1        cost 2
                                         via 30.1.1.1        cost 3
route to 2.2.0.0        ,255.255.0.0     via 10.2.2.2        cost 1
                                         via 20.2.2.2        cost 2

IP config>change route
IP destination []? 1.1.0.0
Address mask [255.0.0.0]? 255.255.0.0
Via gateway 1 at [.10.1.1.1]? 10.10.10.1
Cost [1]? 10
Via gateway 2 at [20.1.1.1]? 20.20.20.1
Cost [2]? 20
Via gateway 3 at [30.1.1.1]? 30.30.30.1
Cost [3]? 30
Via gateway 4 at []? 40.40.40.1
Cost [1]? 40
IP config>change route 2.2.0.0 255.255.0.0 10.10.10.2 10
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.10.10.1      cost 10
                                         via 20.20.20.1      cost 20
                                         via 30.30.30.1      cost 30
                                         via 40.40.40.1      cost 40
route to 2.2.0.0        ,255.255.0.0     via 10.10.10.2      cost 10
```

Delete

delete コマンドは、**add** コマンドによって前に導入された IP 構成項目を削除するのに使用します。**add** コマンドで項目を指定したのと同様に、一般に、削除したい項目を指定する必要があります。

構文:

delete accept-rip-route . . .

access-control . . .

address . . .

bootp-server

default network/subnet-gateway . . .

filter . . .

packet-filter

redundant-default-gateway

route . . .

route-table-filter

udp-destination . . .

vrid . . .

vr-address . . .

accept-rip-route *net-number*

ネットワークのリストから RIP プロトコルが必ず受け入れるルートを除去します。

有効値: 受け入れられたネットワークのリストに含まれている任意の IP アドレス

省略時値: なし

例: delete accept-rip-route 10.0.0.0

access-control *rule-number*

グローバル・アクセス制御リストからアクセス制御規則の 1 つを削除します。

例: delete access-control 2

address *ip-interface-address*

ルーターの IP インターフェース・アドレスの 1 つを削除します。

有効値: 任意の有効な IP アドレス

省略時値: なし

例: delete address 128.185.123.22

bootp-server *server-IP-address*

IP 構成から BOOTP サーバーを除去します。

有効値: 任意の構成済み BOOTP サーバー IP アドレス

省略時値: 0.0.0.0

例: delete bootp-server 128.185.123.22

default network/subnet-gateway *[ip-network-address]*

指定したサブネットされたネットワークについて省略時のゲートウェイまたは省略時のサブネット・ゲートウェイのいずれかを削除します。

有効値: 任意の有効な IP アドレス

省略時値: 0.0.0.0

例: delete default subnet-gateway 128.185.0.0

filter *dest-addr dest-mask*

ルーターのフィルターされたネットワークの 1 つを削除します。このコマンドは即時に有効になります。コマンドを有効にするためにルーターをリブートする必要はありません。

dest-addr

有効値: 任意の有効な IP アドレス

省略時値: 0.0.0.0

dest-mask

有効値: 0.0.0.0 ～ 255.255.255.255

省略時値: なし

例: delete filter 127.0.0.0

```
            Address mask [0.0.0.0]?
255.0.0.0
```

packet-filter *filter-name*

ルーターの構成から指定されたパケット・フィルターを削除します。

有効値: 任意の 16 文字の名前

この名前には、ダッシュ (-) および下線 (_) を含めることができます。

省略時値: なし

例:

```
IP config> delete packet-filter pf-in-0
All access controls defined for 'pf-in-0' will also be deleted.
Are you sure you want to delete(Yes or [No]): y
Deleted
IP config>
```

redundant *interface-number*

LEC インターフェースから冗長 IP ゲートウェイを削除します。

interface-number

有効値: 冗長省略時 IP ゲートウェイをもつ LEC のインターフェース番号

省略時値: なし

例 :

```
Enter the Net number of Redundant Gateway to delete:? 1
Gateway deleted.
```

route *dest-addr dest-mask [delete-next-hop1 [delete-next-hop2 [delete-next-hop3 [delete-next-hop4]]]]*

装置の構成済みの静的ルートの 1 つを削除します。このコマンドは即時に有効になります。コマンドを有効にするためにルーターをリブートする必要はありません。

dest-addr

有効値: 任意の有効な IP アドレス

省略時値: なし

dest-mask

有効値 任意の有効な IP マスク

省略時値: なし

delete-next-hop

有効値: Yes または No

省略時値: No

例 :

```
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.10.10.1      cost 10
                                         via 20.20.20.1      cost 20
                                         via 30.30.30.1      cost 30
                                         via 40.40.40.1      cost 40
route to 2.2.0.0        ,255.255.0.0     via 10.10.10.1      cost 10

IP config>delete route 1.1.0.0 255.255.0.0
Delete gateway 10.10.10.1? [No]:
Delete gateway 20.20.20.1? [No]: y
Delete gateway 30.30.30.1? [No]:
Delete gateway 40.40.40.1? [No]: y
IP config>delete route 2.2.0.0 255.255.0.0
IP config>delete route 1.1.0.0 255.255.0.0 n y
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.10.10.1      cost 10

IP config>
```

route-table-filter *destination mask mask-definition[both | exact | more specific]*

add route-table-filter を使用して追加されたフィルターをルート・テーブル・フィルターから削除します。コマンドの拡張定義については、276 ページの『route-table-filter』 の項を参照してください。

destination

有効値 任意の有効な IP マスク

省略時値: なし

mask **有効値** 任意の有効な IP マスク

省略時値: なし

mask-definition

有効値 任意の有効な IP マスク

省略時値: なし

例: delete route-table-filter

```
IP config>delete route-table-filter
Route Filter IP address []? 7.0.0.0
Route Filter IP mask []? 255.0.0.0
Enter Match type (B, E, or M) [B]?
Enter Definition type (I or E) [E]?
Route filter deleted
IP config>
```

udp-destination *port-number address*

add udp-destination コマンドを使用して構成された UDP 転送あて先アドレスを削除します。その結果、指定のポートで受信された、ローカルで送達された UDP データグラムは、指定の IP アドレスには転送されません。

port-number

有効値: 0 ～ 65535 の範囲内の任意の整数

省略時値: なし

address

有効値: 任意の有効な IP アドレス

省略時値: なし

例:

```
delete udp-destination 36 20.1.2.2
```

vrid *interface-ip-address vrid*

VRRP ルーターについて構成済みのバーチャル・ルーター ID 定義を削除します。

interface-ip-address

この VRID が削除される IP インターフェースを指示します。

有効値: 任意の構成済み IP インターフェース

省略時値: なし

vrid バーチャル・ルーター識別子。*ip-interface-address* と *vrid* を組み合わせることにより、VRID は一意に定義されます。これは、削除される VRID を識別するのに使用されます。

有効値: 1 〜 255

省略時値: なし

例:

```
IP
config>delete vrid
IP Interface [ ]? 153.2.2.25
Virtual Router ID (1-255) [0]? 1
VRID 153.2.2.25/1 deleted.
```

vr-address *interface-ip-address vrid ip-address*

構成済みのバーチャル・ルーター ID (VRID) 定義から 2 次アドレスを削除します。

interface-ip-address

VRID の IP インターフェース

有効値: 任意の構成済み IP インターフェース

省略時値: なし

vrid バーチャル・ルーター識別子。*ip-interface-address* と *vrid* を組み合わせることにより、VRID は一意に定義されます。VRID が構成されていないと、その定義からアドレスを削除することはできません。

有効値: 1 〜 255

省略時値: なし

ip-address

VRRP 定義から削除される追加の IP アドレス

有効値: 任意の IP アドレス

省略時値: なし

例:

```
IP
config>delete vr-address
IP Interface [ ]? 153.2.2.25
Virtual Router ID (1-255) [0]? 1
IP Address to delete [ ]? 5.1.1.1
VRID 153.2.2.25/1 addr 5.1.1.1 deleted.
```

Disable

disable コマンドは、以前に **enable** コマンドを使用して使用可能にした IP フィーチャーを使用不能にするのに使用します。

構文:

disable

- arp-net-routing
- arp-subnet-routing
- bootp-forwarding
- classless
- directed-broadcast
- echo-reply
- fragment-offset-check
- icmp-redirect . . .
- nexthop-awareness . . .
- override default/static-routes . . .
- packet-filter
- per-packet-multipath
- receiving rip . . .
- receiving dynamic all/hosts/nets/subnets . . .
- record-route
- rip
- rip2
- route-table-filtering
- same-subnet
- sending default/net/subnet/poisoned/host/static/...
- sending outage-only . . .
- sending rip1-routes-only
- source-addr-verification
- source-routing
- tftp-server
- timestamp
- udp-forwarding . . .
- vrrp . . .

arp-net-routing

ARP ネットワーク・ルーティングをオフにします。これが使用可能になっていると、ルーターが、ルーターを通じて正常に到達されるリモートあて先についての ARP 要求すべてに代理応答します。これは省略時値であり、一般的に推奨される設定値です。

例: `disable arp-net-routing`

arp-subnet-routing

使用可能にすると、IP サブネットをサポートしないホストを扱う、ARP サブネット・ルーティングまたはプロキシー ARP と呼ばれる IP フィーチャーをオフにします。これは省略時値であり、一般的に推奨される設定値です。

例: `disable arp-subnet-routing`

bootp-forwarding

BOOTP/DHCP リレー機能をオフにします。

例: `disable bootp-forwarding`

classless

クラスなしドメイン間ルーティング (CIDR) をサポートしないルーティング・プロトコルのサポートを使用不能にします。そのネットワーク・マスク (例えば、RIPv1) を公示しないプロトコルで公示できるように自然なネットワーク・ルート (例えば、クラス A、B、または C ルート) が自動的に生成されることはありません。

例: `disable classless`

directed-broadcast

あて先が非ローカル (例えば、リモート LAN) の同報通信アドレスである IP パケットの転送を使用可能にします。発信元ホストはパケットをユニキャストとして発信し、その後パケットはユニキャストとしてあて先サブネットに転送され、『展開されて』同報通信になります。これらのパケットを使用して、ネットワーク・サーバーを探し出すことができます。

注: 転送と展開を個別に使用不能にすることはできません。

例: `disable directed-broadcast`

echo-reply

ルーターの ICMP エコー応答機能を使用不能にします。したがって、ルーターのインターフェースのいずれかに送信された PING は応答を生成しません。ルーターは省略時にはエコー応答を使用可能にします。

例: `disable echo-reply`

fragment-offset-check

受信された IP パケットのフラグメント・オフセットの検査を使用不能にします。この検査が使用可能になっているときは、ルーターは、各フラグメントを検査して、最初のフラグメントのペイロードの最初の 8 バイトをオーバーレーしている 2 次フラグメントがないことを学習します。省略時解釈では、この検査は使用不能になります。

icmp-redirect *ip-interface-address*

ルーターが、指定の IP インターフェースで ICMP リダイレクト・メッセー

ジを送信できないようにします。IP インターフェース・アドレスの入力を求めるプロンプトになにも入力しないと、ルーターは、すべての IP インターフェース上で ICMP リダイレクト・メッセージを送信できなくなります。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例:

```
IP config> disable icmp-redirect
Interface address (NULL for all) []? 192.9.200.44
IP config>
```

override default/static-routes *ip-interface-address*

インターフェース *ip-interface-address* 上で RIP により受信された省略時ルートが、IP ルーティング・テーブルにすでにインストールされている省略時ルートを置き換えられないようにします。**disable override static-routes** コマンドは、インターフェース *ip-interface-address* で受信された RIP ルートがルーターの静的ルートをどれも指定変更しないようにします。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: disable override default 128.185.123.22

nexthop-awareness *ip-interface-address*

IP インターフェース上でのネクスト・ホップ認識を使用不能にします。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例:

```
IP config> enable icmp-redirect
Interface address (NULL for all) []? 192.9.200.44
IP config>
```

packet-filter *filter-name*

指定されたインターフェースに固有のアクセス制御リスト (packet-filters) を使用不能にします。

filter-name

Valid Values: Any 16-character name. この名前には、ダッシュ (-) および下線 (_) を含めることができます。

省略時値: なし

例: disable packet-filter pf-in-0

per-packet-multipath

per-packet-multipath が使用不能にされると、ルーターはあて先への最初に使用可能なパスを選択します。このフィーチャーの省略時値は使えません。

例: disable per-packet-multipath

receiving rip *ip-interface-address*

インターフェース *ip-interface-address* 上で受信された RIP 更新を RIP が処理できないようにします。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `disable receiving rip 128.185.123.22`

receiving dynamic all/hosts/nets/subnets *ip-interface-address*

disable receiving dynamic nets コマンドにより、インターフェース *ip-interface-address* で受信された RIP 更新について、ルーターは **add accept-rip-route** コマンドで入力されたネットワーク・レベルのルートだけを受け入れることになります。**disable receiving dynamic subnets** コマンドはサブネット・ルートについて類似した動作を生じさせます。**disable receiving dynamic host** はホスト・ルートについて類似した動作を生じさせます。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `disable receiving dynamic nets 128.185.123.22`

record-route

ルーターが、レコード・ルート IP オプションを含む IP パケットを送受信しないようにします。省略時解釈では、ルーターは、これらのパケットを送受信します。

rip RIP プロトコルをオフにします。

例: `disable rip`

rip2 インターフェース上で RIP2 モードを使用不能にします。

ip-interface-address

有効値: RIP2 が使用可能になっているインターフェースの任意の有効な IP アドレス

省略時値: なし

例: `disable rip2 128.185.123.22`

route-table-filtering

ルーティング・テーブルにルートが追加されるときにルート・テーブル・フィルターの適用を使用不能にします。

例: `disable route-table-filtering`

same-subnet

同じサブネット・オプションを使用不能にします。ルーターはリブートされると、同じサブネットまでの複数の IP インターフェースをインストールしないようにします。これが省略時値です。

例: `disable same-subnet`

sending rip-routes-only *ip-interface-address*

RIP2 マルチキャスト・パケット内の RIP ルートのみの公示を停止します。

ip-interface-address

有効値: RIP2 が使用可能になっているインターフェースの任意の有効な IP アドレス

省略時値: なし

例: `disable sending rip1-routes-only 128.185.123.22`

sending all/default/host/net/poisoned/static/subnet *ip-interface-address*

ルーターが、インターフェース ip-interface-address を使用して送信された RIP 更新で指定のタイプのルートを公示しないようにします。インターフェースから送信された RIP ルートを制御する、それ以外のフラグは、**host-routes**、**static-routes**、**net-routes**、および **subnet-routes** です。これらは個別にオフにすることができます。ルートを使用可能にしたフラグのどれかによって指定している場合には、ルートは公示されます。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `disable sending net-routes 128.185.123.22`

sending outage-only *interface-IP-address*

類似の enable コマンドに指定されたルートがある場合に RIP 更新の送信を使用不能にします。この機能が使用不能になっていると、RIP 公示は無条件で送信されます。

interface-IP-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `disable sending outage-only`

source-addr-verification

このインバウンド・パケット・フィルター・オプションは、IP ルーティング・テーブルに基づいて、受信されたパケットの発信元 IP アドレスが発信元のインターフェースと矛盾していないか検査します。このオプションを選択すると、自分のものではない発信元 IP アドレスを使用している誤動作 IP ホストからパケットが転送されないようにすることができます。この誤動作は、スプーフィング と呼ばれます。 このコマンドは、パケット・フィルター構成コンソール (**update packet-filter** コマンドでアクセスします) でのみ有効です。

source-routing

ルーターがソース・ルーティング・パケット (つまり、ソース・ルート・オプションを含む IP パケット) を転送しないようにします。このオプションは、省略時には、ソース・ルーティングを使用可能にします。

例: `disable source-routing`

tftp-server

ルーターがネットワークから TFTP GET または PUT 要求を受け入れないよ

うにします。これにより、構成ファイルまたはロード・イメージが別の装置から不注意にオーバーレーされることが防げます。これを指定しても、直接に接続されている端末または装置との Telnet セッションから GET または PUT を実行することはできます。

例: `disable tftp-server`

timestamp
ルーターが、タイム・スタンプ IP オプションを含む IP パケットを送受信しないようにします。省略時解釈では、ルーターは、これらのパケットを送受信します。

udp-forwarding *port-number*
指定した UDP あて先ポート番号を使ってルーターによって受信されたパケットについて UDP 転送を使用不能にします。

省略時値: すべてのポート番号について UDP 転送が使用不能にされます。

port-number

有効値: 0 ～ 65535 の範囲内の整数

省略時値: 0

例: `disable udp-forwarding 36`

vrrp バーチャル・ルーター冗長プロトコルを使用不能にします。

例: `disable vrrp`

Enable

enable コマンドは、IP フィーチャー、機能、および IP 構成に追加される情報を活動化するのに使用します。

構文:

enable arp-net-routing
arp-subnet-routing
bootp-forwarding
classless
directed-broadcast
echo-reply
fragment-offset-check
icmp-redirect
nexthop-awareness
override default ...
override static-routes ...
packet-filter
per-packet-multipath
receiving rip ...

receiving dynamic all ...

receiving dynamic hosts...

receiving dynamic nets ...

receiving dynamic subnets ...

record-route

rip

rip2

route-table-filtering

same-subnet

sending all-routes ...

sending default-routes ...

sending host-routes ...

sending net-routes ...

sending outage-only . . .

sending poisoned-reverse-routes

sending rip1-routes-only

sending static-routes ...

sending subnet-routes ...

source-address-verification

source-routing

tftp-server

timestamp

udp-forwarding ...

vrrp ...

arp-net-routing

ARP ネットワーク・ルーティングをオンにします。これを使用可能にすると、ルーターは、ルーターを通じて正常に到達されるリモートあて先についてのすべての ARP 要求に代理応答します。このコマンドを使用するのは、LAN 上に、(本来はそうあるべきですが) ローカルあて先だけではなく、すべてのあて先について ARP を送信するホストがある場合です。

例: `enable arp-net-routing`

arp-subnet-routing

ルーターの ARP サブネット・ルーティング (プロキシー ARP と呼ばれることもある) 機能をオンにします。この機能が使用されるのは、直接接続された IP サブネットに接続されたサブネット化を認識していないホストがある場合です。このフィーチャーが有用になるためには、サブネット対応不能なホストをもつ直接接続されたサブネットは ARP を使用する必要があります。

ARP サブネット・ルーティングが働く仕組みは次のとおりです。サブネット対応不能なホストが IP パケットをリモート・サブネット上のあて先に送信したい場合、そのホストはパケットをルーターに送信する必要があることを理解していません。したがって、サブネット対応不能なホストは単に、ARP 要求を同報通信します。ARP 要求はルーターによって受信されます。arp-subnet-routing が使用可能にされ、かつあて先に対するネクスト・ホップが ARP 要求を受信しているインターフェースとは異なるインターフェースを通じて行われる場合には、ルーターはあて先として応答します (そこから代理という名前が付けられています)。

LAN 上に“サブネット対応不能の”ホストがない場合は、ARP サブネット・ルーティングを使用可能にしないでください。ARP サブネット・ルーティングが LAN 上で必要な場合には、そのルーティングはその LAN上のすべてのルーターで使用可能にする必要があります。

例: `enable arp-subnet-routing`

bootp-forwarding

BOOTP/DHCP パケット転送をオンにします。BOOTP 転送を使用するには、**add bootp-server** コマンドを使って 1 つまたは複数の BOOTP サーバーを追加する必要もあります。

例: `enable bootp-forwarding`

```
Maximum number of forwarding hops [4]?
Minimum seconds before forwarding [0]?
```

Maximum number of forwarding hops

BOOTP 要求をクライアントからサーバーに転送できる許容可能な BOOTP エージェントの最大数 (これはサーバーまでの IP ホップの最大数ではありません)。

省略時値: 4

Minimum seconds before forwarding

このパラメーターは普通は使用しません。このパラメーターを使用するのは、クライアントとサーバーの間に余分なパスがあり、2 次パスを待機として使用したいときです。

省略時値: 0

classless

ルーターがクラスなし IP アドレス環境で動作することを指示します。このオプションが使用可能になっていない場合は、IBM 2210 は RFC 1817 に記述されている CIDR をアドレス指定をそのまま全面的にサポートします。このオプションを使用可能にすると、IP ルート・テーブルに追加されたルートに対応する自然なネットワーク・ルート (例えば、クラス A、B、または C ネットワーク・ルート) は自動的に生成されません。 RIPv1 を実行しない場合には、自然なネットワーク・ルートが必要です。

例: `enable classless`

directed-broadcast

あて先がネットワーク宛てかサブネットあての同報通信アドレスである IP パケットの転送を使用可能にします。パケットは発信元ホストによってユニキャストとして発信され、その後ユニキャストとしてあて先サブネットへ転送され、『展開して』 同報通信になります。これらのパケットを使用して、ネ

ットワーク・サーバーを探し出すことができます。このコマンドは指定した同報通信の転送と展開の両方を使用可能にします。 IP パケット転送側は、リンク・レベル同報通信/マルチキャストがクラス D の IPアドレスに対応していない限り、リンク・レベル同報通信/マルチキャストを転送しません。(OSPF **enable multicast-routing** コマンドを参照してください。) このフィーチャーの省略時の設定値は使用可能です。

注: 転送および展開は個別に使用可能にはできません。また、ルーターは全サブネットの IP 同報通信を転送しません。

例: `enable directed-broadcast`

echo-reply

ICMP エコー要求に応答して ICMP エコー応答の作成および送信を使用可能にします。

例: `enable echo-reply`

fragment-offset-check

IP プロトコル番号が 6 (つまり、TCP) である、受信された IP パケットのフラグメント・オフセットの検査を使用可能にします。1 というフラグメント・オフセットをもつパケットは切り捨てられます。省略時解釈では、この検査は使用不能になります。

注: この機能は、使用可能にされた後は、IP の他のどの機能にも影響を与えないで、起動できます。詳しくは、 talk 5 **reset IP** コマンドを参照してください。

icmp-redirect *ip-interface-address*

ルーターが、指定の IP インターフェースで ICMP リダイレクト・メッセージを送信できるようにします。IP インターフェース・アドレスの入力を求めるプロンプトになにも入力しないと、装置は使用可能になり、すべての IP インターフェース上で ICMP リダイレクト・メッセージを送信します。

ip-interface-address

有効値: 任意の有効な IP アドレス、あるいはすべての IP インターフェースについてなにも指定しない

省略時値: なし

例:

```
IP config> enable icmp-redirect
Interface address (NULL for all) []? 192.9.200.44
IP config>
```

nexthop-awareness *ip-interface-address*

IP インターフェース上でのネクスト・ホップ認識を使用可能にします。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: disabled

例:

```
IP config>enable nexthop-awareness 1.1.1.1
IP config>enable nexthop-awareness
Interface address []? 2.2.2.2
IP config>
```

override default *ip-interface-address*

受信された RIP 情報が IP ルーティング・テーブルに入れられた省略時ルートを指定変更できるようにします。このコマンドは IP インターフェースごとに呼び出されます。 **enable override default** コマンドが呼び出されると、新規の省略時値のコストの方が安い場合には、インターフェース ip-interface-address で受信された省略時の RIP ルートがルーターの現在の省略時ルートを指定変更します。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `enable override default 128.185.123.22`

override static-routes *ip-interface-address*

受信された RIP 情報がルーターの静的に構成されたルーティング情報のいくつかを指定変更することを可能にします。このコマンドは IP インターフェースごとに呼び出されます。**enable override static-route** コマンドが呼び出されると、RIP 情報のコストの方が安い場合には、インターフェース ip-interface-address で受信された RIP ルーティング情報が静的に構成されたネットワーク/サブネット・ルートを指定変更します。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `enable override static-routes 128.185.123.22`

packet-filter *filter-name*

指定したインターフェースに固有なアクセス制御リスト (packet-filters) を使用可能にします。

filter-name

有効値: 任意の 16 文字の名前。この名前には、ダッシュ (-) および下線 (_) を含めることができます。

省略時値: なし

例: `enable packet-filter pf-in-0`

per-packet-multipath

per-packet-multipath が使用可能にされていて、あて先へ複数の等コストのパスがある場合は、ルーターは各パケットをラウンドロビン方式で転送するためのパスを選択します。このフィーチャーの省略時値は使えません。

例: `enable per-packet-multipath`

receiving rip *ip-interface-address*

特定のインターフェースで受信された RIP 更新の処理を使用可能にします。このコマンドには類似する disable コマンドがあります。(**disable receiving** コマンドを参照してください。) このコマンドの省略時値は使用可能です。

disable receiving rip コマンドを実行すると、インターフェース *ip-interface-address* アドレスでは RIP 更新は受け入れられません。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: enable receiving rip 128.185.123.22

receiving dynamic nets *ip-interface-address*

特定のインターフェースで受信される RIP 更新の処理を修正します。このコマンドには類似する disable コマンドがあります。(**disable receiving** コマンドを参照してください。) このコマンドの省略時値は使用可能です。

disable receiving dynamic nets コマンドを実行すると、ルーターはインターフェース *ip-interface-address* で受信された RIP 更新を、ネットワーク・レベル・ルートが **add accept-rip-route** コマンドで指定されていない限り、ネットワーク・レベル・ルートをどれも受け入れません。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: enable receiving dynamic nets 128.185.123.22

receiving dynamic subnets *ip-interface-address*

特定のインターフェースで受信される RIP 更新の処理を修正します。このコマンドには類似する disable コマンドがあります。(**disable receiving** コマンドを参照してください。) このコマンドの省略時値は使用可能です。

disable receiving dynamic subnets コマンドを実行すると、インターフェース *ip-interface-address* で受信された RIP 更新を、サブネット・レベル・ルートが **add accept-rip-route** コマンドで指定されていない限り、ルーターはサブネット・レベル・ルートをどれも受け入れません。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: enable receiving dynamic subnets 128.185.123.22

record-route

ルーターが、レコード・ルート IP オプションを含む IP パケットの送受信を行えるようにします。これが省略時値です。

注: この機能は、使用可能にされた後は、IP の他のどの機能にも影響を与えないで、起動できます。詳しくは、 talk 5 **reset IP** コマンドを参照してください。

rip ルーターの RIP プロトコル処理を使用可能にします。

RIP が使用可能にされる場合は、次の省略時行動が確立されます。

- ルーターは、その構成された各 IP インターフェースから送信される RIP 更新内にすべてのネットワークおよびサブネットのルートを含んでいます。

- ルーターは、その構成された IP インターフェースのそれぞれで受信されるすべての RIP 更新を処理します。

省略時の送信/受信行動のいずれかを変更するには、各 IP インターフェースごとに定義される IP 構成コマンドを使用してください。

例: enable rip

rip2

インターフェース上で RIP2 モードを使用可能にします。RIP2 公示パケットは、アドレス 224.0.0.9 でマルチキャスト同報通信になります。RIP2 がインターフェース上で使用可能になると、認証キーを設定するかどうか尋ねられます。N (No) と応答すると、RIP2 パケット公示についての認証は行われません。Y (Yes) と応答した場合は、認証キーを入力するよう求められます。この認証キーは、妥当性検査のために 2 度入力する必要があります。認証キーは、その特定のインターフェースから送信される RIP2 公示パケットに入れられます。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: enable rip2 128.185.123.22

```
IP config>enable rip2 153.2.2.25 yes clear-password clear-password
RIP2 is enabled on this interface.
RIP2 Authentication is enabled on this interface.
```

route-table-filtering

ルート・テーブル・フィルターを、ルーティング・テーブルに追加されるルートに適用します。ルート・テーブル・フィルターは、あて先およびネットワーク・マスクの最も詳細な一致に基づいて適用されます。ルート・テーブル・フィルターが、ルートまたは静的ルートを転送するために適用されることはありません。

例: enable route-table-filtering

same-subnet

同じサブネット・オプションを使用可能にします。装置はリブートされると、同じサブネットまでの複数の IP インターフェースをインストールできるようにします。同じサブネットに複数の IP インターフェースがつながっていても、次の条件の 1 つでしか役に立ちません。

- OSPF ポイント・マルチポイントが IP インターフェースに構成されている場合
- ネクスト・ホップ認識がIP インターフェースで使用可能になっており、IP インターフェースを通るルートについて静的ルートが定義されている場合

省略時解釈では、このオプションは使用不能です。

例: enable same-subnet

sending default-routes *ip-interface-address*

特定のインターフェースから送信される RIP 更新の内容を判別します。このコマンドには類似する disable コマンドがあります。(**disable sending** コマンドを参照してください。) **enable sending** コマンドの効果は付加的です。

各個別の enable sending コマンドは、特定の組み合わせのルートが特定のインターフェースから公示されるよう指定します。あるルートが RIP 更新に含まれるのは、そのルートが enable sending コマンドの少なくとも 1 つによって組み込まれている場合に限ります。**enable sending default-routes** コマンドは、省略時のルート (それが存在する場合) がインターフェース ip-interface-address から送信される RIP 更新に含まれるよう指定します。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `enable sending default-routes 128.185.123.22`

注: enable sending ... コマンドの設定値のうちには冗長なものもあります。例えば、特定のインターフェースについて **enable sending net-routes**、**enable sending subnet-routes**、および **enable sending host-routes** を実行する、(各静的ルートはネットワーク・レベル、サブネット、またはホスト・ルートなので) **enable sending static-routes** も指定する必要はありません。省略時では、最初に RIP を使用可能にすると、各インターフェースについて sending net-routes、sending subnet-routes、および sending host-routes が使用可能にされるのに対し、sending static-routes および sending default は使用不能にされます。

sending net-routes *ip-interface-address*

特定のインターフェースから送信される RIP 更新の内容を判別します。このコマンドには類似する disable コマンドがあります。(**disable sending** コマンドを参照してください。)

enable sending コマンドの効果は付加的です。 各個別の **enable sending** コマンドは、特定の組み合わせのルートが特定のインターフェースから公示されるよう指定します。あるルートが RIP 更新に含まれるのは、そのルートが **enable sending** コマンドの少なくとも 1 つによって含まれている場合に限ります。 **enable sending network-routes** コマンドは、すべてのネットワーク・レベル・ルートがインターフェース ip-interface-address から送信される RIP 更新に含まれるよう指定します。ネットワーク・レベル・ルートは単一のクラスの A、B、または C の IP ネットワークへのルートです。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `enable sending net-routes 128.185.123.22`

sending outage-only *interface-ip-address outage-network outage-network-mask*

outage-network および *outage-network-mask* によって指定された IP ルートが存在する場合に *interface-ip-address* によって指定されたインターフェースでの RIP 更新パケットの送信を使用可能にします。通常、更新は、RIP ルートを公示するために構成されたインターフェースで無条件で送信されます。また、指定のルートが存在する場合、RIP更新は、故障専用インターフェース

では無視されます。この機能は、バックアップ・サーキットがダイヤル・オンデマンド・サーキットとして構成されているバックアップ・シナリオで役に立ちます。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

outage-network

有効値: 任意の有効な IP アドレス

省略時値: なし

outage-network-mask

有効値 任意の有効な IP マスク

省略時値: なし

例: enable sending outage-only

```
IP config>enable sending outage-only
Set for which interface address [0.0.0.0]? 0.0.0.2
Outage network []? 10.50.0.0
Outage network mask []? 255.255.0.0
```

この例では、ルート 10.50.0.0/255.255.0.0 がルーティング・テーブルに含まれていない場合、RIP 公示は無番号インターフェースでのみ送信されます。

sending poisoned-reverse-routes *ip-interface-address*

ルートが変更されるときの収束時間を改善するために RIP によって使用される技法 (この技法の完全な詳細については、rfc 1058 を参照してください)。この技法を使用すると、RIP 更新メッセージのサイズが拡大します。いくぶん遅い収束を受け入れることにより、ルーティング・オーバーヘッドを最小限に抑える方が無難です。**disable sending poisoned-reverse-routes** コマンドは、 **enable ip-interface-address** コマンドによって指定されたインターフェースで送信された RIP 更新に有害な逆ルートが含まれるべきでないことを指定します。

省略時値: 使用可能

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

sending rip-routes-only *ip-interface-address*

RIP2 マルチキャスト・パケット内の RIP ルートのみを公示します。

ip-interface-address

有効値: RIP2 が使用可能になっているインターフェースの任意の有効な IP アドレス

省略時値: なし

例: enable sending rip-routes-only 128.185.123.22

sending subnet-routes *ip-interface-address*

特定のインターフェースから送信される RIP 更新の内容を判別します。このコマンドには類似する disable コマンドがあります。(**disable sending** コマ

ンドを参照してください。) **enable sending** コマンドの効果は付加的です。各個別の **enable sending** コマンドは、特定の組み合わせのルートが特定のインターフェースから公示されるよう指定します。 あるルートが RIP 更新に含まれるのは、そのルートが enable sending コマンドの少なくとも 1 つに含まれている場合に限ります。**enable sending subnet-routes** コマンドは、すべてのサブネット・ルートがインターフェース ip-interface-address から送信される RIP 更新に含まれるよう指定します。 ただし、サブネット・ルートが含まれるのは、ip-interface-address が同じ IP サブネット・ネットワークのサブネットに直接接続されている場合に限られます。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `enable sending subnet-routes 128.185.123.22`

sending static-routes *ip-interface-address*

特定のインターフェースから送信される RIP 更新の内容を判別します。このコマンドには類似する disable コマンドがあります。(**disable sending** コマンドを参照してください。) **enable sending** コマンドの効果は付加的です。各個別の **enable sending** コマンドは、特定の組み合わせのルートが特定のインターフェースから公示されるよう指定します。 あるルートが RIP 更新に含まれるのは、そのルートが enable sending コマンドの少なくとも 1 つに含まれている場合に限ります。**enable sending static-routes** コマンドは、静的に構成され、直接接続されたすべての・ルートが、インターフェース ip-interface-address から送信された RIP 更新に含まれているよう指定します。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `enable sending static-routes 128.185.123.22`

sending host-routes *ip-interface-address*

特定のインターフェースから送信される RIP 更新の内容を判別します。このコマンドには類似する **disable ...** コマンドがあります。(**disable sending** コマンドを参照してください。) **enable sending** コマンドの効果は付加的です。各個別の **enable sending** コマンドは、特定の組み合わせのルートが特定のインターフェースから公示されるよう指定します。 あるルートが RIP 更新に含まれるのは、そのルートが **enable sending** コマンドの少なくとも 1 つによって含まれている場合に限ります。**enable sending host-routes** コマンドは、すべてのホスト・ルートがインターフェース ip-interface-address から送信される RIP 更新に含まれるよう指定します。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

source-addr-verification

このインバウンド・パケット・フィルター・オプションは、IP ルーティング・テーブルに基づいて、受信されたパケットの発信元 IP アドレスが発信元

のインターフェースと矛盾していないか検査します。このオプションを選択すると、自分のものではない発信元 IP アドレスを使用している誤動作 IP ホストからパケットが転送されないようにすることができます。この誤動作は、スプーフィング と呼ばれます。 このコマンドは、パケット・フィルター構成コンソール (**update packet-filter** コマンドでアクセスします) でのみ有効です。

source-routing
ルーターが IP ソース・ルート・オプションを含む IP パケットを転送できるようにします。

例: `enable source-routing`

tftp-server
ルーターが、構成ファイルまたはイメージ・ロードについてのネットワークからの TFTP GET または PUT 要求を受け入れられるようにします。

例: `enable tftp-server`

timestamp
ルーターが、タイム・スタンプ IP オプションを含む IP パケットの送受信を行えるようにします。これが省略時値です。

注: この機能は、使用可能にされた後は、IP の他のどの機能にも影響を与えないで、起動できます。詳しくは、 talk 5 **reset IP** コマンドを参照してください。

udp-forwarding *port-number*
指定した UDP あて先ポート番号を使ってルーターが受信したパケットについて UDP 転送を使用可能にします。

省略時値: すべてのポート番号について UDP 転送が使用不能にされます。

port-number
有効値: 0 ～ 65535 の範囲内の整数

省略時値: 0

例: `enable udp-forwarding 36`

vrrp バーチャル・ルーター冗長プロトコルを使用可能にします。

例: `enable vrrp`

List

list コマンドは、呼び出された特定のサブコマンドに応じて、IP 構成データのさまざまな部分を表示するのに使用します。

構文:

list all
access-control
addresses
bootp
filters

icmp redirect

igmp

mtu

nexthop-awareness

packet-filter

parameters

protocols

redundant-default-gateway

rip-routes-accept

routes

route-table-filtering

sizes

tags

udp-forwarding

vrid

all IP 構成全体を表示します。

例: `list all`

access-control
構成済みのアクセス制御モード (enabled または disabled) および構成済みのグローバル・アクセス制御レコードのリストを表示します。各レコードはそのレコード番号とともにリストされます。このレコード番号は、IP **move access-control** コマンドを使ってリストの順番を変えるのに使用することができます。

例: `list access control`

addresses
ルーターに割り当てられた IP インターフェース・アドレスを、それらの構成済みの同報通信形式とともに表示します。*BDG/0* によって識別されるインターフェースは、ブリッジング・インターフェースです。

例: `list addresses`

bootp BOOTP 転送が使用可能か使用不能かのどちらか、ならびに BOOTP サーバーの構成済みリストを示します。

例: `list bootp`

icmp-redirect
ICMP リダイレクト・メッセージの送信が各 IP インターフェース上で使用可能か、使用不能かをリストします。

igmp IGMP 構成が表示されます。

例 :

```
IP config>list igmp
Net          IGMP          Query          Response          Leave Query
```

```
            Version       Interval        Interval          Interval
                            (secs)          (secs)            (secs)
---         -------       --------        --------          ----------
  0             2            250              10                 1
  1             1            125              10                 1
  4             2            125              10                 2
  5             2            125              20                 1

IP config>
```

mtu 構成済み MTU 値の一覧表が表示されます。

nexthop-awareness

すべての IP インターフェース上でのネクスト・ホップ認識の設定をリストします。

例:

```
IP config>list nexthop-awareness
Nexthop awareness for each IP interface address:
   intf  0   1.1.1.1          255.0.0.0        nexthop awareness enabled
   intf  1   2.2.2.2          255.0.0.0        nexthop awareness disabled
IP config>
```

packet-filter *filter-name*

パケット・フィルターに関する情報をリストします。名前を指定した場合は、コマンドはそのフィルターに関して構成されたアクセス制御情報をリストします。フィルター名を指定しない場合、コマンドは構成済みのパケット・フィルターをリストします。ブリッジ・インターフェース上にパケット・フィルターを構成してある場合、そのインターフェースは、*BDG/0* で識別されます。

例: `list packet-filter pf-in-0`

```
Name              Direction     Interface
pf-in-0           In            0

Access Control is: enabled

List of access control records:

1  Type=E    Source=128.185.0.0   Dest=0.0.0.0           Prot=0-255
             Mask=255.255.0.0     Mask=0.0.0.0
             Sports=  0-65535     Dports=  1-65535
             ACK0=N  T/C= **/**   Log=No

2  Type=INS  Source=10.1.1.1      Dest=10.1.1.2          Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.254
             Sports=  N/A         Dports=  N/A           Tid=5279
                                  Log=Yes ELS=N SNMP=Y SLOG=L(Emergency)

3  Type=I    Source=0.0.0.0       Dest=0.0.0.0          Prot=0-255
             Mask=0.0.0.0         Mask=0.0.0.0
             Sports= 1-65535      Dports=  1-68835
                                  Log=No
```

parameters

同じサブネットを含む、各種のグローバル IP パラメーターをリストします。

例: `list parameters`

```
IP config>list parameters
ARP-SUBNET-ROUTING    : enabled
ARP-NET-ROUTING       : enabled
CLASSLESS             : disabled
DIRECTED-BROADCAST    : enabled
ECHO-REPLY            : enabled
FRAGMENT-OFFSET-CHECK : enabled
PER-PACKET-MULTIPATH  : disabled
REASSEMBLY-SIZE       : 12000 bytes
RECORD-ROUTE          : enabled
ROUTING TABLE-SIZE    : 768 entries (52224 bytes)
(Routing) CACHE-SIZE  : 64 entries
SAME-SUBNET           : disabled
SOURCE-ROUTING        : enabled
TIMESTAMP             : enabled
TTL                   : 64
```

protocols

IP ルーティング・プロトコル (OSPF、RIP、BGP) の構成済みの状態を一般構成設定値とともに表示します。

例: `list protocols`

redundant-default-gateway

構成された各インターフェースについて冗長省略時ゲートウェイを表示します。

例: `list redundant`

```
Redundant Default IP Gateways for each interface:
   inf 4  11.1.1.6     255.0.0.0     00.00.00.00.00.BA  primary
   inf 8  33.3.3.6     255.0.0.0     00.00.00.00.00.AB  backup
```

rip-routes-accept

RIP ルーティング・プロトコルが常に受け入れるルートの組み合わせを表示します。詳しくは、IP 構成コマンド **enable/disable receiving dynamic nets/subnets/hosts** を参照してください。

例: `list rip-routes-accept`

route-table-filtering

ルーティング・フィルターに追加されたルート・フィルターのリストを表示します。

例: `list route-table-filtering`

```
IP config>list route-table-filtering

Route Filtering Disabled

Destination     Mask            Match Type
10.1.1.0        255.255.255.0   BOTH  E
50.50.0.0       255.255.0.0     BOTH  I
10.1.1.1        255.255.255.255 EXACT I
50.0.0.0        255.0.0.0       BOTH  E

MORE-Match more-specific routes   EXACT-Match route exactly
BOTH-Match exact and more-specific routes  E-Exclude  I-Include
IP config>
```

routes

構成済みの静的ルートのリストを表示します。

例: `list routes`

```
IP config>list routes

route to 1.1.0.0        ,255.255.0.0     via 10.1.1.1        cost 1
                                         via 20.1.1.1        cost 2
                                         via 30.1.1.1        cost 3
route to 2.2.0.0        ,255.255.0.0     via 10.2.2.2        cost 10
route to 3.3.0.0        ,255.255.0.0     via 10.3.3.3        cost 100
                                         via 20.3.3.3        cost 200
```

sizes ルーティング・テーブル・サイズ、再アセンブリー・バッファー・サイズ、およびルート・キャッシュ・サイズを表示します。

例: `list sizes`

tags 受信した RIP 情報に関連するインターフェースごとのタグを表示します。これらのタグはルートをグループ化し、後で BGP を介して再公示するのに使用できます。その際、タグはルートの発信元自律システム (AS) であるかのように扱われます。 タグは OSPF ルーティング・プロトコルによっても伝送されます。

例: `list tags`

udp-forwarding

UDP 転送機能について、すべてのポートおよびすべての IP アドレスを含む、すべての構成済みの情報を表示します。

例: `list udp-forwarding`

vrid 構成済みの VRRP 状況、VRID、および VRID アドレスを表示します。

例:

```
IP config>list vrid

VRRP Enabled

                              --VRID Definitions--

IP address      VRID  Priority Interval Auth   Auth-key Flags Address(es)
153.2.2.25         1       255        1 None   N/A      P     5.1.1.1
```

Move

move コマンドは、グローバル・アクセス制御リスト内のレコードの配列を変更するのに使用します。 このコマンドはレコード番号 to# の直後にレコード番号 from# を入れます。レコードを移動した後、新しい順序を反映するためにレコードはただちに番号を付け直されます。

ルーターは、リスト内のアクセス制御レコードを、作成された順序で適用します。インターフェースで受信された各パケットごとに、ルーターは、各アクセス制御レコードを一致が見つかるまで順に適用します。パケットに一致する最初のレコードは、それが廃棄されるか、そのあて先に転送されるのかどうかを判別します。

したがって、アクセス制御レコードの配列が非常に重要になります。アクセス制御項目の配列が間違っていると、特定のパケットがユーザーの意図に反して、脱落したりブロックされたりすることになりかねません。

例えば、アクセス制御レコード 1 で、*ネットワーク 10.0.0.0 からのパケットはすべて、このインターフェースでブロックされるものとする* という規則が有効であるとします。これに対して、アクセス制御レコード 2 では、*ネットワーク 10.0.0.0 内のサブネット 10.5.5.0 からの、アドレス 1.2.3.4 をあて先とするパケットは通過できるものとする* と規定しているものとします。アクセス制御レコードがこの順序で割り当てられている場合は、レコード 2 で特定のタイプのパケットの通過を明示的に認めているにもかかわらず、10.0.0.0 からのトラフィックはすべてブロックされることになります。

この例では、レコード 1 はレコード 2 を議論の余地があるものにします。レコード 1 は、特定のパケットが転送されるべきものであるとする、レコード 2 の意向にもかかわらず、ルーターが10.0.0.0 からのすべてのパケットを廃棄するよう保証します。この種の問題を修正するかぎは、アクセス制御レコードの配列にあります。そうすれば、サブセット 10.5.5.0 にあってアドレス 1.2.3.4 をあて先とするパケットはインターフェースを通過し、10.0.0.0 からのそれ以外のパケットは、意図どおりルーターによってすべて廃棄されることになります。

構文:

move access-control *from# to#*

例: `move 5 2`

Set

set コマンドは、IP 構成内で特定の値、ルート、および形式を設定するのに使用します。

構文:

set

- access-control...
- access-control log-facility
- broadcast-address...
- cache-size .
- default network-gateway...
- default subnet-gateway...
- igmp ...
- internal-ip-address
- mtu
- originate-rip-default
- reassembly-size
- rip-in-metric
- rip-out-metric
- router-id
- routing table-size
- tag . . .
- ttl

access-control *on* **or** *off*

ルーターに IP アクセス制御を使用可能または使用不能にするよう構成できます。アクセス制御を *on* に設定すると、グローバル・アクセス制御リストならびにインターフェース固有のリストが使用可能にされます。アクセス制御を *off* に設定するとすべてのリストが使用不能にされますが、それらを削除はしません。

例: `set access-control on`

access-control log-facility *log-facility*

SysLog 機能をアクセス制御用に設定します。SysLog 機能オプションは、SysLog メッセージが表示されるシステムを定義します。

注: この機能は、使用可能にされた後は、IP の他のどの機能にも影響を与えないで、起動できます。詳しくは、 talk 5 **reset IP** コマンドを参照してください。

log-facility

有効値: KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7, USER

省略時値: USER

例:

```
IP config>
set access-control log-facility
SYSLOG facility? (KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR,
NEWS, UUCP, CRON, AUTHPRIV, LOCAL0, LOCAL1, LOCAL2,
LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7) [USER]?
```

broadcast-address *ip-interface-address style fill-pattern*

ルーターが特定のインターフェースでパケットを同報通信するときに使用する IP 同報通信形式を指定します。ルーターは RIP 更新パケットを送信するときに IP 同報通信を最も一般的に使用します。

スタイル・パラメーターは、ローカル・ワイヤーの値またはネットワークの値のどちらかを取ることができます。ローカル・ワイヤーの同報通信アドレスはすべて 1 (255.255.255.255) またはすべてゼロ (0.0.0.0) です。ネットワーク・スタイルの同報通信は ip-interface-address のネットワークおよびサブネットの部分から開始されます。

充てんパターン・パラメーターは 1 または 0 に設定できます。これは、同報通信アドレスの残りの部分 (つまり、ネットワークおよびサブネットの部分がある場合は、それ以外) がすべて 1 またはすべて 0 のどちらに設定されるかを示します。

ルーターは受信するときに、すべての形式の IP 同報通信アドレスを認識します。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

style **有効値**: *local-wire* または *network*

省略時値: local-wire

fill-pattern

有効値: *0* または *1*

省略時値: 1

下の例は、255.255.255.255 の同報通信アドレスを構成しています。 2 番目の例では、ネットワーク 192.9.1.0 がサブネットされていないとして、192.9.1.0 の同報通信アドレスを生成します。

例: set broadcast-address 192.9.1.11 local-wire 1 set broadcast-address 192.9.1.11 network 0

cache-size *entries*

IP ルーティング・キャッシュ用の最大数の項目を構成します。このキャッシュは、ルーターが最近パケットを転送した先の特定の IP アドレスについての情報を保管します。キャッシュは、同じあて先に複数のパケットを転送するために要する時間を短縮します。

このキャッシュとは対照的に、IP ルーティング・テーブル は、アクセス可能なすべてのネットワークに関する情報を保管しますが、特定の IP 着信先アド

レスは含んでいません。 IP ルーティング・テーブルのサイズを構成するには、**set routing table-size** コマンドを使用してください。

有効値: 64 ～ 10000

省略時値: 64

例: set cache-size 64

default network-gateway *next-hop cost*

権限のあるルーターへのルート (省略時のゲートウェイ) を構成します。ルーターの省略時のゲートウェイはルーター自体より完全なルーティング情報をもつものと想定する必要があります。

ルートは次のホップの IP アドレス (next-hop) および省略時のゲートウェイへの距離 (cost) によって指定します。

不明のあて先をもつすべてのパケットは権限のあるルーター (省略時のゲートウェイ) へ転送されます。

nexthop

有効値: 任意の有効な IP アドレス

省略時値: 1 というゲートウェイ・コストをもつ 0.0.0.0

cost **有効値**: 0 ～ 255 の範囲内の任意の整数

省略時値: 1

例: set default network-gateway 192.9.1.10 10

default subnet-gateway *subnetted-network next-hop cost*

サブネット・ネットワークの権限のあるルーターへのルート (省略時のサブネット・ゲートウェイ) を構成します。各サブネット・ネットワークについて個別の省略時サブネット・ゲートウェイを構成できます。

次のホップの IP アドレス (next-hop) および省略時のサブネット・ゲートウェイへの距離 (cost) がルートを指定します。

既知のサブネット・ネットワークの不明のサブネットへのすべてのパケットは、サブネット・ネットワークの権限のあるルーター (省略時のサブネット・ゲートウェイ)に転送されます。

subnetted network

有効値: 任意の有効な IP アドレス

省略時値: 0.0.0.0

next-hop

有効値: 任意の有効な IP アドレス

省略時値: 0.0.0.0

cost

有効値: 0 ～ 255 の範囲内の任意の整数

省略時値: 1

例: set default subnet-gateway 128.185.0.0 128.185.123.22 6

igmp ...

インターネットグループ管理 (IGMP) パラメーターが構成されます。次のパラメーターについて値が指定できます。

query interval *net interval*

IGMP 一般照会間のインターバルを変更します。

net
構成中のインターフェースについてネットワーク番号を指定します。

有効値 : 有効なネットワーク番号のどれか

省略時値 : なし

interval
一般照会の送信間の秒数を指定します。

有効値 : 1 ～ 3600

省略時値 : 125

response-interval *net interval*

IGMP 一般照会に挿入されている最大応答時間を変更します。

net
構成中のインターフェースについてネットワーク番号を指定します。

有効値 : 有効なネットワーク番号のどれか

省略時値 : なし

interval
照会の送信とホストによる応答としての IGMP レポートの送信の間の秒数を指定します。

有効値 : 1 ～ 60

省略時値 : 10

robustness-variable *net variable*

ネットワークに関する耐性変数を変更します。

net
構成中のインターフェースについてネットワーク番号を指定します。

有効値 : 有効なネットワーク番号のどれか

省略時値 : なし

variable
ネットワーク上でのパケット紛失に対処するために送信される IGMP パケットの数を指定します。

有効値 : 2 ～ 10

省略時値 : 2

leave-interval *net interval*

IGMP 特定照会に挿入されている最大応答時間を変更します。

net
構成中のインターフェースについてネットワーク番号を指定します。

有効値 : 有効なネットワーク番号のどれか

省略時値 : なし

interval

特定照会の送信とホストによる応答としての IGMP レポートの送信の間に許容される秒数を指定します。

有効値 : 1 ～ 60

省略時値 : 1

version *net vernum*

ネットワーク上で稼働する IGMP のバージョンを変更します。

net 構成中のインターフェースについてネットワーク番号を指定します。

有効値 : 有効なネットワーク番号のどれか

省略時値 : なし

vernum

ネットワーク上で稼働するバージョン番号を指定します。

有効値 : 1 または 2

省略時値 : 2

internal-ip-address *ip-address*

どのインターフェースの状態からも独立した IP アドレスを構成します。内部アドレスは常にアクティブにあります。内部アドレスを定義するための主な理由は、インターフェースが非アクティブになるときに非アクティブにならない TCP 接続用のアドレスを提供することです。データ・リンク交換 (DLSw) にはこのアドレスが使用され、インターフェースが非アクティブになるときに DLSw 接続を中断するのを避けるために代替パスが使用できるようにします。内部アドレスがアクティブのまま残るためと、OSPF がこの着信先へのアクティブの IP ルートを維持するため、IP ルーティングは TCP 接続をダウンさせたり、 DLSw の最上位で稼働している SNA セッションを中断することなく、 DLSw トラフィックを代替パスに切り替えることができます。

内部 IP アドレスは、無番号インターフェースが使用される場合に、何らかの値も提供します。これはこのルーターによって発信され、無番号インターフェースを通じて伝送されるパケット用の発信元アドレスとしての最初の選択です。このアドレスは安定しているので、そのようなパケットを追跡することをより容易にします。同じ IP アドレスがルーター ID および内部アドレスの両方に使用されるときに混乱する確率がさらに小さくなります。したがって、ルーター ID は省略時には内部アドレスとして解釈されます。

内部アドレスが定義される場合、このアドレスは OSPF によって、ルーターに直接接続されるすべての区域へのホスト・ルートとして公示されます。

有効値: 任意の有効な IP アドレス

省略時値: なし

例: `set internal-ip-address 142.82.10.1`

mtu このインターフェース上の IP プロトコルについて MTU 値を設定します。

有効値: 0、68 ～ 65535

省略時値: ネットワーク上のすべての非ゼロ MTU の最大値

originate-rip-default

RIP にこのルーターを省略時のゲートウェイとして公示させます。このコマンドは、次の環境で使用してください。

- このルーターのルーティング・テーブル内の IP ルートが、多くのプロトコルによって判別されている場合
- RIP がこれらのプロトコルの 1 つである場合
- 他のプロトコルからインポートされ、RIP によって公示されるのが、せいぜい部分的なルーティング情報である場合

RIP ネットワーク内のトラフィックで RIP に不明のあて先へのものは、このルーターへの省略時のパスをたどることができます。このノードのルート・テーブル内のさらに完全なルーティング情報を使用して、そのあて先への該当するパスに沿ってトラフィックを転送することができます。このルーターに RIP ネットワークで公示されないルートが知られている場合だけ、省略時値を発信するようにルーターを構成することができます。

このコマンドを出すと、ルーターが必ず RIP 省略時値を発信するのか、それとも他のプロトコルからのルートが使用可能な場合にのみ RIP 省略時を発信するのかを指定するようプロンプト指示されます。

この省略時のルートは、非 RIP ネットワークに向けられたトラフィックを境界ルーターに導きます。単一の省略時ルートを開始するということは、境界ルーターが、他のネットワークのルーティング情報をそのネットワーク内の他のノードに配布する必要がないことを意味します。

from AS number

有効値: 0 ～ 65535 の範囲内の整数

省略時値: なし

to network number

有効値: 任意の有効な IP アドレス

省略時値: なし

default cost

有効値: 0 ～ 255 の範囲内の任意の整数

省略時値: 1

例: set originate-rip-default

```
IP config> set originate rip-default
Always originate default route? [No]:?
Originate default if BGP routes available? [No] yes
  From AS number [6]?
  To network number [0.0.0.0]?
Originate default if OSPF routes available? [No]
Originate default cost [1]?
```

- 『Always originate』 に 『Yes』 と応答すると、省略時ルートが常に起点となります。
- 『BGP』 に 『Yes』 と応答すると、ルーティング・テーブルに BGP ルートがある場合は必ず省略時値が起点となります。

- 『if OSPF routes available』 に 『yes』 と応答すると、OSPF ルートがルーティング・テーブルにある場合に RIP 省略時値が公示されます。
- ルーターは、RIP 省略時値を開始しようと決めると、『original default cost』番号を使用します。
- BGP ルート AS (類似システム) 番号に 0 が指定されると、任意の AS からのネットワーク基準に合致するルートは、RIP 省略時値が起点となります。
- BGP または OSPF にネットワーク基準に 0.0.0.0 が指定されると、AS 基準に合致する任意の BGP は、RIP 省略時値が起点となります。

reassembly-size *bytes*

断片化された IP パケットの再アセンブリーに使用されるバッファーのサイズを構成します。

有効値 2048 ～ 65535

省略時値 12000

例: `set reassembly-size 12000`

rip-in-metric *ip-interface-address metric*

ルート距離の構成を、ルーティング・テーブルに入れられる前にインターフェースの RIP ルートに追加できるようにします。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

メトリック (metric)

有効値: 1 ～ 15 の範囲内の整数

省略時値: 1

例: `set rip-in-metric 128.185.120.209 1`

rip-out-metric *ip-interface-address metric*

ルート距離の構成を、RIP または RIP2 ルートを公示するよう構成されたインターフェースに公示されている RIP ルートに追加できるようにします。

ip-interface-address

有効値: 任意の有効な IP アドレス

省略時値: なし

メトリック (metric)

有効値: 1 ～ 15 の範囲内の整数

省略時値: 0

例: `set rip-out-metric 128.185.120.209 0`

router-id *ip-address*

さまざまな IP パケットの発信元を指定するときにルーターが使用する省略時の IP アドレスを設定します。このアドレスはマルチキャストおよび OSPF では特に重要です。

ルーター ID は、ルーターの構成済みの IP インターフェース・アドレスまたは構成済みの内部 IP アドレスの 1 つに合致する必要があります。合致していない場合は、そのルーター ID は無視されます。無視されるか、単に構成されていない場合は、ルーターの省略時の IP アドレス (およびその OSPF ルーター ID) はルーターの構成内の内部 IP アドレス (構成されている場合) または最初の IP アドレスに設定されます。

有効値: 任意の有効な IP アドレス

省略時値: なし

例: set router-id 128.185.120.209

routing table-size *number-of-entries*

ルーターの IP ルーティング・テーブルのサイズを設定します。省略時のサイズは 768 項目です。ルーティング・テーブル・サイズを小さく設定しすぎると、動的ルーティング情報が廃棄されることになります。ルーティング・テーブル・サイズを大きく設定しすぎると、ルーターのメモリー資源を浪費することになります。テーブル・サイズの詳細については、328ページの『Sizes』を参照してください。

有効値: 範囲 64 〜 65535 内の項目の整数値

省略時値: 768 項目

例: set routing table-size 1000

tag 受信された RIP 情報に関連するインターフェースごとのタグを構成します。これらのタグはルートをグループ化し、後で BGP を介して再公示するのに使用できます。その際、タグはルートの発信元自律システム (AS) 番号であるかのように扱われます (*プロトコルの構成と監視 解説書 第 1 巻* の「BGP の使用と構成」の章の発信、送信、受信の各ポリシーの説明を参照してください)。タグは OSPF ルーティング・プロトコルによっても伝送されます。

有効値: 0 〜 65535 の範囲内の整数

省略時値: 0

例: set tag

```
Interface address [0.0.0.0]? 1.1.1.1
Interface tag (AS number) [0]? 1
```

ttl ルーターによって発信されたパケットについて活動時間を指定します。

有効値: 範囲 1 〜 255 内の数値

省略時値: 64

例: set ttl 255

Update

update packet-filter コマンドは、パケット・フィルターを構成するのに使用します。次に、このコマンドの例を示します。

```
IP config> update packet-filter
Packet-filter name [ ]? pf-1-in
Packet-filter 'pf-1-in' Config>
```

Packet-filter-name は、IP config> プロンプトから **add packet-filter** *packet-filter-name* コマンドを使用して作成された任意のパケット・フィルター名です。パケット・フィルターを使用可能にするためには、**set access-control on** コマンドを使用します。Packet-filter '*packet-filter-name*' Config> プロンプトから、次のコマンドを入力できます。

構文:

add access-control

change access-control

delete access-control

disable

enable

list access-control

move access-control

Packet-filter '*filter-name*' Config> プロンプトの **add access-control**、**change access-control**、**delete access-control**、**list access-control**、および **move access-control** コマンドについては、IP config> プロンプトに表示される **access-control** パラメーターの下にあるパラメーターの説明を参照してください。例えば、**update packet-filter add access-control** コマンドのパラメーターの説明については、**add access-control** を参照してください。

コマンド **disable** および **enable** については、キーワード **source-addr-verification** は、Packet-filter '*filter-name*' Config> プロンプトからしか構成できません。

以下の項では、コマンド**update packet-filter** に固有なパラメーターをリストします。これらは、パケット・フィルターには適用されますが、ルーター全体のフィルターには適用されないパラメーターで、Packet-filter '*filter-name*' Config> プロンプトでしか入力できません。

add/change access-control *type*

Network Address Translation (NAT)

このタイプのパケット・フィルター・アクセス制御規則は、アドレス変換のためにパケットを NAT に引き渡します。このタイプは、inclusive (組み込み) と組み合わせて指定された場合 (例えば、***IN***) に限り有効です。タイプ NAT と IPsec は、同じ規則に指定できます (例えば、***INS***)。詳しくは、*ソフトウェア 使用者の手引き* に記載されている NAT フィーチャーの説明を参照してください。NAT に関するアクセス制御フィルターの例は、 *ソフトウェア 使用者の手引き* の IP セキュリティーの使用に関する章に記載されています。

有効値: N

省略時値: なし

IP Secure Tunnel (IPsec)

アウトバウンド・パケット・フィルター内のこのタイプのアクセス制御規則は、IPsec 内でのカプセル化のため (および場合によっては暗号化のため) に IPsec にパケットを引き渡します。インバウンド・パ

ケット・フィルターでは、IPsec (S) アクセス制御規則は、パケットが正しい IP 保護トンネルを通じて受信されたか検査します。このタイプは、inclusive (組み込み) と組み合わせて指定された場合 (例えば、***IS***) に限り有効です。タイプ NAT と IPsec は、同じ規則に指定できます (例えば、***INS***)。IPsec のアクセス制御フィルターの例は、ソフトウェア使用者の手引きの IP セキュリティー・フィーチャーの使用に関する章に示されています。

有効値: S

省略時値: なし

add/change access-control *IPsec-tunnel-ID*

このパラメーターは、規則タイプが IPsec の場合にのみ有効です。出力パケット・フィルターでは、このパラメーターは、パケットの送信に使用される IP 保護 (IPsec) トンネルを指定します。入力パケット・フィルターでは、このパラメーターは、パケットの受信に使用される IPsec トンネルを指定します。

有効値 1 ～ 65536

省略時値: 1

disable/enable source-addr-verification

このインバウンド・パケット・フィルター・オプションは、IP ルーティング・テーブルに基づいて、受信されたパケットの発信元 IP アドレスが発信元のインターフェースと矛盾していないか検査します。このオプションを選択すると、自分のものではない発信元 IP アドレスを使用している誤動作 IP ホストからパケットが転送されないようにすることができます。この誤動作は、スプーフィング と呼ばれます。

例:

```
Packet-filter 'filter-name' Config> enable source-addr-verification
```

例:

以下の例では、パケット・フィルター用の各種のアクセス制御規則の構成方法を示します。 NAT および IPsec のアクセス制御規則の例については、ソフトウェア使用者の手引きの IP セキュリティー・フィーチャーの使用に関する章を参照してください。

例 1-- 排他的タイプ・アクセス制御規則

この例には、ネットワーク 128.185.0.0 を起点とし、インターフェース 0 で受信される着信パケットをすべて排除する方法を示します。

```
    Packet-filter 'pf-in-0' Config> add access-control
    Enter type [E]?
    Internet source [0.0.0.0]? 128.185.0.0
    Source mask [255.255.255.255]? 255.255.0.0
    Internet destination [0.0.0.0]?
    Destination mask [255.255.255.255]? 0.0.0.0
    Enter starting protocol number ([CR] for all) [-1]?
Enable Logging? (Yes or [No]):
```

例 2-- アクセス制御規則からの削除

list access control コマンドを使用して、アクセス制御インデックス番号を見付けます。

```
    Packet-filter 'test' Config> delete access-control
    Enter index of access control to be deleted [1]? 4
```

ルーターは、ユーザーが指定したアクセス制御レコードを表示することによって応答します。

```
4  Type=I    Source=1.2.9.9       Dest=0.0.0.0          Prot=0-255
             Mask=255.0.0.255     Mask=0.0.0.0
             Sports=  0-65535     Dports=  1-65535
                                  Log=No
Are you sure this is the record you want to delete (Yes or [No]): y
    Deleted
    Packet-filter 'test' Config>
```

Dports はあて先ポートで、*Sports* は発信元ポートです。

例 3 -- List access-control コマンド

list access-control コマンドを使用すると、各パケット・フィルターごとに構成されたアクセス制御を表示して見ることができます。

```
Packet-filter 'pf-in-0' Config> list access-control
Access Control is: enabled
Access Control facility: USER

List of access control records:

1  Type=E    Source=128.185.0.0   Dest=0.0.0.0           Prot=0-255
             Mask=255.255.0.0     Mask=0.0.0.0
             Sports=  0-65535     Dports=  1-65535
             ACK0=N  T/C= **/**   Log=No

2  Type=IS   Source=9.67.8.3      Dest=128.54.67.8     Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.254
             Sports=  N/A         Dports=  N/A      Tid=5279
                                  Log=Yes ELS=N SNMP=Y SLOG=L(Emergency)

3  Type=I    Source=0.0.0.0       Dest=0.0.0.0           Prot=0-255
             Mask=0.0.0.0         Mask=0.0.0.0
             Sports= 1-65535      Dports=  1-68835
                                  Log=No
```

例 4--Move access-control コマンド

下に示すように **move access-control** コマンドを使用すると、パケット・フィルターのアクセス制御レコードの配列を変更することができます。

```
    Packet-filter 'pf-in-0' Config> move access-control
    Enter index of control to move [1]?
    Move record AFTER record number [2]? 2
    About to move:

1  Type=E    Source=128.185.0.0   Dest=0.0.0.0           Prot=0-255
             Mask=255.255.0.0     Mask=0.0.0.0
             Sports=  0-65535     Dports=  1-65535
             ACK0=N  T/C= **/**   Log=No
to be after:
2  Type=IS   Source= 9.67.8.3     Dest= 128.54.67.8      Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.254
             Sports=  N/A         Dports=  N/A      Tid=5279
                                  Log=Yes ELS=N SNMP=Y SLOG=L(Emergency)
Are you sure this is what you want to do (Yes or [No]): y
```

IP 監視環境へのアクセス

IP 監視コマンドにアクセスする場合は、次の手順を使用します。このプロセスによって、IP *監視* プロセスへのアクセスができます。

1. OPCON プロンプトで、**talk 5** を入力します。 (このコマンドについて詳しくは、ソフトウェア *使用者の手引き* の中の “OPCON プロセス” を参照してください)。例えば、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 **protocol ip** コマンドを入力すると、 IP> プロンプトが表示されます。

   例:

```
+ prot ip
IP>
```

IP 監視コマンド

この節では、IP 監視コマンドについて説明します。 表19 に、IP 監視コマンドをリストします。これらのコマンドにより、ルーターの IP 転送プロセスを監視することができます。監視機能には、 次のようなものがあります。つまり、インターフェース・アドレス や 静的ルートなどの構成済みパラメーターが表示でき、IP ルーティング・テーブルの現在の状態 が表示でき、IP ルーティング・エラーのカウントが一覧できます。

表 19. IP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Access controls	現行の IP アクセス制御モードを、構成済みのアクセス制御レコードとともにリストします。
Cache	最近ルーティングされたすべてのあて先のテーブルを表示します。
Counters	ルーティング・エラーおよび除去されたパケットのカウントを含む、さまざまな IP 統計をリストします。
Dump routing tables	IP ルーティング・テーブルの内容をリストします。
IGMP	IGMP のカウンターとパラメーターを表示します。
Interface addresses	ルーターの IP インターフェース・アドレスをリストします。
Packet-filter	指定されたパケット・フィルター、またはすべてのフィルターに関して定義されたアクセス制御情報を表示します。
Parameters	各種のパラメーター値をリストします。
Ping	ICMP エコー要求を別のホストに送信し、応答を観察します。このコマンドを使用して、インターネットワーク環境での問題を分離できます。
Redundant Default Gateway	冗長省略時ゲートウェイが存在するかどうか、また、それがアクティブか非アクティブかをリストします。
Reset	IP/RIP 構成を動的にリセットできるようにします。
RIP	RIP プロトコルの状況を表示します。
Route	特定の IP あて先へのルートが存在するかリストし、存在する場合は、そのルートに対応するルーティング・テーブル項目をリストします。
Route-table-filtering	定義済みのルート・フィルターがあればリストし、さらに、ルート・フィルターが使用可能か使用不能かを示します。
Sizes	特定の IP パラメーターのサイズを表示します。
Static routes	構成済みの静的ルートを表示します。これには省略時のゲートウェイが含まれます。
Traceroute	特定のあて先への完全なパス (通過する全ホップ) を表示します。

表 19. IP 監視コマンドの要約 (続き)

コマンド	機能
UDP-Forwarding	**add** コマンドや **enable** コマンドを使用して追加した、UDP ポート番号と着信 IP アドレスを表示します。
VRID	特定の VRID 定義についての詳しい情報を表示します。
VRRP	VRRP プロトコルの要約状況をリストします。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Access Controls

access controls コマンドは、使用中のグローバル・アクセス制御モードを、構成済みのアクセス制御規則のリストとともに印刷するのに使用します。

アクセス制御は、disabled (使用不能) (アクセス制御が行われておらず、アクセス制御レコードが無視されていることを意味します) または enabled (使用可能) (アクセス制御が行われており、アクセス制御規則が認識されていることを意味します) のいずれかです。**set access on** talk 6 コマンドは、アクセス制御を使用可能にします。

構文:

access

例: access

```
           Access Control currently enabled
           Access Control facility: USER
           Access Control run 702469 times, 657159 cache hits

           List of access control records:

1  Type=I    Source=2.2.2.2        Dest=2.2.2.128       Prot= 0-255
             SMask =255.255.255.254  DMask=255.255.255.128  Use=271
             Sports=  2-200          Dports=  1-100
                     T/C= 1/4      Log=Yes ELS=L SNMP=Y SLOG=S(Information)

2  Type=E    Source=0.0.0.0        Dest=0.0.0.0         Prot= 1
             SMask =255.255.255.255  DMask=255.255.255.255  Use=18962
             Sports=  N/A          Dports=  N/A
                      T/C= 1/**    Log=Yes ELS=N SNMP=N SLOG=L(Alert)

3  Type=I    Source=1.1.1.1        Dest=1.1.1.2         Prot= 6
             SMask =255.255.255.255  DMask=255.255.255.254  Use=42
             Sports=  2-200          Dports=  1-100
                                  Log=No

4  Type=I    Source=9.1.2.3          Dest=0.0.0.0       Prot=  0-255
             SMask =255.255.255.255  DMask=0.0.0.0      Use=0
             SPorts=  0-65535        DPorts=  0-65535
                      T/C= **/**     Log=N
             Tos=xE0/x00-x00         ModifyTos=x1F/x08
             PbrGw=9.2.160.1         UseDefRte=Y

5  Type=I    Source=0.0.0.0        Dest=0.0.0.0         Prot= 0-255
             Mask=0.0.0.0          Mask=0.0.0.0         Use=683194
             Sports=  1-65535      Dports=  1-65535
                                  Log=No
```

Exclusive (E) は、アクセス制御規則に合致するパケットが廃棄されることを意味します。Inclusive (I) は、アクセス制御規則に合致するパケットが転送されることを意味します。アクセス制御が enabled のときは、どのアクセス制御レコードにも合致しないパケットは廃棄されます。*Prot* (protocol) は IP プロトコル番号を示します。 *Sports* は TCP/UDP 送信元ポート番号の範囲を指示し、*Dports* は TCP/UDP 着信先ポート番

号の範囲を指示します。 *SYN* は、TCP 接続確立フィルターを指示します。 *T/C* は ICMP のタイプとコードを、また、*SLOG* は SysLog をそれぞれ表します。

Use フィールドでは、アクセス制御システムが特定のレコードを着信パケットに一致させた回数、例えば、IP アクセス制御システム内の特定のレコードが着信または発信パケットの特性によって呼び出された回数を指定します。

この例では、アクセス制御規則番号 4 で TOS フィルターが起動しました。 TOS パラメーターが表示されています。これらのパラメーターの説明については、 talk 6 の **add access-control** コマンドを参照してください。

Cache

cache コマンドは、最近にルーティングされたあて先を含む、IP ルーティング・キャッシュを表示するのに使用します。あて先がキャッシュにない場合は、ルーターがルーティング情報テーブルのあて先を順に調べて、転送の判断を行います。

構文:

cache

例: cache

```
            Destination     Usage           Next hop
            128.185.128.225 1               128.185.138.180 (Eth/0)
            192.26.100.42   1               128.185.138.180 (Eth/0)
            128.185.121.1   18              128.185.123.18  (PPP/0)
            128.185.129.219 76              128.185.125.25  (PPP/1)
            128.185.129.41  130             128.185.125.25  (PPP/1)
            128.185.129.134 546             128.185.125.40  (PPP/1)
            128.185.129.221 1895            128.185.125.40  (PPP/1)
            128.185.129.193 96              128.185.125.40  (PPP/1)
            128.197.3.4     4               128.185.123.18  (PPP/0)
            128.185.128.25  98              128.185.125.41  (PPP/1)
            128.185.124.121 4               128.185.124.121 (Eth/0)
            128.185.136.203 95              128.185.125.39  (PPP/1)
            128.185.194.4   581             128.185.125.39  (PPP/1)
            128.185.123.17  2               128.185.123.17  (PPP/0)
            192.26.100.42   1               128.185.125.38  (PPP/1)
            128.52.22.6     2               128.185.123.18  (PPP/0)
            128.197.3.2     1               128.185.123.18  (PPP/0)
            128.185.126.24  61              128.185.125.25  (PPP/1)
            128.185.138.150 482             128.185.125.39  (PPP/1)
            128.185.123.18  152             128.185.123.18
(PPP/0)
```

Destination
IP あて先ホスト

Usage あて先ホストに最近送信されたパケットの数

Next hop
あて先ホストへのパス上の次のルーターの IP アドレス。 パケットを転送するために送信ルーターによって使用されるインターフェースのネットワーク名も表示されます。

Counters

IP 転送プロセスに関連する統計を表示するには、**counters** コマンドを使用してください。これには、輻輳 (ふくそう) により除去されたパケットの数とともに、ルーティング・エラーのカウントが含まれます。

IP 監視コマンド (Talk 5)

構文:

counters

例: counters

```
Routing errors
Count   Type
    0   Routing table overflow
 2539   Net unreachable
    0   Bad subnet number
    0   Bad net number
    0   Unhandled broadcast
58186   Unhandled multicast
    0   Unhandled directed broadcast
 4048   Attempted forward of LL broadcast

Packets discarded through filter  0
IP multicasts accepted:           60592
 IP input packet overflows
    Net   Count
   TKR/0  0
    FR/0  0
```

Routing table overflow
ルーティング・テーブルがいっぱいであるために廃棄されたルートの数をリストします。

Net unreachable
あて先が不明であるため転送できなかったパケットの数を示します。これには、権限のあるルーター (省略時のゲートウェイ) に転送されたパケットの数は含まれません。

Bad subnet number
無効のサブネット (すべて 1 またはすべて 0) について受信されたパケットまたはルートの数を数えます。

Bad net number
無効の IP あて先 (例えば、クラス E のアドレス) について受信されたパケットまたはルートの数を数えます。

Unhandled broadcasts
受信された (非ローカルの) IP 同報通信 (これらは転送されません) の数を数えます。

Unhandled multicasts
受信されたが、そのアドレスがルーターによって認識されなかった IP マルチキャスト (これらは廃棄されます) の数を数えます。

Unhandled directed broadcasts
これらのパケットの転送が不能であるときの指定された (非ローカルの) IP 同報通信の受信数を数えます。

Attempted forward of LL broadcast
非ローカルの IP アドレスをもって受信されたが、リンク・レベル同報通信アドレスに送信されたパケットの数を数えます。これらは廃棄されます。

Packets discarded through filter
フィルターされたネットワーク/サブネットにアドレスされて受信されたパケットの数を数えます。これらは暗黙に廃棄されます。

IP multicasts accepted
ルーターによって受信され、正常に処理された IP マルチキャストの数を数えます。

IP packet overflows
転送側の入力待ち行列で輻輳 (ふくそう) (ふくそう) のために廃棄されたパケットの数を数えます。これらのカウントは受信するインターフェースによって分類されます。

Dump Routing Table

dump コマンドは、IP ルーティング・テーブルを表示するのに使用します。到達可能な各 IP ネットワーク/サブネットについて個別の項目が印刷されます。使用中の IP 省略時ゲートウェイ (ある場合) は、表示の末尾にリストされます。

構文:

dump

例: dump

```
Type   Dest net         Mask     Cost Age   Next hop(s)
SPE1   0.0.0.0          00000000  4    3    128.185.138.39  (2)
SPF*   128.185.138.0    FFFFFF00  1    1    Eth/0
Sbnt   128.185.0.0      FFFF0000  1    0    None
SPF    128.185.123.0    FFFFFF00  3    3    128.185.138.39  (2)
SPF    128.185.124.0    FFFFFF00  3    3    128.185.138.39  (2)
SPF    192.26.100.0     FFFFFF00  3    3    128.185.131.10  (2)
RIP    197.3.2.0        FFFFFF00  10   30   128.185.131.10
RIP    192.9.3.0        FFFFFF00  4    30   128.185.138.21
Del    128.185.195.0    FFFFFF00  16   270  None


Default gateway in use.

Type Cost Age  Next hop
SPE1 4    3    128.185.138.39

Routing table size: 768 nets (36864 bytes), 36 nets known
```

Type ルートがどのように派生したかを示します。

Sbnt - ネットワークがサブネット化されることを示します。このような項目はプレースホルダーのみです。

Dir - 直接接続されたネットワークまたはサブネットを示します。

RIP - ルートは RIP プロトコルを介して学習されたことを示します。

Del - ルートが削除されたことを示します。

Stat - 静的に構成されたルートを示します。

BGP - ルートが BGP プロトコルを介して学習されたことを示します。

BGPR - BGP プロトコルを介して学習され、OSPF および RIP によって再公示されるルートを示します。

Fltr - ルーティング・フィルターを示します。

SPF - ルートが OSPF 区域内ルートであることを示します。

SPIA - OSPF 区域間ルートであることを示します。

SPE1、SPE2 - OSPF 外部ルート (それぞれタイプ 1 および 2) を示します。

Rnge - 活動 OSPF 区域のアドレス範囲であり、パケットの転送に使用されないルート・タイプを示します。

Dest net
IP あて先ネットワーク/サブネット

Mask IP アドレス・マスク

Cost ルート・コスト

Age RIP および BGP ルートの場合、ルーティング・テーブル項目が最後に最新表示されてから経過した時間

Next Hop
あて先ホストへのパス上の次のルーターの IP アドレス。 送信ルーターがパケットを転送するのに使用するインターフェース・タイプも表示されます。

ルート・タイプの後のアスタリスク (*) は、そのルートが静的バックアップまたは直接接続されたバックアップをもつことを示します。ルート・タイプの後のパーセント記号 (%) は、このネットワーク/サブネットについて RIP 更新が常に受け入れられることを示します。

欄の末尾の括弧内の数は、あて先への等コスト・ルートの数を示しています。これらのルートに属する最初のホップは IP **route** コマンドを使って表示できます。

IGMP

IGMP カウンターや IGMP に関する稼働パラメーターを表示させる場合は、 **igmp** コマンドを使用します。

構文 :

igmp counters
parameters

counters
送受信された IGMP メッセージのカウントを表示します。

例 :

```
IP+ igmp counters
     Net      Querier      Polls Sent      Polls Rcvd      Reports Rcvd
     ---      -------      ----------      ----------      ------------
      0         Y            4973             0              0
      2         N               1             4921           0
      5         Y            4972             0              0
```

Net ネットワーク番号を指定します。

Querier
装置が指定されたネットワーク上の照会元であるかどうか指定します。

Polls Sent
送信された IGMP 照会の数

Polls Rcvd
受信された IGMP 照会の数

Reports Rcvd
受信された IGMP レポートの数

parameters
装置の接続インターフェースの稼働 IGMP パラメーターを表示します。

例 :

```
IP+ igmp parameters

        Net      Robustness      Query       Response     Leave Query
                  Variable      Interval     Interval      Interval
                                 (secs)       (secs)        (secs)
        ---      ----------     --------     --------     -----------
          0          2            125          10             1
          2          2            125          10             1
          5          2            125          10             1
```

Net IGMP インターフェースのネットワーク番号

Robustness variable
指定されたインターフェースの耐性変数

Query interval
この装置が指定 IGMP 照会元である場合に、そのネットワーク上での IGMP 一般照会間の秒数

Response interval
この装置が指定 IGMP 照会元である場合に、そのネットワーク上での IGMP 一般照会に挿入されている最大応答時間

Leave query interval
この装置が指定 IGMP 照会元である場合に、そのネットワーク上での IGMP 特定照会に挿入されている最大応答時間

Interface Addresses

interface addresses コマンドは、ルーターの IP インターフェース・アドレスを表示するのに使用します。 各アドレスは、その対応するハードウェア・インターフェースおよび IP アドレス・マスクとともにリストされます。 同じインターフェース上でのブリッジングおよびルーティングに使用されるブリッジ・インターフェースに IP アドレスが割り当てられている場合には、それもリストされます。 ブリッジ・インターフェースは、*BDG/0* で識別されます。

構成済みの IP インターフェースをもたないハードウェア・インターフェースは IP 転送プロセスによって使用されません。それらは、Not an IN net としてリストされます。1 つの例外があります。IP トラフィックを転送するためには、シリアル回線に IP インターフェース・アドレスを割り当てる必要はありません。そのようなシリアル回線は無番号と呼ばれます。それらはアドレス 0.0.0.0 をもっているとして示されます。

構文:

interface

例 : interface

```
Interface  IP Address(es)   Mask(s)          MTU
   TKR/0   133.1.169.2      255.255.252.0
    FR/0   133.1.167.2       255.255.254.0
```

Interface
インターフェースのハードウェア・タイプを示します。

IP addresses
インターフェースの IP アドレスを示します。

Mask インターフェースのサブネット・マスクを示します。

Packet-filter

packet-filter コマンドは、特定のパケット・フィルター、またはすべてのフィルターに関して定義された情報を表示するのに使用します。Packet-filters はインターフェースで固有のアクセス制御レコードのリストです。インターフェースは、同じインターフェース上でのルーティングおよびブリッジングに使用されるブリッジ・インターフェースの場合を除き、インターフェース番号で識別されます。ブリッジ・インターフェースの場合は、*BDG/0* で識別されます。

構文:

packet-filter [*name*]

例: packet-filter pf-in-0

```
Name              Direction     Interface  State  SRC-Addr-Check #Access-Controls
pf-in-0           Out           0          On     N/A            3

Access Control is: enabled
Access Control run 563 times, 271 cache hits

List of access control records:

0  Type=INS  Source=10.1.1.1      Dest=10.1.1.2          Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.254   Use=71
             Sports=  N/A         Dports=  N/A           Tid=5279
                                  Log=Yes ELS=N SNMP=Y SLOG=L(Emergency)

1  Type=I S  Source=9.67.1.5      Dest=9.37.192.1        Prot=6-255
             Mask=255.255.255.255 Mask=255.255.255.255   Use=15
             Sports=  N/A         Dports=  N/A           Tid=5
                                  Log=Yes ELS=L SNMP=N SLOG=L(Debug)

2  Type=I    Source=0.0.0.0       Dest=0.0.0.0           Prot=0-255
             Mask=255.255.255.255 Mask=255.255.255.255   Use=477
             Sports=  0-65535     Dports=  1-65535
                                  Log=N
```

Parameters

parameters コマンドは、各種パラメーターの値をリストするのに使用します。

例:

```
IP> parameters
ARP-SUBNET-ROUTING     : disabled
ARP-NET-ROUTING        : disabled
CLASSLESS              : disabled
DIRECTED BROADCAST     : enabled
ECHO-REPLY             : enabled
FRAGMENT-OFFSET-CHECK  : disabled
PER-PACKET-MULTIPATH   : disabled
REASSEMBLY-SIZE        : 12000 bytes
RECORD-ROUTE           : enabled
ROUTING TABLE-SIZE     : 768 entries (52224 bytes)
(Routing) CACHE-SIZE   : 64 entries
SAME-SUBNET            : disabled
SOURCE-ROUTING         : enabled
TIMESTAMP              : enabled
```

```
TTL                     : 64

IP>
```

Ping

ping コマンドは、ルーターに、ICMP Echo メッセージを与えられたあて先へ送信して (つまり、『pinging』)、応答を観察させるのに使用します。このコマンドは、インターネットワークでの問題を分離するのに使用できます。

構文:

ping *dest-addr [src-addr data-size ttl rate tos data-value]*

ping プロセスは継続的に行われ、パケットが 1 つ追加されるごとに ICMP シーケンス番号が増えます。合致する受信された各 ICMP エコー応答が、そのシーケンス番号および往復時間とともに報告されます。往復時間の細分性 (時間レゾリューション) はプラットフォームによって異なりますが、通常は約 20 ミリ秒です。

ping プロセスを停止するには、コンソールで任意の文字を入力してください。そうすると、パケット喪失、往復時間、および到達不能な ICMP あて先の数の要約が表示されます。

同報通信またはマルチキャスト・アドレスがあて先として与えられている場合、各グループ・メンバーについて 1 つずつ送信される各パケットについて複数の応答が印刷されることがあります。戻された各応答は応答側の発信元アドレスとともに表示されます。

PING のサイズ (ICMP ヘッダーを除く ICMP メッセージ内のデータ・バイトの数)、データの値、活動時間 (TTL) 値、PING の速度、設定する TOS ビットを指定できます。発信元 IP アドレスも指定できます。発信元 IP アドレスが指定されない場合、ルーターは、指定されたあて先への発信インターフェースでそのローカル・アドレスを使用します。ルーターの他のインターフェースのどれかからあて先への接続性を妥当性検査する場合は、そのインターフェースへの IP アドレスを発信元アドレスとして入力してください。

指定が必須なのは、destination パラメーターだけです。その他のパラメーターはすべて、任意指定です。省略時には、サイズは 56 バイト、TTL は 64、速度は 1 PING/秒、TOS 設定値は 0 です。ICMP データの最初の 4 バイトはタイム・スタンプに使用します。省略時解釈では、残りのデータは、、X'04' から始まり、X'FF' から X'00' まで (例えば、X'04 05 06 07 . . . FC FD FE FF 00 01 02 03 . . .')、1 ずつ増える値をもつ一連のバイトです。 これらの値は、省略時値が使用された場合にのみ増えます。データ・バイト値が指定された場合には、ICMP データはすべて (最初の 4 バイトは除きます) その値に設定され、その値は増えません。例えば、データ・バイト値を X'FF' に設定した場合、ICMP データは、値 X'FF FF FF . . .' をもつ一連のバイトです。

例 :

```
IP> ping
Destination IP address [0.0.0.0]? 192.9.200.1
Source IP address [192.9.200.77]?
Ping data size in bytes [56]?
Ping TTL [64]?
```

```
   Ping rate in seconds [1]?
   Ping TOS (00-FF) [0]? e0
   Ping data byte value (00-FF) [ ]?
   PING 192.9.200.77-> 192.9.200.1:56 data bytes,ttl=64,every 1 sec.
   56 data bytes from 192.9.200.1:icmp_seq=0.ttl=255.time=0.ms
   56 data bytes from 192.9.200.1:icmp_seq=1.ttl=255.time=0.ms
   56 data bytes from 192.9.200.1:icmp_seq=2.ttl=255.time=0.ms


   ----192.9.200.1 PING Statistics----
   3 packets transmitted, 3 packets received, 0% packet loss
   round-trip min/avg/max=0/0/0 ms
   IP>
IP>ping
```

Redundant Default Gateway

redundant default gateway コマンドは、各インターフェースについて構成された冗長省略時 IP ゲートウェイを表示するのに使用します。

構文:

redundant default gateway

例:

```
Redundant Default IP Gateways for each interface:
   inf  3   22.2.2.6   255.0.0.0   00.00.00.00.00.AB   backup standby
   inf  4   11.1.1.6   255.0.0.0   00.00.00.00.00.BA   primary active
```

注: Type (タイプ) は、『Primary』 (基本) または 『Backup』 (バックアップ) とすることができます。Status (状況) は 『Active』 (アクティブ) または 『Standby』 (待機) とすることができます。

Reset IP

reset IP コマンドは、IP/RIP 構成を動的にリセットするのに使用します。

構文:

reset ip

例:

```
IP>interface
Interface  IP Address(es)   Mask(s)
  Eth/0    30.1.1.2         255.255.255.0
           30.1.1.1         255.255.255.0
           153.2.2.25       255.255.255.240
   FR/0    10.69.1.1        255.255.255.0
  PPP/0    0.0.0.0          255.255.0.0
IP>
*talk 6

IP config>add address 0 5.1.1.1 255.255.0.0
IP config>
*talk 5

IP>reset ip

IP>interface
Interface  IP Address(es)   Mask(s)
  Eth/0    5.1.1.1          255.255.0.0
           30.1.1.2         255.255.255.0
           30.1.1.1         255.255.255.0
           153.2.2.25       255.255.255.240
```

```
   FR/0    10.69.1.1        255.255.255.0
  PPP/0    0.0.0.0          255.255.0.0

IP>
```

reset ip コマンドでは、以下の関数がサポートされます。

accept-rip-route	access-control	address
packet-filter	vrid	vr-address
icmp-redirect	nexthop-awareness	override
receiving	rip	rip2
sending	vrrp	broadcast-address
originate-rip-default	rip-in-metric	rip-out-metric
tag	source-addr-verification	fragment-offset-check
record-route	timestamp	access-control log-facility

RIP

rip コマンドは、RIP プロトコル状況明細を表示するのに使用します。

構文:

rip

例:

```
IP>rip

                                RIP Interfaces

Interface-Addr  Interface-Mask  Version  In Out  Send-Flags      Receive-Flags
10.69.1.1       255.255.255.0      1      1   0                  N,S,H
153.2.2.25      255.255.255.240    1      1   0  P,O             N,S,H
30.1.1.1        255.255.255.0      1      1   0  N,S,St,P        N,S
30.1.1.2        255.255.255.0      2      1   0  N,S,St,P        N,S
5.1.1.1         255.255.0.0        1      1   0  P,O             OFF
0.0.0.2         255.255.0.0        1      1   0  N,S,St,P        N,S
Send Flags: N=Network S=Subnet H=Host St=Static D=Default O=Outage-Only
            P=PoisonReverse
Recv Flags: N=Network S=Subnet H=Host OSt=Override-Static OD=Override-Default

        RIP Outage-Only Interfaces

Interface-Address  Outage-Network    Outage-Mask
153.2.2.25         3.0.0.0           255.0.0.0
5.1.1.1            10.50.0.0         255.255.0.0

RIP originates default with cost 4 under these conditions:
  BGP or OSPF External route from AS 3333 available
  Default origination conditions not satisfied
```

Route

route コマンドは、与えられた IP あて先までのルート (存在する場合) を表示するのに使用します。ルートが存在する場合には、次のホップの IP アドレスが、合致するルーティング・テーブル項目に関する詳しい情報とともに表示されます。(IP **dump** コマンドを参照してください。)

構文:

route *ip-destination*

例: route 133.1.167.2

```
Destination:    133.1.166.0
Mask:           255.255.254.0
Route type:     SPF
Distance:       1
Age:            1
Tag:            0
Next hop(s):    133.1.167.2       (FR/0)
```

例: route 128.185.230.0

```
Destination:   128.185.230.0
Mask:          255.255.255.0
Route type:     SPF
Distance:       1
Age:            1
Next hop(s):   128.185.230.0    (TKR/0)
```

例: route 128.185.232.0

```
Destination:   128.185.232.0
Mask:          255.255.255.0
Route type:    RIP
Distance:      3
Age:           0
Next hop(s):   128.185.146.4   (Eth/0)
```

Route-table-filtering

route-table-filtering コマンドは、ルート・テーブル・フィルターが使用可能になっているかどうかを表示し、定義済みルート・テーブル・フィルターをリストするのに使用します。

構文:

route-table-filtering

例: route-table-filtering

```
IP>route-table-filtering
Route Filters

Destination     Mask            Match Type
10.1.1.0        255.255.255.0   BOTH  E
10.1.1.1        255.255.255.255 EXACT I
50.0.0.0        255.0.0.0       BOTH  E
50.50.0.0       255.255.0.0     BOTH  I

IP>
```

Sizes

sizes コマンドは、特定の IP パラメーターの構成済みサイズを表示するのに使用します。

構文:

sizes

例: sizes

```
Routing table size:         768
Table entries used:         3
Reassembly size:            12000
Largest reassembled pkt:    0
Size of routing cache:      64
# of cache entries in use:  0
```

Routing table size
ルーティング・テーブルが保持する項目の構成済みの数

Table entries used
ルーティング・テーブルから使用される項目の数。この数はアクティブおよび非アクティブの両方の項目を含みます。“dump” コマンドを使用して、“xx nets known” として表示された値は、アクティブなルーティング・テーブル項目の数です。構成されたルーティング・テーブル・サイズは、現行のアクティブ項目ならびに他の予期されるルーティング項目を保持するのに十分なだけ大きい必要があります。

Reassembly buffer size
断片化された IP パケットの組み立てに使用される再アセンブリー・バッファーの構成済みのサイズ。

Largest reassembled pkt
このルーターが組み立てる必要があった最大の IP パケット

Size of routing cache
ルーティング・キャッシュの構成済みのサイズ

# of cache entries in use
現在キャッシュから使用されている項目の数

Static Routes

static routes コマンドは、構成済み静的ルートのリストを表示するのに使用します。構成済みの省略時ゲートウェイおよび省略時サブネット・ゲートウェイもリストされます。

各静的ルートのあて先はアドレスとマスクの対で指定します。省略時ゲートウェイは着信先が 0.0.0.0 でマスクが 0.0.0.0 の静的ルートとして現れます。省略時のサブネット・ゲートウェイも IP サブネット・ネットワーク全体への静的ルートとして現れます。

次の例は、構成済みの省略時ゲートウェイ、構成済みの省略時サブネット・ゲートウェイ (128.185.0.0 がサブネットされていると想定)、およびネットワーク 192.9.10.0 への静的ルートを示しています。

構文:

static

```
IP>static routes
Net             Mask            Cost  Next hop
1.1.0.0         255.255.0.0     1     10.1.1.1        TKR/0
                                2     20.1.1.1        TKR/1
                                3     30.1.1.1        TKR/2
2.2.0.0         255.255.0.0     10    10.2.2.2        TKR/0
3.3.0.0         255.255.0.0     100   10.3.3.3        TKR/0
                                200   20.3.3.3        TKR/1

IP>
```

Net ルートのあて先アドレス

Mask ルートのあて先マスク

Cost このルートを使用するコスト

Next Hop
このルートを使用してパケットが通過する次のルーター

Traceroute

traceroute コマンドは、与えられたあて先までのパス全体をホップ単位で表示するのに使用します。連続するそれぞれのホップごとに、**traceroute** では、省略時値である 3 つのプローブを送り出し、応答側の IP アドレスを応答に対応する往復時間と共に印刷します。特定のプローブが応答を受信しない場合は、アスタリスクが表示されます。画面の各行は、この 3 つのプローブの組み合わせに関連しており、一番左の数はコマンドを実行するルーターからの距離 (ルーター・ホップ数) を示しています。

traceroute は、あて先に到達するか、ICMP あて先到達不能メッセージが受信されるか、パスの長さが省略時の最大値 32 に達すると行われます。

プローブが予期しない結果を受信するときは、表示される可能性のある指示がいくつかあります。『!N』 は、ICMP Destination Unreachable (ネット到達不能) が受信されたことを示します。『!H』 は、ICMP Destination Unreachable (ホスト到達不能) が受信されたことを示します。『!P』 は、ICMP Destination Unreachable (プロトコル到達不能) が受信されたことを示します。プローブは、見知らぬポートに送信された UDP パケットなので、ポート到達不能が予期されます。『!』 では、あて先に到達したが、あて先によって送信された応答は、 TTL が 1 で受信されたことを示します。これは、通常、あて先に UNIX の一部のバージョンに認められるエラーがあり、そのためにあて先で応答にプローブの TTL を挿入していることを示します。運悪くこれが生じると、あて先へ最後に到達する前に、アスタリスクのみから構成される行がいくつも印刷されることになります。

構文:

traceroute *dest-addr [src-addr data-size probes wait tos max-ttl]*

dest-addr
ルートの遠端のアドレス

src-addr
トレース発信元の発信元アドレス

data-size
traceroute メッセージのデータ・フィールドのサイズ (バイト数)。データ・フィールドには、UDP ヘッダーは含まれません。

probes
それぞれのホップから送信された UDP traceroute メッセージの数

wait 再試行間の時間 (秒数)

tos UDP メッセージ内の TOS ビットの設定。例えば、X'10' という値 (B'00010000') では、TOS ビットは B'1000' に設定されます。省略時値は 0 で、TOS ビットは B'1000' に設定されます。

max-ttl
それぞれのメッセージごとの最大活動時間 (秒数)

例 :

```
IP> traceroute
Destination IP address [0.0.0.0]? 128.185.142.239
Source IP address [128.185.142.1]?
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
Traceroute TOS (00-FF) [0]? 10

TRACEROUTE 128.185.142.1 -> 128.185.142.239: 56 data bytes
1 128.185.142.7 16 ms 0 ms 0 ms
2 128.185.123.22 16 ms 0 ms 16 ms
3 * * *
4 * * *
5 128.185.124.110 16 ms ! 0 ms ! 0 ms !
```

TRACEROUTE
あて先区域アドレスおよびそのアドレスに送信されるパケットのサイズを表示します。

1 あて先の NSAP およびパケットがあて先に到達するのに要した時間を示す第１のトレース。パケットは 3 度トレースされます。

Destination unreachable
あて先へのルートがないことを示します。

3 * * *
ルーターがあて先から何らかの形の応答を予期していますが、あて先が応答しないことを示します。

UDP-Forwarding

UDP-forwarding コマンドは、**add udp-destination** コマンドまたは **enable udp-forwarding** コマンドを使用して追加した UDP ポートおよびアドレスを表示するのに使用します。

構文:

udp-forwarding

例: udp-forwarding

```
            UDP Port   IP Address
                35      20.2.1.1
                20      22.2.1.2
```

VRID

VRID コマンドは、インターフェース・アドレスおよび VRID によって識別される特定のバーチャル・ルーターについて詳細状況を表示するのに使用します。

構文:

vrid

例:

```
IP>vrid 153.2.2.25 1

             --- Detailed VRID Information ----

            Interface address:      153.2.2.25
            Interface mask:         255.255.255.240
```

```
                VRID:                   1
                VRID State:             MASTER
                Virtual MAC Address:    00:00:5E:00:00:01
                Source MAC Address:     00:00:5E:00:00:01
                Ethernet V2 Interface:  UP

  Priority:             255       Advertise interval:   1
  Advertise Timer:      1         Skew (in ticks):      0
  Authentication Type:  NONE      Authentication Key:
  State transitions:    1         Advertisements out:   9019
  Advertisements in:    0         Advertisements error: 0
  ARPs Modified:        22        Gratuitous ARPs:      2

                    VRID Addresses
153.2.2.25          5.1.1.1
```

VRRP

VRRP コマンドは、要約情報を表示するのに使用します。

構文:

vrrp

例:

```
                                        --VRID Summary--
IP address       VRID  State  Advertise Master-Dead  Address(es)
153.2.2.25          1  MASTER         1         N/A  153.2.2.25
                                                     5.1.1.1
```

第16章 OSPF の使用

この章では、内部ゲートウェイ・プロトコル (IGP) の 1 つである 最短パス最優先オープン (OSPF) プロトコルの使用法について説明します。ルーターは、IP ルーティング・テーブル、最短パス最優先オープン (OSPF) プロトコルおよび RIP プロトコルを構築するために次の IGP をサポートしています。OSPF は、リンク状態技術または最短パス最優先 (SPF) アルゴリズムに基づいています。RIP は Bellman-Ford または距離ベクトル・アルゴリズムに基づいています。

この章には次の節が含まれています。

共通ルーティング・プロトコルを使用するルーターは、*自律システム* (AS) を形成します。この共通ルーティング・プロトコルが内部ゲートウェイ・プロトコル (IGP) と呼ばれます。IGP は AS 内のネットワーク到達可能性およびルーティング情報を動的に検出し、この情報を使用して IP ルーティング・テーブルを構築します。IGP は外部ルーティング情報を AS にインポートすることもできます。ルーターは OSPF と RIP を同時に実行することができます。その場合は、OSPF ルートが優先されます。一般的に、OSPF プロトコルは堅固で、応答性がよく、帯域幅要件が少ないので、これを使用するようお勧めします。

OSPF ルーティング・プロトコル

ルーターは、RFC 1583 (バージョン 2) で指定されているように、OSPF ルーティング・プロトコルの完全な実施をサポートとします。OSPF は、到達可能なあて先への最適ルートを検出および学習するリンク状態の動的ルーティング・プロトコルです。 OSPF は、AS のトポロジーの変更を即時に認知し、短い収束期間後に新しいルートを計算することができます。OSPF プロトコルは、IP パケットをカプセル化しないで、あて先アドレスのみに基づいて転送します。

OSPF は、(到達可能な) あて先への最適ルートを検出および学習するリンク状態の動的ルーティング・プロトコルです。OSPF は、AS のトポロジーの変更を即時に認知し、短い収束期間後に新しいルートを計算することができます。OSPF プロトコルは、IP パケットをカプセル化しないで、あて先アドレスのみに基づいて転送します。

OSPF ルーティングの要約

ルーターが初期設定されると、ハロー・プロトコルを使用してそのハロー・パケットを近隣に送信します。そうすると、今度は近隣がこのルーターにそれぞれのパケットを送信します。同報通信ネットワークおよびポイント・ポイント・ネットワークでは、ルーターはマルチキャスト・アドレス *ALLSPFRouters (224.0.0.5)* にハロー・

パケットを送信することによって、その近隣ルーターを動的に検出します。非同報通信ネットワークでは、情報を構成してルーターがその*近隣* を見付けるのに役立てる必要があります。すべてのマルチアクセス・ネットワーク (同報通信および非同報通信) で、ハロー・プロトコルはそのネットワークに関する*指定ルーター* も選びます。

注: ATM ネットワークの場合、RFC 1577 があると、IP は、ネットワークを非同報通信複数アクセス・ネットワークとして使用することができます。 したがって、OSPF は非同報通信であるものとみなして構成してください。 LAN エミュレーションを使用している場合、ネットワークは、同報通信ネットワークとして扱われるため、OSPF もそれに準じて構成する必要があります。 RFC 1577 と LAN エミュレーションの両方を単一の物理インターフェース上で使用している場合は、RFC 1577 インターフェース (例えば ATM/0 などの、実インターフェースに割り当てられた IP アドレス) 上で OSPF 非同報通信を構成し、バーチャル・インターフェースまたはエミュレート済みインターフェース (たとえば TKR/0 などの、エミュレート済みインターフェースまたはバーチャル・インターフェース) 上で OSPF 同報通信を構成してください。

その上で、ルーターは近隣との隣接を形成して、近隣のトポロジー・データベースの同期化を試みます。隣接は、ルーティング・プロトコル・パケットの配布 (送信および受信)、ならびにトポロジー・データベースの更新の配布を制御します。マルチアクセス・ネットワークでは、指定ルーターによって隣接になるルーターが決まります。

ルーターはその状況またはリンク状態を定期的に隣接に公示します。*リンク状態公示* (LSA) は区域全体に伝送しますから、すべてのルーターがまったく同じトポロジー・データベースをもつことができます。このデータベースは、1 つの区域に属する各ルーターから受信したリンク状態公示の集合です。このデータベース内の情報から、各ルーターは、それ自体をルートに指定して最短パスのツリーを計算することができます。そこで最短パスのツリーによってルーティング・テーブルが生成されます。

OSPF は、RIP では使用不能なサービスが得られるように設計されています。 OSPF には次のフィーチャーが組み込まれています。

- *最小コストのルーティング。* したがって、どんな組み合わせのネットワーク・パラメーターに基づいてでも、パス・コストを構成することができます。例えば、帯域幅、遅延、およびドル・コスト。
- *無制限のルーティング・メトリック。* RIP ではルーティング・メトリックを 16 ホップに制限しますが、 OSPF には制限がありません。
- *マルチパス・ルーティング。* したがって、同一地点を接続する等コストの複数のパスを使用することができます。そこで、これらのパスを使用して負荷分散を図ることができるので、結果的にネットワーク帯域幅の使用が効率化されます。
- *区域ルーティング。* プロトコルによって使用される資源 (メモリーおよびネットワーク帯域幅) を減らし、追加レベルのルーティング保護が得られます。
- *可変長サブネット・マスク。* IP アドレスを可変サイズ・サブネットに分割して、IP アドレス・スペースを節約して使用することができます。
- *ルーティング認証。* 追加のルーティング・セキュリティーが得られます。

OSPF は次の物理ネットワーク・タイプをサポートします。

- *ポイント・ポイント。* 一対のルーターを結合するための通信回線を使用するネットワーク。2 つのルーターを接続する 56 Kbps のシリアル回線は、ポイント・ポイント・ネットワークの一例です。
- *同報通信。* 3 つ以上の接続されたルーターをサポートし、接続されたルーターのすべてに単一の物理メッセージをアドレス指定することができるネットワーク。トークンリング・ネットワークは同報通信ネットワークの一例です。 ATM を介したエミュレート LAN は、ATM ネットワークを同報通信ネットワークとして扱います。
- *非同報通信マルチアクセス (NBMA)。* 3 つ以上の接続されたルーターをサポートするが、同報通信機能をもたないネットワーク。X.25 公衆データ網は非同報通信ネットワークの一例です。OSPF が正しく機能するためには、このネットワークでは、非同報通信ネットワークに接続された他の OSPF ルーターについての余分な構成情報を必要とします。 ATM を介したクラシカル IP (RFC 1577) は、 ATM インターフェースを非同報通信複数アクセス (NBMA) インターフェースとして扱います。
- *ポイント・マルチポイント。* 3 つ以上の接続されたルーターをサポートするが、同報通信機能をもたず、全メッシュされていないネットワーク。すべての接続されているルーター間に PVC のないフレーム・リレー・ネットワークは、ポイント・マルチポイント・ネットワークの一例です。非同報通信ネットワークと同様、ネットワークに接続された他の OSPF ルーターについての特別な構成情報が必要とします。

指定ルーター

同報通信または非同報通信マルチアクセス・ネットワークにはすべて指定ルーターがあり、ルーティング・プロトコルに関する 2 つの主要な機能を果たしています。つまり、ネットワーク・リンク公示の起点となり、ネットワーク上の他のすべてのルーターの隣接になります。

指定ルーターがネットワーク・リンク公示の起点となる場合は、現在ネットワークに接続されているルーターを、指定ルーター自体も含めて、すべてリストします。この公示のリンク ID は、指定ルーターの IP インターフェース・アドレスです。サブネット/ネットワーク・マスクを使用することによって、指定ルーターは IP ネットワーク番号を入手します。

指定ルーターは、他のすべてのルーターの隣接になり、同報通信ネットワーク上のリンク状態データベースの同期化をタスクとします。

OSPF ハロー・プロトコルは、ハロー・パケットの *Rtr Pri* フィールドからルーターの優先順位を判別した上で、指定ルーターを選びます。ルーターのインターフェースは、最初に機能を果たすようになった時点で、ネットワークに現在指定ルーターがあるかどうか確認検査します。指定ルーターがある場合は、ルーターの優先順位に関係なく、その指定ルーターを受け入れますが、指定ルーターがない場合は、それ自体が指定ルーターを宣言します。ルーター自体が指定ルーターを宣言した時点で、同時に別のルーターもそれ自体が指定ルーター宣言を行っている場合は、ルーター優先順位 (*Rtr Pri*) が上位のルーターが指定ルーターになります。両方の *Rtr Pris* が等しい場合は、より高いルーター ID をもつルーターが選択されます。

指定ルーターが選ばれると、それが多くの隣接の終点になります。同報通信ネットワークでは、これによって、指定ルーターは別個のパケットを各隣接ごとに送信す

るのではなく、そのリンク状態更新パケットをアドレス ALLSPFRouters (224.0.0.5) にマルチキャストすることができるので、伝送手順が最適化されます。

マルチキャスト OSPF

マルチキャストは LAN 技法の 1 つで、これを使用すると、考えられるあて先すべての選択されたサブセットに 1 つのパケットのコピーを渡すことができます。ハードウェアによっては (例えば、イーサネット)、ネットワーク・インターフェースが 1 つまたは複数のマルチキャスト・グループに属することができるようにすることによって、マルチキャストをサポートするものがあります。ルーターのサポートする IP マルチキャストの詳細については、262ページの『IP マルチキャスト・サポート』を参照してください。

OSPF プロトコルは、OSPF へのマルチキャスト拡張 (MOSPF) による IP マルチキャスト・ルーティングをサポートします。

MOSPF ルーターは、新しいタイプ (タイプ 6) のリンク状態公示であるグループ・メンバーシップ LSA を伝送することによって、ルーティング・ドメイン全体にグループ・ロケーション情報を配布します。こうすることで、MOSPF ルーターは、マルチキャスト・データグラムを複数のあて先に効率的に転送することができます。各ルーターは、データグラム発信元をルートとし、グループ・メンバーを含む LAN を端末ブランチとするツリーとして、マルチキャスト・データグラムのパスを計算することによって、これを行います。

MOSPF を実行する一方で、マルチキャスト・データグラム転送は次のように行われます。

- IP マルチキャストの転送は信頼性が高くないが、IP マルチキャスト・データグラムは、IP ユニキャストの送達の場合と同じくベストエフォートで送達されます。
- マルチキャスト・データグラムは、データグラム発信元と特定のあて先の間の最短パスを通ります (OSPF リンク状態コスト)。これが行われるのは、データグラム発信元とあて先をグループとした各対ごとに、それぞれ別個のツリーが構築されるからです。
- マルチキャスト・データグラムは、各ホップごとにデータ・リンク・マルチキャストとして転送されます。ARP プロトコルは使用されません。ネットワーク技術によって、クラス D IP アドレスとデータ・リンク・マルチキャストの間のマッピングが行われるものもあれば、クラス D IP アドレスがデータ・リンク同報通信アドレスとマップされるものもあります。
- データグラム発信元から 2 つの別個のグループ・メンバーに至るパスが初期共通セグメントを共用している場合は、パスが別個の方向に向かうまでは、単一のデータグラムだけが転送されます。パスはルーターとネットワークのいずれかで分割されます。パスがルーターで分割される場合は、ルーターがパケットを複写してから、パケットが送信されます。パスがネットワークで分割される場合は、データ・リンク・マルチキャストを通じて複写します。
- ネットワーク構成は、MOSPF ルーターおよびマルチキャスト拡張がないルーターの両方を含む場合があります。この構成では、すべてのルーターがユニキャストのルーティングで相互運用されます。これによって、マルチキャスト機能をインターネットワークにゆっくり組み入れることができます。

MOSPF ルーターと非 MOSPF ルーターの構成によっては、マルチキャスト・ルーティングで予期しない障害を起こす場合があります。

- ルーターは、特定の SNMP コミュニティー名にグループ・アドレスを追加することにより、SNMP トラップをマルチキャスト・グループ・アドレスに送信するよう構成することができます。

OSPF を構成する

以下の項では、OSPF プロトコルを初期に構成する方法についての情報を提供します。この情報では、OSPF プロトコルの立ち上げと実行に必要な作業を概説します。さらに構成変更を行う方法の説明は、355ページの『OSPF 構成コマンド』で行います。

以下のステップは、OSPF プロトコルの立ち上げおよび実行に必要な作業の概要を示すものです。各ステップの詳細については、例を含めて以下の各項で説明します。

ルーターが OSPF プロトコルを実行できるようにする前に、次のことを行う必要があります。

1. OSPF プロトコルを使用可能にする。これを行う際、OSPF ルーティング・ドメインの最終サイズを見積もる必要があります。(338ページの『OSPF プロトコルを使用可能にする』を参照してください。)
2. OSPF ルーター ID を設定する。データ・リンク・マルチキャストまたは同報通信をサポートしないネットワーク技術 (例えば、フレーム・リレー) の場合、マルチキャスト・データグラムをルーターで複写して、データ・リンク・ユニキャストとして転送する必要があります。 (338ページの『OSPF ルーター ID を設定する』を参照してください。)
3. ルーターに接続された OSPF 区域を定義する。OSPF 区域を定義しない場合は、単一バックボーン区域が想定されます。(339ページの『バックボーン OSPF 区域および接続された OSPF 区域を定義する』を参照してください。)
4. ルーターの OSPF ネットワーク・インターフェースを定義する。各インターフェースからパケットを送信するコストを、OSPF 操作パラメーターの集合とともに設定します。(342ページの『OSPF インターフェースを設定する』を参照してください。)
5. IP マルチキャスト (IP クラス D のアドレス) を転送したい場合は、IP マルチキャスト・ルーティング機能を使用可能にします。(345ページの『マルチキャスト転送』を参照してください。)
6. ルーターが、 RFC 1577 を使用する ATM (ATM を介したクラシカル IP や ARP) など、非同報通信ネットワーク (X.25、ATM を介したクラシカル IP、フレーム・リレー) にインターフェースでつながっている場合は、追加のインターフェース・パラメーターを設定する。 (345ページの『非同報通信ネットワーク・インターフェース・パラメーターを設定する』 および 346ページの『広域サブネットワークを構成する』 を参照してください)。
7. ルーターにこのルーターで実行される他のルーティング・プロトコル (BGP, RIP または静的に構成されたルート) から学習したルートをインポートさせたい場合は、AS 境界ルーティングを使用可能にする。さらに、ルートが外部タイプ 2 または

外部タイプ 1 のどちらとしてインポートされるか定義する必要があります。(347 ページの『AS 境界ルーティングを使用可能にする』を参照してください。)

8. 接続されたポイント・ポイント・インターフェースまたは ポイント・マルチポイント・インターフェースを通じて近隣ルーターにブートしたい場合には、近隣の IP アドレスを構成する。 これは、ポイント・ポイント・インターフェースのあて先の OSPF 近隣を追加することによって行います。

OSPF プロトコルを使用可能にする

OSPF ルーティング・プロトコルを使用可能にするときは、OSPF リンク状態データベースのサイズを見積もるために次の 2 つの値を指定する必要があります。

- OSPF ルーティング・ドメインにインポートされる AS 外部ルートの総数。単一のあて先が別個の AS 境界ルーターによってインポートされるときは、単一のあて先から複数の外部ルートが発生することがあります。例えば、OSPF ルーティング・ドメインに 2 つの AS 境界ルーターがあり、両方のルーターが同じ 100 のあて先へのルートをインポートしているとすると、AS 外部ルートの数は 200 に設定します。
- ルーティング・ドメインでの OSPF ルーターの総数

これら 2 つの値は、すべての OSPF ルーターで同様に構成します。 OSPF プロトコルを実行する各ルーターには、ルーティング・ドメインのマップを記述するデータベースがあります。このデータベースは、参加するすべてのルーターで同一です。このデータベースから、IP ルーティング・テーブルは、ルーター自体をルートとする、最短パスのツリーの構築を通して作成されます。ルーティング・ドメインは、OSPF プロトコルを実行する AS を参照します。

OSPF ルーティング・プロトコルを使用可能にするには、次の例に示すように **enable** コマンドを使用してください。

```
OSPF Config> enable ospf
Estimated # external routes[100]? 200
Estimated # OSPF routers [50]? 60
Maximum Size LSA [0]? 2048
```

通常、2048 バイトあれば、ルーターによって生成されるどのリンク状態公示 (LSA) にも十分です。ただし、OSPF ダイヤル・リンクが多数あるルーター (例えば、ISDN ダイヤル・リンク) の場合は、もっと大きな LSA が必要であると考えられます。また、そういった状況では、一般構成で **packet-size** も増やなければならない場合があります。

OSPF ルーター ID を設定する

OSPF ルーティング・ドメイン内の各ルーターには、固有の 32 ビットのルーター ID を割り当てる必要があります。次のようにして、OSPF ルーター ID に使用される値を選択してください。

- IP 構成 **set router ID** コマンド使用した場合は、構成された値は OSPF ルーター ID として使用されます。
- IP 構成 **set internal address** コマンド使用した場合は、構成されたアドレスは OSPF ルーター ID として使用されます。ルーター ID と内部アドレス (定義されている場合) には同じ値を使用するようお勧めします。

- IP 構成時にルーター ID も内部アドレスも構成されていない場合は、最初の OSPF インターフェース・アドレスが OSPF ルーター ID として使用されます。

バックボーン OSPF 区域および接続された OSPF 区域を定義する

340ページの図34 に OSPF ルーティング・ドメインの構造のサンプル図を示します。1 つの分割は、OSPF ドメイン内の IP サブネットワークと OSPF ドメインの外部の IP サブネットワークの間で行われます。OSPF ドメイン内に含まれるサブネットワークは *区域* と呼ばれる領域に細分されます。OSPF 区域は、連続する IP サブネットワークの集合です。区域の機能は、異なる区域にあるあて先へのルートを見つけるために必要な OSPF オーバーヘッドを減らすことです。ルーター間で交換される情報が少なくなるためと、より単純なルート・テーブル計算に必要な CPU サイクルが減るための両面から、オーバーヘッドが減ります。

各 OSPF ルーティング・ドメインは少なくともバックボーン*区域* をもっている必要があります。 バックボーンは常に区域番号 0.0.0.0 によって識別されます。小さな OSPF ネットワークでは、バックボーンは必要とされる唯一の区域です。複数の区域をもつ大きなネットワークでは、バックボーンは区域を接続するコアを提供します。他の区域と異なり、バックボーンのサブネットは物理的に別個であることができます。この場合、バックボーンの論理接続性は、バックボーン・ルーター間のバーチャル・リンク を、介在する非バックボーン通過区域を横切るように構成することによって維持されます。

2 つ以上の区域に接続されたルーターは、*境界ルーター* として機能します。すべての境界ルーターはバックボーンの部分ですから、境界ルーターは直接バックボーン IP サブネットに接続されるか、バーチャル・リンクを介して別のバックボーン・ルーターに接続される必要があります。さらに、すべてのバックボーン・ルーターを接続する、バックボーン・サブネットワークとバーチャル・リンクの集合がなければなりません。

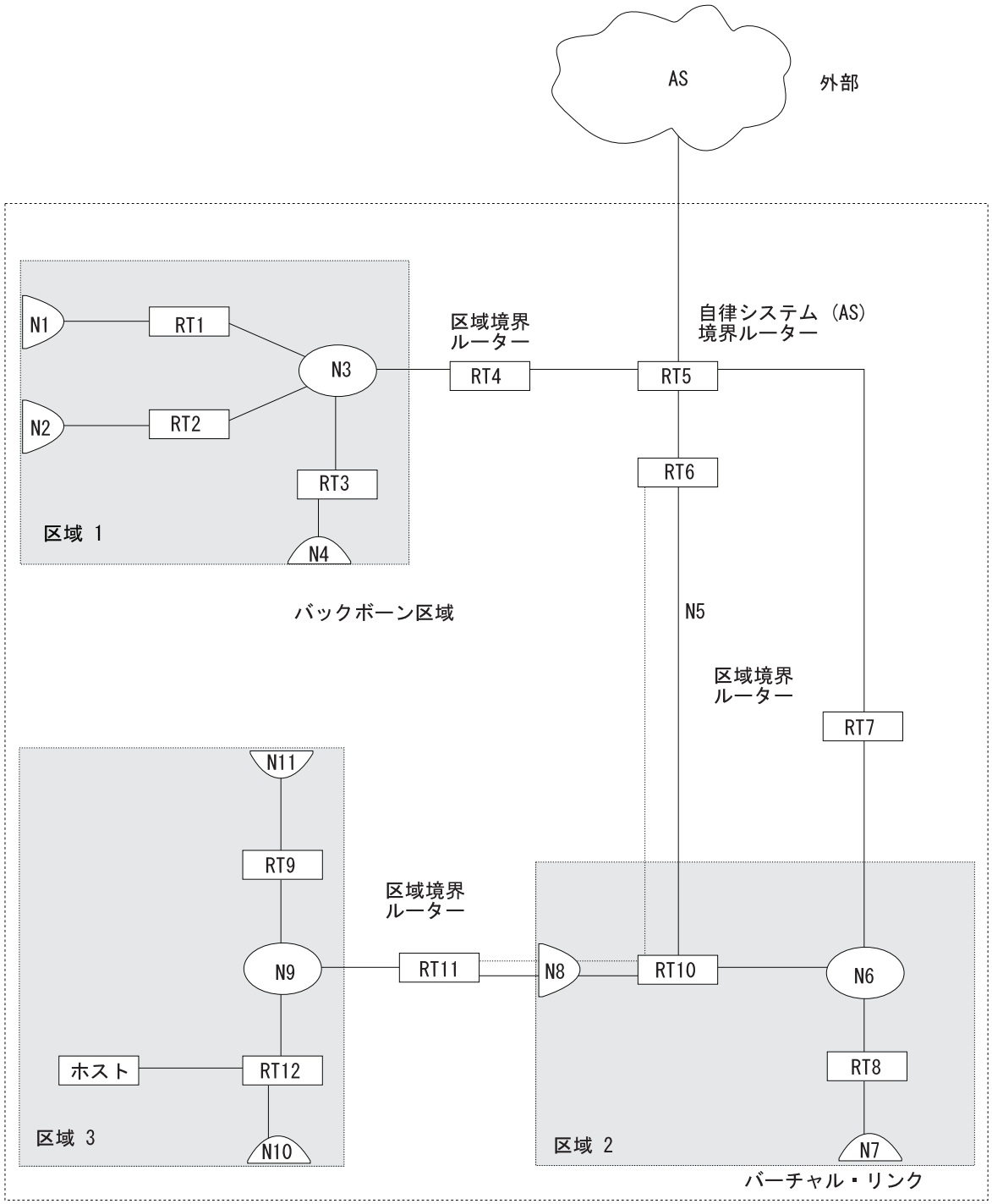


図 34. OSPF 区域

ルートを計算するために OSPF によって使用される情報およびアルゴリズムは、着信先 IP サブネットワークが同じ区域内にあるか、同じドメイン内の異なる区域内にあるか、または OSPF ドメインの外部にあるかによって異なります。各ルーターは、その区域内のすべてのリンクの完全なマップを保持しています。マルチアクセス・ネットワークへのすべてのルーター、マルチアクセス・ルーターへのネットワーク、およびルーター間のリンクがマップに含まれています。このマップから区域内の着信先への最善のルートを計算するために、最短パス最優先のアルゴリズムが使用さ

れます。区域間のルーターは、IP サブネットワークについての区域境界ルーター、IP サブネットワーク範囲、および OSPF ドメインの他の区域にある自律システム外部 (ASE) 境界ルーターによって発信される要約公示から計算されます。外部ルートは、ASE 境界ルーターによって発信される ASE 公示から計算され、OSPF ルーティング・ドメイン全体に伝送されます。

バックボーンは区域間ルーティング情報の配布を担当します。バックボーン区域は次のいずれでも構成されます。

- 区域 0.0.0.0 に属するネットワーク
- それらのネットワークに接続されたルーター
- 複数の区域に属するルーター
- 構成済みバーチャル・リンク

set area コマンドを使用して、ルーターが接続する区域を定義してください。**set area** コマンドを使用しないと、省略時値では、ルーターのすべてのインターフェースがバックボーンに接続されます。

区域境界ルーターが構成される場合は、どの OSPF ルート情報が区域境界を横断するかを制御するために、**set area** および **add range** コマンドのオプションを使用することができます。

1 つのオプションは、**set area** コマンドを使用して、区域をスタブ として定義することです。OSPF ASE 公示がスタブ区域に伝送されることは決してありません。**set area** コマンドには、さらに、区域間ルートについて要約公示のスタブへの発信を抑制するためのオプションがあります。区域境界ルーターは、スタブ区域への省略時のルートを公示します。スタブ内で不明の IP サブネットに宛てられるトラフィックは、区域境界ルーターに転送されます。区域ルーターはそのより完全なルーティング情報を使用して、トラフィックをそのあて先への適切なパスに転送します。区域は、それがバーチャル・リンク用の通過区域に使用されている場合は、スタブとして構成することはできません。

他方のオプションは、IP サブネット・アドレス範囲を使用して、区域のサブネットの区域間公示に使用される要約公示の数を制限することです。範囲は、IP アドレスおよびアドレス・マスクによって定義されます。サブネット IP アドレスおよび範囲 IP アドレスが、範囲マスクが両方のアドレスに適用された後に一致する場合は、サブネットは範囲内にあると見なされます。

区域境界ルーターで区域について範囲が追加される場合、境界ルーターは、範囲内に含まれている区域の中にあるサブネットについての要約公示を抑制します。抑制された公示は、境界ルーターが接続されている他の区域に発信されていたかもしれません。その代わりに、区域境界ルーターは、add range コマンドを使って選択されたオプションに応じて、範囲に単一の要約公示を発信する場合と、公示をまったく発信しない場合があります。

範囲が公示されない場合は、範囲内にあるどのあて先についても区域間ルートがなくなることに注意してください。バーチャル・リンクによって通過区域として使用された区域については、範囲を使用することができないことにも注意してください。

OSPF 区域のパラメーターを設定するには、**set area** コマンドを使用し、次のプロンプトに応答してください。

```
OSPF Config> set area
Area number [0.0.0.0]? 0.0.0.1
Authentication type [1]? 1
Is this a stub area?  [No]:
```

次の場合は、区域をスタブとして定義します。

1. 区域が通過バックボーン・トラフィックを取り扱う必要がない場合
2. AS の外側をあて先とするトラフィックに関する区域境界ルーター生成の省略時値の区域ルーターによる使用が受け入れ可能である場合
3. 区域ルーターが AS 境界ルーター (AS 外部公示として外部発信元からルートを公示する OSPF ルーター) である必要がない場合

この場合、区域境界ルーターとバックボーン・ルーターだけは AS 外部ルートを計算して保管する必要があります。

OSPF インターフェースを設定する

OSPF インターフェースは、IP 構成時に定義された IP インターフェースのサブセットです。 OSPF インターフェース用に構成されたパラメーターは、OSPF ドメインのトポロジー、ドメインを通じて選択されるルート、および直接接続された OSPF ルーター間の対話の特性を決めます。OSPF インターフェースを定義し、その特性の一部を指定するには、**set interface** コマンドが使用されます。インターフェースの他の特性は、IP 構成時に **add address** プロンプトに応答して指定されました。

OSPF ドメイン・トポロジー

OSPF ドメインのトポロジーの定義は、どのルーターが一部の物理媒体またはサブネットワーク技術を介して直接接続されているかの定義およびこれらの接続がその部分である区域によって決まります。基本的な場合は、物理サブネットワークに接続されているすべてのルーターが直接接続されることですが、単一の物理サブネットワークを介して複数の IP サブネットワークを定義することが可能です。その場合、OSPF は、ルーターが同じ IP サブネットワークに接続される OSPF インターフェースをもつ場合のみ、ルーターが直接接続されていると見なします。同じサブネットワークに接続されているルーターが直接リンク・レイヤー接続をもたない場合も可能です。

LAN 媒体では、直接接続された OSPF ルーターは、IP サブネットワークおよび OSPF インターフェースに関連する物理媒体から判別されます。OSPF インターフェースの IP アドレスは、**Interface IP address** プロンプトに応答して指定されます。このアドレスは、IP 構成時に **add address** コマンドを使って定義された IP インターフェースのアドレスと同じものでなければなりません。IP アドレスは、**add address** コマンドを使って定義されたサブネットワーク・マスクとともに、OSPF インターフェースが接続されている IP サブネットワークを判別します。add address コマンドによって IP インターフェースに関連付けられた *net index* は、OSPF インターフェースが接続されている先の物理サブネットワークを判別します。LAN の同報通信機能により、OSPF はマルチキャスト・ハロー・メッセージを使用して、同じ IP サブネットワークに接続されたインターフェースをもつ他のルーターを発見します。したがっ

て、インターフェース・パラメーターは、どのルーターが LAN を通じて直接接続されているかを判別するのに OSPF が必要とするすべてのものです。

LAN を使用して、OSPF ルーターを IP ホストと接続することができます。この場合、LAN について定義されたどの IP サブネットワークにも OSPF インターフェースを定義することが必要です。それ以外の場合は、OSPF はこれらの IP サブネットワークをあて先としてもつルートを生成しません。他の接続ルーターを使用せずにこれらの LAN 上で OSPF ハロー・トラフィックが生じないようにするために、ネットワークを非同報通信マルチアクセス・ネットワークとして定義することができます。指定ルーターは必要ないため、ルーター優先順位もゼロに設定してください。

シリアル回線に接続された OSPF インターフェースを構成するための要件は、下位層の技術によって異なります。

ポイント・ポイント回線の場合、インターフェースを介してアクセス可能な他のルーターは 1 つしかないので、直接接続されたルーターは追加の構成をせずに判別することができます。実際、IP サブネットワークを構成するための要件はないので、ポイント・ポイント回線には無番号の OSPF インターフェースを使用することができます。この場合、IP add address コマンド用の IP アドレスとして使用されるのと同じネット・インデックスが、OSPF set interface コマンド用の IP アドレスとして使用されます。

単一のシリアル回線を介する複数のルーターへの接続をサポートするフレーム・リレー、ATM、X.25 のようなサブネットワーク・テクノロジーの場合は、OSPF インターフェースの構成は LAN の場合に似ていますが、直接接続されたルーターは、これらのサブネットワーク・テクノロジーでは動的に検出されないため、直接接続された近隣を指定するには、追加の構成が必要です。必要な構成についての詳細は、346 ページの『広域サブネットワークを構成する』を参照してください。

OSPF リンクのコスト

OSPF は、あて先への最小コストのパスを見つけることにより、ルートを計算します。各パスのコストは、パス内の異なるリンクについてのコストの合計です。直接接続されたルーターへのリンクのコストは、**set interface** コマンドで **Type of Service 0 cost** について指定されます。

データ・トラフィック用にインターフェースを使用する必要性に応じてコストを正しく構成することは、OSPF ドメインを通じて必要なルートを入手するのに決定的に重要です。個別のリンクを多少とも必要なものにする要因は、ネットワークによって異なる場合がありますが、最も一般的なゴールは、最小の遅延および最大の容量をもつルートを選択することです。一般に、この方針は、リンクのコストを物理サブネットワークについて使用される媒体の帯域幅と反比例させることによって得られます。

推奨される方法は、最高の帯域幅技術について 1 のコストを使用することです。例えば、100 Mbps ATM が稼働するインターフェースのコストとして 値 1 を使用します。

表 20. OSPF リンクのサンプル・コスト

インターフェース帯域幅	コスト
155 Mbps ATM	1
イーサネット	10
16 Mbps トークンリング	6
4 Mbps トークンリング	25
シリアル回線	帯域幅に基づくコスト
エミュレート済みトークンリング (注を参照)	1
エミュレート済みイーサネット (注を参照)	1

注: エミュレートされたトークンリングやイーサネットは、インターフェース速度 (例えば、155 Mbps) で稼働するので、 1 というコストで構成する必要があります。

ATM は、最大回線速度よりも遅い速度でネットワークに接続できます。 例えば、ルーターに 155 Mbps が可能なポートがあり、ルーターが 25 Mbps でそれに接続すると、そのリンクはまだ、1 というコストとして扱われます。OSPF の加重は、インターフェースに基づいて行われます。

OSPF インターフェースのコストは、ルーターの監視環境から動的に変更できます。この新しいコストは、OSPF ルーティング・ドメインを通じて迅速に伝送され、ルーティングを即時に修正します。

ルーターが再始動/再ロードするとき、インターフェースのコストは SRAM 内で構成された値に戻ります。

近隣ルーター間の対話

set interface コマンドを使って構成されるいくつかの値は、直接接続されたルーターの対話を制御するパラメーターを指定するために使用されます。それらには次のものが含まれています。

- Retransmission interval (再伝送時間間隔)
- Transmission delay (伝送遅延)
- Router priority (ルーター優先順位)
- Hello interval (ハロー間隔)
- Dead router interval (ルーター停止時間間隔)
- Demand Circuit (要求サーキット)
- Hello Suppression (ハロー抑止)
- Poll Interval (ポーリング間隔)
- Authentication key (認証キー)

ほとんどの場合、省略時値を使用することができます。

注: ハロー時間間隔、ルーター停止時間間隔、および認証キーは、同じ IP サブネットワークに接続されるすべての OSPF ルーターについて同じ値をもつ必要があります。値が同じでない場合、ルーターは直接接続 (隣接) を形成するのに失敗します。

マルチキャスト転送

enable multicast-routing コマンドは、IP マルチキャスト (クラス D) データグラムを使用可能にするのに使用します。マルチキャスト・ルーティングを使用可能にする際、ルーターに OSPF 区域間でマルチキャストを転送させたいかどうかもプロンプト指示されます。

```
OSPF Config>enable multicast forwarding
Inter-area multicasting enabled?  [No]: yes
```

enable multicast forwarding コマンドを最初に呼び出すと、省略時パラメーターによって、マルチキャストがすべての OSPF インターフェース上で使用可能にされます。

MOSPF パラメーターを変更したい場合は、**set interface** コマンドを使用してください。最初にマルチキャスト転送を使用可能にした場合のみ、マルチキャスト・パラメーターが照会されます。

複数のマルチキャスト・ルーティング・プロトコル (または単一のマルチキャスト・ルーティング・プロトコルの複数のインスタンス) が存在することのある、自律システムの端にあるネットワーク上では、不必要なデータグラムの複写を回避するため、転送をデータ・リンク・ユニキャストとして構成する必要があります。いずれにせよ、共通のネットワークに接続されたすべてのルーターについて、インターフェース・パラメーターの forward multicast datagrams と forward as data-link unicasts は同じに構成する必要があります。

非同報通信ネットワーク・インターフェース・パラメーターを設定する

ルーターが非同報通信、X.25 PDN などのマルチアクセス・ネットワークに接続されている場合は、ルーターがその OSPF 近隣を発見するのに役立つ次のパラメーターを構成する必要があります。 この構成が必要なのは、ルーターが非同報通信ネットワークの指定ルーターになる適格性がある場合に限ります。

まず、次のコマンドを使用して OSPF ポーリング間隔 (poll interval) を構成します。

```
OSPF Config> set non-broadcast
Interface IP address [0.0.0.0]? 128.185.138.19
Poll Interval [120]?
```

次に、非同報通信ネットワークに接続される他のすべての OSPF ルーターの IP アドレスを構成します。構成される各ルーターごとに、それが指定ルーターになる適格性も指定する必要があります。

```
OSPF Config> add neighbor
Interface IP address [0.0.0.0]? 128.185.138.19
IP Address of Neighbor [0.0.0.0]? 128.185.138.21
Can that router become Designated Router [Yes]?
```

非同報通信の設定 (set non-broadcast) を使用しても、他の OSPF ルーターのないネットワークを強制的に公示することができます。インターフェースについてのルーター優先順位をゼロに設定し、近隣は定義しないでください。

広域サブネットワークを構成する

フレーム・リレー、ATM を介したクラシカル IP、 X.25 では、単一のシリアル回線を通して複数のルーター間で直接接続ができます。この種のネットワークを接続する OSPF インターフェースには、**set interface** コマンドを使って得られる構成以上の追加の構成が必要です。 OSPF プロトコル・メッセージはこれらのネットワーク上での特定の近隣に直接送信されるので、近隣関係およびルーターの役割を判別するには動的発見の代わりに構成が使用されます。

注: この節で説明される構成は、ポイント・ポイント・ネットワークには適用されません。

OSPF は、これらのサブネットワークを通じてのルーター間の直接接続に次の 2 つのパターンのいずれかを想定することができます。

- ポイント・マルチポイント
- 非同報通信マルチアクセス (NBMA)

これら 2 つのパターンを区別する重要な要因は、サブネットワークに接続されたルーターのすべてのペア間に直接接続があるかどうか (*全メッシュ接続性*) または、ルーターの一部がマルチホップ・パスを通じて中間として他のルーターに接続されているだけであるかどうか (*部分メッシュ接続性*) です。

非同報通信マルチアクセス (NBMA) では、*全メッシュ接続性* が必要であるのに対し、ポイント・マルチポイントは*部分メッシュ接続性* のみを必要とします。

ポイント・マルチポイントは、全メッシュ接続性と部分メッシュ接続性の両方に働くので、これが省略時選択です。しかし、全メッシュ接続性が使用可能な場合は、NBMA の方が効率的な解決法です。

ポイント・マルチポイント・サブネットワークを構成する

DR がないので、ポイント・マルチポイントは NBMA よりも容易に構成することができますが、ポイント・マルチポイント・サブネットを通じて直接データ・トラフィックを交換するルーターのすべてのペアについて近隣関係を構成する必要があります。直接接続されたルーターの各ペアは、ハロー・メッセージを交換するので、一方の側はこれらのメッセージを通じて他方を発見することができます。ただし、最初のハロー・メッセージを送信するように構成されたルーターは、**add neighbor** コマンドを使用して構成されたその近隣の IP アドレスをもつ必要があります。

サブネットワークに接続されるルーターの一部がそれを NBMA として表し、他のルーターがそれをポイント・マルチポイントとして表す場合は、OSPF が正しいルートを計算しないことを覚えておくことが重要です。したがって、ポイント・マルチポイント・ネットワークへのどのインターフェースにも **set non-broadcast** コマンドを使用しないでください。

NBMA サブネットワークを構成する

NBMA IP サブネットワークの場合、OSPF ルーターに接続された一部のサブセットは、指定ルーター (DR) として適格であるように構成されています。DR として適格な各ルーターは、DR として適格な他のすべてのルーターにハロー・メッセージを定

期的に送信します。これらのメッセージはプロトコルで DR およびバックアップ DR を選択するために使用されます。DR およびバックアップ DR は、NBMA IP サブネットワークに接続された他のすべての OSPF ルーターとハロー・メッセージを定期的に交換します。また、NBMA IP サブネットワークを通じての OSPF ルート情報の流れは、接続された各ルーターと DR またはバックアップ DR の間だけです。

NBMA は、NBMA サブネットワークに接続するインターフェースについて **set non-broadcast** コマンドを使用することによって選択してください。このコマンドは、NBMA ネットワークに接続するすべてのインターフェースについて使用する必要があります。

NBMA サブネットワークに接続する OSPF ルーターに必要な構成は、そのルーターが DR になる適格性があるかどうかによって決まります。

- DR となる適格性がないルーターの場合、**set interface** コマンドを使用して、ルーター優先順位を 0 に設定する必要があります。
- DR になる適格性があるルーターの場合、**set interface** コマンドを使用して、ルーター優先順位を非ゼロ値に設定する必要があり、**add neighbor** を使用して、インターフェースが NBMA サブネットワークに接続されたすべての OSPF ルーターを識別し、それらのどれが DR になる適格性をもつか示す必要があります。

注: 星形構成では、ハブで **add neighbor** コマンドを使用してください (リモート・サイトの近隣は構成する必要がありません)。**add neighbor** コマンドは、ルーターを再始動しなくても、即時有効になります。

AS 境界ルーティングを使用可能にする

他のプロトコル (RIP および静的に構成された情報) から学習したルートを OSPF ドメインにインポートするには、AS boundary routing を使用可能 (enable) にしてください。インポートしたい唯一のルートが省略時ルート (あて先 0.0.0.0) である場合でも、これを行う必要があります。

AS 境界ルーティングを使用可能にする際、どの外部ルートをインポートしたいか尋ねられます。以下のカテゴリーに属するルートをインポートするかどうかを選択できます。

- BGP ルート
- RIP ルート
- 静的ルート
- 直接ルート

例えば、BGP および直接ルートをインポートするよう選択することはできますが、RIP または静的ルートをインポートするよう選択することはできません。

上の外部カテゴリーとは独立して、サブネット・ルートを OSPF ドメインにインポートするかしないかも構成できます。この構成項目は、省略時では ENABLED (サブネットがインポートされる) と解釈されます。

ルートをインポートする際に使用されるメトリック・タイプは、インポートされたコストが OSPF ドメインによってどのように見られるかを判別します。2 つのタイプ 2 のメトリックを比較する場合、最適のルートを選ぶのに外部コストだけが考慮され

ます。2 つのタイプ 1 のメトリックを比較する場合、比較を行う前に、ルートの外部コストと内部コストが結合されます。例えば、省略時ルートが開始されるのは、10.0.0.0 へのルートが AS 番号 12 から受信される場合のみになるように、ルーターを設定できます。AS 番号を 0 に設定するのは、『任意の AS から』を意味します。ネットワーク番号を 0.0.0.0 に設定するのは、『受信された任意のルート』を意味します。

enable コマンドの構文は次のとおりです。

```
OSPF Config>enable as boundary
Import BGP routes? [No]: yes
Import RIP routes? [No]:
Import static routes? [No]:
Import direct routes? [No]: yes
Import subnet routes? [No]:
Always originate default route? [No]: yes
Originate as type 1 or 2 [2]? 2
Default route cost [1]?
Default forwarding address [0.0.0.0]? 10.1.1.1
```

ATM を介した OSPF を構成する

ATM を介した OSPF を構成するためのオプションは、IP レイヤー用に LAN エミュレーションまたは ATM を介したクラシカル IP が使用されているかどうかによって異なります。LAN エミュレーションの場合、OSPF は実際の LAN の場合と同様に構成されます。ATM を介したクラシカル IP の場合、OSPF 構成オプションはワイド・エリア・サブネットの場合と同様です。346ページの『広域サブネットワークを構成する』を参照してください。NBMA および Point-to-Multipoint (ポイント・マルチポイント) の両方の構成がサポートされています。

ATM を介した OSPF を構成する (RFC 1577)

RFC 15777 を実行する ATM を介した OSPF には、以下の構成ステップが必要です。

1. `IP Config>` **add address** コマンドを使用して、ATM インターフェースに 1 つまたは複数の IP アドレスを割り当てる。各 IP アドレスは、接続されている論理 IP サブネット (LIS) に対応しています。
2. ATM インターフェース上に構成された IP アドレスのそれぞれについて、`OSPF Config>` **set interface** コマンドを使用する。Designated-Router(DR) eligibility を含む OSPF パラメーターを設定します。
3. ATM インターフェース上に構成された IP アドレスのそれぞれについて、`OSPF Config>` **set non-broadcast** コマンドを使用する。これは、ATM RFC 1577 LIS に接続されている各ルーターのすべてのインターフェースでも設定する必要があります。
4. `OSPF Config>` **add neighbor** コマンドを使用して、論理 IP サブネット (LIS) 上の、OSPF ルーティング情報を共用したい相手のルーターを定義する。

   注: 指定ルーター (Designated Routers (DR)) となるのに適格なルーターはすべて、近隣情報で構成する必要があります。DR になる必要があるルーターは、各 LIS で 1 つだけです。ただし、他のルーターも DR に適格であるように構成されている方が、故障が発生した場合の LIS の回復機能は高くなります。

その他の構成作業

バーチャル・リンクを設定する

バックボーンの接続性を維持するには、すべてのバックボーン・ルーターを永続リンクまたはバーチャル・リンクのいずれかにより相互接続させる必要があります。バーチャル・リンクは、共通の非バックボーンで非スタブの区域を共用する任意の 2 つの区域境界ルーターの間に構成することができます。バーチャル・リンクは、バックボーン区域を接続する別個のルーター・インターフェースと見なされます。したがって、バーチャル・リンクを構成するときは、多くのインターフェース・パラメーターも指定するよう指示されます。

下の例は、バーチャル・リンクの構成を示しています。バーチャル・リンクはリンクの 2 つの終点のそれぞれで構成する必要があります。OSPF ルーター ID は IP アドレスと同じ形式で入力する必要があることに注意してください。

```
OSPF
Config>set virtual
Virtual endpoint (Router ID) [0.0.0.0]? 128.185.138.21
Link's transit area [0.0.0.1]?
Retransmission Interval (in seconds) [10]?
Transmission Delay (in seconds) [5]?
Hello Interval (in seconds) [30]?
Dead Router Interval (in seconds) [180]?
Authentication Type (0 - None, 1 - Simple) [0]? 1
Authentication Key []? 41434545
Retype Auth. Key []? 41434545
```

コストは中継区域を通るバーチャル・リンク終点間の OSPF 区域内コストであるため、バーチャル・リンク用に構成されるコストはありません。

ルーティング・プロトコル比較を構成する

OSPF に加えてルーティング・プロトコルを使用する場合、またはルーティング・プロトコルを OSPF に変更する場合、ルーティング・プロトコル比較を設定する必要があります。

AS 内での OSPF ルーティングは次の 3 つのレベルで発生します。区域内、区域間、および外部。

区域内ルーティングが行われるのは、パケットの発信元アドレスおよびあて先アドレスが同じ区域に存在している場合です。他の区域についての情報は、このタイプのルーティングに影響を与えません。

区域間ルーティングが行われるのは、パケットの発信元アドレスとあて先アドレスが同じ AS の異なる区域に存在している場合です。OSPF は、区域間ルーティングを行う際に、パスを次の 3 つの連続する断片に分割します。つまり、発信元から区域境界ルーターまでの区域内パス、発信元区域とあて先区域間のバックボーン・パス、および着信先へのもう 1 つの区域内パスです。この高水準のルーティングは、バックボーンがハブでそれぞれの区域がスポークである星形のトポロジーとして思い浮かべることができます。

外部ルートは、AS の外部にあるネットワークへのパスです。これらのルートは、境界ゲートウェイ・プロトコル (BGP) のようなルーティング・プロトコルから、またはネットワーク管理担当者によって入力された静的ルートから作られます。BGP によっ

て提供される外部ルーティング情報は、OSPF プロトコルによって提供された内部ルーティング情報に干渉することはありません。

AS 境界ルーターは外部ルートを OSPF ルーティング・ドメインにインポートできます。OSPF はこれらのルートを AS 外部リンク公示として表します。

OSPF は外部ルートを個別のレベルでインポートします。タイプ 1 ルートと呼ばれる第 1 のレベルが使用されるのは、外部メトリックが OSPF メトリックに比較可能な場合 (例えば、これらのメトリックが両方ともミリ秒単位での遅延を使用するような場合) です。外部タイプ 2 ルートと呼ばれる第 2 のレベルは、外部コストがどの内部 OSPF (リンク状態) パスのコストより大きいと想定しています。

インポートされた外部ルートは、32 ビットの情報がタグ付けされます。ルーターでは、この 32 ビットのフィールドは、ルートがそこから受信された AS 番号を示します。これにより、他の自律システムへの外部情報を再公示するかどうか判別するときにさらに高機能の行動が使用可能になります。

OSPF には 4 レベルのルーティング階層があります (図35 を参照してください)。 **set comparison** コマンドはルーターに OSPF 階層のどこに BGP/RIP/静的ルートを入れるかを指示します。下から 2 つのレベルは OSPF 内部ルートから構成されます。OSPF の区域内ルートおよび区域間ルートは他の発信元 (これらはすべて単一のレベルにあります) から得られた情報より優先されます。

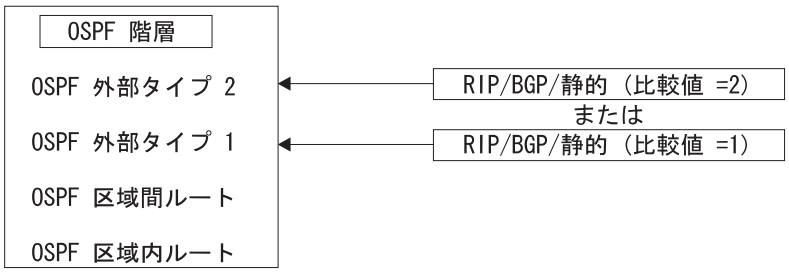


図 35. OSPF ルーティング階層

BGP/RIP/静的ルートを OSPF 外部タイプ 1 のルートと同じレベルにするには、比較値を 1 に設定してください。BGP/RIP/静的ルートを OSPF 外部タイプ 2 のルートと同じレベルにするには、比較値を 2 に設定してください。省略時の設定値は 2 です。

例えば、比較値が 2 に設定されていると想定します。この場合、RIP ルートが OSPF ドメインにインポートされると、タイプ 2 としてインポートされます。OSPF 外部タイプ 1 のすべてのルートは、受信された RIP ルートを、メトリックとは無関係に、指定変更します。ただし、RIP ルートの方がコストが低い場合には、RIP ルートは OSPF 外部タイプ 2 のルートを指定変更します。すべての OSPF ルーターの比較値は合致していなければなりません。ルーターについて設定された比較値が一貫していない場合には、ルーティングは正しく機能しません。

set comparison コマンドの構文は次のとおりです。

```
OSPF Config> set comparison
Compare to type 1 or 2 externals [2]?
```

Demand Circuit

要求サーキット (demand circuit) は、任意のインターフェースについて構成できます。物理媒体や、ルート計算のために OSPF が使用するモデルには依存しません。要求サーキットが構成されており、しかも互換性の問題がない場合は、次のようになります。

- 実変更のあるリンク状態公示 (LSA) だけがインターフェースを介して公示されます。通常、トポロジーの変更が発生した場合でも、OSPF の信頼性の高い伝送アルゴリズムにより、LSA は 30 分おきに新しいインスタンスで更新されます。
- DoNotAge ビットは、インターフェースを介して伝送された LSA に合わせて設定されます。それらの LSA は、インターフェースを介して更新されないためです。

Request Hello Suppression

これは、ハロー抑止を要求するようインターフェースを構成するのに使用できる追加のパラメーターです。このパラメーターは、ポイント・ポイント・インターフェースおよびポイント・マルチポイント・インターフェースについての値をもちます。さらに、そのインターフェースが接続されるサブネットワークは、接続を介してデータを送達できないことを OSPF に知らせられるものでなければなりません。現在は、Hello suppression (ハロー抑止) がサポートされるインターフェースのタイプとしては、ATM と ISDN ダイヤル・オンデマンド・インターフェースがあるだけです。

Poll Interval

Hello suppression (ハロー抑止) がアクティブでない場合、poll interval (ポーリング間隔) は、非同報通信マルチアクセス・サブネットワークでのみ使用され、設定は **set non-broadcast** コマンドで行われます。このパラメーターの構成は、インターフェースがデマンド・サーキットとして構成され、しかも Hello suppression (ハロー抑止) が要求されてからでないと行えません。このパラメーターは、データを転送する上で障害が発生したためにポイント・ポイント回線がダウンしているが、ネットワークはまだ作動可能であると考えられるときに、OSPF が接続の再確立を試みるのに使用します。

RIP から OSPF へ変換する

自律システムを RIP から OSPF に変換するには、RIP を稼働したまま、OSPF を 1 つのルーターごとに導入してください。次第に、すべての内部ルートが RIP を介して学習されたルートから OSPF によって学習されたルートにシフトします (OSPF ルートは RIP ルートより優先されます)。ルートを RIP のもとで見られたのと同じ状態にしたい場合 (変換が正しく機能していることを確認したい場合)、ホップ・カウントを OSPF メトリックとして使用してください。これは、各 OSPF インターフェースのコストを 1 と割り当てることによって行ってください。

プロトコルを使用可能にするときに OSPF システムのサイズを見積もる必要があることを忘れないでください。このサイズの見積値は OSPF ルーティング・ドメインの最終的なサイズを反映している必要があります。

OSPF の使用

ルーターに OSPF を導入した後、他のプロトコルを介してのルート (BGP、RIP、および静的に構成されたルート) をまだ学習する必要のあるすべてのルーターで AS 境界ルーティングをオンにしてください。 これらの AS 境界ルーターの数は、最小に保つ必要があります。

最後に、AS 境界ルーターでないすべてのルーターで RIP 情報の受信を使用不能にできます。

OSPF 構成パラメーターを動的に変更する

OSPF 構成パラメーターは、OSPF 構成機能を通じて構成を更新し、続いて、OSPF コンソールを通じ OSPF プロトコルをリセットすることによって、動的に変更することができます。この手法により、OSPF 近隣、インターフェース、区域、および AS 境界ルーティング・ポリシーの追加、削除、または変更が可能です。ほとんどの場合、これらの変更は、完全に非破壊的です。例えば、OSPF インターフェースを追加しても、他の OSPF インターフェースには影響しません (ただし、新しい OSPF リンク状態公示の発信元は除きます)。

ルーターの OSPF 公示すべてが再発信される必要のある変更があると、OSPF は再始動されます。これらの変更には次のものが含まれています。

- OSPF マルチキャスト転送 (MOSPF) の使用可能/使用不能
- デマンド・サーキット (RFC 1793) の使用可能/使用不能
- ルーターのルーター ID の値の変更

ほとんどの場合、唯一の障害は OSPF 近隣隣接が再確立されるまでの時間であるため、これは、ユーザーには影響ありません。

ルーター・メモリーは入出力バッファーを割り振る前に OSPF 用に予約されているため、最後のルーターが再始動した時点で使用可能になっていない限り、OSPF を動的に使用可能にすることはできません。また、システム再始動なしでは、OSPF 用に予約されているメモリーの量を増やすことはできません。予約済みのメモリーの量は、ルーターと、enable OSPF コマンドに指定された AS 外部ルートについての見積もりによって決められます。

例 :

```
  OSPF Config>enable OSPF
Estimated # external routes [100]? 300
Estimated # OSPF routers [50]? 100
Maximum Size LSA [2048]?
```

IBM 6611 からの移行

次の機能強化によって、既存の IBM 6611 から 2210 への移行が可能です。

- **Least-cost area ranges (最小コスト区域範囲)**

  OSPF 合計範囲については、 6611 では、構成要素ネットワークの最小コストを基にしてコストを計算しますが、 2210 では、構成要素ネットワークの最大コストをに基にして合計範囲コストを計算します。**Least-cost area ranges (最小コスト区域範囲)** によって、最小コストを計算するオプションが使用できます。
- **Point-to-multipoint neighbor cost (ポイント・マルチポイント近隣コスト)**

6611 では、論理ポイント・ポイント・フレーム・リレー・リンクの概念はサポートしていますが、フレーム・リレーを介した OSPF ポイント・マルチポイントはサポートしません。ポイント・マルチポイントでは、効率は高くなりますが、各近隣ごとにそれぞれ異なるコストを指定することはできません。 **Point-to-multipoint neighbor cost (ポイント・マルチポイント近隣コスト)** は、それぞれの近隣ごとに代替 TOS 0 コストを指定できるようにするために追加されました。

第17章 OSPF の構成と監視

この章では、最短パス最優先オープン (OSPF) を構成する方法について説明します。 OSPF は、内部ゲートウェイ・プロトコル (IGP) です。ルーターは、IP ルーティング・テーブル、最短パス最優先オープン (OSPF) プロトコルおよび RIP プロトコルを構築するために次の IGP をサポートしています。 OSPF は、リンク状態技術または最短パス最優先 (SPF) アルゴリズムに基づいています。 RIP は Bellman-Ford または距離ベクトル・アルゴリズムに基づいています。 この章は以下の節に分かれています。

OSPF 構成環境へのアクセス

OSPF 構成環境へアクセスするには、Config> プロンプトで次のコマンドを入力します。

```
Config> protocol ospf
Open SPF-based Routing Protocol configuration monitoring
OSPF Config>
```

OSPF 構成コマンド

OSPF を使用できるようにするには、OSPF 構成コマンドを使用して OSPF を構成する必要があります。 次の節では、OSPF コマンドを要約してから説明します。これらのコマンドは、OSPF config> プロンプトで入力します。 表21 はコマンドを示しています。

表 21. OSPF 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	すでに存在する OSPF 情報に追加します。区域に範囲を追加し、非同報通信ネットワークに近隣を追加できます。
Delete	SRAM から OSPF 情報を削除します。
Disable	OSPF プロトコル全体、AS 境界ルーティング機能、または IP マルチキャストルーティングを使用不能にします。
Enable	OSPF プロトコル全体、AS 境界ルーティング機能、または IP マルチキャストルーティングを使用可能にします。
Join	ルーターを 1 つまたは複数のマルチキャスト・グループに属するように構成します。
Leave	ルーターをマルチキャスト・グループのメンバーシップから除去します。
List	OSPF 構成を表示します。

表 21. OSPF 構成コマンドの要約 (続き)

コマンド	機能
Set	OSPF 区域、インターフェース、非同報通信ネットワーク、またはバーチャル・リンクに関する構成情報を確立または変更します。このコマンドでは、OSPF ルートを他のルーティング・プロトコルから入手された情報と比較する方法も設定できます。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、すでに存在している OSPF 情報にさらに情報を追加するのに使用します。このコマンドを使って、区域に範囲を追加したり、非同報通信ネットワークに近隣を追加したりできます。

構文 :

add range . . .

neighbor . .

range *area# IP-address IP-address-mask*

OSPF 区域に範囲を追加します。 OSPF 区域はアドレス範囲で定義することができます。 区域の外部では、各アドレス範囲について単一のルートが公示されます。 例えば、OSPF 区域がクラス B のネットワーク 128.185.0.0 のすべてのサブネットから構成されるとすると、この区域は単一のアドレス範囲から構成されると定義されることになります。 アドレス範囲は、128.185.0.0 のアドレスならびに 255.255.0.0 のマスクとして定義されることになります。区域の外部では、サブネットされたネットワーク全体は、ネットワーク 128.185.0.0 への単一のルートとして公示されることになります。

範囲は、区域の外部でどのルートが公示されるかを制御するように定義することができます。 選択項目は 2 つあります。

- OSPF が範囲を公示するように構成される場合は、範囲の少なくとも 1 つの構成要素ルートが区域内でアクティブであれば、範囲に関して単一の区域間ルートが公示されます。
- OSPF が範囲を公示しないように構成される場合は、範囲内に入るルートに関して区域間ルートは公示されません。

バーチャル・リンクの通過区域として使用される区域では範囲は使用できません。 また、範囲が区域に関して定義されると、区域が区分されているが、バックボーンで接続されている場合は、OSPF は正しく機能しません。

例 :

```
add range 0.0.0.2 128.185.0.0 255.255.0.0
inhibit advertisement ? [No]
```

1. *area number* は、次の値をもちます。

   有効値: 任意の有効な区域番号

   省略時値: なし

2. *IP address* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

省略時値: なし

3. *IP address mask* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス・マスク

   省略時値: なし

neighbor

このインターフェースを介してルーターに隣接する近隣を構成します。 非同報通信マルチアクセス・ネットワークでは、近隣は指定ルーターになる適格性があるルーターにのみ構成する必要があります。ポイント・マルチポイント・ネットワークでは、すべての論理接続の少なくとも一端には、構成済みの近隣が必要です。ポイント・マルチポイント・ネットワークの場合は、代替 TOS 0 コストが構成できます。 コストが構成されていなければ、インターフェース・コストが使用されます。

例: add neighbor

```
Interface IP address [0.0.0.0]? 128.185.138.19
IP Address of Neighbor [0.0.0.0]? 128.185.138.21
Can that router become Designated Router on this net [Yes]?
Alternate TOS 0 cost [0]? 100
```

1. *Interface IP address* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

2. *IP Address of Neighbor* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

3. `Can that router become designated router on this net?` (そのルーターはこのネット上の指定ルーターですか) という質問に答えます。ポイント・マルチポイント・インターフェースの場合は、このパラメーターは該当しないので、『No』 に設定する必要があります。

   有効値: Yes または No

   省略時値: Yes

4. `Alternate TOS 0 cost` によって、代替コストの使用ができます。

   有効値: 0 〜 65534

   省略時値: 0 (インターフェース・コストを使用する必要があることを示す)

Delete

delete コマンドは、SRAM から OSPF 情報を削除するのに使用します。

構文 :

delete range . . .
area . . .
interface . . .
neighbor . . .
non-broadcast . . .
virtual-link

range *area# IP-address*

OSPF 区域から範囲を削除します。

例: delete range 0.0.0.2 128.185.0.0 255.255.0.0

1. この範囲の *area number* は、次の値をもちます。

   有効値: 任意の有効な区域アドレス

   省略時値: なし

2. *IP Address of Range* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

3. *IP Address Mask of Range* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス・マスク

   省略時値: なし

area *area#*

現行の OSPF 構成から OSPF 区域を削除します。

例: delete area 0.0.0.1

area number は、次の値をもちます。

有効値: 任意の有効な区域番号

省略時値: なし

interface *interface-IP-address*

現行の OSPF 構成からインターフェースを削除します。

例: delete interface 128.185.138.19

interface IP address は、次の値をもちます。

有効値: 任意の有効な IP アドレス

省略時値: なし

neighbor *interface-IP-address neighbor-IP-address*

現行の OSPF 構成から構成済みの近隣を削除します。

例: delete neighbor

```
Interface IP address [0.0.0.0]? 128.185.138.19
IP Address of Neighbor [0.0.0.0]? 128.185.138.21
```

1. *interface IP address* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

2. *neighbor IP address* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

non-broadcast *interface-IP-address*

現行の OSPF 構成から非同報通信ネットワーク情報を削除します。

例: delete non-broadcast 128.185.133.21

1. *interface IP address* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

省略時値: なし

virtual-link

set virtual-link コマンドを使用して設定したバーチャル・リンクを削除します。

例: delete virtual-link

```
Virtual endpoint (Router ID) [0.0.0.0]? 10.1.1.1
Link's transit area [0.0.0.1]? 0.0.0.2
```

1. バーチャル近隣の ID を定義する *virtual endpoint (router ID)* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

2. *link's transit area* は、次の値をもちます。

   有効値: 任意の有効な区域アドレス

   省略時値: 0.0.0.1

Disable

disable コマンドは、OSPF プロトコル全体または AS 境界ルーティング機能だけのいずれかを使用不能にするのに使用します。

構文 :

disable as boundary routing
demand-circuits
least-cost-ranges
multicast forwarding
OSPF routing protocol
RFC1583Compatibility
subnet

as boundary routing

AS 境界ルーティング機能を使用不能にします。 使用不能にすると、ルーターは外部情報を OSPF ドメインにインポートしません。

例: disable as boundary routing

demand-circuits

デマンド・サーキット機能を使用不能にします。使用不能にされると、ルーターは、そのルーター・リンクのリンク状態公示 (LSA) 内でデマンド・サーキット処理をサポートすることを指示せず、DoNotAge ビットが設定された状態で LSA を発信しません。ルーティング・ドメインまたは OSPF スタブ区域内の 1 つのルーターがデマンド・サーキットをサポートしない場合、そのルーティング・ドメインまたは OSPF スタブ区域内のルーターはいずれも DoNotAge LSA を発信しません。

例: disable demand-circuits

least-cost-ranges
最も近接した構成要素ネットワークのコスト (最低コスト) に基づく OSPF 区域範囲の計算を使用不可にします。このオプションは、 disabled (使用不可) が省略時値です。

multicast forwarding
すべてのインターフェースで IP マルチキャスト・ルーティングを使用不能にします。 使用不能にされると、ルーターは IP マルチキャスト (クラス D) データグラムを転送しません。

例: disable multicast forwarding

OSPF routing protocol
OSPF プロトコル全体を使用不能にします。

例: disable OSPF routing protocol

RFC1583Compatibility
RFC 1583 と互換性のある AS 外部ルート選択を使用不能にします。同じ外部ルートが複数の OSPF 区域からアクセス可能になっておらず、RFC2178 に記載されているものと類似のルーティング・ループ問題が発生していない限り、RFC1583 compatibility は使用不能にしないことをお勧めします。省略時値は enabled (使用可能) です。

例: disable rfc1583Compatibility

subnet
ポイント・ポイント・シリアル回線につながっているインターフェースの場合は、このオプションは、他のルーターのアドレスへのホストルートではなく、シリアル回線を表すサブネットへのスタブルートの公示を使用不能にします。 インターフェースがこのルーターのアドレスを識別するように、アドレスを与える必要があります。

例 :

```
OSPF Config> disable subnet
Interface IP address [0.0.0.0]? 8.24.3.1
```

interface IP address は、次の値をもちます。

有効値: 任意の有効な IP アドレス

省略時値: なし

Enable

enable コマンドは、全体の OSPF プロトコル、サブネットまでルーティングするスタブの公示、または AS 境界ルーティング機能のみのいずれかを使用可能にするのに使用します。

構文 :

enable as boundary routing
demand-circuits
least-cost-ranges
multicast forwarding
OSPF routing protocol

RFC1583Compatibility

send outage-only

subnet

as boundary routing

他のプロトコル (BGP、RIP、および静的に構成された情報) から学習したルートを OSPF ドメインにインポートできるようにする AS 境界ルーティング機能を使用可能にします。 **enable** コマンドの使用の詳細については、337ページの『OSPF を構成する』を参照してください。

例: enable as boundary routing

```
Import RIP routes? [No]:
Import static routes? [No]:
Import direct routes? [No]: yes
Import subnet routes? [No]:
Always originate default route? [No]: yes
Originate as type 1 or 2 [2]? 2
Default route cost [1]?
Default forwarding address [0.0.0.0]? 10.1.1.1
```

1. *Originate as type 1 or 2* は、OSPF から発信された省略時値は 1 または 2 の AS 外部メトリック・タイプをもつことを指示します。タイプ 1 のメトリックは OSPF コストと同じコンテキストにあるものとみなされますが、タイプ 2 のメトリックは OSPF メトリックより高位であるとみなされます。

   有効値: 1 または 2

   省略時値: 2

2. *Default route cost* は、OSPF がその区域境界ルーターまでの省略時ルートと関連付けるコストを指定するパラメーターです。コストは、その区域境界ルーターまでの省略時ルートの最短パスを判別するのに使用されます。

   有効値: 0 〜 16777215

   省略時値: 1

3. *Default forwarding address* は、インポートされた省略時ルートで使用される転送アドレスを指定するパラメーターです。

   有効値: 有効な IP アドレス

   省略時値: なし

multicast forwarding

IP マルチキャスト (クラス D) データグラムの転送を使用可能にします。 マルチキャスト・ルーティングを使用可能にするときに、IP マルチキャスト・データグラムを OSPF 区域間で転送したいのかどうかもプロンプトで尋ねられます。 MOSPF (マルチキャスト拡張付きの OSPF) を稼働するには、現在 OSPF を実行しているルーターは、このコマンドを使用するだけで事足ります。構成情報を再入力する必要はありません。

例: enable multicast forwarding

```
Inter-area multicasting enabled (Yes or No): yes
```

demand-circuits

ルーターのデマンド・サーキット処理を使用可能にします。ルーターは、そのルーター・リンクのリンク状態公示 (LSA) 内でデマンド・サーキット処理

をサポートすることを指示します。省略時値は、OSPF ルーティング・ドメイン内のすべてのルーターを認識せずにデマンド・サーキットを配置できるように、enabled (使用可能) がとられます。

```
OSPF Config> enable demand-circuits
```

least-cost-ranges

最も近接した構成要素ネットワークのコスト (最低コスト) に基づく OSPF 区域範囲の計算を使用可能にします。同じ区域の区域境界ルーターとして使用されている IBM 6611 との互換性が必要な場合は、このパラメーターは使用可能にする必要があります。最低コスト構成要素ネットワークを使用すると、コストが変わるため、OSPF LSA 再発信の数が大幅に減る状況でも、使用できます。このオプションは、disabled (使用不可) が省略時値です。

OSPF routing protocol

OSPFプロトコル全体を使用可能にします。 OSPF ルーティング・プロトコルを使用可能にする際、OSPF リンク状態データベースのサイズを推定するのに使用される次の 2 つの値を提供する必要があります。

- OSPF ルーティング・ドメインにインポートされる AS 外部ルートの総数。単一のあて先が別個の AS 境界ルーターによってインポートされるときは、単一のあて先から複数の外部ルートが発生することがあります。 例えば、OSPF ルーティング・ドメインに 2 つの AS 境界ルーターがあり、両方のルーターが同じ 100 のあて先へのルートをインポートしているとすると、AS 外部ルートの数は 200 に設定する必要があります。

  有効値: 0 ～ 65535

  省略時値: 100

- ルーティング・ドメインでの OSPF ルーターの総数

  有効値: 0 ～ 65535

  省略時値: 50

- さらに、最大 LSA サイズを指定できます。同じ OSPF 区域内に OSPF ダイヤル・リンクが多数存在する大型のルーター (例えば、ISDN 基本) がある場合は、この値を増やす必要があります。 一般的に、どの単一 LSA の場合でも、2048 で十分です。

  有効値: 2048 ～ 65535

  省略時値: 2048

  例: enable OSPF routing protocol

```
Estimated # external routes[100]? 200
Estimated # OSPF routers [50]? 60
Maximum LSA Size [2048]?
```

RFC1583Compatibility

RFC 1583 と互換性のある AS ギアブ・ルート選択を使用可能にします。 省略時値は enabled (使用可能) です。

例: enable rfc1583Compatibility

subnet

ポイント・ポイント・シリアル回線へのインターフェースの場合は、このオプションは、他のルーターのアドレスへのホスト・ルートではなく、シリア

ル回線を表すサブネットへのスタブ・ルートの公示を使用可能にします。 インターフェースがこのルーターのアドレスを識別するように、アドレスを与える必要があります。

例 :

```
OSPF Config> enable subnet
Interface IP address [0.0.0.0]? 8.24.3.1
```

interface IP address は、次の値をもちます。

有効値: 任意の有効な IP アドレス

省略時値: なし

Join

join コマンドは、ルーターをマルチキャスト・グループのメンバーとして構成するのに使用します。ルーターがマルチキャスト・グループのメンバーである場合は、グループ・アドレスに送信された PING および SNMP 照会に応答します。

グループ・メンバーシップをより短時間で有効になる方法 (再始動/再ロードが不要) で要求するには、OSPF 監視から **join** コマンドを出してください。また、OSPF 監視から、join コマンドは、特定のグループが結合された回数も追跡します。 OSPF 監視を通じて結合された IP マルチキャスト・グループは、ルーターの再始動および再ロードが行われると保存されません。

構文 :

join *multicast-group-address*

例: join 224.185.0.0

multicast group address パラメーターは、IP クラス D グループ/マルチキャスト・アドレスを指定します。

有効値: 224.0.0.1 ～ 239.255.255.255 のクラス D IP アドレス

省略時値: なし

Leave

leave コマンドは、マルチキャスト・グループからルーターのメンバーシップを除去するのに使用します。これにより、ルーターはグループ・アドレスに送信された PING および SNMP 照会に応答しなくなります。

グループ・メンバーシップをより短時間で有効になる方法 (再始動/再ロードが不要) で削除するには、OSPF 監視から **leave** コマンドを出してください。また、OSPF 監視からでは、実行された leave の回数が前に実行された join の回数に等しくなるまでは、グループ・メンバーシップは削除されません。

構文 :

leave *multicast-group-address*

例: leave 224.185.0.0

multicast group address パラメーターは、IP クラス D グループ/マルチキャスト・アドレスを指定します。

有効値: 224.0.0.1 ～ 239.255.255.255 のクラス D IP アドレス

省略時値: なし

List

list コマンドは、OSPF 構成情報を表示するのに使用します。

構文 :

list all

areas

interfaces

neighbors

non-broadcast

virtual-links

all OSPF から発信された構成情報をすべてリストします。

例: `list all`

```
        --Global configuration--
OSPF Protocol:          Enabled
# AS ext. routes:       300
Estimated # routers:    100
Maximum LSA Size:       2048
External comparison:    Type 2
RFC 1583 compatibility: Disabled
AS boundary capability: Enabled
Import external routes: BGP RIP STA DIR SUB
Orig. default route:    No (0,0.0.0.0)
Default route cost:     (1, Type 2)
Default forward. addr.: 0.0.0.0
Multicast forwarding:   Enabled
Inter-area multicast:   Enabled
Demand Circuits:        Enabled
Least Cost Ranges:      Disabled
LSA Max Random Initial Age:    0

        --Area configuration--
Area ID          AuType          Stub? Default-cost Import-summaries?
0.0.0.0          0=None          No         N/A           N/A


   --Interface configuration--
IP address        Area    Cost  Rtrns  TrnsDly  Pri  Hello Dead
128.185.184.11    0.0.0.1   1      5       1     1    10    60
128.185.177.11    0.0.0.1   1      5       1     1    10    60
128.185.142.11    0.0.0.0   1      5       1     1    10    60
```

OSPF protocol	OSPF が使用可能か使用不能かを表示します。
# AS ext. routes	自律システム外部ルートの推定数を表示します。ルーターはこの数を上回る AS 外部ルートを受け入れられません。
Estimated # routers	OSPF 構成にあるルーターの推定数を表示します。
Maximum LSA size	このルーターによって発信される最大サイズの LSA を表示します。
External comparison	外部情報を OSPF ドメインにインポートするときと、OSPF 外部ルートを RIP/BGP ルートと比較するときに OSPF が使用する外部ルート・タイプを表示します。
RFC 1583 compatibility	OSPF AS external route (OSPF AS 外部ルート) が RFC 1583 と互換であるかどうかを指示します。

AS boundary capability	ルーターが外部ルートを OSPF ドメインにインポートするかどうかを表示します。
Import external	どのルートがインポートされるかを表示します。
Orig default route	ルーターが省略時値を OSPF ドメインにインポートするかどうかを表示します。値が 『YES』 のときは、ゼロ以外のネットワーク番号が括弧で囲まれて表示されます。これは、そのネットワークへのルートがある場合のみ、省略時のルートが開始されることを示します。
Default route cost	インポートされた省略時のルートで使用されるコストおよびタイプを表示します。
Default forward addr	インポートされた省略時のルートで使用される転送アドレスを表示します。
Multicast forwarding	IP マルチキャスト・データグラムが転送されるかどうかを表示します。
Demand circuits	デマンド・サーキット処理がサポートされているかどうかを表示します。
Least Cost Area Ranges	最小コスト区域範囲を計算するかどうか表示します。
LSA Max Random Initial Age	自己発信 LSA に関する最大初期経時を表示します。この値がゼロ (省略時値) なら、LSA はすべて経時 0 で発信されます。
External comparison	外部情報を OSPF ドメインにインポートするときと、OSPF 外部ルートを RIP/BGP ルートと比較するときに OSPF が使用する外部ルート・タイプを表示します。
Inter-area multicast	IP マルチキャスト・データグラムが区域間で転送されるかどうかを表示します。
Area-ID	接続された区域 ID (区域要約情報) を表示します。
AuType	区域の認証に使用される方法を表示します。『Simple-pass』 は、区域の認証で単純パスワード方式が使用されていることを意味します。
Stub area	要約されている区域がスタブ区域であるかどうかを表示します。 スタブ区域は外部ルートを通さないので、結果的にルーティング・データベースは小さくなります。 ただし、スタブ区域は AS 境界ルーターを含むことができず、構成済みのバーチャル・リンクもサポートできません。
OSPF interfaces	各インターフェースごとに、IP アドレスが、構成済みのパラメーターとともに印刷されます。『Area』 は、インターフェースが接続される OSPF 区域です。 『Cost』 は、インターフェースに関連する TOS 0 コスト (またはメトリック) を示します。 『Rtrns』 は再送間隔で、無応答ルーティング情報の再送間の秒数です。 『TrnsDly』 は伝送遅延で、インターフェースを通じてルーティング情報を伝送するのに要する秒数の推定値 (0 より大であることが必要) です。 『Pri』 はインターフェースのルーター優先順位で、指定ルーターの選択時に使用されます。『Hello』 は、インターフェースから送信されるハロー・パケット間の秒数です。 『Dead』 は、Hello が聞こえなくなってルーターがダウンしたと宣言されるまでの秒数です。
Virtual links	このルーターで端点として構成されたすべてのバーチャル・リンクをリストします。『Virtual endpoint』 は、もう一方の終点の OSPF ルーター ID を示します。 『Transit area』 は、バーチャル・リンクが構成される非バックボーン区域を示します。 バーチャル・リンクは OSPF プロトコルによりポイント・ポイント・ネットワークと同様に扱われると見なされます。 コマンドでリストされる他のパラメーター (『Rtrns』、『TrnsDly』、『Hello,』、および 『Dead』) は、すべてのインターフェースについて保持されます。 詳しくは、OSPF list interfaces コマンドを参照してください。

areas 構成済みの OSPF 区域に関するすべての情報をリストします。

例: `list areas`

```
                                    --Area configuration--
Area ID          AuType          Stub? Default-cost Import-summaries?
0.0.0.0          0=None           No         N/A           N/A
0.0.0.1          1=Simp-Pass      No         N/A           N/A
```

Area-ID　接続された区域 ID (区域要約情報) を表示します。

AuType　区域の認証に使用される方法を表示します。『Simple-pass』 は、区域の認証で単純パスワード方式が使用されていることを意味します。

Stub area　要約されている区域がスタブ区域であるかどうかを表示します。スタブ区域は外部ルートを通さないので、結果的にルーティング・データベースは小さくなります。 ただし、スタブ区域は AS 境界ルーターを含むことができず、構成済みのバーチャル・リンクもサポートできません。

Default-cost　スタブ区域の場合は、OSPF 要約 (タイプ 3) リンク状態公示 (LSA) として発信される 省略時値のコスト。中継区域 (例えば、非スタブ区域) の場合、このフィールドは N/A です。

Import-summaries　スタブ区域の場合は、OSPF 要約 (タイプ 3) リンク状態公示 (LSA) がスタブ区域内で発信されるかどうかを指示します。この質問は、省略時の要約には適用されません。中継区域 (例えば、非スタブ区域) の場合、このフィールドは N/A です。

interfaces

各インターフェースごとに、IP アドレスが、構成済みのパラメーターとともに印刷されます。 『Area』 は、インターフェースが接続される OSPF 区域です。『Cost』 は、インターフェースに関連する TOS 0 コスト (またはメトリック) を示します。『Rtrns』 は再送間隔で、無応答ルーティング情報の再送間の秒数です。 『TrnsDly』 は伝送遅延で、インターフェースを通じてルーティング情報を伝送するのに要する秒数の推定値 (0 より大であることが必要) です。 『Pri』 はインターフェースのルーター優先順位で、指定ルーターの選択時に使用されます。 『Hello』 は、インターフェースから送信されるハロー・パケット間の秒数です。 『Dead』 は、Hello が聞こえなくなってルーターがダウンしたと宣言されるまでの秒数です。

例: `list interfaces`

```
OSPF Config>list interface

                        --Interface configuration--
IP address        Area            Auth   Cost  Rtrns  Delay  Pri  Hello   Dead
200.1.1.2         0.0.0.2           0      10      5     1     1     10     40
10.69.1.2         0.0.0.0           1       1      5     1     1     10     40
OSPF Config>list virtual-link

                        --Virtual link configuration--
Virtual endpoint     Transit area    Auth   Rtrns  Delay Hello  Dead
4.4.4.4              0.0.0.1           1       10    5     30   180
10.1.1.2             0.0.0.1           1       10    5     30   180
OSPF Config>
OSPF Config>list area

               --Area configuration--
Area ID         Stub? Default-cost Import-summaries?
0.0.0.2          No         N/A           N/A
0.0.0.0          No         N/A           N/A
0.0.0.1          No         N/A           N/A
0.0.0.3          Yes        10            Yes
```

注: マルチキャストが使用不能にされた場合は、マルチキャスト・パラメーターは表示されません。 インターフェースがどれもデマンド・サーキットとして構成されない場合には、Demand circuit パラメーターは表示されません。

neighbors

非同報通信ネットワークの近隣をリストします。 近隣の IP アドレスおよびその近隣へのインターフェースの IP アドレスを表示します。また、ネットワ

ーク上で 『指定ルーター』 になる適格性がその近隣にあるかどうかについても示し ポイント・マルチポイント・ネットワークに関する代替 TOS 0 コストも示します。

例: `list neighbors`

```
          --Neighbor configuration--
Neighbor Addr     Interface Address   DR eligible?      Alternate TOS 0 Cost
2.3.4.5           1.2.3.4             yes               0
2.5.6.7           5.6.7.8             no                100
```

non-broadcast

非同報通信マルチアクセス・ネットワークに接続されたインターフェースに関連するすべての情報をリストします。 各非同報通信インターフェースごとに、ルーターが接続されたネットワークで指定ルーターになる適格性がある限り、ポーリング間隔が、非同報通信ネットワーク上でのルーターの近隣のリストとともに表示されます。

例: `list non-broadcast`

```
          --NBMA configuration--
Interface Addr      Poll Interval
128.185.235.34      120
```

virtual-links

このルーターで端点として構成されたすべてのバーチャル・リンクをリストします。 『Virtual endpoint』 は、もう一方の終点の OSPF ルーター ID を示します。『Transit area』 は、バーチャル・リンクが構成される非バックボーン区域を示します。 バーチャル・リンクは OSPF プロトコルによりポイント・ポイント・ネットワークと同様に扱われると見なされます。 コマンドでリストされる他のパラメーター (『Rtrns』、『TrnsDly』、『Hello,』、および『Dead』) は、すべてのインターフェースについて保持されます。 詳しくは、OSPF **list interfaces** コマンドを参照してください。

例: `list virtual-links`

```
            --Virtual link configuration--
Virtual endpoint   Transit area   Rtrns  TrnsDly Hello Dead
0.0.0.0            0.0.0.1         10      5     30    180
```

Set

set コマンドは、OSPF 区域、インターフェース、非同報通信ネットワーク、またはバーチャル・リンクに関する構成情報を表示または変更するのに使用します。このコマンドでは、OSPF ルートが他のルーティング・プロトコルから得られた情報と比較される方法を設定することもできます。

構文 :

set
- area
- comparison
- interface
- non-broadcast
- virtual-link
- max-random-initial-lsa-age

area OSPF 区域用のパラメーターを設定します。 区域が定義されない場合は、ル

ーター・ソフトウェアでは、ルーターに直接接続されたネットワークはすべてバックボーン区域 (区域 ID 0.0.0.0) に属するものと想定します。

例: set area

```
Area number [0.0.0.0]? 0.0.0.1
Is this a stub area? [No]:  yes
Stub default cost? [0]:
Import summaries? [Yes]:
```

- *Area number (区域番号)* - OSPF 区域アドレスです。
- *Stub area designation (スタブ区域の指定)*。 『Yes』 を指定した場合は、次のようになります。
  - 区域は AS 外部リンク公示を受信せず、データベースのサイズを縮小し、スタブ区域でのルーター用のメモリー使用率を減少させる。
  - スタブ区域を通じてのバーチャル・リンクを構成できない。
  - スタブ区域内のルーターを AS 境界ルーターとして構成することができない。

  スタブ区域内の外部ルーティング。 バックボーンをスタブ区域として構成できません。 スタブ区域での外部ルーティングは省略時ルートに基づいて行われます。 スタブ区域に接続する各境界区域ルーターは、このために省略時ルートを開始します。 この省略時ルートのコストも、**set area** コマンドを用いて構成可能です。

comparison

ルーターに BGP/RIP/静的ルートが OSPF 階層のどこに入るかを知らせます。下から 2 つのレベルは OSPF 内部ルートから構成されます。 OSPF 内部ルートは他の発信元 (これらはすべて単一のレベルにあります) から得られた情報より優先されます。

例: set comparison

```
OSPF Config> set comparison
Compare to type 1 or 2 externals [2]?
```

interface

ルーターのネットワーク・インターフェースに関する OSPF パラメーターを設定します。

1. *interface IP address* は、ルーター内の各インターフェースごとのものです。
2. *attaches to area* は、インターフェースが接続する区域です。
3. タイマー値は、共通のネットワーク・セグメントに接続されているすべてのルーターについて同じ値です。
   a. *retransmission interval* は、1 つまたは複数のリンク状態公示についてのリンク要求が再送信されるまでの間隔です。

      有効値: 1 ～ 65535 秒

      省略時値: 5

   b. *Transmission delay* は、インターフェースを介してリンク状態情報を伝送するのにかかる秒数の推定値です。

      各リンク状態公示ごとに定数 MaxAge に相当する有限の存続時間が決まっています (1 時間)。 各リンク状態公示は、特定のインターフェ

ースに送信されるため、この構成済み伝送遅延によって経年処理されます。 最小限の遅延は 1 秒です。

有効値: 1 ～ 65535 秒

省略時値: 1

c. *Hello Interval* は、インターフェースで送信されるハロー・パケット間の間隔です。

有効値: 1 ～ 65535 秒

省略時値: 10

d. *Dead Router Interval*

Dead Router Interval (ルーター停止間隔) は、ハローをまだ送信していないルーターが停止したとみなされるまでの間隔です。Dead Router Interval の省略時値は、構成済みの Hello Interval (ハロー間隔) の 4 倍です。このパラメーターの値は、Hello Interval よりも大きくなければなりません。

有効値: 2 ～ ≥ 65535 秒

省略時値: 40 (または構成済みのハロー間隔の 4 倍)

4. *Router Priority* 値は、同報通信および非同報通信マルチアクセス・ネットワークが指定ルーターを決めるのに使用します。ポイント・ポイント・リンクの場合、この値は **0** でなければなりません。これは、このルーターをそのネットワークの指定ルーターとして決めてはならないことを意味します。

有効値: 0 ～ 255

省略時値: 1

5. *Type of service 0 cost* は、その区域について最短パス・ルートが計算されるときにインターフェースに使用されるコストです。

有効値 : 1 ～ 65534

省略時値: 1

6. *Demand Circuit* は、インターフェースを LSA (リンク状態公示) を伝送する目的でデマンド・サーキットとして扱うかどうかを指示します。デマンド・サーキットについて、LSA は、DoNotAge ビットがこのインターフェースを超えて設定されていれば伝送し、LSA に対して実際に変更が行われない場合は伝送されません。詳細については、RFC 1793 を参照してください。

有効値: Yes または No

省略時値: No

7. *Hello Suppression* は、近隣がフル状態に達すると、ハロー・パケットはインターフェースで抑止されることを指示します。Hello Suppression (ハロー抑止) が要求または許可されるためには、デマンド・サーキットがインターフェースで使用可能になっている必要があります。現在は、Hello Suppression (ハロー抑止) がサポートされるのは、ATM と ISDN ダイヤル・オンデマンド・リンクだけです。詳細については、RFC 1793 を参照してください。

有効値: Allow、Request、または Disable

省略時値: Allow

Allow 近隣が Hello Suppression (ハロー抑止) を要求できるようにします。

Request 近隣に Hello Suppression を要求します。

Disable Hello Suppression を使用不能にし、ハローの送信を続行します。

8. *Demand Circuit Down Poll Interval* は、Hello Suppression がアクティブな状態でデマンド・サーキットでデータを送信できない場合に送信されるハロー・ポーリング間の期間を指示します。現在は、Hello Suppression (ハロー抑止) がサポートされるのは、 ATM と ISDN ダイヤル・オンデマンド・リンクだけです。詳細については、RCF 1793 を参照してください。

   有効値: 1 〜 65535

   省略時値: 60

9. *Authentication type* は、インターフェース上の OSPF パケットのために使用される認証手順を定義します。選択肢としては、1 (単純パスワードを示します) または 0 (OSPF パケットの交換に認証が必要でないことを示します) があります。 1 を指定する場合は、認証キーも指定する必要があります。

   有効値: 0、1

   Default Value: 0

10. *Authentication key* は、この OSPF 区域に使用されるパスワードを定義するパラメーターです。パスワード認証が使用された場合は、正しい認証キーをもつパケットだけが受け入れられます。

    有効値: 任意の 1 〜8 文字

    省略時値: ヌル・ストリング

例: set interface

```
Interface IP address [0.0.0.0]? 10.69.1.2
Attaches to area [0.0.0.0]?
Retransmission Interval (in seconds) [5]?
Transmission Delay (in seconds) [1]? 1
Router Priority [1]? 1
Hello Interval (in seconds) [10]?
Dead Router Interval (in seconds) [40]?
Type Of Service 0 cost [1]?
Demand Circuit (Yes or NO) ?[No]:
Authentication Type (0 - none, 1 - simple) [0]? 1
Authentication Key []? AceeOSPF
Retype Auth.  Key []? AceeOSPF
```

プロンプトに応答する際、ルーター内の各インターフェースごとにインターフェースの IP アドレスを提供し、それに続く質問に応答してください。 下記のパラメーターに関しては、共通のネットワークに接続されたルーターのすべてについて同じ値を入力する必要があります。

- Hello interval (ハロー間隔)
- Dead router interval (ルーター停止間隔)
- Authentication key (認証キー) (1 の認証が使用される場合)

最初のプロンプトは、インターフェースが接続される OSPF 区域を尋ねます。 例えば、インターフェース・アドレス・マスクが 255.255.255.0 と想定し、インターフェースがネットワーク 128.185.0.0 のサブネット (128.185.138.0) に接続されることを示します。 サブネット 128.185.138.0 に接続された他の

すべての OSPF ルーターも、*Hello interval* が 10 に設定され、*dead router interval* が 40 に設定され、インターフェースの *authentication key* が xyz_q に設定されている必要があります。

ポイント・ポイント接続回線への IP インターフェースは無番号の場合もあることに注意してください。 この場合、IP アドレスの代わりにネット・インデックスが構成されます。 OSPF のこの実施は、これらの無番号のインターフェースとともに働きますが、正しく働くためには、ポイント・ポイント回線の両端は無番号のインターフェースを使用する必要があります。

マルチキャスト・ルーティング構成 (マルチキャストが使用可能になっている) では、各 OSPF インターフェースについての MOSPF パラメーターは省略時値に設定されます。 これは以下のことを意味します。

- マルチキャスト転送が使用可能になっている。
- マルチキャスト・データグラムはデータ・リンク・マルチキャストとして転送される。
- IGMP ホスト・メンバーシップはインターフェースから 60 秒ごとに送信される。
- グループへの IGMP ホスト・メンバーシップ報告がインターフェースによって受信されなくなってから 180 秒後に、ローカル・グループ・データベース項目が除去される。

MOSPF パラメーターを変更したい場合は、**set interface** コマンドを使用してください。 最初にマルチキャスト転送を使用可能にした場合のみ、マルチキャスト・パラメーター (上の出力表示で示される最後の 5 つのパラメーター) が照会されます。

複数のマルチキャスト・ルーティング・プロトコル (または単一のマルチキャスト・ルーティング・プロトコルの複数のインスタンス) が存在することのある、自律システムの端にあるネットワーク上では、不必要なデータグラムの複写を回避するため、転送をデータ・リンク・ユニキャストとして構成する必要があります。いずれにせよ、共通のネットワークに接続されたすべてのルーターについて、インターフェース・パラメーターの 『forward multicast datagrams』 と 『forward as data-link unicast』 は同じに構成する必要があります。

non-broadcast

ポイント・マルチポイント省略時値を上書きして、X.25、フレーム・リレー、 ATM のネットワークでは、NBMA を選択します。このパラメーターは、非活動状態にある近隣に送信されるハローの頻度を決める間隔を指定します。 OSPF が正しく機能するためには、同じサブネットワークに接続するすべてのインターフェースを通じて非同報通信を一貫して設定する必要があります。

ただし、フレーム・リレーや ATM のネットワークの場合は、**set non-broadcast** コマンドを使用して、OSPF インターフェースを非同報通信マルチアクセス・ネットワークへの接続として構成します。 **set non-broadcast** コマンドが使用されないと、インターフェースは、ポイント・マルチポイント・ネットワークに接続されるものと想定されます。 フレーム・リレー・ネットワークでは、すべての OSPF インターフェースが同じタイプのネットワークに接続するものとして構成されている必要があるため、

あるルーターのインターフェースについて **set non-broadcast** コマンドが使用された場合、ネットワークに接続するすべてのルーターのインターフェース上に構成する必要があります。

例: set non-broadcast

```
Interface IP address [0.0.0.0]? 128.185.138.19
Poll Interval [120]
```

interface IP address は、次の値をもちます。

有効値: 任意の有効な IP アドレス

省略時値: なし

NBMA Poll Interval (NBMA ポーリング間隔) は非アクティブな近隣にハロー・パケットを送信するのに使用されます。 (非アクティブ近隣とは、Dead Router interval (ルーター停止間隔) より長い期間の間、ルーターになにも聞こえてきていない近隣のことです。)ルーターは、速度を落として、これらの近隣をまだポーリングします。NBMA Poll Interval は、ルーターの構成済みの Hello Interval (ハロー間隔) よりもはるかに大きく設定してください。

有効値: 1 ～ 65535 秒

省略時値: 120 秒

例: set non-broadcast

```
Interface IP address [0.0.0.0]? 128.185.138.19
Poll Interval [120]?
```

virtual-link

任意の 2 つの区域境界ルーター間でバーチャル・リンクを構成します。 バックボーンの接続性を維持するには、すべてのバックボーン・ルーターを永続リンクまたはバーチャル・リンクのいずれかにより相互接続させる必要があります。 バーチャル・リンクは、バックボーン区域を接続する別個のルーター・インターフェースと見なされます。 したがって、バーチャル・リンクを構成するときは、多くのインターフェース・パラメーターも指定するよう指示されます。

バーチャル・リンクは、共通の非バックボーン区域へのインターフェースをもつ任意の 2 つのバックボーン・ルーターの間に構成できます。 バーチャル・リンクは、バックボーンの接続性を保持するために使用され、両方の端点で構成される必要があります。

注: この OSPF の実施は、バーチャル・リンクの一方の端が無番号のポイント・ポイント接続回線でもよい場合には、バーチャル・リンクをサポートします。 この構成が働くためには、バーチャル・リンクを介して送信された OSPF プロトコル・メッセージ内の発信元アドレスとしてルーター ID を使用する必要があります。ルーター ID の使用は、ルーター ID として使用されるアドレスを使って内部 IP アドレスを構成することによって保証することができます。 この構成が働くためのもう 1 つの要件は、バーチャル・リンクの両端で OSPF 実施がそれをサポートすることです。

1. *virtual endpoint (router ID)* は、バーチャル近隣の ID を定義します。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

2. *Link's transit area* は、バーチャル・リンクが構成されるときに使用される非バックボーン、非スタブ区域です。バーチャル・リンクは、共通の非バックボーンおよび非スタブ区域につながっているインターフェースをもつ任意の 2 つの区域境界ルーターの間に構成できます。 バーチャル・リンクは、リンクの 2 つの終点のそれぞれに構成する必要があります。

   有効値: 0.0.0.1 〜 255.255.255.255

   省略時値: 0.0.0.1

3. タイマー値は、共通のネットワーク・セグメントに接続されているすべてのルーターについて同じ値です。

   a. *retransmission interval* は、1 つまたは複数のリンク状態公示についてのリンク要求が再送信されるまでの間隔です。

      有効値 1 〜 65535 秒

      省略時値: 10

   b. *Transmission delay* パラメーターは、インターフェースを介してリンク状態情報を伝送するのにかかる秒数の推定値です。

      各リンク状態公示ごとに定数 MaxAge に相当する有限の存続時間が決まっています (1 時間)。 各リンク状態公示は、特定のインターフェースに送信されるため、この構成済み伝送遅延によって経年処理されます。 最小限の遅延は 1 秒です。

      有効値: 1 〜 65535 秒

      省略時値: 5

   c. *Hello Interval* は、インターフェースで送信されるハロー・パケット間の間隔です。

      有効値: 1 〜 255 秒

      省略時値: 30

   d. *Dead Router Interval* は、ハローをまだ送信していないルーターが停止したとみなされるまでの間隔です。このパラメーターの省略時値は、構成済みの Hello Interval (ハロー間隔) の 6 倍です。このパラメーターは、Hello Interval より大きな値に設定する必要があります。

      有効値: 2 〜 65535 秒

      省略時値: 180

4. *Authentication type* は、バーチャル・リンク上の OSPF パケットのために使用される認証手順を定義します。選択肢としては、1 (単純パスワードを示します) または 0 (OSPF パケットの交換に認証が必要でないことを示します) があります。 1 を指定する場合は、認証キーも指定する必要があります。

   有効値: 0、1

   Default Value: 0

5. *Authentication key* は、この OSPF 区域に使用されるパスワードを定義します。パスワード認証が使用された場合は、正しい認証キーをもつパケットだけが受け入れられます。

有効値: 任意の 1 〜8 文字

省略時値: ヌル・ストリング

例: set virtual-link

```
Virtual endpoint  (Router ID) [0.0.0.0]? 10.1.1.2
Link's transit area [0.0.0.1]?
Virtual link already exists - record will be modified.
Retransmission Interval (in seconds) [10]?
Transmission Delay (in seconds) [5]?
Hello Interval (in seconds) [30]?
Dead Router Interval (in seconds) [180]?
Authentication Type (0 - none, 1 - simple) [0] 1
Authentication Key []? AceeOSPF
Retype Auth. Key []? AceeOSPF
```

max-random-initial-lsa-age

自己発信 LSA に関する最大初期経時を指定します。省略時値は 0 で、通常、これを変更する必要があるのは、LSA 発信の同期に問題が検出された場合だけです。

有効値: 0 〜 1770

省略時値: 0

例 :

```
OSPF Config>  set max-random-initial-lsa-age
Maximum initial LSA age [0]?
```

OSPF 監視環境にアクセスする

OSPF 監視コマンドにアクセスする場合は、次の手順を使用します。このプロセスによって、OSPF *監視* プロセスへのアクセスができます。

1. OPCON プロンプトで、**talk 5** を入力します。 (このコマンドについて詳しくは、*ソフトウェア 使用者の手引き* の中の “OPCON プロセス” を参照してください)。例えば、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 **protocol ospf** コマンドを入力すると、 OSPF> プロンプトが表示されます。

   例 :

   ```
   + prot ospf
   OSPF>
   ```

OSPF 監視コマンド

この節では、すべての OSPF 構成コマンドについて要約してから説明します。これらのコマンドにより、OSPF ルーティング・プロトコルを監視できます。 375ページの表22 に、OSPF 監視コマンドをリストします。

OSPF 監視コマンドは、OSPF> プロンプトで入力してください。

表 22. OSPF 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Advertisement	OSPF データベースに属するリンク状態公示を表示します。
Area summary	OSPF 区域の統計およびパラメーターを表示します。
AS external	OSPF リンク状態データベースに属する AS 外部公示をリストします。
Database summary	OSPF 区域のリンク状態データベースに属する公示を表示します。
Dump routing tables	ルーティング・テーブルに含まれる OSPF ルートを表示します。
Interface summary	OSPF インターフェースの統計およびパラメーターを表示します。
Join	ルーターを 1 つまたは複数のマルチキャスト・グループに属するように構成します。
Leave	ルーターをマルチキャスト・グループのメンバーシップから除去します。
Mcache	現在アクティブなマルチキャスト転送キャッシュ項目のリストを表示します。
Mgroups	ルーターの接続されたインターフェースのグループ・メンバーシップを表示します。
Mstats	さまざまなマルチキャスト・ルーティング統計を表示します。
Neighbor summary	OSPF 近隣の統計およびパラメーターを表示します。
Ping	所定のあて先に ICMP エコー要求 (または PING) を継続的に送信し、受信された各応答ごとに 1 行を印刷します。
Reset	OSPF 構成を動的にリセットします。
Routers	到達可能な OSPF 区域境界ルーターおよび AS 境界ルーターを表示します。
Size	タイプ別に分類された、現在、リンク状態データベースにある LSA の数を表示します。
Statistics	メモリーおよびネットワークの使用を詳細に示す OSPF 統計を表示します。
Traceroute	所定のあて先への完全なルート (通過する全ホップ) を表示します。
Weight	OSPF インターフェースのコストを動的に変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Advertisement Expansion

advertisement expansion コマンドは、OSPF データベースに含まれるリンク状態公示の内容を印刷するのに使用します。ルーターの公示の要約を入手するには、**database** コマンドを使用してください。

リンク状態公示は、そのリンク状態タイプ、リンク状態 ID およびその公示ルーターによって定義されます。 各 OSPF 区域ごとに別個のリンク状態データベースがあります。 コマンド行に区域 ID を入力すると、どのデータベースを探索したいかをソフトウェアに知らせることになります。 link-state-type に示された値によって決まる公示には次のような種類があります。

- ルーター・リンク - 単一のルーターのインターフェースの記述が含まれます。
- ネットワーク・リンク - 特定のインターフェースに接続されたルーターのリストが含まれます。

- 要約ネット - 単一の区域間ルートの記述が含まれます。
- 要約 AS 境界ルーター - 別の区域にある AS 境界ルーターへのルートの記述が含まれます。
- AS 外部ネット - 単一ルートの記述が含まれます。
- マルチキャスト・グループ・メンバーシップ - 公示ルーターの近隣における特定のグループのメンバーシップの記述が含まれます。

注: リンク状態 ID、公示ルーター (それらのルーター ID によって指定されます)、および区域 ID は IP アドレスと同じ形式をとります。 例えば、バックボーン区域は 0.0.0.0 として入力できます。

例 1 ではルーター・リンク公示の拡張を示します。ルーターの ID は 128.185.184.11 です。 これは AS 境界ルーターであり、バックボーン区域への 3 つのインターフェース (すべてコストは 1) があります。 マルチキャスト・ルーティングが使用可能になっています。 フィールドの詳しい説明は例で示されています。

このコマンドも 2 つの方法で機能拡張されています。 まず第一に、router-LSA および network-LSA を表示するときに、各ルーター間リンクおよびルーターと通過ネットワーク間のリンクの着信コスト、ならびに前に表示された転送コストが表示されます。 これが行われるのは、発信元が異なる区域/自律システムにあるマルチキャスト・データグラムのルーティングは転送コストではなく着信コストに基づいているからです。 逆方向リンクがない (リンクが Dijkstraによって使用されることは決してないことを意味します) 場合は、着信コストは 『1-way』 として示されます。

さらに、LSA の OSPF オプションは、詳細な OSPF **neighbor** コマンドで表示されるのと同様の方法で表示されます。

新しいグループ・メンバーシップ LSA も表示できます。 各グループ・メンバーシップ LSA の 『LS destination』 はグループ・アドレスです。 ルーターは、ルーターの接続されたネットワークの 1 つまたは複数にメンバーをもつ各グループに対してグループ・メンバーシップ LSA を作成します。 グループのグループ・メンバーシップ LSA は、グループ・メンバーをもつ接続された通過ネットワーク (タイプ 『2』 の頂点) をリストし、1 つまたは複数の接続されたスタブ・ネットワークに属するメンバーがある場合、またはルーター自体がマルチキャスト・グループのメンバーである場合は、ID がルーターの OSPF ルーター ID であるタイプ 『1』 の頂点が含まれます。

構文 :

advertisement *ls-type link-state-id advertising-router area-id*

例 1: `advertisement 1 128.185.184.11 0.0.0.0`

```
LS age:     173
LS options:  E,MC,DC
LS type:     1
LS destination (ID): 128.185.184.11
LS originator:   128.185.184.11
LS sequence no:  0x80000047
LS checksum:     0x122
LS length:       60
Router type:  ASBR,W
# router ifcs:   3
         Link ID:          128.185.177.31
         Link Data:        128.185.177.11
         Interface type:   2
```

```
          No. of metrics: 0
          TOS 0 metric:   3 (0)
Link ID:          128.185.142.40
Link Data:        128.185.142.11
Interface type:   2
          No. of metrics: 0
          TOS 0 metric:   4 (0)
Link ID:          128.185.184.0
Link Data:        255.255.255.0
Interface type:   3
          No. of metrics: 0
          TOS 0 metric:   1
```

LS age	公示の経過時間を秒単位で示します。
LS options	公示によって記述されるルーティング・ドメインの断片によってサポートされる任意選択の OSPF 機能を示します。これらの機能は、E (外部タイプ 5 を処理します。これが公示が属している区域に設定されていない場合は、スタブとして構成されています)、T (TOS に基づきルーティングできます)、MC (IP マルチキャスト・データグラムを転送できます)、およびDC (デマンド・サーキット処理が可能です) によって表示されます。
LS type	公示を分類し、その内容を示します。1 (ルーター・リンク公示)、 2 (ネットワーク・リンク公示)、3 (要約リンク公示)、4 (要約 ASBR 公示)、 5 (AS 外部リンク) および 6 (グループ・メンバーシップ公示)
LS destination	公示によって記述されているものを識別します。これは、公示タイプによって決まります。 ルーター・リンクおよび ASBR 要約の場合は、OSPF ルーター ID です。 ネットワーク・リンクの場合は、ネットワークの指定ルーターの IP アドレスです。 要約リンクおよび AS 外部リンクの場合は、ネットワーク/サブネット番号です。 グループ・メンバーシップ公示の場合は、特定のマルチキャスト・グループです。
LS originator	起点ルーターの OSPF ルーター ID
LS sequence number	同一の公示の別個のインスタンスを区別するために使用されます。符号付きの 32 ビットの整数として見る必要があります。 0x80000001 から開始し、公示が更新されるたびに 1 ずつ増えます。
LS checksum	公示内容のチェックサムで、データ破壊を検出するために使用されます。
LS length	公示のサイズ (バイト単位)
Router type	ルーターの機能のレベルを示します。ASBR はルーターが AS 境界ルーターであることを意味し、ABR はルーターが区域境界ルーターであることを意味し、W はルーターがワイルドカード・マルチキャスト受信側であることを意味します。
# Router ifcs	公示に記述されるルーター・インターフェースの番号
Link ID	インターフェースが接続されているものを示します。インターフェース・タイプによって決まります。 ルーターのインターフェース (つまり、ポイント・ポイント・リンク) の場合は、リンク ID は近隣のルーター ID です。 通過ネットワークへのインターフェースの場合は、ネットワークの指定ルーターの IP アドレスです。スタブ・ネットワークにつながっているインターフェースの場合は、ネットワークのネットワーク/サブネット番号です。
Link Data	リンクに関する 4 バイトの追加情報。インターフェースの IP アドレス (ポイント・ポイント・ネットワークおよび通過ネットワークへのインターフェースの場合)、またはサブネット・マスク (スタブ・ネットワークへのインターフェースの場合) のいずれかです。
Interface type	次のいずれか 1 つ。1 (別のルーターへのポイント・ポイント接続)、2 (通過ネットワークへの接続)、3 (スタブ・ネットワークへの接続) または 4 (バーチャル・リンク)
No. of metrics	このインターフェースについてメトリックが提供されている非ゼロの TOS 値の番号

TOS 0 metric　インターフェースのコスト。括弧内にはリンクのリバース・コスト (別の公示から導かれたもの) が示されています。 逆方向リンクがない場合は、『1-way』 が表示されます。

LS age、LS options、LS type、LS destination、LS originator、LS sequence no、LS checksum および LS length のフィールドはすべての公示について共通です。 Router type および # router ifcs はルーター・リンク公示のみで見られます。ルーター公示内の各リンクは、Link ID、Link Data、および Interface type フィールドによって記述されます。 各リンクには、各 Type of Service (TOS) ごとに別個のコストが割り当てられます。これは、No. of metrics および TOS of metric フィールドによって記述されます (ルーターは現在、TOS に基づいてルートしておらず、TOS 0 コストのみを見ます)。

例 2 ではグループ・メンバーシップ公示の拡張を示します。 所定のグループ/公示ルーターの組み合わせについてのグループ・メンバーシップ公示は、グループ・メンバーを含む公示ルーターに直接接続されたネットワークをリストします。 この公示は、ルーター自体が指定されたグループのメンバーであるかどうかもリストします。 下の例は、ネットワーク128.185.184.0 にグループ224.0.1.1 のメンバーがあることを示しています。

例 2: `adv 6 224.0.1.1 128.185.184.114`

```
For which area 0.0.0.0?
LS age:     168
LS options:  E
LS type:     6
LS destination (ID): 224.0.1.1
LS originator:   128.185.184.114
LS sequence no:  0x80000001
LS checksum:     0x7A3
LS length:       28
Vertex type: 2
Vertex ID:   128.185.184.114
```

Vertex type　グループ・メンバーを含むオブジェクトを記述します。次のいずれか一方。 1 (ルーター自体、またはルーターに接続されたスタブ・ネットワーク) または 2 (通過ネットワーク)。

Vertex ID　頂点タイプ (vertex type) が 1 の場合は、常に、公示ルーターの ID。頂点タイプが 2 の場合は、通過ネットワークの指定ルーターの IP アドレス。

Area Summary

area summary コマンドは、ルーターに接続されたすべての OSPF 区域について統計およびパラメーターを表示するのに使用します。

下の例では、ルーターは単一の区域 (バックボーン区域) に接続されます。 区域の認証には単純パスワード方式が使用されています。ルーターには、区域に接続されている 3 つのインターフェースがあり、バックボーンについての SPF ツリー計算を行うときに 4 つの通過ネットワーク、7 つのルーターおよび 0 の区域境界ルーターを見つけました。

構文 :

area

例 :

```
Area ID            #ifcs  #nets  #rtrs  #brdrs  DC-Status
0.0.0.1              1      1      2       2      On
0.0.0.0              3      0      3       2     Off
```

# ifcs	特定の区域に接続されているルーター・インターフェースの数を示します。これらのインターフェースは必ずしも機能しません。
# nets	この区域についての SPF ツリー計算を行うときに見つかった通過ネットワークの数を示します。
# rtrs	この区域についての SPF ツリー計算を行うときに見つかったルーターの数を示します。
# brdrs	この区域についての SPF ツリー計算を行うときに見つかった区域境界ルーターの数を示します。
DC-Status	デマンド・サーキット処理が区域についてアクティブであるかどうかを指示します。

AS-external advertisements

AS-external advertisements コマンドは、OSPF ルーティング・ドメインに属する AS 外部公示をリストするのに使用します。各公示ごとに 1 行が印刷されます。各公示は、次の 3 つのパラメーターによって定義されます。そのリンク状態タイプ (AS 外部公示の場合は常に 5)、そのリンク状態 ID (LS destination と呼ばれます)、および公示ルーター (LS originator と呼ばれます)。

構文 :

as-external

例: as-external

```
Type LS destination LS originator    Seqno     Age  Xsum
  5  0.0.0.0       128.185.123.22  0x80000084 430   0x41C7
  5  128.185.131.0 128.185.123.22  0x80000080 450  0x71DC
  5  128.185.132.0 128.185.123.22  0x80000080 450  0x66E6
  5  128.185.144.0 128.185.123.22  0x80000002 329  0xF2CA
  5  128.185.178.0 128.185.123.22  0x80000081 450  0x72AA
  5  128.185.178.0 128.185.129.40  0x80000080 382  0xDD28
  5  129.9.0.0     128.185.123.22  0x80000082 451  0x4F30
  5  129.9.0.0     128.185.126.24  0x80000080 676  0x324A
  5  134.216.0.0   128.185.123.22  0x80000082 451  0x505A
  5  134.216.0.0   128.185.126.24  0x80000080 676  0x3374
  5  192.9.3.0     128.185.123.22  0x80000082 451  0xF745
  5  192.9.3.0     128.185.126.24  0x80000080 677  0xDA5F
  5  192.9.12.0    128.185.123.22  0x80000082 452  0x949F
  5  192.9.12.0    128.185.128.41  0x80000080 679  0x31B2
  5  192.26.100.0  128.185.123.22  0x80000081 452  0xFDCD
  5  192.26.100.0  128.185.126.24  0x80000080  21  0xDEE8
                              etc.
             # advertisements:             133
             Checksum total:               0x43CC41
```

Type	AS 外部公示の場合は常に 5 です。
LS destination	IP ネットワーク/サブネット番号を示します。これらのネットワーク番号は他の自律システムに属しています。
LS originator	公示ルーター
Seqno, Age, Xsum	任意の一時点に OSPF ルーティング・ドメインに 1 つの公示のいくつかのインスタンスが存在することがあります。ただし、OSPF リンク状態データベースには最新のインスタンスのみが保管され (このコマンドによって印刷され) ます。 どのインスタンスが最新であるか調べるために、LS シーケンス番号 (Seqno)、LS 経過時間 (Age) および LS チェックサム (Xsum) フィールドが比較されます。 LS 経過時間フィールドは秒単位で示されます。 その最大値は 3600 です。

表示の末尾に、AS 外部公示の合計が、それらの内容のすべてを通じてのチェックサムの合計とともに印刷されます。 チェックサムの合計とは、個々の公示の LS チェックサム・フィールドの 32 ビットの和 (繰り上がりは廃棄) です。 2 つの OSPF ルーターが同期化されたデータベースをもつかどうか迅速に判別するには、この情報を使用できます。

Database Summary

database summary コマンドは、特定の OSPF 区域のリンク状態データベースの内容の記述を表示するのに使用します。AS 外部公示は表示から省略されます。 各公示ごとに単一行が印刷されます。 各公示は次の 3 つのパラメーターによって定義されます。そのリンク状態タイプ (Type と呼ばれます)、そのリンク状態 ID (LS destination と呼ばれます)、および公示ルーター (LS originator と呼ばれます)。

構文 :

database *area-id*

例: database 0.0.0.0

```
          Type LS destination LS originator    Seqno     Age  Xsum
            1  128.185.123.22 128.185.123.22 0x80000084  442 0xCE2D
            1  128.185.125.38 128.185.125.38 0x80000082  470 0x344D
            1  128.185.126.24 128.185.126.24 0x80000088 1394 0xCC47
            1  128.185.128.41 128.185.128.41 0x80000082  471 0x16A2
            1  128.185.129.25 128.185.129.25 0x8000008D 1624 0x8B64
            1  128.185.129.40 128.185.129.40 0x8000008A 1623 0xABBE
            1  128.185.136.39 128.185.136.39 0x80000082  469 0x5045
            2  128.185.125.40 128.185.129.40 0x80000049  457 0xA31
            2  128.185.126.25 128.185.129.25 0x80000002 1394 0x56B8
            2  128.185.127.24 128.185.126.24 0x8000007F 1031 0x592D
            2  128.185.129.25 128.185.129.25 0x8000005F 2295 0x8219
            2  128.185.129.40 128.185.129.40 0x80000001 1623 0x12C9
            6  224.0.2.6      128.185.142.9  0x8000003D  232 0x513F
            6  224.0.2.6      128.185.184.11 0x80000003  376 0x2250
                       # advertisements:             14
                       Checksum total:               0x4BBC2
```

Type	別個の LS タイプは数字で表示されます。タイプ 1 (ルーター・リンク公示)、タイプ 2 (ネットワーク・リンク公示)、タイプ 3 (ネットワーク要約), タイプ 4 (AS 境界ルーター要約)、およびタイプ 6 (グループ・メンバーシップ LSA)。
LS destination	公示によって記述されているものを示します。
LS originator	公示ルーター
Seqno, Age, Xsum	任意の一時点に 1 つの公示のいくつかのインスタンスが OSPF ルーティング・ドメインを提示していることが可能です。ただし、OSPF リンク状態データベースには最新のインスタンスのみが保管され (このコマンドによって印刷され) ます。 どのインスタンスが最新であるか調べるために、LS シーケンス番号 (Seqno)、LS 経過時間 (Age) および LS チェックサム (Xsum) フィールドが比較されます。 LS 経過時間フィールドは秒単位で示されます。 その最大値は 3600 です。

表示の末尾に、区域データベース内の公示の合計が、それらの内容のすべてを通じてのチェックサム合計とともに印刷されます。チェックサムの合計とは、個々の公示の LS チェックサム・フィールドの 32 ビットの和 (繰り上がりは廃棄) です。 2 つの OSPF ルーターが同期化されたデータベースをもつかどうか迅速に判別するには、この情報を使用できます。

注: マルチキャスト可能なルーターを非マルチキャスト・ルーターと比較するときは、非マルチキャスト・ルーターはグループ・メンバーシップ LSA を処理したり保管したりしないので、上記のデータベース・チェックサム (および公示の #) は必ずしも一致しません。また、OSPF ルーティング・ドメインまたは OSPF スタブ区域内でデマンド・サーキット処理がアクティブであると、データベース・チェックサムは、ほとんどの場合、デマンド・サーキットをもつルーター間で異なります。詳細については、RFC 1793 を参照してください。

Dump Routing Tables

dump routing tables コマンドは、OSPF によって計算され、現在ルーティング・テーブルにあるすべてのルートを表示するのに使用します。このコマンドの出力は、IP 監視の dump routing tables コマンドと形式が似ています。

構文 :

dump

例: dump

```
Type   Dest net         Mask     Cost Age   Next hop(s)
SPE1   0.0.0.0          00000000  4    3    128.185.138.39
SPF*   128.185.138.0    FFFFFF00  1    1    Eth/0
Sbnt   128.185.0.0      FFFF0000  1    0    None
SPF    128.185.123.0    FFFFFF00  3    3    128.185.138.39
SPF    128.185.124.0    FFFFFF00  3    3    128.185.138.39
SPF    192.26.100.0     FFFFFF00  3    3    128.185.131.10
RIP    197.3.2.0        FFFFFF00  10   30   128.185.131.10
RIP    192.9.3.0        FFFFFF00  4    30   128.185.138.21
Del    128.185.195.0    FFFFFF00  16   270  None

Default gateway in use.

Type Cost Age  Next hop
SPE1 4    3    128.185.138.39

Routing table size: 768 nets (36864 bytes), 36 nets known
```

Type (route type)

ルートがどのように派生したかを示します。

Sbnt - ネットワークがサブネット化されることを示します。このような項目はプレースホルダーのみです。

Dir - 直接接続されたネットワークまたはサブネットを示します。

RIP - ルートが RIP プロトコルを介して学習されたことを示します。

Del - ルートが削除されたことを示します。

Stat - 静的に構成されたルートを示します。

BGP - ルートが BGP プロトコルを介して学習されたことを示します。

BGPR - BGP プロトコルを介して学習され、OSPF および RIP によって再公示されるルートを示します。

Fltr - ルーティング・フィルターを示します。

SPF - ルートが OSPF 区域内ルートであることを示します。

SPIA - OSPF 区域間ルートであることを示します。

SPE1、SPE2 - OSPF 外部ルート (それぞれタイプ 1 および 2) を示します。

Rnge - 活動 OSPF 区域のアドレス範囲であり、パケットの転送に使用されないルート・タイプを示します。

Dest net	IP あて先ネットワーク/サブネット
Mask	IP アドレス・マスク
Cost	ルート・コスト
Age	RIP および BGP ルートの場合、ルーティング・テーブル項目が最後に最新表示されてから経過した時間。
Next Hop	あて先ホストへのパス上の次のルーターの IP アドレス。送信側ルーターがパケットを転送するのに使用するインターフェース・タイプも表示されます。

ルート・タイプの後のアスタリスク (*) は、そのルートが静的バックアップまたは直接接続されたバックアップをもつことを示します。 ルート・タイプの後のパーセント記号 (%) は、このネットワーク/サブネットについて RIP 更新が常に受け入れられることを示します。

欄の末尾の括弧内の数は、あて先への等コスト・ルートの数を示しています。これらのルートに属する最初のホップは、IP 監視の **route** コマンドを使って表示できます。

Interface Summary

interface summary コマンドは、OSPF インターフェースに関連する統計およびパラメーターを表示するのに使用します。引き数が与えられない (例 1 を参照) 場合は、単一の行が印刷されて、各行ごとに要約します。 インターフェースの IP アドレスが与えられる (例 2 を参照) 場合は、そのインターフェースに関する詳細な統計が表示されます。

構文 :

interface *interface-ip-address*

例 1: `interface`

```
Ifc Address      Phys    assoc. Area     Type   State   #nbrs #adjs
9.67.217.66      TKR/0   2.2.2.2        Brdcst   64        0    0
128.185.123.22   PPP/0   0.0.0.0        Brdcst   64        0    0
```

Ifc Address	インターフェースの IP アドレス
Phys	物理インターフェースを表示します。
Assoc Area	接続された区域の ID
Type	Brdcst (同報通信、例えばイーサネット・インターフェース)、P-P (ポイント・ポイント・ネットワーク、例えば同期シリアル回線)、P-2-MP (ポイント・マルチポイント、例えばフレーム・リレー・ネットワーク)、Multi (非同報通信のマルチアクセス、例えば X.25 接続)、または VLink (OSPF バーチャル・リンク) のいずれでも構いません。
State	次のうちどれか 1 つです。1 (down (ダウン))、2 (loop back (ループバック))、 4 (waiting (待機))、8 (point-to-point (ポイント・ポイント))、16 (DR other (他の DR))、32 (backup DR (バックアップ DR))、または 64 (designated router (指定ルーター))。

#nbrs	近隣の数。そのハローが受信されたルートの数に構成済みのルートの数を加えたもの。
#adjs	隣接の数。 これは、状態 (state) が交換 (Exchange) 以上の近隣の数です。 これらは、ルートがそれとすでに同期化されている、または同期化のプロセスにある近隣です。

例 2: `interface 128.185.125.22`

```
Interface address:      128.185.125.22
Attached area:          0.0.0.1
Physical interface:     Eth/1
Interface mask:         255.255.255.0
Interface type:         Brdcst
State:                  32
Authentication Type:    None
Designated Router:      128.185.184.34
            Backup DR:              128.185.184.11

DR Priority:       1  Hello interval:   10  Rxmt interval:     5
Dead interval:    40  TX delay:          1  Poll interval:     0
Demand Circuit   off  Max pkt size:   2044  TOS 0 cost:        1

# Neighbors:       0  # Adjacencies:     0  # Full adjs.:      0
# Mcast floods:    0  # Mcast acks:      0

MC forwarding:    on  DL unicast:      off  IGMP monitor:     on
# MC data in:      0  # MC data acc:     0  # MC data out:     0

Network Capabilities:    Broadcast    Real Network
IGMP polls snt:   75  IGMP polls rcv:    0  Unexp polls:       0

IGMP reports:      0
```

Interface Address	インターフェースの IP アドレス
Attached Area	接続された区域の ID
Physical interface	物理インターフェースのタイプと数を表示します。
Interface Mask	インターフェースのサブネット・マスクを表示します。
Interface type	Brdcst (同報通信、例えばイーサネット・インターフェース)、PP (ポイント・ポイント・ネットワーク、例えば同期シリアル回線)、P-2-MP (ポイント・マルチポイント、例えばフレーム・リレー・ネットワーク)、Multi (非同報通信のマルチアクセス、例えば X.25 接続)、および VLink (OSPF バーチャル・リンク) のいずれでも構いません。
State	次のうちどれか 1 つです。1 (Down (ダウン))、2 (Loop back (ループバック))、 4 (Waiting (待機))、8 (Point-to-point (ポイント・ポイント))、16 (DR other (他の DR))、32 (backup DR (バックアップ DR))、または 64 (Designated router (指定ルーター))。
Authentication Type	インターフェースについてアクティブな認証のタイプを指示します。サポートされているタイプは、none または simple です。
Designated Router	指定ルーターの IP アドレス
Backup DR	バックアップの指定ルーターの IP アドレス
DR Priority	指定ルーターに割り当てられる優先順位を表示します。
Hello interval	現行のハロー間隔値を表示します。
Rxmt interval	現行の再送間隔値を表示します。
Dead interval	現行の停止間隔値を表示します。
TX delay	現行の伝送遅延値を表示します。
Poll interval	現行のポーリング間隔値を表示します。
Max pkt size	このインターフェースから送信される OSPF パケットについての最大サイズを表示します。
Demand circuit	デマンド・サーキット処理がインターフェースでアクティブかどうかを指示します。
TOS 0 cost	インターフェースの TOS 0 コストを表示します。

# Neighbors	近隣の数。そのハローが受信されたルートの数に構成済みのルートの数を加えたもの。
# Adjacencies	隣接の数。 これは、状態 (state) が交換 (Exchange) 以上の近隣の数です。
# Full adj	フル状態隣接の数。フル隣接の数とは、その状態がフルである (したがって、ルーターがそれと同期化したデータベースを持つ) 近隣の数です。
# Mcast Floods	インターフェースから伝送したリンク状態更新の数 (再送は数えません)
# Mcast acks	インターフェースから伝送したリンク状態確認の数 (再送は数えません)。
MC forwarding	インターフェースに対してマルチキャスト転送が使用可能にされているかどうかを表示します。
DL unicast	マルチキャスト・データグラムがデータ・リンク・マルチキャストとして転送されるのか、データ・リンク・ユニキャストとして転送されるのかを表示します。
IGMP monitor	IGMP がインターフェース上で使用可能であるかどうかを表示します。
# MC data in	このインターフェースで受信されてから正常に転送されたマルチキャスト・データグラムの数を表示します。
# MC data acc	正常に転送されたマルチキャスト・データグラムの数を表示します。
# MC data out	インターフェースから (データ・リンク・マルチキャストまたはデータ・リンク・ユニキャストのいずれかとして) 転送されたデータグラムの数を表示します。
Network Capabilities	インターフェースのネットワーク機能を表示します。
IGMP polls sent	インターフェースから送信された IGMP ホスト・メンバーシップ照会の数を表示します。
IGMP polls rcv	インターフェースで受信された IGMP ホスト・メンバーシップ照会の数を表示します。
Unexp polls	インターフェースで受信されたが、予期されていなかった (つまり、ルーター自体がそれを送信していたときに受信された) IGMP ホスト・メンバーシップ照会の数を表示します。
IGMP reports	インターフェースで受信された IGMP ホスト・メンバーシップ報告の数を表示します。
Nbr node: type and ID	ルーターがこのインターフェースでデータグラムを受信すると想定されていた場合には、上流ノードの ID を表示します。ここには、1 ～ 3 の整数をタイプしてください。ただし、1 はルーターを示し、2 は通過ネットワークを示し、3 はスタブ・ネットワークを示します。

Join

join コマンドは、ルーターをマルチキャスト・グループのメンバーとして確立するのに使用します。

このコマンドは OSPF 構成監視の join コマンドと同様ですが、次の 2 つの点が異なります。

- コマンドが OSPF モニターから与えられている (つまり、再始動/再ロードが必要とされない) 場合は、グループ・メンバーシップに及ぼす効果は即時に有効になります。同様に、通じて結合された IP グループは、ルーターの再始動および再ロードが行われると保存されません。
- コマンドによって、特定のグループが『結合される』回数が把握されます。

ルーターがマルチキャスト・グループのメンバーである場合は、グループ・アドレスに送信された PING および SNMP 照会に応答します。

構文 :

join *multicast-group-address*

例: join 224.185.0.0

Leave

leave コマンドは、マルチキャスト・グループ内のルーターのメンバーシップを除去するのに使用します。これにより、ルーターはグループ・アドレスに送信された PING および SNMP 照会に応答しなくなります。

このコマンドは OSPF 構成監視の leave コマンドと同様ですが、次の 2 つの点が異なります。

- コマンドが OSPF モニターから与えられている (つまり、再始動/再ロードが必要とされない) 場合は、グループ・メンバーシップに及ぼす効果は即時に有効になります。
- 実行された 『leave』 の回数が前に実行されていた 『join』 の回数と等しくなるまで、コマンドはグループ・メンバーシップを削除しません。 同様に、残された IP マルチキャスト・グループは、ルーターの再始動およびアンロードが行われると保存されません。

構文 :

leave *multicast-group-address*

例: leave 224.185.0.0

Mcache

mcache コマンドは、現在アクティブなマルチキャスト・キャッシュ項目のリストを表示するのに使用します。最初の突き合わせマルチキャスト・データグラムが受信されるたびに、マルチキャスト・キャッシュ項目がオンデマンドで作成されます。データグラム送信元ネットワークと着信先グループの各組み合わせごとに、別個のキャッシュ項目 (したがって、別個のルート) があります。

トポロジーの変更時 (例えば、MOSPF システムのポイント・ポイント回線が起動またはダウンする)、およびグループ・メンバーシップの変更時に、キャッシュ項目は消去されます。

構文 :

mcache

例 1: mcache

```
               0: TKR/0          1: SDLC/0         2: FR/0
               3: Internal

          Source          Destination     Count   Upst    Downstream
          133.1.169.2     225.0.1.10      8       Local   2 (4),3
          133.1.169.2     225.0.1.20      8       Local   2 (4),3
          3.3.3.3         225.0.1.10      8       2       3
```

Source 突き合わせデータグラムの発信元ネットワーク/サブネット

Destination　突き合わせデータグラムのあて先グループ

Count　受信されたデータグラムのうちキャッシュ項目に一致したものの数を表示します。

Upst　転送されるためにはそこからデータグラムを受信する必要がある近隣ネットワーク/ルーターを表示します。これが 『none』 であると、データグラムは決して転送されません。

Downstream　データグラムが転送される先のダウンストリーム・インターフェース/近隣の総数を表示します。これが 0 の場合は、データグラムは転送されません。

マルチキャスト転送キャッシュ記入項目にはさらに情報が入っています。コマンド行に突き合わせデータグラムの発信元およびあて先を入力すると、キャッシュ記入項目を詳細に表示することができます。突き合わせキャッシュ記入項目が見つからない場合は、項目が 1 つ作成されます。このコマンドの例を、例 2 に示します。

例 2: `mcache 128.185.182.9 224.0.1.2`

```
source Net:     128.185.182.0
Destination:    224.0.1.2
Use Count:      472
Upstream Type:  Transit Net
Upstream ID:    128.185.184.114
Downstream:     128.185.177.11 (TTL = 2)
```

短形式の mcache コマンドで示された情報のほか、以下のフィールドが表示されます。

Upstream Type　データグラムの転送のためにはそこから受信される必要のあるノードのタイプを指示します。このフィールドに可能な値は、『none』 (データグラムが転送されないことを指示します)、『router』 (データグラムがポイント・ポイント接続を介して受信される必要があることを指示します)、『transit network』、『stub network』、および 『external』 (データグラムは別の自立システムから受信されると予想されることを指示します) です。

Downstream　データグラムが送信される各インターフェースまたは近隣ごとに別個の行を印刷します。TTL 値も与えられます。この値は、このインターフェースとの間でやり取りされるデータグラムは、少なくとも、それぞれの IP ヘッダーに指定 TTL 値をもっている必要があることを指示します。ルーター自身がマルチキャスト・グループのメンバーであれば、『internal Application』 を指定する行がダウンストリーム・インターフェース/近隣の 1 つとして現れます。

Mgroups

mgroups コマンドは、ルーターの接続されたインターフェースのグループ・メンバーシップを表示するのに使用します。ルーターがその上で指定ルーターまたはバックアップ指定ルーターのいずれかであるインターフェースのグループ・メンバーシップだけが表示されます。

構文 :

mgroups

例: mgroups

```
                    Local Group Database
 Group                  Interface                 Lifetime (secs)

224.0.1.1           128.185.184.11 (Eth/1)          176
224.0.1.2           128.185.184.11 (Eth/1)          170
224.1.1.1           Internal                        1
```

Group　特定のインターフェースで (IGMP を介して) 報告されたグループ・アドレスを表示します。

Interface　グループ・アドレスが (IGMP を介して) 報告された先のインターフェース・アドレスを表示します。

ルーターの内部グループ・メンバーシップは 『internal』 の値によって示されます。 これらの項目では、lifetime フィールド (下を参照) は、特定のグループで要求されたメンバーシップをもつアプリケーションの数を示します。

Lifetime　所定のグループについてインターフェースでメンバーシップ報告がなくなってから、項目が存続する秒数を表示します。

Mstats

さまざまなマルチキャスト・ルーティング統計を表示するには、 **mstats** コマンドを使用してください。 このコマンドは、マルチキャスト・ルーティングが使用可能になっているかどうか、およびルーターが区域間または AS 間 (あるいはその両方) の転送側であるかどうかを示します。

構文 :

mstats

例: mstats

```
                    MOSPF forwarding:       Enabled
                    Inter-area forwarding:  Enabled
                    DVMRP forwarding:       Disabled

Datagrams received:           2496  Datagrams (ext source):    0
Datagrams fwd (multicast):       0  Datagrams fwd (unicast):   0
Locally delivered:               0  No matching rcv interface: 0
Unreachable source:              3  Unallocated cache entries: 0
Off multicast tree:              0  Unexpected DL multicast:   0
Buffer alloc failure:            0  TTL scoping:               0

# DVMRP routing entries:         0  # DVMRP entries freed:     0
# fwd cache alloc:               1  # fwd cache freed:         0
# fwd cache GC:                  0  # local group DB alloc:    0
# local group DB free:           1
```

MOSPF forwarding　ルーターが IP マルチキャスト・データグラムを転送するかどうかを表示します。

Inter-area forwarding　ルーターが区域間で IP マルチキャスト・データグラムを転送するかどうかを表示します。

DVMRP forwarding　ルーターがマルチキャスト・ルーティング用に DVMRP を使用するように構成されているかどうかを表示します。

Datagrams received　ルーターによって受信されたマルチキャスト・データグラムの数を表示します (あて先グループが 224.0.0.1 ～ 224.0.0.255 の範囲にあるデータグラムはこの合計に含まれていません)。

Datagrams (ext source)　受信され、その発信元が AS の外部にあるデータグラムの数を表示します。

Datagrams fwd (multicast)　データ・リンク・マルチキャストとして転送されたデータグラムの数を表示します (これには、必要な場合には、パケット複写が含まれます。したがって、このカウントは受信された数より大きくなることがあります)。

Datagrams fwd (unicast)　データ・リンク・ユニキャストとして転送されたデータグラムの数を表示します。

Locally delivered　内部アプリケーションに転送されたデータグラムの数を表示します。

No matching rcv interface　非 MOSPF インターフェースの非 AS 間マルチキャスト転送者によって受信されたデータグラムのカウントを表示します。

Unreachable source	その発信元アドレスが到達不能なデータグラムのカウントを表示します。
Unallocated cache entries	資源の不足により、そのキャッシュ項目を作成できなかったデータグラムのカウントを表示します。
Off multicast tree	突き合わせキャッシュ項目にアップストリーム近隣がなかったか、ダウンストリーム・インターフェース/近隣がなかったために、転送されなかったデータグラムのカウントを表示します。
Unexpected DL multicast	データ・リンク・ユニキャスト用に構成されたインターフェースでデータ・リンク・マルチキャストとして受信されたデータグラムのカウントを表示します。
Buffer alloc failure	バッファーが不足するために複写できなかったデータグラムのカウントを表示します。
TTL scoping	TTL がグループ・メンバーに到達できないことを示しているために転送されなかったデータグラムを示します。
DVMRP routing entries	DVMRP ルーティング項目の数を表示します。
DVMRP entries freed	解放された DVMRP 項目の数を示します。このサイズは、ルーティング項目の数から解放された項目の数を引いたものになります。
# fwd cache alloc	割り振られたキャッシュ項目の数を示します。現行の転送キャッシュ・サイズは、割り振られた項目の数 (『# fwd cache alloc』) から解放されたキャッシュ項目の数 (『# fwd cache freed』) を引いたものです。
# fwd cache freed	解放されたキャッシュ項目の数を示します。現行の転送キャッシュ・サイズは、割り振られた項目の数 (『# fwd cache alloc』) から解放されたキャッシュ項目の数 (『# fwd cache freed』) を引いたものです。
# fwd cache GC	最近使用されておらず、キャッシュがオーバーフローしたために消去されたキャッシュ項目の数を示します。
# local group DB alloc	割り振られたローカル・グループ・データベース項目の数を示します。割り振られた数 (『# local group DB alloc』) から解放された数 (『# local group DB free』) を引いたものが、ローカル・グループ・データベースの現行サイズに等しくなります。
# local group DB free	割り振られたローカル・グループ・データベース項目の数を示します。割り振られた数 (『# local group DB alloc』) から解放された数 (『# local group DB free』) を引いたものが、ローカル・グループ・データベースの現行サイズに等しくなります。

キャッシュ・ヒットの数は、受信されたデータグラムの数 (『Datagrams received』) から、『No matching rcv interface』、『Unreachable source』、および 『Unallocated cache entries』 のために廃棄されたデータグラムの合計を引き、さらに 『# local group DB alloc』 を引いた数として計算できます。 キャッシュ・ミスの数は単に 『# local group DB alloc』 です。

Neighbor Summary

neighbor summary コマンドは、OSPF 近隣に関連する統計およびパラメーターを表示するのに使用します。引き数が与えられない (例 1 を参照) 場合は、単一の行が印刷されて、各近隣ごとに要約します。 近隣の IP アドレスが与えられた (例 2 を参照) 場合は、その近隣に関する詳細な統計が表示されます。

構文 :

neighbor *neighbor-ip-address*

例 1: `neighbor`

```
Neighbor addr   Neighbor ID     State  LSrxl  DBsum  LSreq  Ifc
128.185.125.39  128.185.136.39  128      0      0      0   PPP/1
128.185.125.41  128.185.128.41    8      0      0      0   PPP/1
128.185.125.38  128.185.125.38    8      0      0      0   PPP/1
128.185.125.25  128.185.129.25    8      0      0      0   PPP/1
128.185.125.40  128.185.129.40  128      0      0      0   PPP/1
128.185.125.24  128.185.126.24    8      0      0      0   PPP/1
```

Neighbor addr	近隣アドレスを表示します。
Neighbor ID	近隣の OSPF ルーター ID を表示します。
Neighbor State	次のうちどれか 1 つです。1 (Down)、2 (Attempt)、 4 (Init)、8 (2-Way)、16 (ExStart)、32 (Exchange)、 64 (Loading) または 128 (Full)。
LSrxl	この近隣用の現行のリンク状態再送リストのサイズを表示します。
DBsum	近隣に送信されるのを待機しているデータベース要約リストのサイズを表示します。
LSreq	近隣から要求されている最近の公示の数を表示します。
Ifc	ルーターと近隣によって共用されるインターフェースを表示します。

例 2: `neighbor 128.185.138.39`

表示されるフィールドのほとんどについての意味は、 OSPF 仕様 (RFC 2178) のセクション 10 に記述されています。

```
            Neighbor IP address:    128.185.184.34
            OSPF Router ID:         128.185.207.34
            Neighbor State:         128
            Physical interface:     Eth/1
            DR choice:              128.185.184.34
            Backup choice:          128.185.184.11
            DR Priority:            1
            Nbr options:            E,MC
            Alternate TOS 0 cost:   5

DB summ qlen:      0  LS rxmt qlen:      0  LS req qlen: 0
Last hello:        7  No Hello         Off

# LS rxmits:     108  # Direct acks:    13  # Dup LS rcvd: 572
# Old LS rcvd:     2  # Dup acks rcv:  111  # Nbr losses:   29
# Adj. resets:    30
```

Neighbor IP addr	近隣 IP アドレス
OSPF router ID	近隣の OSPF ルーター ID
Neighbor State	次のうちどれか 1 つです。1 (Down)、2 (Attempt)、 4 (Init)、8 (2-Way)、16 (ExStart)、32 (Exchange)、 64 (Loading) または 128 (Full)。
Physical interface	ルーターおよび近隣の共通のネットワークの物理インターフェース・タイプおよび番号を表示します。
DR choice, backup choice, DR priority	近隣から受信された最後のハローに見られる値を示します。
Nbr options	近隣によってサポートされる任意選択の OSPF 機能を示します。これらの機能は、E (外部タイプ 5 を処理します。これが共通ネットワークが属している区域に設定されていない場合は、スタブとして構成されています)、T (TOS に基づきルーティングできます) および MC (IP マルチキャスト・データグラムを転送できます) で示されます。 このフィールドは、状態 (state) が Exchng 以上の近隣でのみ有効です。
Alternate TOS 0 cost	ポイント・マルチポイント・インターフェースの場合は、この近隣の代替 TOS 0 コストを示します。ルーターのタイプ 1 (ルーター・リンク) LSA では、インターフェースの TOS 0 コストではなく、このコストが公示されます。
DBsumm qlen	データベース記述パケットで要約されるのを待機している公示の数を示します。 近隣が Exchange の状態である以外は、ゼロでなければなりません。
LS rxmt qlen	近隣に伝送したが、まだ学習されていない公示の数を示します。

LS req qlen	近隣から Loading の状態で要求された公示の数を示します。
Last hello	近隣からハローが受信されてからの秒数を示します。
# LS rxmits	伝送時に発生した再送の数を示します。
# direct acks	重複リンク状態公示に対する応答を示します。
# Dup LS rcvd	伝送時に発生した重複再送の数を示します。
# Old LS rcvd	伝送時に受信された古い公示の数を示します。
# Dup acks rcvd	受信された重複確認の数を示します。
# Nbr losses	近隣が状態 Down に変換された回数を示します。
# Adj. resets	状態 ExStart への項目をカウントします。

Ping

Ping コマンドの説明については、325ページの『Ping』を参照してください。

Reset

OSPF **reset** コマンドは、ルーターを再始動することによって OSP ルーティング構成を動的に修正するのに使用します。詳細については、352ページの『OSPF 構成パラメーターを動的に変更する』を参照してください。

注: 再始動の際に、OSPF ルートは、IP 転送を維持するためにルーティング・テーブルに保存されます。

構文 :

reset ospf

例 :

```
OSPF>interface

Ifc Address      Phys    assoc. Area     Type    State   Auth   #nbrs  #adjs
153.2.2.25       Eth/0   0.0.0.1         Brdcst   16     None       3      2
10.69.1.1        FR/0    0.0.0.0         P-2-MP    8     None       1      1

OSPF>
*t 6

OSPF Config>delete interface 10.69.1.1
OSPF Config>
*t 5

OSPF>reset ospf
OSPF>interface

Ifc Address      Phys    assoc. Area     Type    State   Auth   #nbrs  #adjs
153.2.2.25       Eth/0   0.0.0.1         Brdcst   16     None       3      2
```

Traceroute

Traceroute コマンドの説明については、330ページの『Traceroute』を参照してください。

Routers

routers コマンドは、OSPF によって計算され、現在ルーティング・テーブルにあるすべてのルーター・ルートを表示するのに使用します。 **dump routing tables** コマ

ンドでは、 Net フィールドはあて先がネットワークであることを示します。 routers コマンドでは、他のすべてのあて先が扱われます。

構文 :

routers

例 :

```
DType RType Destination       AREA          Cost   Next hop(s)
 ASBR  SPF   128.185.142.9    0.0.0.1         1   128.185.142.9
 Fadd  SPF   128.185.142.98   0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.7    0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.48   0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.111  0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.38   0.0.0.1         1    0.0.0.0
 Fadd  SPF   128.185.142.11   0.0.0.1         1    0.0.0.0
   BR  SPF   128.185.142.9    0.0.0.2         1   128.185.142.9
   BR  SPF   128.185.142.9    0.0.0.2         2   128.185.184.114
 Fadd  SPF   128.185.142.47   0.0.0.2         1    0.0.0.0
```

DType　あて先タイプを示します。

- **Net**　あて先がネットワークであることを示します。
- **ASBR**　あて先が AS 境界ルーターであることを示します。
- **ABR**　あて先が区域境界ルーターであることを示します。
- **Fadd**　転送アドレス (外部ルートの) を示します。

RType　ルート・タイプおよびルートがどのように派生したかを示します。

- **SPF**　ルートが区域内ルート (Dijkstra 計算によって求められた) であることを示します。
- **SPIA**　区域間ルート (要約リンク公示の考慮によって求められた) であることを示します。

Destination　あて先ルーターの OSPF ID。タイプ D の項目では、ルーターの IP アドレスが表示されます (別の AS にあるルーターに対応します)。

Area　それが属する AS 区域を表示します。

Cost　ルート・コストを表示します。

Next hop　あて先ホストへ向かうパス上の次のルーターのアドレス。欄の末尾の括弧内の数は、あて先への等コスト・ルートの数を示しています。

Size

size コマンドは、現在、タイプ別に分類されたリンク状態データベースにある LSA の数を表示するのに使用します。

構文 :

size

例 :

```
# Router-LSAs:            6
# Network-LSAs:           2
# Summary-LSAs:           45
# Summary Router-LSAs:    6
# AS External-LSAs:       2
# Group-membership-LSAs:  11
```

```
# Intra-area routes:      11
# Inter-area routes:      15
# Type 1 external routes: 0
# Type 2 external routes: 2
```

Statistics

statistics コマンドは、OSPF ルーティング・プロトコルによって生成された統計を表示するのに使用します。統計は実施がどれだけよく実行されているかを、その記憶域およびネットワークの使用率を含めて、示しています。表示されるフィールドの多くは、OSPF 構成の確認です。

構文 :

statistics

例 :

```
OSPF>statistics

               OSPF Router ID:         1.1.1.1
               External comparison:    Type 2
               RFC 1583 compatibility: Yes
               Multicast OSPF (MOSPF): Yes (Inter-Area Multicast Forwarder)
               Demand circuit support: Yes
               AS boundary capability: No
               Import external routes: None
               Orig. default route:    No (0,0.0.0.0)
               Default route cost:     (1, Type 2)
               Default forward. addr:  0.0.0.0

  Attached areas:                   1  Estimated # external routes:   1000
  Estimated # OSPF routers:        50  Estimated heap usage:        148000
  OSPF packets rcvd:               63  OSPF packets rcvd w/ errs:        1
  Transit nodes allocated:         21  Transit nodes freed:             17
  LS adv. allocated:               83  LS adv. freed:                   61
  Queue headers alloc:             64  Queue headers avail:             64
  Maximum LSA size:              2048

  # Dijkstra runs:                  7  Incremental summ. updates:        2
  Incremental VL updates:            0  Buffer alloc failures:           0
  Multicast pkts sent:              31  Unicast pkts sent:              19
  LS adv. aged out:                  9  LS adv. flushed:                11
  Ptrs To Invalid LS adv:            0  Incremental ext. updates:       14
  LSA Max Random Initial Age:     1770  LSA MINARRIVAL rejects:          1
  External LSA database:
  Current state:                Normal
  Number of LSAs:                   10  Number of overflows:             0
```

S/W version	現行の OSPF ソフトウェア改訂レベルを表示します。
OSPF Router ID	ルーターの OSPF ID を表示します。
External comparison	外部ルートをインポートするときにルーターが使用する外部ルート・タイプを表示します。
RFC 1583 compatibility	OSPF AS external route (OSPF AS 外部ルート) が RFC 1583 と互換であるかどうかを指示します。
AS boundary capability	外部ルートがインポートされるかどうかを表示します。
Import external routes	どの外部ルートがインポートされるかを表示します。
Orig default route	ルーターが OSPF 省略時ルートを公示するかどうか表示します。値が『Yes』 で、ゼロ以外の数が括弧内に表示されている場合は、省略時ルートが公示されるのは、ネットワークへのルートが存在するときだけです。
Default route cost	省略時ルート (公示される場合) のコストおよびタイプを表示します。

Default forward addr	省略時ルート (公示される場合) で指定される転送アドレスを表示します。
Attached areas	ルートがそこへの活動インターフェースをもつ区域の数を示します。
Estimated heap usage	OSPF リンク状態データベースのサイズ (バイト数) のおおまかな表示
Transit nodes	ルーター・リンクおよびネットワーク・リンクの公示を保管するために割り振られます。
LS adv.	要約リンクおよび AS 外部リンクの公示を保管するために割り振られます。
Queue headers	リンク状態公示のリストを作成します。これらのリストは、伝送プロセスおよびデータベース交換プロセスで使用されます。割り振られた待ち行列ヘッダーの番号が解放された数に等しくない場合は、近隣とのデータベース同期化が進行中です。
# Dijkstra runs	OSPF ルーティング・テーブルがスクラッチから何度計算されたかを示します。
Maximum LSA size	このルーターによって発信できる最大サイズの LSA。これは、OSPF 構成を介して構成された値の最小値と、一般的な構成を介して計算または構成された最大パケット・サイズです。
Incremental summ updates, incremental VL updates	新しい要約リンク公示によってルーティング・テーブルが部分的に再作成されたことを示します。
Buffer alloc failures.	バッファー割り振りの障害を示します。OSPF システムはパケット・バッファーの一時的不足から回復します。
Multicast pkts sent	OSPF ハロー・パケットおよび伝送手順の過程で送信されたパケットを扱います。
Unicast pkts sent	OSPF パケットの再送およびデータベース交換手順を扱います。
LS adv. aged out	60 分に達した公示の数を数えます。リンク状態公示は 60 分を超えると時間切れになります。 通常はこの時間になる前に更新されます。
LS adv. flushed	リンク状態データベースから除去された (置換されなかった) 公示の数を示します。
Ptrs to Invalid LS adv	データベース内にある、異常形成で変換処理できなかった公示の数を表示します。
Incremental ext. updates.	ルーティング・テーブルに累積導入される外部着信先への変更回数を表示します。
LSA Max Random Initial Age	自己発信 LSA に関する最大初期ランダム経時を表示します。
LSA MINARRIVAL Rejects	MINARRIVAL (1 秒) 以内に新しいインスタンスを受信したためリジェクトされた LSA の数を表示します。
External LSA database:	LSA データベースに関する情報が得られます。

Current state
現行の AS 外部 LSA のデータベースが正常な状態にあるか、過負荷状態にあるかどうか。

Number of LSA
現在データベースにある外部 LSA の数

Number of overflows
外部 AS LSA データベースが過負荷状態に入った回数

Weight

weight コマンドは、ルーター OSPF インターフェースの 1 つのコストを変更するのに使用します。この新しいコストは即時に OSPF ルーティング・ドメイン全体に伝送され、それに従ってルートが更新されます。

ルーターが再始動または再ロードされるたびに、インターフェースのコストはその構成済みのコストに戻ります。 コストの変更を永続的にするには、weight コマンドを呼び出した後で該当する OSPF インターフェースを再構成する必要があります。インターフェースのコストが変化しない限り、このコマンドにより、新しいルーター・リンク公示が開始されます。

構文 :

weight *ip-interface-address new-cost*

例: `weight 128.185.124.22 2`

第18章 BGP4 の使用

この章では、BGP 構成コマンドを使用する境界ゲートウェイ・プロトコル (BGP) の使用方法について説明します。

この章には次の節が含まれています。

- 『境界ゲートウェイ・プロトコルの概要』
- 『BGP4 の動作』
- 400ページの『BGP4 をセットアップする』
- 401ページの『ポリシー定義の例』

境界ゲートウェイ・プロトコルの概要

BGP は、自律システム間でネットワーク到達可能度情報を交換するのに使用される外部ゲートウェイ・ルーティング・プロトコルです。AS は、基本的に、単一の管理編成の下で動作するルーターとエンド・ノードの集合です。各 AS 内では、ルーターとエンド・ノードが、内部ゲートウェイ・プロトコルを使用してルーティング情報を共用します。内部ゲートウェイ・プロトコルは、RIP でも OSPF でも構いません。

BGP は、自律システム間でのルーティング情報のループなし交換でインターネットに取り入れられました。無クラス・ドメイン間ルーティング (CIDR) に基づき、BGP は、それ以来、ルーティング情報の集約と縮小をサポートするまでになりました。

本質において、CIDR は、以下の問題を扱うよう設計された戦略です。

- クラス B アドレス空間の消耗
- ルーティング・テーブルの成長

CIDR により、アドレス・クラスの概念は払しょくされ、*n* 個の異なるルートを単一のルートにまとめる方法が提供されます。これにより、BGP ルーターが保管し、交換する必要のあるルーティング情報の量は著しく削減されます。

注: IBM は、BGP の最新バージョン、BGP4 のみをサポートします。これは、RFC 1654 で定義されています。この章および IBM のルーターのインターフェースにおける BGP の参照はすべて BGP4 を対象とするものであり、以前の BGP のバージョンには適用されません。

BGP4 の動作

BGP は、自律システム間ルーティング・プロトコルです。本質において、BGP ルーターは、それぞれ固有のシステムおよび他の自律システム内の BGP 近隣との間での到達可能度情報を選択的に収集し、公示します。到達可能度情報は、特定の BGP スピーカーまでのパスを形成する一連の AS 番号と、公示済みの各パスを介して到達可能な IP ネットワークのリストで構成されます。AS は、RIP または OSPF など、1 つまたは複数の内部ゲートウェイ・プロトコル (IGP) を使用して到達可能度情報を共用するネットワークとルーターの管理グループです。

BGP4 の使用

BGP を実行するルーターは、BGP スピーカーと呼ばれます。これらのルーターは、それぞれの BGP 近隣 (クライアント) に関してサーバーとして機能します。各 BGP ルーターは、ポート 179 での受動 TCP 接続をオープンし、この既知のアドレスからの着信接続を listen します。 ルーターは、使用可能になっている BGP 近隣への能動 TCP 接続もオープンします。この TCP 接続により、BGP ルーターは、同じ自律システムまたは他の自律システム内で近隣と到達可能度情報を共用したり、更新したりできます。

同じ AS 内の BGP スピーカー間の接続は内部 BGP (IBGP) 接続と呼ばれ、異なる自律システム内の BGP スピーカー間の接続は外部 BGP (EBGP) 接続と呼ばれます。

単一の AS が、外側の自律システムに対して BGP 接続を 1 つもつ場合もあれば、多数もつ場合もあります。図36 は、2 つの自律システムを示しています。 AS1 内の BGP スピーカーは、AS2 内のその近隣と TCP 接続を確立しようとしています。この接続が確立されると、ルーターは、到達可能度情報を共用できるようになります。

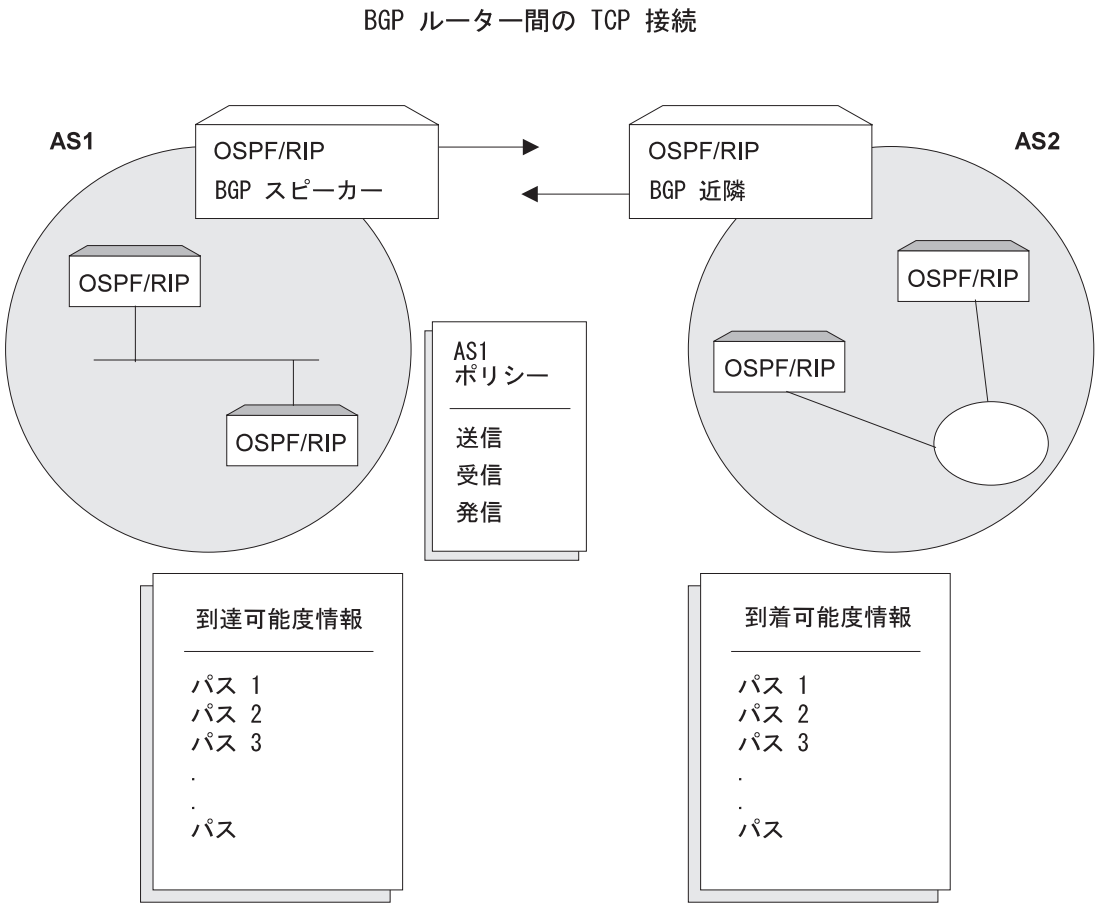


図 36. 2 つの自律システム間の BGP 接続. AS1 内の BGP スピーカーが AS2 内のその近隣と TCP 接続を確立すると、その 2 つのルーターは、到達可能度情報を選択的に交換できます。各ルーターが送信または受け入れる情報は、各ルーターについて定義されたポリシーによって決められます。

図36 に示されている自律システムには BGP ルーターが 1 つしかありませんが、いずれも、他の自律システムへの接続を複数もつことが可能です。この例として、397 ページの図37 は、3 つの相互接続された自律システムを示しています。AS1 は外側

の自律システムに対して 3 つの BGP 接続をもっています。AS2、AS3、および ASx との接続がそれぞれ 1 つずつです。同様に、AS3 には、AS1、AS2、および ASy との接続があります。

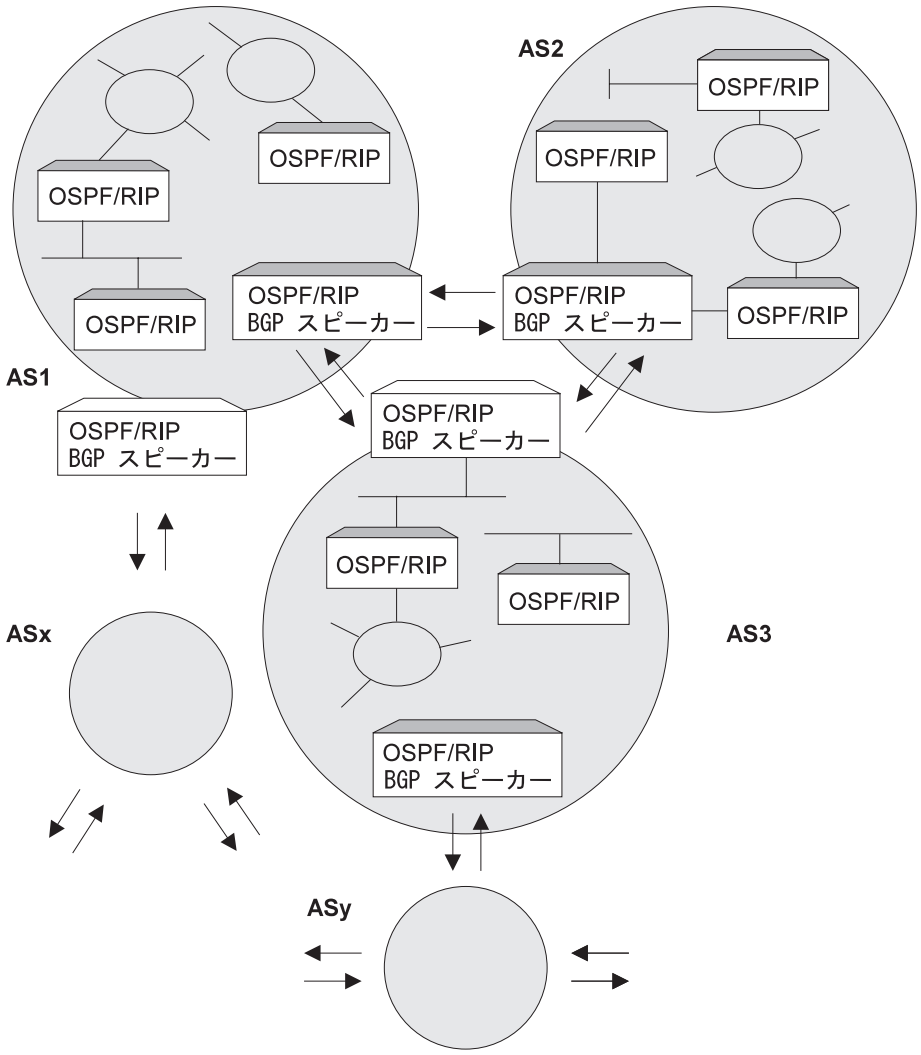


図 37. 3 つの自律システム間の BGP 接続. AS1 と AS3 には BGP スピーカーが 2 つあることに注意してください。

TCP 接続が確立されると、396ページの図36 に示されている BGP スピーカーは、そのルーティング・テーブル全体を AS2 内のその BGP 近隣に送信できます。 ただし、セキュリティーやその他の理由から、各ネットワークに関する到達可能度情報を AS2 に送信することは望ましくありません。同様に、AS1 内の各ネットワークに関する到達可能度情報を AS2 が受信することも望ましいことではありません。

発信、送信、および受信のポリシー

公示する (送信する) 到達可能度情報と受け入れる (受信する) 到達可能度情報の決定は、明示的に定義されたポリシー・ステートメントに基づいて行われます。 IBM の BGP 実装により、次の 3 つのタイプのポリシー・ステートメントがサポートされます。

- 発信ポリシー (Originate Policies)
- 送信ポリシー (Send Policies) - 送信ポリシーには、次の 2 つのタイプがあります。
  - AS ベースの送信ポリシーが適用されるのは、特定の AS かすべての AS の場合だけです。送信ポリシーが構成されていないと、あて先アドレスは除去されます。
  - 近隣ベースの送信ポリシーが適用されるのは、特定の近隣 (複数の場合もある) の場合だけです。特定の近隣に対して近隣ベースの送信ポリシーが構成されていないと、AS ベースの送信ポリシーが適用されます。近隣ベースの送信ポリシーが構成されれば、AS ベースの送信ポリシーは無視されます。

  各送信ポリシー・ステートメントには、あて先ネットワーク公示分類子と一組の対応処置がそれぞれ含まれています。

  あて先ネットワーク分類は、次の基準で行われます。
  - 正確なあて先ネットワーク
  - あて先ネットワークの範囲
  - 発信 AS 番号
  - AS パス属性内にある AS 番号

  次のような処置が考えられます。
  - 公示のためにあて先ネットワークを除外する
  - 特定の AS やすべての AS (AS ベースのポリシーを使用) または特定の近隣 (近隣ベースのポリシーの使用) への公示のためにあて先ネットワークを組み込む
  - MED 値を設定する
  - ASpath パディング

  注: MED と ASpath パディングが適用できるのは、近隣ベースのポリシーの場合だけです。

  MED 属性値では、外部 BGP 近隣にそのルート優先の手掛かりを与えます。MED 属性値が最も低いルートが優先されます。詳しくは、404ページの『ルート優先プロセス』 を参照してください。
- ASpath パディングでは、追加のローカル AS 番号を BGP ルートの ASpath に複数回 (1 ～ 10) 追加できます。ASpath が最も低いルートが優先されます。詳しくは、404ページの『ルート優先プロセス』 を参照してください。
- 受信ポリシー (Receive Policies) - 受信ポリシーには、次の 2 つのタイプがあります。
  - AS ベースの受信ポリシーが適用されるのは、特定の AS かすべての AS の場合だけです。受信ポリシーが構成されていないと、あて先アドレスは除去されます。
  - 近隣ベースの受信ポリシーが適用されるのは、特定の近隣 (複数の場合もある) の場合だけです。特定の近隣に対して近隣ベースの受信ポリシーが構成されていないと、AS ベースの受信ポリシーが適用されます。近隣ベースの受信ポリシーが構成されれば、AS ベースの受信ポリシーは無視されます。

  各受信ポリシー・ステートメントには、あて先ネットワーク公示分類子と一組の対応処置がそれぞれ含まれています。

あて先ネットワーク分類は、次の基準で行われます。

- 正確なあて先ネットワーク
- あて先ネットワークの範囲
- 発信 AS 番号
- AS パス属性内にある AS 番号

次のような処置が考えられます。

- あて先ネットワークを除外する
- 特定の AS やすべての AS (AS ベースのポリシーを使用) または特定の近隣 (近隣ベースのポリシーを使用) からのあて先ネットワークを組み込む
- MED 値をリセットする
- 重み値を設定する
- IGP メトリック値を設定する
- ローカル優先値を設定する

注: MED、重み、ローカル優先が適用できるのは、近隣ベースのポリシーの場合だけです。

重み値では、ローカル BGP ルーターに最高重み値に基づいてルートを選択する手掛かりを与え、ルート優先アルゴリズムは無視します。

BGP メッセージ

BGP ルーターは、4 種類のメッセージ、つまり、OPEN、KEEP ALIVE、UPDATE、および NOTIFICATION メッセージを使用して、それぞれの近隣と通信します。

OPEN

Open メッセージは、BGP 近隣までのリンクが起動され、接続を確立したときに最初に伝送されるメッセージです。

KEEP ALIVE

Keep alive メッセージは、BGP ルーターが、特定の接続が有効で機能していることを互いに知らせ合うために使用します。

UPDATE

Update メッセージには、内部ルーティング・テーブル情報が含まれています。BGP スピーカーは、それぞれのルーティング・テーブルに変更があった場合にのみ update メッセージを送信します。

NOTIFICATION

Notification メッセージは、BGP スピーカーが既存の接続を強制的に終了させられる条件を検出するたびに送信されます。このメッセージは、接続が伝送される前に公示されます。

BGP4 をセットアップする

BGP をセットアップするには、次の 3 つの基本的なステップが必要です。

1. 『BGP を使用可能にする』.

   BGP を使用可能にするために、BGP ルーターの固有の AS 番号を指定する必要があります。AS 番号は、Stanford Research Institute Network Information Center (スタンフォード・リサーチ・インスティチュート・ネットワーク情報センター) によって割り当てられます。

2. 『BGP 近隣を定義する』.

   BGP 近隣 は、BGP が TCP 接続を確立するときの BGP ルーターです。近隣が定義されると、それらへの接続は省略時値によって確立されます。

3. 401ページの『ポリシーを追加する』.

   ユーザーが設定したポリシーは、BGP スピーカーによってインポートおよびエクスポートされるルーターを決めます。ポリシーは、異なる目的別に設定することができます。詳細については、401ページの『ポリシー定義の例』を参照してください。

BGP を使用可能にする

BGP を使用可能にするには、次のように **enable BGP speaker** コマンドを使用して行います。

```
BGP Config> enable BGP speaker
AS [0]? 167
TCP segment size [1024]?
```

AS 番号 は 1 ～ 65535 の範囲内にあることが必要です。 *TCP セグメント* のサイズは、1 ～ 65535 の範囲内のものでなければなりません。 *TCP セグメント* の省略時値は 1024 です。この数値は、BGP が受動 TCP 接続に使用する最大セグメント・サイズを表します。

enable bgp コマンドを発行したら、その後で装置をリブートして、BGP を使用可能にする必要があります。

BGP 近隣を定義する

BGP スピーカーを使用可能にした後で、その近隣を定義する必要があります。BGP 近隣は、内部でも外部でも構いません。内部近隣は、同じ AS 内に存在するもので、互いに直接接続している必要はありません。外部近隣は、別の自律システム内に存在するものです。外部近隣は、互いに直接接続している必要があります。

内部または外部 BGP 近隣を定義するためには、**add neighbor** コマンドを使用してください。近隣の IP アドレスを指定して、次のようにその近隣に AS 番号を割り当てる必要があります。内部近隣は、BGP スピーカーと同じ AS 番号をもっていなければなりません。

```
BGP Config> add neighbor 192.0.190.178
AS [0]? 178
Init timer [12]? 30
Connect timer [120]?
Hold timer [90]? 30
TCP segment size [1024]? 512
```

構成メモリーに保管されている近隣構成パラメーターに基づいて、 **reset neighbor** コマンドを使用して、指定された BGP 近隣を起動します。

ポリシーを追加する

IBM の BGP 実装により、次の 3 つのタイプのポリシー・コマンドがサポートされます。

- *Originate Policy*。これは、エクスポートする内部ゲートウェイ・プロトコル (IGP) ネットワークをユーザーが選択できるようにします。
- *Receive Policy*。これは、BGP ピアからインポートするルート情報をユーザーが選択できるようにします。
- *Send Policy*。これは、BGP ピアへエクスポートするルート情報をユーザーが選択できるようにします。エクスポート可能なルート情報には、近接する自律システムから収集された情報だけでなく、IGP を起点とするルートも含めることができます。

近隣ベースのポリシーを追加したり変更したりした場合は、**reset neighbor** コマンドを使用して、近隣ポリシーを起動します。AS ベースのポリシーを追加したり変更したりした場合は、装置をリブートする必要があります。

ポリシー定義の例

この節では、ユーザーが BGP スピーカーのために設定できる特定のポリシーの例を示しています。ポリシーはすべて、BGP **add** コマンドを使用して定義されます。**add** コマンドの構文については、408ページの『Add』を参照してください。

発信ポリシー (Originate Policy) の例

公示のためにすべてのルートを組み込む

この例には、BGP スピーカーの IGP ルーティング・テーブルにあるすべてのルートが公示のために組み込まれています。この意味では、このコマンドは、BGP の “省略時”発信ポリシーと見ることができます。

コマンドは、単一の (正確な) アドレスではなく、ある範囲のアドレスを指定することに注意してください。

```
BGP Config> add originate-policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

ある範囲のルートを除外する

この例も範囲を指定しますが、この場合は、BGP スピーカーがこの範囲内のアドレスをその近隣に公示しないようにすることが目的です。

この例では、194.10.16.0 ～ 194.10.31.255 の範囲のルートすべてを IGP ルーティング・テーブルから除外し、そうすることでそれらが公示されないようにしています。

```
BGP Config> add originate-policy exclusive
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

タグは、受信済みの RIP 情報です。特定のタグ値に基づいて、公示用にネットワークを選択できます。タグ値の設定については、 265ページの『第15章 IP の構成と監視』の **Set** コマンドの説明を参照してください。

公示のためにすべての無クラス・ルートを組み込む

省略時値では、BGP スピーカーからの IGP ルーティング・テーブルからのクラス付きルートだけが公示用に選択されます。サブネット公示のために無クラスとクラス付きの両方のルートを選択する場合は、 **enable classless-bgp** コマンドか **patch bgp-subnets** コマンドを使用します。

AS ベースの受信ポリシーの例

すべての BGP 近隣からのすべてのルートをインポートする

この例では、BGP スピーカーが、必ず、その近隣のすべてから自分の IGP ルーティング・テーブルへすべてのルートをインポートするようになっています。

```
BGP Config> add receive-policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]?
Adjacent AS# [0]?
IGP-metric [0]?
```

IGP-metric は、受け入れられたルートがスピーカーの IGP ルーティング・テーブルにインポートされるときに使用されるメトリック値を指定します。 IGP-metric の値を入力するようプロンプト指示されるのは、ポリシーをルートの組み込み用に設定するときだけです。

IGP-metric が -1 の場合、これらのルートは IGP にインポートされません。したがって、ルートは再公示できません。

発信 AS からの特定のルートをブロックする

この例では、BGP スピーカーが、AS 168 を起点とするルートを隣接 AS 165 からインポートできないようにします。このコマンドは、セキュリティー上の理由から AS 168 からのルートを BGP スピーカーに受け取らせたくない場合に使用できます。

```
BGP Config> add receive-policy exclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]? 168
Adjacent AS# [0]? 165
```

特定の ASpath をブロックする

この例では、BGP スピーカーが、ASpath リストに AS 175 が入っているルートをインポートするのを阻止します。

```
BGP Config> add no-receive
Enter AS: [0]? 175
```

近隣ベースの受信ポリシーの例

特定の BGP 近隣からのすべてのルートをインポートする場合は、重み = 100 に設定する

この例では、BGP 近隣 192.0.190.178 からのルートすべてをインポートできます。すべてのルートが重み値 100 で、IGP メトリック値 1 になります。

受信ポリシーのポリシー・リスト名を定義します。

```
BGP Config> add policy-list
Name[]?S1_100_r
Policy Type(Receive/Send)[Receive]?Receive
```

定義した受信ポリシー・リスト名を特定の近隣に接続します。

```
BGP Config> attach policy-to-neighbor
Neighbor address [0.0.0.0]?192.0.190.178
First receive policy list name (none for global AS based policy)[]?S1_100_r
Second receive policy list name (none for exit)[]?
```

update コマンドと **add** コマンドを使用して、近隣の受信ポリシーを追加します。

```
BGP Config>update policy S1_100_r
Policy-list S1_100_r Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Weight [0]? 100
Local-Pref [0]?
IGP-metric [0]? 1
```

AS ベースの送信ポリシーの例

特定の AS へのルート公示を制限する

この例では、BGP スピーカーを制限します。 スピーカーは、アドレス範囲 143.116.0.0 ～ 143.116.255.255 までにあるルート、つまり AS 165 を起点とするルートを自律システム 168 に対して公示できません。

```
BGP Config> add send exclusive
Network Prefix [0.0.0.0]? 143.116.0.0
Network Mask [0.0.0.0]? 255.255.0.0
Address Match (Exact/Range) [Exact]? range
Tag [0]? 165
Adjacent AS# [0]? 168
```

既知のルートをすべて公示する

この例では、BGP スピーカーは、必ず、その IGP を起点とするすべてのルート、ならびにその隣接自律システムから学習されたすべてのルートを公示します。

```
BGP Config> add send policy inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
Adjacent AS# [0]?
```

近隣ベースの送信ポリシーの例

MED 属性値 = 100 を使用して既知のルートすべてを特定の近隣に公示する

この例では、BGP 近隣 192.0.190.178 にすべてのルートを公示できます。公示ルートのすべてで MED 値が 100 になります。

送信ポリシーのポリシー・リスト名を定義します。

```
BGP Config> add policy-list
Name[]?S1_100_s
Policy Type(Receive/Send)[Receive]?Send
```

定義した送信ポリシー・リスト名 (複数の場合もある) を特定の近隣に接続します。

```
BGP Config> attach policy-to-neighbor
Neighbor address [0.0.0.0]?192.0.190.178
First send policy list name (none for global AS based policy)[]?S1_100_s
Second send policy list name (none for exit)[]?
```

update コマンドと **add** コマンドを使用して、近隣の送信ポリシーを追加します。

```
BGP Config>update policy S1_100_s
Policy-list S1_100_s Config>add
Policy type (Inclusive/Exclusive) [Exclusive]?
Network prefix [0.0.0.0]?
Network mask [0.0.0.0]?
Address match (exact/range) [range]?
Originating AS# [0]?
TAG [0]?
MED [0]? 100
# of AS to pad[0]?
```

ルート優先プロセス

BGP スピーカーがそのピアから特定のあて先に関するパスを受信すると、 BGP では、次のプロセスに従って可能な限り最善のパスを選択します。

- 構成に基づいて受信ポリシーを適用する。
- あて先が受信ポリシーによって許可されれば、最短 ASpath 長さと起点タイプに基づいて、受信したあて先の優先度を計算する。
- 同一あて先へのパスが幾つもあるときは、パス選択プロセスを実行する。新規パスと既存の選択済み最善パスを比較して、可能な限り最善のパスを選択します。新規パスが最善パスとして選択されたときは、新規パスを IP 転送テーブルにインストールします。
- 送信ポリシーに応じて、選択した最善パスを外部/内部 BGP ピアに公示する。

パス選択プロセス

最善パスの選択は、次の順序に従って行います。

- このルーターが起点となっているパスを優先する。
- このルーターが起点となっているパスがなければ、構成済み重み値が最も高いパスを優先する。
- 重み値が同じパスであれば、構成済みローカル優先値が最も高いパスを優先する。

- ローカル優先値が同じパスであれば、優先度が最も高いパスを優先する。
  - ASpath 長さが短いパスほど高い優先度が与えられる。
  - ASpath 長さが同じパスであれば、起点タイプが IGP の方が EGP や Incomplete より優先する。
- 優先度が同じパスであれば、MED 属性値が最も低いパスが優先する。
- MED 属性値が同じパスであれば、外部 (EBGP) ルートが内部 (IBGP) ルートより優先する。
- これでもなおパスが同等であるときは、BGP-ID が最も低いパスを優先する。

第19章 BGP4 の構成と監視

この章では、BGP の構成と監視コマンドについて説明し、次の節を含んでいます。

- 『BGP4 構成コマンド』
- 『BGP4 構成環境へのアクセス』
- 423ページの『BGP 監視環境にアクセスする』
- 424ページの『BGP4 監視コマンド』

BGP4 構成環境へのアクセス

BGP 構成環境へアクセスするには、Config> プロンプトで次のコマンドを入力します。

```
Config> Protocol BGP
BGP Config>
```

BGP4 構成コマンド

この節では、BGP 構成コマンドについて説明します。これらのコマンドを使用して、ユーザーの特定の要件に合うように BGP プロトコルの動作を修正できます。完全に機能しうる BGP ルーターを作成するには、ある程度の構成が必要です。BGP 構成コマンドは、BGP config> プロンプトに入力します。

表 23. BGP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	BGP 近隣とポリシーを追加します。
Attach	特定の近隣に受信と送信のポリシー・リストを接続します。
Change	**add** コマンドを用いて当初入力した情報を修正します。
Delete	**add** コマンドを用いて入力されていた BGP 構成情報を削除します。
Disable	**enable** コマンドによってオンにされていた特定の BGP フィーチャーを使用不能にします。
Enable	BGP スピーカーや BGP 近隣や無クラス BGP を使用可能にします。
List	BGP 構成項目を表示します。
Move	ポリシーおよび集合が定義される順序を変更します。
Set	IP-route-table-scan-timer (IP ルート・テーブル・スキャン・タイマー) を設定します。

表 23. BGP 構成コマンドの要約 (続き)

コマンド	機能
Update	サブメニュー **add**、**delete**、**change**、**move** コマンドを使用して、構成済みポリシー・リスト名内のポリシーを操作します。
Exit	直前のコマンド・レベルに戻ります。 xxxiv ページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、構成に BGP 情報を追加するのに使用します。

構文:

add aggregate . . .
neighbor . . .
no-receive asnum . . .
originate-policy . . .
policy-list . . .
receive-policy . . .
send-policy. . .

aggregate *network prefix network mask*

add aggregate コマンドを使用すると、BGP スピーカーは 1 ブロック分のアドレスを統合し、その BGP 近隣に対して単一のルートを公示します。統合されるルートすべてとそのマスクに共通のネットワーク・プレフィックスを指定する必要があります。次の例は、194.10.16.0 から 194.10.31.255 までのアドレスのブロックを統合する方法を示します。

1. *Network Prefix (ネットワーク・プレフィックス)* は、影響を受けるアドレスです。 prefix (プレフィックス) は、BGP ポリシーに指定されたアドレスの範囲内にある最初のアドレスです。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

2. *Network Mask (ネットワーク・マスク)* は、BGP ポリシーで使用されるアドレスを生成するために Network Prefix (ネットワーク・プレフィックス) に指定されたアドレスに適用されます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

例: **add aggregate**

```
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
```

統合定義を追加するときは、必ず、統合されたルートがエクスポートされないようにするポリシーを定義してください。 これを定義しないと、ルーター

は、個々のルートと、ユーザーが定義した集合の両方を公示します。 これは、その IGP ルーティング・テーブルを起点とするルートを統合している場合には適用されません。

neighbor *neighbor IP address as# init timer connect timer hold timer keep alive timer tcp segment size*

add neighbor コマンドは、BGP 近隣を定義するのに使用します。近隣は、BGP スピーカーの AS に対して内部であっても、外部であってもかまいません。この近隣を動的に起動する場合は、 BGP 監視で **reset neighbor** コマンドを使用します。

1. IP アドレスは、ユーザーがピアツーピア通信を行いたい近隣のアドレスです。近隣は、ユーザー自身の自律システム内にあっても、別の自律システム内にあってもかまいません。外部近隣の場合には、両方の BGP スピーカーが同じネットワークを共用する必要があります。内部近隣の場合は、そのような制限はありません。アドレスは、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

2. AS 番号は、内部近隣のユーザー固有の自律システム番号または近隣の自律システム番号です。近隣の AS 番号は、次の値をもちます。

   有効値: 0 〜 65535 の範囲の整数

   省略時値: なし

3. *Init timer* は、スピーカーがエラーにより以前に IDLE (アイドル) 状態に変化していた場合に BGP スピーカーが資源を初期化して、近隣とのトランスポート接続を再開するのに待機する時間の長さを指定します。エラーが続くと、このタイマーは指数関数的に増えます。

   有効値: 0 〜 65535 秒

   省略時値: 12 秒

4. *Connect timer* は、CONNECT (接続) または ACTIVE (能動) 状態のどちらかであるのに TCP 接続に障害が発生した場合に BGP スピーカーがその近隣へのトランスポート接続を再開するのに待機する時間の長さを指定します。しばらくの間、BGP スピーカーは、その近隣によって接続が開始されないか listen を続けます。

   有効値: 0 〜 65535 秒

   省略時値: 120 秒

5. 近隣が到達不能であると想定する前に BGP スピーカーが待機する時間の長さを指定するために、*Hold timer* を入力してください。両方の近隣は、OPEN メッセージで構成済みの情報を交換し、それぞれの折衝された Hold Timer 値として 2 つのタイマーのうち値の小さい方を選びます。

   近隣は BGP 接続を確立すると、頻繁に Keepalive メッセージを交換して、接続がまだ有効で、近隣が到達可能であることを確認します。Keep-Alive タイマー間隔は、折衝された hold timer (保留タイマー) 値の 3 分の 1 になるように計算されます。そのため、hold timer の値は、ゼロか、少なくとも 3 秒のどちらかでなければなりません。

   交換回線では、Keepalive を頻繁に送信せずに帯域幅を保管するためにゼロという Hold Timer 値をもちたい場合があることに注意してください。

有効値: 0 ～ 65535 秒

省略時値: 90 秒

6. *TCP segment size* は、近隣とのTCP 接続で交換される最大データ・サイズを指定します。この値は、近隣との能動 TCP 接続に使用されます。

   有効値: 0 ～ 65535 バイト

   省略時値: 1024 バイト

例: **add neighbor**

```
Neighbor address [0.0.0.0]? 192.0.251.165
AS [0]? 165
Init timer [12]?
Connect timer [120]?
Hold timer [90]?
TCP segment size [1024]?
```

no-receive *asnum*

add no-receive asnum は、AS パス・リストのどこかに特定の AS 番号が入っている場合に AS パスを除外するために使用します。

AS 番号 は、次の値をもちます。

有効値: 0 ～ 65535

省略時値: なし

例: **add no-receive**

```
Enter AS: [0]? 178
```

originate-policy *(exclusive/ inclusive) network prefix network mask address match (Exact/Range) tag*

add originate-policy コマンドは、特定のアドレスまたはある範囲のアドレスを IGP ルーティング・テーブルから BGP スピーカーのルーティング・テーブルへインポートできるかどうかを決定するポリシーを作成するのに使用します。

Exclusive
Exclusive ポリシーは、ルート情報が BGP スピーカーのルーティング・テーブルに組み込まれないようにします。

Inclusive
Inclusive ポリシーは、特定のルートが必ず BGP スピーカーのルーティング・テーブルに組み込まれるようにします。

Network prefix
影響を受けるアドレスのネットワーク・プレフィックス

Address match
ポリシー・ステートメントによって影響されるアドレスまたはアドレスの範囲

Tag 特定の AS について設定されている値。すべてのタグ値は、学習の際に使用された AS のものと突き合わされます。

Exclusive ポリシーは、ルート情報が BGP スピーカーのルーティング・テーブルに組み込まれないようにします。

1. *Network Prefix (ネットワーク・プレフィックス)* は、影響を受けるアドレスです。

有効値: 任意の有効な IP アドレス

省略時値: なし

2. BGP ポリシーで使用されるアドレスを生成するために、Network Prefix に指定されたアドレスに適用される *Network Mask (ネットワーク・マスク)* を入力してください。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

3. *Address match* がアドレスの範囲であるのか、正確なアドレスであるのか選択してください。
4. *TAG* は、特定の AS について設定されている値です。Tag の値は、学習の際に使用された AS のものと突き合わされます。

   有効値: 0 ～ 65535

   省略時値: なし

次の例では、BGP スピーカーの IGP ルーティング・テーブルにある、公示されるすべてのルートが組み込まれます。

例: add originate-policy exclusive

```
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

この policy コマンドの詳細な例については、401ページの『発信ポリシー (Originate Policy) の例』を参照してください。

policy-list

add policy-list コマンドを使用して、ポリシーのグループを作成すると、**attach policy-to-neighbor** コマンドを使用して、特定の近隣に接続できます。

例 : add policy-list

```
Name[]? nbr1-rcv
Policy Type(Receive/Send)[Receive]?Receive
```

例 : add policy-list

```
Name[]? nbr1-snd
Policy Type(Receive/Send)[Receive]?Send
```

注: このポリシー・コマンドの詳しい例については、 403ページの『近隣ベースの受信ポリシーの例』 と 404ページの『近隣ベースの送信ポリシーの例』 を参照してください。

receive-policy *(exclusive/ inclusive) network prefix network mask address match originating as# adjacent as# igpmetric (inclusive only)*

add receive-policy コマンドは、BGP スピーカーのルーティング・テーブルにインポートされるルートを判別するのに使用します。

Exclusive ポリシーは、ルート情報が BGP スピーカーのルーティング・テーブルに組み込まれないようにします。

1. *Network Prefix (ネットワーク・プレフィックス)* は、影響を受けるアドレスです。

有効値: 任意の有効な IP アドレス

省略時値: なし

2. *Network Mask (ネットワーク・マスク)* は、BGP ポリシーで使用されるアドレスを生成するために Network Prefix (ネットワーク・プレフィックス) に指定されたアドレスに適用されます。

   有効値: 任意の有効な IP マスク

   省略時値: なし

3. *Address match* は、アドレスの範囲または正確なアドレスです。
4. *Originating AS#* は、次の値をもちます。

   有効値: 0 〜 65535

   省略時値: なし

5. *Adjacent AS#* は、隣接 AS 番号を指定します。

   有効値: 0 〜 65535

   省略時値: なし

例: **add receive-policy exclusive**

```
Network Prefix [0.0.0.0]? 10.0.0.0
Network Mask [0.0.0.0]?  255.0.0.0
Address Match (Exact/Range) [Exact]? range
Originating AS# [0]? 168
Adjacent AS# [0]? 165
```

この policy コマンドの詳細な例については、402ページの『AS ベースの受信ポリシーの例』を参照してください。

send-policy *(exclusive/ inclusive) network prefix network mask address match tag adjacent as#*

add send-policy コマンドは、再公示する BGP スピーカーの学習済みルートを判別するのに使用します。これらのルートは、BGP スピーカーの AS にとって内部でも外部でもかまいません。

Exclusive ポリシーは、ルート情報が BGP スピーカーのルーティング・テーブルに組み込まれないようにします。

1. *Network Prefix (ネットワーク・プレフィックス)* は、影響を受けるアドレスです。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

2. *Network Mask (ネットワーク・マスク)* は、BGP ポリシーで使用されるアドレスを生成するために Network Prefix (ネットワーク・プレフィックス) に指定されたアドレスに適用されます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

3. *Address match* は、アドレスの範囲または正確なアドレスです。
4. *TAG* は、特定の AS について設定されている値です。Tag の値は、学習の際に使用された AS のものと突き合わされます。

   有効値: 0 〜 65535

   省略時値: なし

5. *Adjacent AS#* は、隣接 AS 番号を指定します。

   有効値: 0 ～ 65535

   省略時値: なし

例: **add send exclusive**

```
Network Prefix [0.0.0.0]? 180.220.0.0
Network Mask [0.0.0.0]? 255.255.0.0
Address Match (Exact/Range) [Exact]? range
Tag [0]?
Adjacent AS# [0]? 25
```

この policy コマンドの詳細な例については、403ページの『AS ベースの送信ポリシーの例』を参照してください。

Attach

構成済みポリシー・リスト名を特定の近隣に接続する場合は、**attach policy-to-neighbor** コマンドを使用します。最大で受信ポリシー・リスト名が 3 つ、送信ポリシー・リスト名が 3 つ接続できます。

構文:

attach policy-to-neighbor

例 : attach policy-to-neighbor

```
Neighbor address [0.0.0.0]? 192.0.251.165
First receive policy list name (none for global AS based policy)[]? nbr1-rcv
Second receive policy list name (none for exit)[]?
First send policy list name (none for global AS based policy)[]? nbr1-snd
Second send policy list name (none for exit)[]?
```

注: このポリシー・コマンドの詳しい例については、 403ページの『近隣ベースの受信ポリシーの例』 と 404ページの『近隣ベースの送信ポリシーの例』 を参照してください。

Change

change コマンドは、add コマンドによって以前にインストールされた BGP 構成項目を変更するのに使用します。

構文:

change aggregate . . .
neighbor . . .
originate-policy . . .
policy-to-neighbor
receive-policy . . .
send-policy. . .

aggregate *index# network prefix network mask*

この例では、現在の集合 (aggregate 1) を変更します。この変更により、

aggregate 1 は、128.185.0.0 ～ 128.185.255.255 のアドレス範囲内のすべてのルートを統合するために、別のネットワーク・プレフィックスとマスクを使用します。

例: **change aggregate 1**

```
Network Prefix [128.185.0.0]? 128.128.0.0
Network Mask [255.255.0.0]? 255.192.0.0
```

neighbor *neighbor IP address as# init timer connect timer hold timer keep alive timer tcp segment size*

次の例では、近隣 192.0.251.165 について hold timer の値をゼロに変更します。

修正される *neighbor address* は、次の値をもちます。

有効値: 任意の有効な IP アドレス

省略時値: なし

この近隣を再起動するために、BGP 監視から **reset neighbor** コマンドを動的に使用してください。

例: **change neighbor 192.0.251.165**

```
AS [165]?
Init timer [12]?
Connect timer [60]?
Hold timer [12]? 0
TCP segment size [1024]?
```

originate-policy *index# (exclusive/ inclusive) network prefix network mask address match tag*

change originate-policy コマンドは、既存の発信ポリシー定義を更新するのに使用します。

この例では、BGP スピーカーの発信ポリシーを更新します。プレフィックス 194.10.16.0 をもつネットワークを IGP ルーティング・テーブルから除外するのではなく、ポリシーには、すべてのルートが組み込まれます。

例: **change originate-policy**

```
Enter index of originate-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [194.10.16.0]? 0.0.0.0
Network Mask [255.255.240.0]? 0.0.0.0
Address Match (Exact/Range) [Range]?
Tag [0]?
```

policy-to-neighbor

特定の近隣へのポリシー・リスト接続を変更する場合は、 **change policy-to-neighbor** コマンドを使用します。

例: **change policy-to-neighbor**

```
Neighbor address [0.0.0.0]? 192.0.251.165
First receive policy list name to be changed[nbr1-rcv]?
Second receive policy list name to be changed[]?
Third receive policy list name to be changed[]?
First send policy list name to be changed[nbr1-snd]?
Second send policy list name to be changed[]?
Third send policy list name to be changed[]?
```

receive-policy *index# (exclusive/inclusive) network prefix network mask address match originating as# adjacent as# igpmetric (inclusive only)*

change receive-policy コマンドは、既存の受信ポリシー定義を更新するのに使用します。

この例では、BGP スピーカーの受信ポリシーに制限を追加します。ルート情報をすべての BGP ピアからインポートしてその IGP ルーティング・テーブルに入れるのではなく、AS 165 からのルートをインポートできないようにします。

例: **change receive-policy**

```
Enter index of receive-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Adjacent AS# [0]? 165
```

send-policy *index# (exclusive/ inclusive) network prefix network mask address match tag adjacent as#*

change send-policy コマンドは、既存の送信ポリシーをより包含的 (inclusive) またはより排他的 (exclusive) なものに更新するのに使用します。

この例では、BGP スピーカーの送信ポリシーに制限を追加します。この制限により、アドレス範囲 194.10.16.0 ～ 194.10.31.255 にあるすべてのルートが、自律システム 165 に対して公示されるときに除外されます。

例: **change send-policy**

```
Enter index of send-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0.0.0.0]? 194.10.16.0
Network Mask [0.0.0.0]? 255.255.240.0
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]? 165
```

Delete

delete コマンドは、**add** コマンドによって以前に導入された BGP 構成項目を削除するのに使用します

構文 :

delete

- aggregate . . .
- neighbor . . .
- no-receive . . .
- originate-policy . . .
- policy-list . . .
- policy-to-neighbor
- receive-policy . . .
- send-policy. . .

aggregate *index#*

削除したい集合のインデックス番号を指定する必要があります。インデックス番号は、AS 番号と同じです。

例: delete aggregate 1

neighbor *neighbor IP address*

このコマンドは、BGP 近隣を削除するのに使用します。近隣のネットワーク・アドレスを指定する必要があります。

削除される近隣のネットワーク・アドレス は、次の値をもちます。

有効値: 任意の有効な IP アドレス

省略時値: なし

この近隣を非活動化するために、BGP 監視から **reset neighbor** コマンドを動的に使用してください。

例: delete neighbor 192.0.251.165

no-receive *as*

このコマンドは、特定の AS について設定された非受信ポリシーを削除するのに使用します。AS 番号を指定する必要があります。

AS 番号 は、次の値をもちます。

有効値: 0 ～ 65535

省略時値: なし

例: delete no-receive 168

originate-policy *index#*

特定の開始方針を削除するには、このコマンドを使用します。ポリシーと関連付けられたインデックス番号を指定する必要があります。

例: delete originate-policy 2

policy-list

ポリシー・リストを削除する場合は、**delete policy-list** コマンドを使用します。

例 : delete policy-list

```
Name of policy-list to delete []? nbr1-rcv
All policies defined for 'nbr1-rcv' will be deleted.
Are you sure you want to delete (Yes or [No]? Yes
Policy-list 'nbr1-rcv' is deleted.
```

ポリシーと近隣の接続は、これに応じて調整されます。

policy-to-neighbor

特定の近隣への既存のポリシー・リスト名接続を削除する場合は、 **delete policy-to-neighbor** コマンドを使用します。

例 : delete policy-to-neighbor

```
Neighbor address [192.0.251.165]?
Remove first receive policy-list name [nbr1-rcv]
Are you sure you want to remove (Yes or [No])? yes
Remove first send policy-list name [nbr1-snd]
Are you sure you want to remove (Yes or [No])? yes
```

receive-policy *index#*

このコマンドは、特定の受信ポリシーを削除するのに使用します。ポリシーと関連付けられたインデックス番号を指定する必要があります。

例: delete receive-policy

```
Enter index of receive-policy to be deleted [1]?
```

send-policy *index#*

このコマンドは、特定の送信方針を削除するのに使用します。ポリシーと関連付けられたインデックス番号を指定する必要があります。

例: delete send-policy 4

Disable

disable コマンドは、以前に使用可能にされた BGP 近隣またはスピーカーを使用不能にするのに使用します。近隣は、**add** コマンドを使用して追加された場合には必ず、暗黙的に使用可能にされることに注意してください。

構文:

disable BGP speaker
classless-bgp
compare-med-from-diff-AS
neighbor . . .

bgp speaker

BGP プロトコルを使用不可にする場合は、**disable bgp speaker** コマンドを使用します。

例: disable bgp speaker

classless-bgp

公示のために無クラス・ルートを使用不可にする場合は、このコマンドを使用します。

例 : disable classless-bgp

注: patch bgp-subnets コマンドは、必ず使用不可にしておきます。

compare-med-from-diff-AS

異なる AS 間の MED 比較を使用不可にする場合は、このコマンドを使用します。

例 : disable compare-med-from-diff-AS

neighbor *neighbor IP address*

近隣アドレス は、次の値をもちます。

有効値: 任意の有効な IP アドレス

省略時値: なし

例: disable neighbor 192.0.190.178

Enable

enable コマンドは、BGP フィーチャー、機能、および BGP 構成に追加される情報を活動化するのに使用します。

構文:

enable BGP speaker

classless-bgp

compare-med-from-diff-AS

neighbor . . .

bgp speaker *as# tcp segment size*

enable bgp speaker コマンドは、BGP プロトコルを使用可能にするのに使用します。

注: IBM では、BGP の最新バージョン、BGP4 のみをサポートします。これは、RFC 1654 で定義されています。

1. *AS 番号* は、このルーターとノードの集合と関連付けられています。

   有効値: 0 〜 65535

   省略時値: なし

2. BGP が受動 TCP 接続に対して使用すべき最大セグメント・サイズを指定するために、*TCP segment size* を入力してください。

   有効値: 0 〜 65535 バイト

   省略時値: 1024 バイト

例:

```
enable bgp speaker

AS [0]? 165
TCP segment size [1024]?
```

classless-bgp neighbor

公示のために無クラス・ルートを使用可能にする場合は、このコマンドを使用します。

例 : enable classless-bgp

compare-med-from-diff-AS

異なる AS 間の MED 比較を使用可能にする場合は、このコマンドを使用します。

例 : enable compare-med-from-diff-AS

neighbor *neighbor IP address*

このコマンドは、BGP 近隣を使用可能にするのに使用します。

近隣アドレス は、次の値をもちます。

有効値: 任意の有効な IP アドレス

省略時値: なし

例: enable neighbor 192.0.190.178

List

list コマンドは、呼び出された特定のサブコマンドに応じて、BGP 構成データのさまざまな部分を表示するのに使用します。

構文:

list aggregate

all

BGP speaker

neighbor

no-receive

originate-policy

policy-list . . .

policy-to-neighbor

receive-policy

send-policy

aggregate

list aggregate コマンドは、**add aggregate** コマンドを用いて定義したすべての集約されたルートをリストするのに使用します。

例: `list aggregate`

```
Aggregation:
Index  Prefix            Mask
1      194.10.16.0       255.255.240.0
```

all **list all** コマンドは、現行の BGP 構成内の BGP 近隣、ポリシー、統合されたルート、および no-receive-as レコードをリストするのに使用します。

例: `list all`

```
BGP Protocol:          Enabled
                  AS:                    167
TCP-Segment Size:      1024
Neighbors and their AS:

                                      Init    Conn    Hold    TCPSEG
Address            State     AS       Timer   Timer   Timer   Size
128.185.250.168    ENABLD    168      12      60      12      1024
192.0.251.165      ENABLD    165      12      60      12      1024

Receive-Policies:
Index  Type  Prefix      Mask        Match  OrgAS  AdjAS  IGPmetric
1      INCL  0.0.0.0      0.0.0.0   Range  0      0      0

Send-Policies:
Index  Type  Prefix      Mask           Match Tag    AdjAS
1      INCL  0.0.0.0      0.0.0.0   Range  0      0

Originate-Policies:
Index  Type  Prefix           Mask             Match  Tag
1      EXCL  194.10.16.0      255.255.240.0    Range  0

Aggregation:

Index  Prefix            Mask
1      194.10.16.0       255.255.240.0
No no-receive-AS records in configuration.
```

bgp speaker

list bgp speaker コマンドは、BGP スピーカーに関する情報を引き出すのに使用します。与えられる情報は、次のとおりです。

例: `list BGP speaker`

```
BGP Protocol:          Enabled
AS:                    165
TCP-Segment Size:      1024
```

neighbor

list neighbor コマンドは、BGP 近隣に関する情報を引き出すのに使用します。

例: `list neighbor`

```
Neighbors and their AS:

                                        Init    Conn    Hold    TCPSEG
Address            State     AS         Timer   Timer   Timer   Size

128.185.252.168    ENABLD    168        12      60      12      1024
192.0.190.178      DISBLD    178        12      60      12      1024
192.0.251.167      ENABLD    167        12      60      12      1024
```

no-receive

list no-receive コマンドは、BGP 構成に追加されている no-receive-AS 定義を引き出すのに使用します。

例: list no-receive

```
AS-PATH with following autonomous systems will be discarded:
AS  178
AS  165
```

originate-policy *all index prefix*

list originate-policy コマンドは、BGP 構成に追加されている発信ポリシーに関する情報を引き出すのに使用します。

例: list originate-policy

```
Originate-Policies:
Index  Type  Prefix          Mask            Match  Tag
1      EXCL  194.10.16.0     255.255.240.0   Range  0
2      INCL  0.0.0.0         0.0.0.0         Range  0
```

policy-list

構成済みポリシー・リスト名の一覧表を表示させる場合は、 **list policy-list** コマンドを使用します。

例 : list policy-list

```
BGP Config>li policy list
Policy list:
nbr1-rcv  Receive
nbr1-snd  Send
```

policy-to-neighbor

近隣に接続されているポリシーの一覧表を表示させる場合は、 **list policy-to-neighbor** コマンドを使用します。

例 : list policy-to-neighbor

```
Neighbor addrs  receive         send
192.0.251.165   nbr1-rcv        nbr1-snd
```

receive-policy adj-as-number *all* **or** *index* **or** *prefix*

list receive-policy コマンドは、BGP 構成に追加されている受信ポリシーに関する情報を引き出すのに使用します。 AS について定義されているすべての受信ポリシーを表示したり、インデックスまたはプレフィックス番号別にポリシーを表示したりできます。

例: list receive-policy

```
Receive-Policies:
Index  Type  Prefix      Mask        Match  OrgAS  AdjAS  IGPmetric
1      EXCL  0.0.0.0     0.0.0.0     Range  178    165
2      INCL  0.0.0.0     0.0.0.0     Range  0      0      0
```

send-policy adj-as-number *all* **or** *index* **or** *prefix*

list send-policy コマンドは、指定された自律システムについて定義された送信ポリシーに関する情報を表示するのに使用します。AS について定義されているすべての送信ポリシーを表示したり、インデックスまたはプレフィックス番号別にポリシーを表示したりできます。

例: list send-policy

```
Send-Policies:
Index  Type  Prefix      Mask           Match Tag    AdjAS
1      EXCL  194.10.16.0 255.255.240.0  Range   0    165
2      INCL   0.0.0.0          0.0.0.0  Range   0    0
```

Move

move コマンドは、ポリシーおよび集合が定義された順序を変更するのに使用します。これにより、ルーターが既存のポリシーをルート情報に適用する順序が変更されます。このコマンドを使用する前に、**list** コマンドを使用して、どのようなポリシーが定義されているのか確認してください。

構文 :

move *aggregate* or *originate-policy* or *receive-policy* or *send-policy*

例 :

```
move originate-policy
Enter index of originate-policy to move [1]? 3
Move record AFTER record number [0]?
```

Set

IP ルート・テーブル・スキャン・タイマーを設定する場合は、 **set** コマンドを使用します。 IP ルート・テーブル・スキャン・タイマーは、BGP 更新の IP 転送テーブル・スキャン時間を設定する場合に使用します。

構文 :

set ip-route-table-scan-timer

例 :

```
set ip-route-table-scan-timer
```

Update

ポリシーを操作する場合は、**update** コマンドとサブコマンドを使用します。

構文 :

update *policy-list*

受信ポリシーの例 :

```
update policy-list
Name[]? nbr1-rcv
```

Add

update コマンド内で受信ポリシーを追加する場合は、 **Add** コマンドを使用します。

```
BGP nbr1-rcv: Receive Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
```

```
MED [0]?
Weight [0]?
Local-Pref [0]?
IGP-metric [0]?
```

注: exclusive (除外) 受信ポリシーの場合は、MED、ローカル優先、重み、 IGP メトリックのパラメーターの入力を指示するプロンプトは出ません。MED とローカル優先の値が受信公示から使用されるのは、値 '0' として構成されている場合です。重みパラメーターの値が '0' では、ルート選択プロセスで重みの値の無視を指示します。

Change

update コマンド内でポリシーを変更する場合は、 **Change** コマンドを使用します。

例 :

```
Enter index of receive-policy to be modified [1]?
```

Delete

update コマンド内でポリシーを削除する場合は、 **delete** コマンドを使用します。

例 :

```
Enter index of receive-policy to be deleted [1]?
```

Move

update コマンド内でポリシーを移動する場合は、 **Move** コマンドを使用します。

例 :

```
Enter index of receive-policy to move [1]?
Move record after record number [0]?
```

List

update コマンド内で受信ポリシーの一覧表を表示させる場合は、**list policy-list** コマンドを使用します。

例 : list policy-list

```
Receive policy list for 'name':
                  T Prefix            Match OrgAS AnyAS MED   Weight Lpref IGPmetric
               1  I 0.0.0.0/0         Range 0     0     0     0      0     1
```

送信ポリシーの例 :

```
update policy-list
Name[]? nbr1-rcv
```

Add

update コマンド内で送信ポリシーを追加する場合は、 **Add** コマンドを使用します。

```
BGP nbr1-rcv: Send Config>add
Policy type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
```

```
Any AS# [0]?
TAG [0]
MED [0]?
# of AS to pad[0]?
```

注: exclusive (除外) 送信ポリシーの場合は、MED と ASpad のパラメーターの入力を指示するプロンプトは出ません。MED パラメーターの値が 0 では、MED 属性が公示に組み込まれないことを示します。ASpad パラメーターの値が 0 では、ASpath に追加のローカル AS 番号が挿入されないことを示します。

Change

update コマンド内でポリシーを変更する場合は、 **Change** コマンドを使用します。

例 :

```
Enter index of send-policy to be modified [1]?
```

Delete

update コマンド内でポリシーを削除する場合は、 **delete** コマンドを使用します。

例 :

```
Enter index of send-policy to be deleted [1]?
```

Move

update コマンド内でポリシーを移動する場合は、 **Move** コマンドを使用します。

例 :

```
Enter index of send-policy to move [1]?
Move record after record number [0]?
```

List

update コマンド内で送信ポリシーの一覧表を表示させる場合は、**list policy-list** コマンドを使用します。

例 : list policy-list

```
Send policy list for 'name':
                    T Prefix            Match OrgAS AnyAS Tag   MED    ASpad
                1   I 0.0.0.0/0         Range 0     0     0     0      0
```

BGP 監視環境にアクセスする

BGP 構成環境へアクセスするには、Config> プロンプトで次のコマンドを入力します。

```
Config> Protocol BGP
BGP>
```

BGP4 監視コマンド

この節では、BGP 監視コマンドについて説明します。これらのコマンドを使用して、ユーザーの特定の要件に合うように BGP プロトコルの動作を修正できます。完全に機能しうる BGP ルーターを作成するには、ある程度の構成が必要です。BGP 構成コマンドは、BGP> 監視プロンプトに入力します。

表 24. BGP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Destinations	BGP ルーティング・テーブル内のすべての記入項目を表示します。
Disable neighbor	特定の近隣またはすべての近隣を使用不能にします。
Dump routing tables	IP ルーティング・テーブルの内容をリストします。
Enable neighbor	特定の近隣またはすべての近隣を使用可能にします。
Neighbors	現在能動的な近隣を表示します。
Parameter	BGP システム内のインストール済み BGP グローバルを表示します。
Paths	データベース内のすべての使用可能なパスを表示します。
Ping	ICMP エコー要求を別のホストに 1 秒間に 1 回送信し、応答を待ちます。このコマンドを使用して、インターネットワーク環境での問題を分離できます。
Policy-list	特定の近隣に関する現行インストール済みポリシーと各ポリシーの使用統計を表示します。
Reset neighbor	特定の近隣をリセットします。
Traceroute	特定のあて先への完全なパス (通過する全ホップ) を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Destinations

destinations コマンドは、すべての BGP ルーティング・テーブル項目のダンプをとったり、指定された BGP 近隣アドレス (あて先) に対して公示されたり、あるいはそこから受信されるルートに関する情報を表示したりするのに使用します。

構文:

destinations

net address/net address net mask

advertised-to *network address*

received-from *network address*

例 : destination

```
Network/MaskLen    NextHop         MED   Weight LPref AAG AGRAS ORG AS-Path
142.4.0.0/16       192.0.251.165   100   0      0     No  0     IGP seq[165-178]
```

destinations *net address*

指定されたルートまたはあて先ネットワークに関する詳細情報を表示しま

す。このコマンドは、特定のルートがどのように学習されたか、特定のあて先までの最良のパス、ルートと関連付けられたメトリック、およびその他の情報を示します。

例: destinations 142.4.0.0

```
Network/MaskLen   NextHop        MED  Weight LPref     AAG AGRAS ORG ASPath
142.4.0.0/16      192.0.251.165  100  0      0         No  0     IGP seq[165-178]

Dest:142.4.0.0/16, Age:180, Upd#:13,LastSent:0001:53:32

Eligible paths: 2
PathID: 8  (Best Path)
        ASpath: seq[165-178]
        Origin: IGP, Pref: 507, LocalPref: 0
        Metric: 0, Weight: 0, MED: 100
        NextHop: 192.0.251.165, Neighbor: 192.0.251.165
        AtomicAggr: No

PathID: 21
        ASpath: seq[168-165-178]
        Origin: IGP, Pref: 505, LocalPref: 0
        Metric: 0, Weight: 0, MED: 0
        NextHop: 128.185.250.168, Neighbor: 128.185.250.168
        AtomicAggr: No
```

ASpath
パス沿いの自律システムの列挙

-seq: パス内の順に並んだ一連の自律システム

-set: パス内の自律システムの集合

Origin あて先の発信元。これは、EGP、IGP、または Incomplete (未知の、他のなんらかの方法で発信されたもの) です。

LocalPref
あて先についての、発信元ルーターの優先度

Metric ルートがインポートされるときのパス・メトリック

Weight
パスの重み

MED 複数出口判別プログラムの値。同じ AS までの複数の入り口/出口点のなかから判別するのに使用されます。

NextHop
与えられたパスを介して到達可能なあて先の転送アドレスとして使用されるルーターのアドレス

AtomicAggr
パスを公示するルーターが原子集合体にパスを組み込んだかどうかを指示します。

destinations *net address net mask*

指定されたルートまたはあて先ネットワークに関する詳細情報を表示します。このコマンドは、特定のルートがどのように学習されたか、特定のあて先までの最良のパス、ルートと関連付けられたメトリック、およびその他の情報を示します。

このコマンドが有用なのは、複数のネットワーク・アドレスが同じ接頭部と異なるマスクをもつ場合です。そのような場合、ネットワーク・マスクを指定すると、提示される情報の範囲が狭くなります。

例: destinations 194.10.16.0 255.255.240.0

```
Dest:194.10.16.0/21, Age:0, Upd#:3, LastSent:0002:00:00

Eligible paths: 1
PathID: 0 - (Best Path)
        ASpath:
        Origin: IGP, Pref: 0, LocalPref: 0
        Metric: 0, Weight: 0, MED: 0
        NextHop: 194.10.16.167, Neighbor: 194.10.16.167
        AtomicAggr: No, Aggregator AS167/194.10.16.167
```

destinations advertised-to *net address*

指定された BGP 近隣に対して公示されるすべてのルートをリストします。

例: destinations advertised-to

```
BGP neighbor address [0.0.0.0]? 192.0.251.165

        Destinations advertised to BGP neighbor 192.0.251.165

Network             NextHop         MED Weight  LPref      AAG AGRAS ORG ASPath
194.10.16.0/20  194.10.16.167   0    0       0          No  167   IGP
192.0.190.0/24  192.0.251.165   0    0       0          No  0     IGP seq [165]
142.4.0.0/16    192.0.251.165   0    0       0          No  0     IGP seq [165-178]
143.116.0.0/16  128.185.250.168 0    0       0          No  0     IGP seq [168]
```

destinations received-from *net address*

指定された BGP 近隣から受信されたすべてのルートをリストします。

例: destinations received-from

```
BGP neighbor address [0.0.0.0]? 128.185.250.167

        Destinations obtained from BGP neighbor 128.185.250.167

Network             NextHop         MED Weight  LPref      AAG AGRAS ORG ASPath
194.10.16.0/20      128.185.250.167 0   0       0          No  167   IGP seq[167]
192.0.190.0/24      128.185.250.167 0   0       0          No  0     IGP seq[167-165]
142.4.0.0/16        128.185.250.167 0   0       0          No  0     IGP seq[167-165-178]
```

Disable Neighbor

disable neighbor コマンドは、使用可能にされている特定の近隣またはすべての近隣を使用不能にするのに使用します。このコマンドを使用すると、BGP セッションはダウンされ、その近隣から学習されたルートは削除されます。

構文:

disable neighbor *internet address*

例 : **disable neighbor**

```
Neighbor address (255.255.255.255 for all) [0.0.0.0]? 128.185.250.167
```

Dump Routing Tables

dump routing tables コマンドの詳しい説明については、 *プロトコルの構成と監視解説書 第 1 巻* の「IP の監視」の章の「ルーティング・テーブルのダンプ」の項を参照してください。

Enable Neighbor

enable neighbor コマンドは、使用不能にされている特定の近隣またはすべての近隣を使用可能にするのに使用します。このコマンドにより、近隣との BGP セッションが開始されます。

構文:

enable neighbor *internet address*

例:

```
Neighbor address (255.255.255.255 for all) [0.0.0.0]? 128.185.250.167
```

Neighbors

neighbors コマンドは、すべての能動 BGP 近隣に関する情報を表示するのに使用します。

構文 :

neighbors *internet address*

例: **neighbors**

```
IP-Address       Status   State        DAY-HH:MM:SS  BGPID           AS     Upd#

128.185.252.168  ENABLD  Established  00000:48:52  128.185.142.168  168     16
192.0.190.178    ENABLD  Established  00002:01:49  142.4.140.178    178     16
192.0.251.167    DISBLD  Established  00002:01:45  194.10.16.167    167     16
```

IP-Address

BGP 近隣の IP アドレスを指定します。

State 接続の状態を指定します。考えられる状態は、次のものです。

Connect

近隣への TCP 接続が完了するのを待機します。

Active TCP 接続が不良になると、状態は Active に変わり、近隣を獲得する試みは続行します。

OpenSent

この状態では、OPEN がすでに送信されているため、BGP は、近隣からの OPEN メッセージを待機します。

OpenConfirm

この状態では、近隣の OPEN に応答して KEEPALIVE がすでに送信されているため、近隣からの KEEPALIVE/NOTIFICATION を待機します。

Established

BGP 接続が正常に確立されているため、いますぐ、UPDATE メッセージの交換を開始できます。

BGP-ID

近隣の BGP 識別番号を指定します。

AS 近隣の AS 番号を指定します。

Upd# 近隣に最後に送信された UPDATE メッセージの順序番号を指定します。

internet-address

neighbor コマンドを使用して、特定の BGP 近隣で詳細データを表示してください。

例: neighbor 192.0.251.167

```
  Active Conn: Sprt:1026  Dprt:179    State: Established KeepAlive/Hold
  Time: 4/12
  Passve Conn: None
```

```
TCP connection errors: 0          TCP state transitions: 0

BGP Messages:     Sent       Received                    Sent
Received
Open:             1          1          Update:          11         11
Notification:     0          0          KeepAlive:       1828       1830
Total Messages:   1840       1842

Msg Header Errs:  Sent       Received                    Sent
Received
Conn sync err:    0          0          Bad msg length:  0          0
Bad msg type:     0          0

Open Msg Errs:    Sent       Received                    Sent
Received
Unsupp versions:  0          0          Unsupp auth code: 0         0
Bad peer AS ident:0          0          Auth failure:    0          0
Bad BGP ident:    0          0          Bad hold time:   0          0

Update Msg Errs:  Sent       Received                    Sent
Received
Bad attr list:    0          0          AS routing loop: 0          0
Bad wlkn attr:    0          0          Bad NEXT_HOP atr: 0         0
Mssng wlkn attr:  0          0          Optional atr err: 0         0
Attr flags err:   0          0          Bad netwrk field: 0         0
Attr length err:  0          0          Bad AS_PATH attr: 0         0
Bad ORIGIN attr:  0          0

Total Errors:     Sent       Received                    Sent
Received
Msg Header Errs:  0          0          Hold Timer Exprd: 0         0
Open Msg Errs:    0          0          FSM Errs:        0          0
Update Msg Errs:  0          0          Cease:           0          0
```

Parameter

BGP システム内のインストール済み BGP グローバルを表示させる場合は、 BGP **parameter** コマンドを使用します。

構文 :

parameter

例 :

```
BGP> parameter

classless-bgp is enabled.
compare-med-from-diff-as is enabled.
IP-route-table-scan-timer value is 5 seconds.
```

Paths

paths コマンドは、パス記述データベースに保管されたパスを表示するのに使用します。

構文 :

paths

例 :

```
paths
PathId   NextHop   MED  AAG   AGRAS  RefCnt   ORG   ASPath
0        10.2.0.3    0   No     0      2      IGP
4        192.2.0.2   0   No     0      2      IGP    seq[2]
5        192.2.0.2   0   No     2      1      IGP    seq[2]
6        192.2.0.2   0   No     0      1      IGP    seq[2-1]
7        10.2.0.168  0   No     0      4      IGP
8        192.3.0.1   0   No     0      2      IGP    seq[1]
9        192.2.0.2   0   No     2      1      IGP    seq[2]
10       10.2.0.3    0   No     0      1      IGP
```

PathId
パス識別子

NextHop
与えられたパスを介して到達可能なあて先の転送アドレスとして使用されるルーターのアドレス

MED 同じ AS までの複数の入り口/出口点のなかから判別するのに使用される複数出口判別プログラム

AAG パスが原子集合状態になっているかどうか、すなわち、重なり合うルートと一緒に示された場合に、与えられたパスを公示しているルーターが、特異性の高い方のルートよりも特性の低い方のルートを選択したかどうかを指示します。

AGRAS
ルートを統合した BGP スピーカーの AS 番号を指示します。

RefCnt
記述子を参照するパス・エンティティーの数を示します。

ORG 与えられたパス内の公示されたあて先の発信元、つまり、EGP、IGP、または Incomplete (未知の、他のなんらかの方法で発信されたもの) を指定します。

AS Path
パス沿いの自律システムの列挙

seq: パス内の順に並んだ一連の自律システム

set: パス内の自律システムの集合

Ping

ping コマンドの詳しい説明については、 *プロトコルの構成と監視 解説書 第 1 巻* の「IP の監視」の章の IP Ping コマンド の項を参照してください。

Policy-List

特定の近隣に関する現行インストール済みポリシーと各ポリシーの使用統計を表示させる場合は、**policy-list** コマンドを使用します。

例 : policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Receive
```

近隣ベースのポリシー構成に関する表示 :

```
Receive policy list for neighbor '192.0.251.167':
Idx T Prefix             Match OrgAS AnyAS MED   Weight LPref IGPmet Usage
1   I 0.0.0.0/0          Range 0     0     0     0      0     1      1
```

AS ベースのポリシー構成に関する表示 :

```
Receive policy :
Idx Type  Prefix            Match OrgAS AdjAS IGPmetric Usage
1   INCL  0.0.0.0/0         Range 0     0     1         1
```

例 : policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Send
```

近隣ベースのポリシー構成に関する表示 :

```
send policy list for neighbor '0.0.0.0': 192.0.251.167
Idx T Prefix             Match OrgAS AnyAS TAG   MED   ASpad Usage
1   I 0.0.0.0/0          Range 0     0     0     0     0     1
```

AS ベースのポリシー構成に関する表示 :

```
send policy :
Idx Type  Prefix             Match OrgAS AdjAS TAG   Usage
1   INCL  0.0.0.0/0          Range 0     0     0     1
```

例 : policy-list

```
Neighbor address[0.0.0.0]? 192.0.251.167
Policy Type(Receive/Send/Origin)[All]?Origin

Origin policy list for neighbor '0.0.0.0':
Idx T Prefix             Match TAG   Usage
1   I 0.0.0.0/0          Range 0     1
```

Reset Neighbor

reset neighbor コマンドは、構成メモリー内に保管されている近隣構成パラメーターに基づいて指定の BGP 近隣をリセットするのに使用します。

構文:

reset neighbor *internet address*

例 : reset neighbor

```
Neighbor address[0.0.0.0]? 128.185.250.167
```

Sizes

BGP **sizes** コマンドは、各種のデータベースに保管されている記入項目の数を表示するのに使用します。

構文 :

sizes

例: sizes

```
# Paths:                                11
# Path descriptors:                      7
  Update sequence#:                     22
# Routing tbl entries (allocated):       6
# Current tbl entries (not imported):    0
# Current tbl entries (imported to IGP): 3
```

Paths BGP ルーティング・テーブル内のすべてのルートについての適格なパスの総数

Path descriptors
共通パス情報を保持するために使用されるデータベース内のパス記述子の総数

Update sequence#
現在の更新順序番号を指示します。

Routing tbl entries (allocated)
BGP ルーティング・テーブル内の記入項目の数を示します。

Current tbl entries (not imported)
IGP にインポートされていない BGP ルートの数を示します。

Current tbl entries(imported to IGP)
IGP にインポートされる BGP ルートの数を示します。

Traceroute

traceroute コマンドの詳しい説明については、 265ページの『第15章 IP の構成と監視』 を参照してください。

第20章 DVMRP の構成と監視

この章では、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) プロトコル活動に関する構成と監視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。

- 『DVMRP 構成環境にアクセスする』
- 『DVMRP 構成コマンド』
- 438ページの『DVMRP 監視コマンド』

DVMRP 構成環境にアクセスする

DVMRP 構成環境にアクセスする場合は、Config> プロンプトで次のようにコマンドを入力します。

```
Config> protocol dvmrp
Distance Vector Multicast Routing Protocol config monitoring
DVMRP Config>
```

DVMRP 構成コマンド

この節では、DVMRP 構成コマンドについて説明します。コマンドは、 DVMRP Config> プロンプトで入力します。

表 25. DVMRP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	既存の DVMRP 情報に追加します。物理インターフェースや IP-IP トンネル・インターフェースが追加できます。
Change	SRAM 内の DVMRP 情報を変更します。物理インターフェース、IP-IP トンネル、MOSPF インターフェースのコストやしきい値、または IP-IP トンネルのエンドポイントを変更します。
Delete	静的構成から DVMRP 情報を削除します。
Disable	DVMRP プロトコル全体や MOSPF インターフェースを使用不可にします。
Enable	DVMRP プロトコル全体や MOSPF インターフェースを使用可能にします。
List	DVMRP 構成を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

既存の DVMRP 情報に追加する場合は、**add** コマンドを使用します。物理インターフェースや IP-IP トンネルが追加できます。

構文 :

add interface *ip-address cost threshold*

tunnel *tunnel-source tunnel-destination cost threshold*

interface

DVMRP インターフェースが追加または更新されます。

ip-address

DVMRP インターフェースの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

省略時値: なし

cost インターフェースの使用に関して発生するコスト (ホップ・カウント数) を指定します。

有効値: 0 より大きい整数

省略時値: 1

threshold

インターフェース上で最も近い近隣に到達する場合に必要な活動時間を指定します。

有効値: 0 より大きい整数

省略時値: 1

tunnel 非マルチキャスト・ネットワークをまたがる IP-IP トンネルを追加または更新します。トンネルを構成する必要があるのは、マルチキャスト・データグラムをサポートしないか、マルチキャスト・ルーティング・プロトコルが稼働していないネットワークを、マルチキャスト・トラフィックが通過する必要がある場合です。

source-address

トンネル発信元の 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

省略時値: なし

destination-address

トンネルあて先の 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

省略時値: なし

cost トンネルの使用に関して発生するコスト (ホップ・カウント数) を指定します。

有効値: 0 より大きい整数

省略時値: 1

threshold

インターフェース上で最も近い近隣に到達する場合に必要な活動時間を指定します。

有効値: 0 より大きい整数

省略時値: 1

Change

既存の DVMRP 情報を変更する場合は、**change** コマンドを使用します。物理インターフェースや IP-IP トンネルや MOSPF インターフェースのコストやしきい値の値が変更できます。

構文 :

change interface *ip-address cost threshold*

tunnel *tunnel-source tunnel-destination cost threshold*

mospf *cost threshold*

interface

DVMRP インターフェースを変更します。

ip-address

有効値: 任意の有効な IP アドレス

省略時値: なし

cost インターフェースの使用に関して発生するコスト (ホップ・カウント数) を指定します。

有効値: 0 より大きい整数

省略時値: 1

threshold

インターフェース上で最も近い近隣に到達する場合に必要な活動時間を指定します。

有効値: 0 より大きい整数

省略時値: 1

tunnel IP-IP トンネルを変更します。

source-address

有効値: 任意の有効な IP アドレス

省略時値: なし

destination-address

有効値: 任意の有効な IP アドレス

省略時値: なし

cost インターフェースの使用に関して発生するコスト (ホップ・カウント数) を指定します。

有効値: 0 より大きい整数

省略時値: 1

threshold

インターフェース上で最も近い近隣に到達する場合に必要な活動時間を指定します。

有効値: 0 より大きい整数

省略時値: 1

mospf MOSPF インターフェースを変更します。

cost インターフェースの使用に関して発生するコスト (ホップ・カウント数) を指定します。

有効値: 0 より大きい整数

省略時値: 1

threshold
インターフェース上で最も近い近隣に到達する場合に必要な活動時間を指定します。

有効値: 0 より大きい整数

省略時値: 1

Delete

静的メモリーから既存の DVMRP 情報を除去する場合は、 **delete** コマンドを使用します。

構文 :

delete interface *ip-address*

tunnel *tunnel-source tunnel-destination*

interface
DVMRP インターフェースを削除します。

ip-address

有効値: 任意の有効な IP アドレス

省略時値: なし

tunnel IP-IP トンネルを削除します。

source-address

有効値: 任意の有効な IP アドレス

省略時値: なし

destination-address

有効値: 任意の有効な IP アドレス

省略時値: なし

Disable

DVMRP プロトコル全体や MOSPF インターフェースを使用不可にする場合は、 **disable** コマンドを使用します。

構文 :

disable dvmrp

mospf

dvmrp
DVMRP プロトコルを使用不可にします。使用不可にすると、装置は DVMRP マルチキャスト・ルーターとして参加しません。

mospf MOSPF ルーティング・プロトコルとのインターフェースを使用不可にします。使用不可にすると、DVMRP プロトコルは、 MOSPF ルーティング・プロトコルとの間でマルチキャスト・データグラムの送受を行いません。

Enable

DVMRP プロトコル全体や MOSPF インターフェースを使用可能にする場合は、**enable** コマンドを使用します。

構文 :

enable dvmrp

mospf *cost threshold*

dvmrp
DVMRP プロトコルを使用可能にします。IP 用として構成され、MOSPF が使用可能にされていないインターフェースすべてと、MOSPF インターフェースが使用可能になります。

mospf DVMRP 用の MOSPF ルーティング・プロトコルとのインターフェースを使用可能にします。このインターフェースによって、 DVMRP は MOSPF ルーティング・プロトコルにマルチキャスト・データグラムを転送できます。このインターフェースは、物理インターフェースとして扱われます。

cost インターフェースの使用に関して発生するコスト (ホップ・カウント数) を指定します。

有効値: 0 より大きい整数

省略時値: 1

threshold
インターフェース上で最も近い近隣に到達する場合に必要な活動時間を指定します。

有効値: 0 より大きい整数

省略時値: 1

List

現行 DVMRP 構成を表示させる場合は、**list** コマンドを使用します。コマンドの出力として、現在の DVMRP の状態 (使用不可か使用可能)、物理インターフェース構成情報、トンネル構成情報、 MOSPF 構成情報が表示されます。

構文 :

list

例 :

DVMRP 構成コマンド (Talk 6)

```
DVMRP config> list

          DVMRP on
          phyint 128.185.138.19 1 1
          phyint 128.185.177.19 2 4
          tunnel 128.185.138.19 128.185.138.21 4 4
```

それぞれのインターフェースについて、次のような情報が表示されます。

DVMRP protocol
DVMRP が使用可能と使用不可のどちらになっているか表示します。

DVMRP physical interfaces
それぞれの物理インターフェースごとに、その IP アドレス、コストとしきい値の値が表示されます。

DVMRP tunnel interfaces
それぞれのトンネル・インターフェースごとに、構成済みのトンネル・エンドポイント、コスト、しきい値が表示されます。

DVMRP MOSPF interface
MOSPF インターフェースについて、コストとしきい値が表示されます。

DVMRP 監視コマンド

DVMRP 監視コマンドを使用すると、DVMRP が使用可能になっているネットワークのパラメーターと統計を表示させて見ることができます。

DVMRP 監視コマンドは、**DVMRP>** プロンプトで入力します。

表 26. DVMRP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Dump routing tables	ルーティング・テーブルに入っている DVMRP ルートを表示します。
Interface summary	DVMRP インターフェースの統計とパラメーターを表示します。
Join	ルーターを 1 つまたは複数のマルチキャスト・グループに属するように構成します。
Leave	マルチキャスト・グループ内のメンバーシップからルーターを除去します。
Mcache	現在アクティブなマルチキャスト転送キャッシュ項目のリストを表示します。
Mgroups	ルーターの接続されたインターフェースのグループ・メンバーシップを表示します。
Mstats	さまざまなマルチキャスト・ルーティング統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Dump Routing Tables

既知の DVMRP マルチキャスト発信元のセットを表示させる場合は、 **dump routing tables** コマンドを使用します。リストには、それぞれの発信元ごとに、確認元の DVMRP ルーター、対応するコスト、ルーティング・テーブル項目の更新後の秒数が一緒に表示されます。

構文 :

dump

例: dump

```
Multicast Routing Table
Type   Origin-Subnet   From-Gateway    Metric  Age  In  Out-Vifs
Direct 18.26.0.0       192.35.82.97      10     30   1    0  2*
Direct 18.58.0.0       192.35.82.97       4     30   1    0  2*
DVMRP  18.85.0.0       192.35.82.97       4     30   1    0  2*
DVMRP  18.180.0.0      192.35.82.97       3     30   1    0  2*
DVMRP  36.8.0.0        192.35.82.97       9     30   1    0  2*
DVMRP  36.56.0.0       192.35.82.97       7     30   1    0  2*
DVMRP  36.103.0.0      192.35.82.97       9     30   1    0  2*
DVMRP  128.61.0.0      192.35.82.97       8     30   1    0  2*
DVMRP  128.89.0.0      192.35.82.97      10     30   1    0  2*
DVMRP  128.109.0.0     192.35.82.97       4     30   1    0  2*
DVMRP  128.119.0.0     192.35.82.97       4     30   1    0  2*
DVMRP  128.150.0.0     192.35.82.97       6     30   1    0  2*
```

Type マルチキャスト発信元のタイプ (つまり、DVMRP) を表示します。

Origin-Subnet
発信サブネットの IP アドレスを表示します。

From-Gateway
項目が着信した元のゲートウェイの IP アドレスを表示します。

Metric そのルートの対応コストを表示します。

Age ルーティング・テーブル項目の経時をルーティング・テーブル項目の更新後の秒数として表示します。

In 発信元からのマルチキャスト・データグラムを受信する必要がある DVMRP VIF を表示します。

Out-Vifs
マルチキャスト・データグラムを送信する VIF を表示します。VIF にアスタリスクが付いている場合は、データグラムの転送が行われるのが、接続ネットワーク上にグループ・メンバーがある場合だけであることを示します。

Interface Summary

DVMRP インターフェース (または VIF) の現行リストを表示させる場合は、 **interface summary** コマンドを使用します。

構文 :

interface *interface-ip-address*

例 : interface

```
Virtual Interface Table
Vif  Local-Address                          Metric  Thresh  Flags
0   10.1.153.22      subnet: 10.1.153.0       1       1    querier
1   10.1.154.22      subnet: 10.1.154.0       1       1    down
```

Vif DVMRP インターフェース (または VIF) に割り当てられた番号を表示します。それぞれの VIF に 1 つずつ番号が割り当てられているので、他のコマンドで VIF の識別に使用されます。

Local Address
DVMRP インターフェースのローカル IP アドレス を表示します。

Metric ルートの対応コスト

Threshold
ネットワークがネットワークの外側のマルチキャスト・パケットの外部フローを制御できる機能が反映されます。

Flags VIF がダウンかどうか、またはルーターがインターフェース上の IGMP ホスト・メンバーシップ照会の送信側であるかどうかが表示されます。

Join

join コマンドは、ルーターをマルチキャスト・グループのメンバーとして確立するのに使用します。

このコマンドは OSPF 構成監視の join コマンドと同様ですが、次の 2 つの点が異なります。

- コマンドがモニターから出されると、グループ・メンバーシップに対する影響が即時に現れます (つまり、再始動/再ロードの必要がありません)。
- コマンドによって、特定のグループが『結合される』回数が把握されます。

ルーターがマルチキャスト・グループのメンバーである場合は、グループ・アドレスに送信された PING および SNMP 照会に応答します。

構文 :

join *multicast-group-address*

例 : join 224.185.00.00

Leave

leave コマンドは、マルチキャスト・グループ内のルーターのメンバーシップを除去するのに使用します。 これにより、ルーターはグループ・アドレスに送信された PING および SNMP 照会に応答しなくなります。

このコマンドは、OSPF 構成監視の **leave** コマンドに似ていますが、次の 2 つの点で異なっています。

- コマンドがモニターから出されると、グループ・メンバーシップに対する影響が即時に現れます (つまり、再始動/再ロードの必要がありません)。
- 実行された 『leave』 の回数が前に実行されていた 『join』 の回数と等しくなるまで、コマンドはグループ・メンバーシップを削除しません。

構文 :

leave *multicast-group-address*

例 : leave 224.185.00.00

Mcache

mcache コマンドは、現在アクティブなマルチキャスト・キャッシュ項目のリストを表示するのに使用します。最初の突き合わせマルチキャスト・データグラムが受信されるたびに、マルチキャスト・キャッシュ項目がオンデマンドで作成されます。 データグラム発信元ネットワークと着信先グループの各組み合わせごとに、別個のキャッシュ項目 (したがって、別個のルート) があります。

トポロジーの変更時 (例えば、DVMRP システムのポイント・ポイント回線がアップまたはダウンする)、およびグループ・メンバーシップの変更時に、キャッシュ項目は消去されます。

注: 出力の最上部の凡例に表示されている番号は、VIF を直接指すのではなく、物理インターフェース (DVMRP と MOSPF のどちらかが稼働している場合がある) とトンネルを指します。

注:

構文 :

mcache

例 :

```
mcache
0: Eth/0           1: TKR/0           2: Internal
3: 128.185.246.17  4: 192.35.82.97

Source          Destination     Count   Upst    Downstream
128.185.146.0   239.0.0.1       1       0       2,4
128.119.0.0     224.2.199.198   9       4       3
128.9.160.0     224.2.127.255   1       4       3
13.2.116.0      224.2.0.1       27      4       3
140.173.8.0     224.2.0.1       31      4       3
128.165.114.0   224.2.0.1       25      4       3
132.160.3.0     224.2.158.99    11      4       3
132.160.3.0     224.2.170.143   56      4       3
128.167.254.0   224.2.199.198   27      4       3
129.240.200.0   224.2.0.1       21      4       3
131.188.34.0    224.2.0.1       28      4       3
131.188.34.0    224.2.199.198   28      4       3
```

Source
突き合わせデータグラムの発信元ネットワーク/サブネット

Destination
突き合わせデータグラムのあて先グループ

Count そのマルチキャスト・グループに関して処理された項目の数を表示します。

Upstream
データグラムを転送のために受信する必要がある元の近隣ネットワーク/ルーターを表示します。これが 『none』 のときは、データグラムが転送されることはありません。

Downstream

データグラムが転送される先のダウンストリーム・インターフェース/近隣の合計数を表示します。これが *none* のときは、データグラムは転送されません。

マルチキャスト転送キャッシュ記入項目にはさらに情報が入っています。 コマンド行に突き合わせデータグラムの発信元およびあて先を入力すると、キャッシュ記入項目を詳細に表示することができます。 突き合わせキャッシュ記入項目が見つからない場合は、項目が 1 つ作成されます。このコマンドのサンプルが下に示してあります。

例 :

```
mcache 128.185.182.9  224.0.1.2
source Net:     128.185.182.0
Destination:    224.0.1.2
Use Count:      472
Upstream Type:  Transit Net
Upstream ID:    128.185.184.114
Downstream:     128.185.177.11 (TTL = 2)
```

短形式の mcache コマンドで示された情報のほか、以下のフィールドが表示されます。

Upstream Type

データグラムを転送のために受信する必要がある元のノードのタイプを表示します。このフィールドの値としては、『none』 (データグラムが転送されないことを示す)、『router』 (ポイント・ポイント接続を通してデータグラムを受信する必要があることを示す)、『transit network』、『stub network』、『external』 (別の自律システムからのデータグラムの受信が予測されることを示す) が考えられます。

Downstream

データグラムが送信される先の各インターフェースや各近隣ごとに、それぞれ別の行を印刷します。 TTL 値も与えられます。この値は、このインターフェースとの間でやり取りされるデータグラムは、少なくとも、それぞれの IP ヘッダーに指定 TTL 値をもっている必要があることを指示します。ルーター自体がマルチキャスト・グループのメンバーであるときは、*internal application* を指定する行がダウンストリーム・インターフェース/近隣の 1 つとして表示されます。

Mgroups

mgroups コマンドは、ルーターの接続されたインターフェースのグループ・メンバーシップを表示するのに使用します。ルーターがその上で指定ルーターまたはバックアップ指定ルーターのいずれかであるインターフェースのグループ・メンバーシップだけが表示されます。

構文 :

mgroups

例 :

```
mgroups
Local Group Database
Group            Interface                Lifetime (secs)
```

```
224.0.1.1         128.185.184.11 (Eth/1)       176
224.0.1.2         128.185.184.11 (Eth/1)       170
224.1.1.1         Internal                     1
```

Group グループ・アドレスを、特定のインターフェースに関して報告された (IGMP 経由で) まま表示します。

Interface
グループ・アドレスが報告された (IGMP 経由で) 先のインターフェース・アドレスを表示します。

ルーターの内部グループ・メンバーシップは、“internal” という値で示されます。これらの項目では、lifetime フィールド (下を参照) は、特定のグループで要求されたメンバーシップをもつアプリケーションの数を示します。

Lifetime
特定のグループに関してインターフェース上でのメンバーシップ・レポートがなくなった場合でも、項目が存続する秒数を表示します。

Mstat

さまざまなマルチキャスト・ルーティング統計を表示させる場合は、 **mstat** コマンドを使用します。このコマンドは、マルチキャスト・ルーティングが使用可能になっているかどうか、およびルーターが区域間または AS 間 (あるいはその両方) の転送側であるかどうかを示します。

構文 :

mstats

例 :

```
mstats
              MOSPF forwarding:       Enabled
              Inter-area forwarding:  Enabled
              DVMRP forwarding:       Enabled

Datagrams received:           45476  Datagrams (ext source):    0
Datagrams fwd (multicast):        0  Datagrams fwd (unicast):   0
Locally delivered:                0  No matching rcv interface: 0
Unreachable source:               4  Unallocated cache entries: 0
Off multicast tree:               0  Unexpected DL multicast:   0
Buffer alloc failure:             0  TTL scoping:               0

# DVMRP routing entries:          0  # DVMRP entries freed:     0
# fwd cache alloc:                5  # fwd cache freed:         0
# fwd cache GC:                   0  # local group DB alloc:    6
# local group DB free:            0
```

MOSPF forwarding
ルーターが IP マルチキャスト・データグラムを転送するかどうか表示します。

Inter-area forwarding
ルーターが区域間で IP マルチキャスト・データグラムを転送するかどうか表示します。

DVMRP forwarding
ルーターが IP マルチキャスト・データグラムを転送するかどうか表示します。

DVMRP 監視コマンド (Talk 5)

Datagrams received
ルーターが受信したマルチキャスト・データグラムの数を表示します (あて先グループが 224.0.0.1 ～ 224.0.0.255 の範囲にあるデータグラムは、この合計に含まれません)。

Datagrams (ext source)
発信元が AS の外部にある、受信されたデータグラムの数を表示します。

Datagrams fwd (multicast)
データ・リンク・マルチキャストとして転送されたデータグラムの数を表示します (これには、必要な場合は、パケット複写が含まれるので、このカウントは受信された数より大きくなることがあります)。

Datagrams fwd (unicast)
データ・リンク・ユニキャストとして転送されたデータグラムの数を表示します。

Locally delivered
内部アプリケーションに転送されたデータグラムの数を表示します。

No matching rcv interface
非 MOSPF インターフェース上で非 AS 間マルチキャスト転送側によって受信されたデータグラムのカウントを表示します。

Unreachable source
発信元アドレスが到達不能であったデータグラムのカウントを表示します。

Unallocated cache entries
資源の不足により、キャッシュ項目が作成できなかったデータグラムのカウントを表示します。

Off multicast tree
突き合わせキャッシュ項目にアップストリーム近隣とダウンストリーム・インターフェース/近隣のどちらもなかったため転送されなかった、データグラムのカウントを表示します。

Unexpected DL multicast
データ・リンク・ユニキャスト用として構成されたインターフェース上でデータ・リンク・マルチキャストとして受信されたデータグラムのカウントを表示します。

Buffer alloc failure
バッファーの不足のため複写できなかったデータグラムのカウントを表示します。

TTL scoping
グループ・メンバーに到達できなかったことが TTL によって示されたため転送されなかったデータグラムを示します。

DVMRP routing entries:
DVMRP ルーティング項目の数を表示します。

DVMRP entries freed:
解放された DVMRP 項目の数を示します。このサイズは、ルーティング項目の数から解放された項目の数を引いたものになります。

 # fwd cache alloc
割り振られたキャッシュ項目の数を示します。現行の転送キャッシュ・サイズは、割り振られた項目の数 (『# fwd cache alloc』) から解放されたキャッシュ項目の数 (『# fwd cache freed』) を引いたものです。

 # fwd cache freed
解放されたキャッシュ項目の数を示します。現行の転送キャッシュ・サイズは、割り振られた項目の数 (『# fwd cache alloc』) から解放されたキャッシュ項目の数 (『# fwd cache freed』) を引いたものです。

 # fwd cache GC
最近使用されたことがなく、キャッシュがオーバーフローしたため消去されたキャッシュ項目の数を示します。

 # local group DB alloc
割り振られたローカル・グループ・データベース項目の数を示します。割り振られた数 (『# local group DB alloc』) から解放された数 (『# local group DB free』) を引いたものが、ローカル・グループ・データベースの現行サイズに等しくなります。

 # local group DB free
解放されたローカル・グループ・データベース項目の数を示します。割り振られた数 (『# local group DB alloc』) から解放された数 (『# local group DB free』) を引いたものが、ローカル・グループ・データベースの現行サイズに等しくなります。

キャッシュ・ヒットの数は、受信されたデータグラムの数 (『Datagrams received』) から 『No matching rcv interface』、『Unreachable source』、『Unallocated cache entries』のため廃棄されたデータグラムの合計を引き、さらに 『# local group DB alloc』 を引いた数として計算できます。キャッシュ・ミスの数は 『# local group DB alloc』だけです。

第21章 RSVP の使用

資源予約プロトコル (Resource ReSerVation Protocol (RSVP)) は、 IP 信号プロトコルの 1 つで、アプリケーションがそのサービス品質 (QOS) 要件を信号で通知する場合に使用します。RSVP は、複数の送信側から複数の受信側へのセッションをサポートする設計になっています。 RSVP 信号がトラフィック管理を起動するすると、パケット送達に必要な QOS を達成するネットワーク資源 (例えば、帯域幅とバッファー) の動的予約が結果的に行われます。RSVP は受信側指向です。つまり、QOS フローを受信するアプリケーションが、ネットワーク資源を予約する RSVP 信号を担当します。したがって、RSVP での QOS は、受信側から送信側へのパス内の各ホップごとに予約を確立して実現します。予約は、トラフィック・フローの QOS を決める一組のパラメーター値で構成されます。送信側と受信側は、RSVP 用として使用可能にされているホスト・アプリケーションで、相互に RSVP メッセージをやり取りして予約を作成します。IBM による機能強化を使用すると、一部の非 RSVP 使用可能アプリケーションでも、それ自体の代わりにその第 1 ホップ・ルーターに RSVP 信号を実行させることができます。RSVP は、IBM ルーター内の IPv4 で稼働し、ユニキャストとマルチキャストの両 IP トラフィックをサポートします。 RSVP の詳しい記述は RFC 2205 に記載されています。

2210 に実装された RSVP では、予約が確立されたそれぞれの IP トラフィック・フローごとに、Controlled Load (負荷制御) サービス品質を提供します。 Controlled Load (負荷制御) QOS は、インターネット技術特別調査委員会 (IETF) のサービス総合モデルに定義されています (RFC 2211)。たとえネットワークが輻輳 (ふくそう) した場合でも、 Controlled Load (負荷制御) QOS では、ネットワークが輻輳 (ふくそう) していないときトラフィック・フローが受けているサービスのレベルを提供し続けます。

この章は以下の節に分かれています。

- 『RSVP はこのように働く』
- 452ページの『RSVP でサポートされるリンクのタイプ』
- 453ページの『サンプル構成』

RSVP はこのように働く

図38 に、RSVP が特定のトラフィック・フローに QOS を提供する予約を確立する場合に使用する一連のメッセージが図示してあります。この例では、ベストエフォート IP トラフィック・フローがルーター間にすでに確立されているものと想定しています。

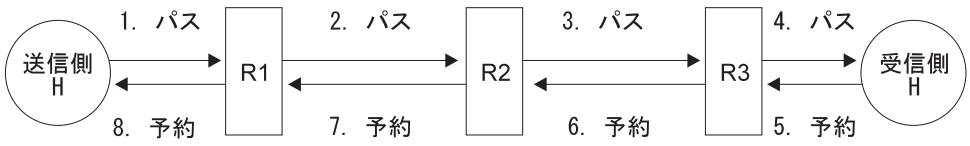


図 38. RSVP 予約 - すべてのルーターで RSVP がサポートされている場合

RSVP 予約の確立が開始されるのは、RSVP 使用可能送信側がデータ・トラフィック・フローの受信側に向けて *PATH* メッセージを送信した時点です。PATH メッセージには、フローについて記述するトラフィック情報が入っています。ルーターでは、PATH メッセージ (IP ヘッダーの「ALERT オプション」フィールドに入っている) を受信すると、その PATH メッセージに関してソフト状態を確立し維持します。また、RSVP ルーターでは、その PATH メッセージにマークを付けて、独自の IP アドレスをもつあて先 (前ホップまたは p ホップと呼ばれる) に向けて転送もします。RSVP 使用可能受信側では、 *RESV* メッセージを返送して、PATH メッセージの 1 つに応答できます。RESV メッセージでは、パス内の各リンク上でのネットワーク資源 (帯域幅など) の予約を要求します。RESV メッセージは、PATH メッセージが通過したのとは逆のパスを通して送信されます。RESV メッセージは、この逆のパス上の最初のルーター (ルーター R3) で受信されます。このルーターでは、アウトバウンド・インターフェース上で、つまり、R3 と受信側ホストの間のリンク上で資源の予約を試みます。要求された資源が使用可能であれば、このフロー用として予約され、使用可能資源の量がこれに相当する量だけ減少します。要求された資源が使用不能であれば、そのノードでは予約は正常に行われず、RESVERR メッセージが受信側ホストに送り返される可能性があります。ここでは、予約が正常に行われた場合を想定することにします。

ルーター R3 では、送信側に向かって戻るパスを通して RESV メッセージを次のルーター (R2) に転送します。R2 では、それ自体と R3 の間のリンク上で予約を設定し、RESV メッセージを R1 に転送します。R1 では、それ自体と R2 の間のリンク上で予約を設定し、RESV メッセージを送信側ホストに転送します。この例では、送信側は RSVP をサポートしています。そこで、それ自体と R1 の間のリンク上に予約を設定します。これで、予約されたリンクからなるパスによって、送信側から受信側まで確立された予約が形成されます。

次に、図39 に示すように、すべてのノードで RSVP がサポートされているとは限らないネットワークについて考察してみます。

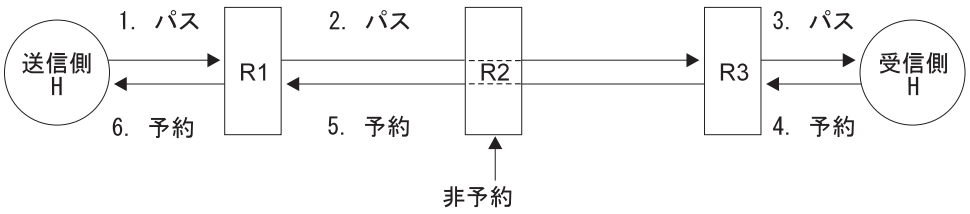


図 39. RSVP 予約 - すべてのルーターで RSVP がサポートされているとは限らない場合

特に、R2 で RSVP がサポートされていないものとします。R2 では、 PATH メッセージを受信すると、通常のパケットとして処理し、 R3 に向けて転送します。R2 で PATH メッセージに入っている p ホップが変更されることはありません。

前の場合と同様に、PATH メッセージが受信側ホストに到達すると、RESV メッセージを R3 に送信することで予約プロセスが開始されます。R3 が RESV メッセージ上で確認する前ホップは、 R1 のアドレスです。R2 では、それ自体の前ホップを PATH メッセージ内に指定しなかったからです。R3 では、RESV メッセージを R1 に送信し、それ自体と受信側ホストの間のリンク上で予約を行います。R1 では、RESV メッセージを R3 から受信すると、それ自体から R3 までの間で予約を行います。これ

で、予約 (送信側に向かう方向) が送信側と R1 と R3 に存在することになりました、パケットは、通常のベストエフォート・パケットとして R2 を通過します。ルーターのすべてで必ずしも RSVP がサポートされているとは限らないネットワークでは、このようにして RSVP が使用できます。

バーチャル・サーキット・リソース・マネージャー

バーチャル・サーキット・リソース・マネージャー (VCRM) は、RSVP が使用可能にされると必ず使用可能にされるフィーチャーです。RSVP からの予約要求に応じて、VCRM では、物理インターフェースを通るデータ・フロー用の接続を作成します。そのために、 VCRM では、まず最初に、予約に対応できる帯域幅が十分存在しているかどうか判別する必要があります。

注: フレーム・リレーや X.25 など、WAN インターフェースを使用している場合は、使用可能な帯域幅がどれだけあるかが VCRM に分かるようにするため、回線速度を設定する必要があります。回線速度を設定するための手順については、 *ソフトウェア使用者の手引き* のフレーム・リレーと X.25 のインターフェース構成に関する章に記載してあります。

ネットワーク内の下位リンクで QOS トラフィックがサポートされて (QOS SVC の ATM サポートなど) いれば、VCRM ではこのリンク機能を活用して、このフロー用としてデータ・トラフィックが使用することになる ATM SVC を確立します。下位リンクが QOS 対応可能でないときは、ネットワーク・レイヤーとデータ・リンク・レイヤーの間のトラフィックのスケジューリングとバッファリングによって、QOS フローを集約し、最善的トラフィックと区別します。

VCRM について詳しくは、*フィーチャーの使用と構成* の中の 『VCRM の構成と監視』 を参照してください。

トラフィック・フローと RSVP セッション

ルーターのパスと予約ソフト状態では、RSVP 予約の存在と、その予約に従ってトラフィック・フローが送信中であることを定義します。RSVP セッションは、予約済みパスを通って同じ IP セッション・アドレス (これは、固有の IP アドレスでもマルチキャスト IP アドレスでも構わない) にルート指定されている、1 つまたは複数の送信側からのトラフィック・フローすべてで構成されます。例えば、451ページの図 41 では、送信側 S1 から受信側 Rec 1 へのトラフィック・フローだけでなく、送信側 S2 から受信側 Rec 1 へのトラフィック・フローも、セッションに組み込まれています。このセッションは、受信側 Rec 1 の IP アドレスで識別されています。

送信側と受信側では、予約済みトラフィック・フローの存在を再確認する最新表示メッセージを送信して、セッション内のそれぞれのパスと予約の存在を維持します。最新表示メッセージは、PATH メッセージと RESV メッセージの単なるコピーに過ぎません。一定の時間内にノードが最新表示メッセージを受信しないと、構成可能タイマーがタイムアウトになり、ソフト状態維持中のノードに予約を廃棄させます。

廃棄メッセージには、RSVTEAR と PATHTEAR の 2 つのタイプがあります。RSVTEAR メッセージは、受信側が送信するもので、予約は廃棄しますが、トラフィック・フローは廃棄しないので、ベストエフォート・サービスによって継続しま

す。PATHTEAR メッセージでは、送信側からセッション・アドレスへのパスを廃棄します。PATHTEAR では、予約もパス・ソフト状態も両方とも廃棄されます。ただし、ベストエフォート・トラフィックのフローに変わりはありません。

予約のスタイル

447ページの図38 では、特定の 1 つの送信側から特定の 1 つの受信側へのトラフィック・ストリーム用としてリンクを予約する、 1 つの RSVP 予約の確立を示しました。複数の送信側が同一受信側に送信する場合は、それぞれの送信側から受信側へ 1 つずつ、複数の IP トラフィックが存在することになります。このような状況では、別々の送信側では、選択された *予約スタイル* によって、一部のリンクを通して受信側に至る予約が共用できる場合とできない場合があります。

図40 に、送信側 S1 と S2 に対して、受信側が固定フィルター (FF) 予約スタイルを要求した場合が図示してあります。この予約スタイルでは、各送信側でそれぞれ独自の個別予約が得られます。ホスト S3 は、 RSVP には参加していませんが、ベストエフォート・トラフィックを受信しています。

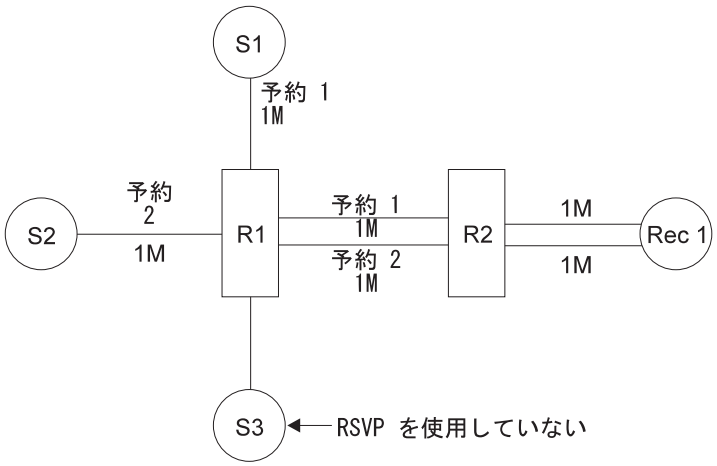


図 40. 固定フィルター予約スタイル

共用明示 (SE) 予約スタイルでは、特定のグループのメンバーとして識別されている送信側では、一部の予約済みリンクが共用できます。あるグループ内の送信側は、送信側が PATH メッセージに入れて送信する情報 (送信側の IP アドレスなど) に応じて、受信側で定義されます。 451ページの図41 では、送信側 S1 と送信側 S2 は、受信側 Rec 1 のあて先アドレスで識別されている RSVP セッションに組み込まれています。グループ内の送信側は、受信側への送信側のパスがマージされしだい、予約を共用します。この場合は、共通予約がルーター R1 から受信側まで続いています。

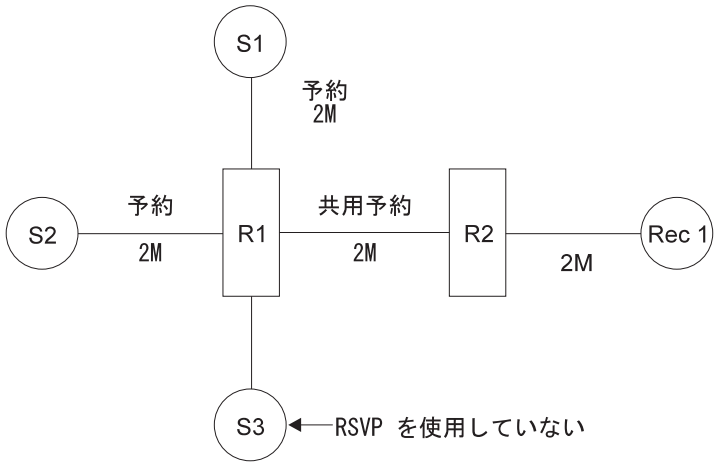


図 41. 共用明示予約スタイル

3 番目のワイルドカード・フィルター (WF) 予約スタイルでは、 *PATH* メッセージをセッション・アドレスに送信する送信側すべてが、図42 に示すように、同一の予約を共用します。

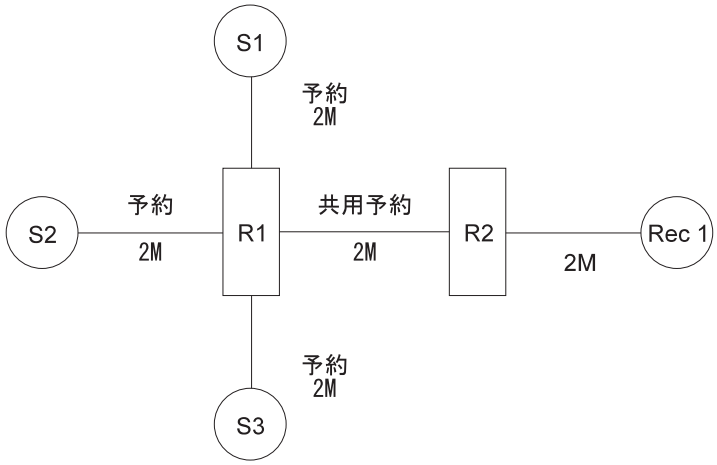


図 42. ワイルドカード・フィルター予約スタイル

OPWA

OPWA (One-Path With Advertising) は、RSVP の任意選択フィーチャーの 1 つです。これによって、受信側では、予約パス上のそれぞれのリンクから入手可能な、帯域幅など、 QOS 値のレコードが入手できます。例えば、447ページの図38 に示したルーター R1 と R3 が OPWA 用として構成されていると、これらのルーターには、それぞれのリンクの特性が通知されます。この情報によって、これらのルーターでは、資源が最も少ないリンクの容量に応じて、PATH メッセージ内の情報を調整できます。

例えば、447ページの図38 で、送信側が平均速度 1 Mbps、ピーク速度 10 Mbps で、受信側に向けて PATH メッセージの送信を始めたものとします。さらに、R2 と R3 の間のリンクは、回線速度が 2 Mbps の PPP リンクであるものとします。R2 の

OPWA は、PATH メッセージ内のピーク速度を変更して、2 Mbps に落とします。ダウンストリーム側のノードのどれにも 2 Mbps を超えるピーク速度を予約する理由はまったくないからです。

RSVP でサポートされるリンクのタイプ

RSVP でサポートされるリンクには、次のタイプがあります。

- ATM ポイント・ポイント SVC
- PPP リンク。RSVP では、サポートされている固定接続基準のリンク・タイプ (V.35、T1/E1、ISDN など) すべてで PPP をサポートします。ダイヤル・オンデマンド、WAN レストラル、短期保留モード、負荷平衡の各構成で使用されるリンクは、RSVP 用として使用しないようにする必要があります。
- フレーム・リレー PVC。PPP の場合と同様、サポートされているリンクすべてが RSVP をサポートしますが、RSVP 用としては、固定接続基準のリンクだけを使用する必要があります。ダイヤル・オンデマンド、WAN 復元、短期保留モード、負荷平衡の各構成で使用されるリンクは、RSVP では使用しないようにする必要があります。
- フレーム・リレー SVC。このサポートは、フレーム・リレー PVC の場合と同様です。つまり、RSVP では、QOS トラフィック用として別の DLCI のセットアップはできませんが、省略時 DLCI の一部を QOS 帯域幅割り振り用として使用することはできます。
- すべての LAN リンク :
  - イーサネット
  - トークンリング

  注: LAN などのような共用媒体ネットワークの場合は、LAN 帯域幅の共用を調整するために、トラフィック・エンジニアリングなど、他の方式が必要です。RSVP では、特定の 1 つのルーターによる帯域幅の使用は制御しますが、複数のルーターとホストによる LAN 帯域幅の使用を調整することはありません。
- X.25。PPP やフレーム・リレー PVC の場合と同様にサポートされます。RSVP では、 QOS トラフィック用として別の VC のセットアップはできません。省略時 VC の一部を QOS 帯域幅割り振り用として使用します。

注:

1. RSVP は、通常の IP ルーティング・テーブルに従ってルーティングが行われます。 ATM のネクスト・ホップ・ルーティング・プロトコル (NHRP) が活用されることはありません。NHRP でルートの追跡に使用するのは、IP の高速パス転送キャッシュであって、IP ルーティングではないからです。
2. 競合を避けるために、帯域幅予約システム (BRS) 用として構成されている PPP リンクや FR リンクでは、RSVP は使用不可にします。

サンプル構成

RSVP の構成に関する指針として、talk 6 コマンド行インターフェース構成が含まれています。RSVP のコマンドとパラメーターの説明については、 457ページの『第22章 RSVP の構成と監視』 を参照してください。RSVP のサンプル構成の手順を説明するステップは、次のとおりです。

1. talk 6 **enable rsvp** コマンドを RSVP config> プロンプトで使用して、ルーター内の RSVP を使用可能にします。RSVP が使用可能にできるのは、IP 用として構成されているインターフェースの場合だけです。このコマンドでは、RSVP ルーター・パラメーターは、インターフェース上の省略時帯域幅としての 0 も含めて、省略時値に設定します。特定のインターフェースを使用可能にし、それに対して帯域幅を設定してからでないと、RSVP がそれらのインターフェースを通して稼働することはできません。
2. **enable interface** コマンドを使用して、特定のインターフェースをそれぞれ RSVP 用として使用可能にします。
3. このインターフェース上で RSVP を即時に有効にしたい場合は、talk 5 **reset interface** コマンドを使用します。
4. 各インターフェースごとにそれぞれ帯域幅の設定を指示するプロンプトが出ます。特定のインターフェースに関する帯域幅が 0 (省略時値) のままになっていると、そのインターフェースを通る予約はできません。
5. すべての RSVP 使用可能インターフェース上で OPWA を使用可能にしたい場合は、**enable opwa-all** コマンドを使用します。1 つのインターフェース上で OPWA を使用可能にしたい場合は、**enable opwa** コマンドとインターフェース番号を使用します。OPWA を使用可能にする場合は、その前にインターフェース上で RSVP を必ず使用可能にしておきます。 RSVP について使用可能にしていないインターフェース上で OPWA を使用可能にしようとすると、Cannot find RSVP i/f rec というメッセージが表示されます。
6. それ以外のパラメーターは任意指定であり、RSVP は省略時値で稼働できます。
7. 必要があれば、**add sender** コマンドと **add receiver** コマンドを使用して、ルーター用の静的送信側や静的受信側が作成できます。静的送信側と静的受信側では、 RSVP を使用していないホスト・アプリケーション用の RSVP 信号を生成します。静的送信側と静的受信側用として構成された IP アドレスとポート番号で、ルーターが RSVP メッセージを送信する対象となる IP トラフィック・フローの発信元とあて先を識別します。静的送信側も静的受信側も構成されなくても、ルーターは RSVP メッセージを転送し、予約リンクを確立しますが、RSVP メッセージを発信することはありません。詳しくは、454ページの『静的送信側と静的受信側のサンプル構成』 を参照してください。

例 :

```
Config> protocol rsvp
Resource ReSerVation Protocol config console
RSVP Config> enable rsvp
RSVP Config> enable interface
Interface [0]?
Creating RSVP i/f record...
Set Link Reservable Bandwidth (bits) [0]? 5000000

Interface enabled.
  To take effect immediately, use talk-5 RSVP's 'reset interface'
RSVP Config> enable interface
Interface [0]? 1
```

```
Creating RSVP i/f record...
Set Link Reservable Bandwidth (bits) [0]? 1024000

Interface enabled.
    To take effect immediately, use talk-5 RSVP's 'reset interface'
RSVP Config>enable opwa
Interface [0]?
Controlled Load installed on interface 0
take effect immediately?(Yes or [No]): y
RSVP Config>enable opwa
Interface [0]? 1
Controlled Load installed on interface 1
take effect immediately?(Yes or [No]): y
Interface enabled.

RSVP Config>list interface

RSVP Interfaces:

If      IP address   RSVP-enabled  Encaps.  max_res_bw SRAM_rec
0       5.0.31.5        Y          IP       5000000      1
1       5.0.31.3        Y          IP       1024000      2

RSVP Config>list opwa

OPWA configuration:

Network OPWA    CTL-LOAD
0       Y       Y
1       Y       Y
```

構成が完了したら、talk 5 **reset rsvp** コマンドか **reset interface** コマンドを使用するか、ルーターを再始動して、RSVP をアクティブにできます。

静的送信側と静的受信側のサンプル構成

453ページの『サンプル構成』 の説明どおりに RSVP を構成すると、RSVP トラフィックのフローとセッションが、ルーターに接続されているホスト内の RSVP 使用可能アプリケーションによって動的に確立されます。RSVP 用として使用可能にされていないホスト・アプリケーションがあって、既知の IP アドレスとポートにパケットを送信する場合は、静的送信側と静的受信側を構成して、ルーターにそのフロー用の RSVP 信号を生成させることができます。

まず最初に、**add sender** コマンドを RSVP config> プロンプトで使用して、送信側を構成します。

```
Config> protocol rsvp
Resource ReSerVation Protocol config console
RSVP Config> add sender
Session> IP Address: [0.0.0.0]? 5.0.31.1  1
Session> Port Number: [1]? 5004
Session> Protocol Type (UDP/TCP): [UDP]?
Sender> IP Address: [0.0.0.0]? 5.0.27.27  2
Sender> Src Port: [1]? 5005
Tspec> Peak Rate (in byte/sec) [250000]? 25000
Tspec> Average Rate (in byte/sec) [200000]? 20000
Tspec> Burst Size (in bytes) [2000]?
Tspec> Max. Pkt Size [1500]?
Tspec> Min Pkt Size [53]?
```

1 トラフィック・フローがユニキャストであれば、セッションの IP アドレスは、IP トラフィック・フローの受信側のユニキャスト・アドレスです。トラフィック・フローがマルチキャストであれば、セッションの IP アドレスは、 IP トラフィック・フローのあて先のマルチキャスト・アドレスです。

2 送信側の IP アドレスは、IP トラフィック・フローの送信側のユニキャスト・アドレスです。送信側と受信側は、ルーターでなければ、ルーターに接続されているホストです。この場合のルーターは、ホストのプロキシーを務めます。

list sender コマンドを使用して、正しい値が構成されていることを確認したら、受信側を務める 2 番目のリモート・ルーター内に静的受信側が構成できます。この例では、送信側ルーターは、IP アドレスが 5.0.27.27 で、受信側ルーターは、IP アドレスが 5.0.31.1 です。静的受信側を作成する場合は、 **add receiver** コマンドを使用します。

```
RSVP Config>add receiver
RESV requestor IP Address: [0.0.0.0]? 5.0.31.1
Session> IP Address: [5.0.31.1]? 1
Session> Port Number: [1]? 5004
Session> Protocol Type (UDP/TCP): [UDP]?
Style> (WF, FF, SE): [FF]? wf 2
Need confirmation?(Yes or [No]):
Service Type: CTL-LOAD
Tspec> Peak Rate (in byte/sec) [250000]? 5000
Tspec> Average Rate (in byte/sec) [200000]? 20000
Tspec> Burst Size (in bytes) [2000]?
Tspec> Max. Pkt Size [1500]?
Tspec> Min Pkt Size [53]?
```

1 受信側の IP セッション・アドレス、ポート、プロトコルが送信側の IP セッション・アドレス、ポート、プロトコルに一致することに注意してください。送信側と受信側で同じトラフィック・フローを識別する必要があります。パス上のルーターがそれぞれのリンク上に確立を試みる帯域幅を判別するのは、受信側であって、送信側ではありません。

2 英字 *wf* は、ワイルドカード・フィルターの意味です。これは、RSVP の 3 つの予約スタイルのうちの 1 つです。詳しくは、 450ページの『予約のスタイル』を参照してください。

第22章 RSVP の構成と監視

この章では、資源予約プロトコル (RSVP) の構成と監視の方法と、 RSVP 監視コマンドの使用法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。

- 『RSVP 構成環境にアクセスする』
- 『RSVP 構成コマンド』
- 468ページの『RSVP 監視環境にアクセスする』
- 468ページの『RSVP 監視コマンド』

RSVP 構成環境にアクセスする

RSVP 構成環境にアクセスする場合は、Config> プロンプトで次のようにコマンドを入力します。

```
Config> protocol rsvp
Resource ReSerVation Protocol config console
RSVP Config>
```

RSVP 構成コマンド

この節では、RSVP 構成コマンドについて説明します。コマンドは、 RSVP Config> プロンプトで入力します。

表 27. RSVP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	送信側と受信側を追加します。
Delete	送信側と受信側を削除します。
Disable	RSVP や OPWA (One-Path With Advertising) を使用不可にします。
Enable	RSVP や OPWA (One-Path With Advertising) を使用可能にします。
List	RSVP についての情報を一覧表示します。
Set	RSVPシステム・パラメーターを設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

ルーターに静的 RSVP 送信側と受信側を追加する場合は、**add** コマンドを使用します。静的送信側や静的受信側によって、ルーターは RSVP メッセージの送信や受信ができます。ルーターが RSVP メッセージを送受信するのは、RSVP 用として構成されていないホスト・アプリケーションの代わりに、ルーターがプロキシーを務めている場合がほとんどです。そのような場合は、送信側の IP アドレスはホスト・アプリケーションのアドレスであり、セッションの IP アドレスはデータ・フローのあて先

アドレスです。ルーター用として静的送信側も静的受信側も構成されなくても、ルーターは RSVP メッセージを動的に転送し、予約を設定し、QOS を提供しますが、RSVP メッセージを発信することはありません。

送信側と受信側の定義は、番号を付けた SRAM レコードとして、構成内に保管されます。talk 5 **activate** コマンドを使用して、それぞれのレコードをアクティブにすることができます。

構文 :

add sender ...

receiver ...

sender

この用語の後に続くパラメーターの適用対象が、 RSVP *path* メッセージの送信側であることを指定するキーワード

receiver

この用語の後に続くパラメーターの適用対象が、 RSVP *resv* メッセージを送信側に戻す受信側であることを指定するキーワード

次のパラメーターのほとんどは、送信側と受信側の両方について指定します。送信側か受信側に固有のパラメーターについては、説明の中で識別してあります。

session-ip-address

1 つまたは複数の送信側からの IP データ・フローのユニキャストまたはマルチキャストあて先 IP アドレスです。トラフィック・フローがユニキャストのときは、このアドレスは受信側のアドレスであり、トラフィック・フローがマルチキャストのときは、このアドレスはマルチキャスト・アドレスです。受信側は、マルチキャスト・アドレスで識別されているグループのメンバーであることが必要です。送信側と受信側では、セッション・ポート番号とプロトコルと共に、セッション IP アドレス使用して、 QOS が確立されている RSVP セッションを識別します。

有効値: 有効な IPv4 アドレス。0.0.0.0 は使用できません。 RSVP がアクティブになっているときは、このアドレスで送信側と受信側にアクセスできる必要があります。

省略時値: なし

session-port

RSVP によって予約されるセッションの IP ポート番号。これは、あて先アプリケーションの UDP ポート番号か TCP ソケット番号です。

有効値: 0 ～ 65535

省略時値: 1

session-protocol

UDP と TCP のどちらか。

有効値: UDP か TCP

省略時値: UDP

sender-ip-address

送信側、つまり、予約されるデータ・フローを発信する送信アプリケーションのアドレス。このパラメーターは、ユニキャストであることが必要です。

有効値: 有効な IPv4 アドレス。

省略時値: なし

sender-port

QOS 用として予約される IP フローの送信側の IP ポート番号。これは、送信アプリケーションの UDP ポート番号か TCP ソケット番号です。

有効値: 0 〜 65535

省略時値: 1

receiver-ip-address

resv メッセージを発行する受信側の IP アドレス。ユニキャスト・セッションの場合は、このアドレスはセッション IP アドレスと同じです。マルチキャスト・セッションの場合は、このアドレスは、マルチキャスト・セッション・アドレス用として予約を行うアプリケーションのユニキャスト・アドレスです。マルチキャスト・セッションであれば、受信側は、このマルチキャスト・アドレスで表されるマルチキャスト・グループに属している必要があります。

有効値: 有効な IPv4 アドレス

省略時値: なし

peak-rate

IP セッションでのピーク・データ速度を指定します。この速度を送信側のピーク・トラフィック生成速度に設定するのは、既知で制御下にある場合であり、物理インターフェース回線速度に設定するのは、既知の場合であり、無限大 (X'FFFFFFFF'、 10 進数 4 294 967 295) に設定するのは、それよりもよい値が使用不能の場合です。ピーク・トラフィック速度は、平均トラフィック速度以上に設定する必要があります。

受信側が要求するピーク・データ速度が送信側が示した速度と異なっている場合は、ルーターでは、受信側の要求に応じるよう試みます。

有効値: 1 〜 4 294 967 295 バイト/秒

省略時値: 250 000

average-rate

IP セッションで送信側が送信するか、受信側が受信する必要がある平均データ速度を指定します。この値が送信側の平均トラフィック生成速度に設定されるのは、既知で制御下にある場合であり、物理インターフェース回線速度に設定されるのは、既知の場合であり、省略時には、200 000 バイト/秒に設定されます。

受信側が要求する平均速度が送信側が示した速度と異なっている場合は、ルーターでは、受信側の要求に応じるよう試みます。

有効値: 1 〜 4 294 967 295 バイト/秒

省略時値: 200 000

data-burst-size

ピーク速度にも平均速度にも関係なく送信できるバイト数を指定します。例えば、ピーク速度が 50 000 バイト/秒で、データ・バースト・サイズが 2000 の場合は、 ある特定のインスタンスに、バーストが原因でピーク速度がたとえ 50 000 バイト/秒を超えたとしても、そのインスタンスに 2000 バイトが送信できます。

受信側が要求する速度が送信側と異なっている場合は、ルーターでは、受信側の要求に応じるよう試みます。

有効値: 1 ～ 4 294 967 295 バイト

省略時値: 2000

max-packet-size

送信側が IP フローで送信するか、受信側が IP フローから受信する最大パケット・サイズを指定します。送信側では、この値は、送信アプリケーションで生成される最大のパケットのサイズに設定する必要があります。受信側では、受信側が RSVP OPWA (One-Path With Advertisement) パケットで到着する情報から確認するか、それ以外の方法で確認する最小パス MTU に設定する必要があります。

最大パケット・サイズがパス上のリンクの MTU より大きいと、予約要求は、その点ではリジェクトされます。例えば、予約のパス上のリンクの 1 つで MTU が 1500 であり、要求された最大パケット・サイズが 2000 であれば、予約要求はリジェクトされます。

受信側が要求する最大パケット・サイズが送信側と異なっている場合は、ルーターでは、受信側の要求に応じるよう試みます。

最大パケット・サイズは、最小パケット・サイズ以上の値を使用して構成する必要があります。例えば、最小パケット・サイズが 64 バイトであれば、最大パケット・サイズは 64 バイト以上であることが必要です。

有効値: 1 ～ 4 294 967 295 バイト

省略時値: 1500

min-packet-size

送信側が IP フローで送信するか、受信側が IP フローから受信する最小パケット・サイズを指定します。送信側では、この値は、送信アプリケーションで生成される最小のパケットのサイズに設定する必要があります。

このパケット・サイズは、最大パケット・サイズより大であることはできません。例えば、最大パケット・サイズが 1500 バイトであれば、最小パケット・サイズは 1500 バイト以下であることが必要です。このパケット・サイズには、アプリケーション・データと IP レベル以上 (IP、TCP、UDP など) のプロトコル・ヘッダーはすべて含まれますが、リンク・レベル・ヘッダーはどれも含まれません。

注: この値は、資源予約のオーバーヘッドを見積もる場合に使用します。最小パケット・サイズが小さいほど、予約オーバーヘッドは大きくなります。

有効値: 1 ～ 4 294 967 295 バイト

省略時値: 48

reservation-style

このパラメーターを構成するのは、受信側だけです。受信側が IP フローで受信する予約スタイルを指定します。RSVP 予約では、IP トラフィック・フローのパケットの特殊処理を保証して、送信側から受信側へのパスを形成するそれぞれのリンクや一連のリンク上で特定の QOS を提供します。示されている 3 つの予約スタイルは、次のようにして定義します。

固定フィルター (FF)

受信側が IP フローで受信するのは、特定の 1 つの送信側からのデータ・トラフィックであることを指定します。送信側 1 つにつき予約が 1 つ確立されます。

共用明示 (SE)

受信側が受信するのは、受信側が定義する同一グループ内の送信側のグループからのデータ・トラフィックであることを指定します。このグループのメンバーが予約を共用します。グループ内の各送信側では、それぞれそのリンクが受信側への共通パスにマージすると、ただちに予約を共用できます。

ワイルドカード・フィルター (WF)

受信側が受信するのは、すべての送信側からのデータ・トラフィックであることを指定します。各送信側は、それぞれそのリンクが受信側への共通パスにマージすると、ただちに予約を共用できます。

詳しくは、450ページの『予約のスタイル』 を参照してください。

有効値: FF、SE、WF

省略時値: FF

confirm-reservation

受信側で *reservation confirm* メッセージの受信を希望するかどうか指定します。このメッセージが resv メッセージを送信した受信側に返送されるのは、要求が該当の予約よりも大きい既存の予約にマージされるか、送信アプリケーションに送達されたときです。

有効値: Yes または No

省略時値: No

Delete

送信側や受信側を削除する場合は、**delete** コマンドを使用します。

構文 :

delete sender *sram-record*

receiver *sram-record*

sender または receiver *sram-record*

それぞれの送信側や受信側は、**delete** コマンドを使用すると表示される、SRAM レコードで識別されます。削除したい送信側や受信側の SRAM レコード番号を入力すると、構成からその送信側や受信側が削除されます。

Disable

インターフェースの 1 つまたはすべての上の RSVP や OPWA を使用不可にする場合は、**disable** コマンドを使用します。

構文 :

disable interface
opwa
opwa-all
rsvp

interface *interface-number*
特定のインターフェース上の RSVP 機能を使用不可にします。RSVP 制御メッセージはこのインターフェースを通って流れますが、 RSVP 予約がこのインターフェース上で行われることはありません。また、このコマンドでは、このインターフェースが QOS を設定できる機能も使用不可になります。

有効値: 有効なインターフェース番号

省略時値: 0

OPWA *interface-number*
特定のインターフェース上の OPWA を使用不可にします。

有効値: 有効なインターフェース番号

省略時値: 0

OPWA-all
すべてのインターフェース上の OPWA を使用不可にします。

RSVP ルーター内の RSVP 機能を使用不可にします。省略時には、 RSVP は disabled (使用不可) です。

Enable

インターフェースの 1 つまたはすべての上の RSVP や OPWA を使用可能にする場合は、**enable** コマンドを使用します。

構文 :

enable interface
opwa
opwa-all
rsvp

interface *interface-number*
特定のインターフェース上の RSVP 機能を使用可能にします。このコマンドによって、このインターフェースは、RSVP メッセージに応答し、それを転送することはできますが、発信はできません。 RSVP メッセージを発信する場合は、静的送信側と静的受信側を構成する必要があります。

使用可能にしたインターフェース上に帯域幅の設定を指示するプロンプトが出ます。後で帯域幅の設定を変更する場合も、**set bandwidth** コマンドが使用できます。このコマンドが作動するのは、ルーターが RSVP 用として使用可能になり、指定されたインターフェースが使用可能で、IP 用として構成されている場合だけです。

RSVP をサポートするリンクの一覧表については、452ページの『RSVP でサポートされるリンクのタイプ』 を参照してください。

有効値: 有効なインターフェース番号

省略時値: 0

OPWA *interface-number*
特定のインターフェース上の OPWA を使用可能にします。OPWA では、送信側と受信側の間のパスがすべてのホップ上でそれぞれ予約できるかどうかということと、パス上のそれぞれのホップでどれだけの帯域幅が使用可能かということを、受信側に通知します。このコマンドがこのように作動するのは、インターフェースが RSVP 用として使用可能になっている場合だけです。

有効値: 有効なインターフェース番号

省略時値: 0

OPWA-all
すべてのインターフェース上の OPWA を使用可能にします。 このコマンドが有効になるためには、RSVP がルーター内で使用可能にする必要があります。

RSVP ルーター内の RSVP 機能を使用可能にします。RSVP を初めて使用可能にするときは、RSVP に関する一組の省略時パラメーターも初期設定する必要があります。

RSVP は、使用可能にしても、起動したことにはなりません。このルーター内で RSVP を起動するためには、**set bandwidth** コマンドを使用して、RSVP を使用するインターフェースの少なくとも 1 つで帯域幅を設定する必要があります。その上で、RSVP 用としてルーターを再始動することが必要です。そのためには、talk 5 コマンド **reset rsvp** を使用するか、ルーターをリブートします。詳しくは、 talk 5 **reset rsvp** コマンドを参照してください。

List

RSVP パラメーターを一覧表示させる場合は、**list** コマンドを使用します。3 つのグループのパラメーターが別々に一覧表示されます。

- すべてのパラメーター
- インターフェース・パラメーター
- すべてのインターフェースに関する OPWA 設定値
- 送信側または受信側レコード
- システム・レベルの RSVP パラメーター

注: **list** コマンドでは、構成された送信側レコードと受信側レコードが一覧表示されます。これらのレコードでは、送信側のアドレスと受信側のアドレスで定義さ

れているアクティブ RSVP トラフィック・フローを識別することはありません。したがって、現在アクティブの RSVP を表示させる場合は、talk 5 **show rsvp flows** コマンドを使用します。

構文 :

list ... all
interface
opwa
receiver
sender
system

例 :

```
RSVP Config>list all

Software Version:

RSVP Control: IBM RSVP Router Release 1.0 (RFC 2205)


RSVP Configuration:

RSVP Status:                    Enabled
Maximum RSVP Msg Size:          1500 (bytes)
Refresh Interval:               30 (sec)
Allowed Successive Msg Loss:    3 (frame)
Flow Life-Time:                 158 (sec)
Refresh Slew Max:               30 (percent)
Total system reservable b/w:    4294967 (kbps)

RSVP Interfaces:

If      IP address   RSVP-enabled  Encaps.  max_res_bw SRAM_rec
0       5.0.27.2        Y          IP       5000000      1
5       5.0.28.2        Y          IP       8000000      2
4       5.0.25.101      Y          IP       1024000      3
2       5.0.45.2        Y          IP       1024000      4

OPWA configuration:

Network OPWA    CTL-LOAD
0       Y       Y
5       Y       Y
4       Y       Y
2       Y       Y

Following senders/receivers are defined in SRAM:
Rec.No   Type     DestAddr 1      Dest Port   Protocol   Src Addr        Src Port

1    Sender(PATH) 5.0.25.100      25          17         5.0.25.101      25
2    Receiv(RESV) 5.0.25.101      26          17         0.0.0.0         0
```

1 表示されているあて先アドレスは、IP セッション・アドレスです。IP セッション・アドレスの定義については、 talk 6 **add session-ip-address** コマンドを参照してください。

Set

RSVP システム・パラメーターを設定します。これらのパラメーターの一部の標準的な値の表示については、talk 6 **list all** コマンドの項の例を参照してください。

構文 :

set ...

allowed-successive-msg-loss ...

bandwidth ...

default

encapsulation ...

lifetime ...

max-msg-size ...

refresh-interval ...

slew ...

total ...

allowed-successive-msg-loss *msg-losses*

このパラメーターでは、RSVP トラフィック・フローについて定義されているパスと予約の状態が RSVP でタイムアウトになる前に紛失する可能性のある、連続する PATH とそれに一致する RESV 最新表示メッセージの数を定義します。特定のトラフィック・フローについてパスと予約の状態が RSVP でタイムアウトになると、そのフローには QOS がなくなります。送信側と受信側で予約を再確立する必要があります。

有効値: 1 ～ 9999

省略時値: 3

bandwidth *interface bps*

このパラメーターでは、インターフェースの予約可能帯域幅を定義します。通常、予約可能帯域幅は、合計リンク帯域幅の小部分である必要があります。 30% を超えないことが格好の目標になります。 予約可能帯域幅が設定できるのは、RSVP 用として使用可能になっているインターフェースの場合だけです。

この talk 6 コマンドは、オプションで、他のパラメーターの値に影響を及ぼさずに、即時に動的に有効にできます。

interface

ネットワーク・インターフェース番号

有効値: 有効なネットワーク・インターフェース番号

省略時値: 0

bps このインターフェース上で予約できるビット/秒 (bps) 単位の帯域幅

有効値: 1 ～ 4 294 967 295 bps (無限を表す)

省略時値: 0

default

このパラメーターでは、RSVP パラメーターをすべて、**enable rsvp** コマンドの使用時に存在している元の省略時値に設定します。個々のインターフェース上に以前構成したパラメーター値があれば、すべて **set default** コマンドで上書きされます。各インターフェース上の帯域幅の省略時値は 0 であり、これは該当のインターフェース上に RSVP 予約が確立されないことを意味するため、 RSVP を使用するインターフェースごとに **set bandwidth** コマンドを使用して、RSVP が再度稼働するよう準備する必要があります。

encapsulation *interface style*

このパラメーターでは、インターフェース上の RSVP メッセージのカプセル化スタイルを IP か UDP、または Both に設定します。通常、PATH メッセージと RESV メッセージなど、RSVP 制御メッセージは、プロトコル・タイプ が 49 のネイティブ IP フレームにカプセル化されます。このルーターに接続されているホストが RSVP メッセージを送信するのに、 UDP パケットしか使用できない場合は、そのホストに接続されているインターフェース上でのカプセル化スタイルは、UDP に設定する必要があります。 IP を使用するホストも UDP を使用するホストも、同一のリンクを通して RSVP メッセージを送信する場合は、カプセル化スタイルは Both (両方) に設定する必要があります。この操作が許容されるのは、指定されたインターフェース上で RSVP が使用可能にされている場合だけです。

この talk 6 コマンドは、オプションで、他のパラメーターの値に影響を及ぼさずに、即時に動的に有効にできます。

interface

ネットワーク・インターフェース番号

有効値: 有効なネットワーク・インターフェース番号

省略時値: 0

style RSVP メッセージのカプセル化スタイル

有効値: IP、UDP、または Both

省略時値: IP

lifetime

このパラメーターでは、確立された RSVP トラフィック・フローが保持される、パスと予約の状態の存続時間を秒数で定義します。この時間は、「allowed successive message loss」パラメーターの値で指定されている最新表示メッセージ紛失の数を RSVP が監視できるだけの十分な長さであることが必要です。この時間の大体の計算には、数式 1.5 x refresh-interval x (allowed-successive-msg-losses + 0.5) を使用します。

予約状態はタイムアウトになったが、パス状態がタイムアウトにならない場合は、予約は廃棄され、IP トラフィック・フローはベストエフォート・サービスで続けられます。パス状態がタイムアウトになった場合は、予約も IP トラフィック・フローも両方とも終了します。

この talk 6 コマンドは、オプションで、他のパラメーターの値に影響を及ぼさずに、即時に動的に有効にできます。このパラメーターの省略時値は、変更しなくても働くはずです。

有効値: 1 ～ 2 147 483 647 秒

省略時値: 158 秒

max-msg-size

このパラメーターでは、ルーター内の総最大 RSVP 制御メッセージ・サイズを定義します。この値は、パス上で RSVP 使用可能インターフェースがサポートする MTU サイズの最小値以下である必要があります。このパラメーターの省略時値は、変更しなくても働くはずです。

有効値:64 ～ 2 147 483 647 バイト (無限を表す)

省略時値: 1500 バイト

refresh-interval

このパラメーターでは、受信側と送信側の間にパスと予約の状態 (RSVP トラフィック・フロー) を保持するために、最新表示メッセージ間で経過する時間間隔を秒数で定義します。

有効値: 10 〜 600 秒

省略時値: 30 秒

slew-max

このパラメーターでは、1 回の最新表示サイクル内で変更できる最新表示間隔を制限します。このパラメーターの省略時値は、変更しなくても働くはずです。ただし、このパラメーターの値を変更して、タイミング・エラーを防ぐ必要がある場合もあります。

例えば、 slew-max が 30% で、最新表示間隔が 30 秒であれば、1 回の最新表示間隔内で最新表示間隔を最大 9 秒 (30 秒の 30%) 変更できます。さらに大幅に変更する場合は、最新表示間隔を再度変更する必要があります。例えば、最新表示間隔が 39 であれば、1 回の最新表示間隔内でこれをプラスまたはマイナス 11 変更できます。また、slew-max の値を大きくしてから変更を行うこともできます。例えば、最新表示間隔が 30 で、これを 50 に変更したいときは、まず最初に slew-max を 70% に上げ (これで 30 をプラスまたはマイナス 21 変更できるようになる)、その上で最新表示間隔を 50 に上げます。

この talk 6 コマンドは、オプションで、他のパラメーターの値に影響を及ぼさずに、即時に動的に有効にできます。

有効値: 0 〜 100%

省略時値: 30%

total すべてのインターフェースのリンク帯域幅を総計すると、合計ルーター・スループットより大きくなる可能性があるため、ルーターの予約可能帯域幅に限度を設定することが必要になる場合があります。例えば、集合リンクの帯域幅の合計が 250 000 000 bps に達するのに対して、合計ルーター・スループットは 200 000 000 bps という場合がありえます。合計予約可能帯域幅が 200 000 000 bps に設定されていて、200 000 000 bps がすべてのインターフェースにわたって現在予約されているとすると、一部が廃棄されない限り、これ以上の RSVP IP 予約は確立できません。

この talk 6 コマンドは、オプションで、他のパラメーターの値に影響を及ぼさずに、即時に動的に有効にできます。

有効値: 1 〜 4 294 967 295 bps

省略時値: 4 294 967 295 bps (無限を表す)

RSVP 監視環境にアクセスする

RSVP 監視環境にアクセスする場合は、 OPCON プロンプト (*) で **t 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで次のようにコマンドを入力します。

```
+ protocol rsvp
RSVP>
```

RSVP 監視コマンド

この節では、RSVP 監視コマンドについて説明します。コマンドは、 RSVP> プロンプトで入力します。

表 28. RSVP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Activate	静的に定義された送信側や受信側を起動します。
List	RSVP 情報を一覧表示します。
Reset	RSVP と RSVP の特性を動的にリセットします。
Send	*data-packet*、*ip ping*、*path*、 *ptear*、*resv*、*rtear* も含めて、さまざまな RSVP メッセージを送信します。
Show	アクティブ RSVP フローについての情報を表示します。
Stop-RSVP	ルーター内の RSVP 機能を停止します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Activate

構成済みの送信側や受信側を動的に起動する場合は、**activate** コマンドを使用します。

構文 :

activate *record-number*

このコマンドを使用すると、talk 6 **add sender** コマンドと **add receiver** コマンドを使用して定義し、該当する talk 6 **enable** コマンドを使用して使用可能にした送信側や受信側が動的に起動できます。

record-number

activate コマンドを使用すると、現在使用可能になっている構成済みの送信側と受信側が表示され、それぞれはレコード番号で識別されます。そこでレコード番号を指定すると、その受信側なり送信側なりが動的に起動されます。起動されている送信側や受信側は、**send ptear**、 **send rtear**、または **reset rsvp** コマンドを発行するか、ルーターを再始動して、talk 5 で停止できます。

静的送信側と静的受信側の構成方法を確認するために、 457ページの『RSVP 構成コマンド』 を参照して、 talk 6 **add sender**、**add receiver**、**enable** の各コマンドの説明をご覧ください。

List

稼働中の RSVP の構成について情報を表示させる場合は、 **list** コマンドを使用します。

注: 既存の RSVP トラフィック・フローを表示させて見る場合は、 talk 5 **show rsvp flow** コマンドを使用します。

構文 :

list interface

opwa

sender/receiver-records-in-sram

system

interface

このコマンドでは、RSVP インターフェースとその現在の状況が表示されます。状態 *bwCtrl* では、RSVP 帯域幅制御下にあるリンクを指示し、帯域幅がこのインターフェース上で RSVP QOS 用として予約できます。状態 *notCnf* では、 RSVP 用として構成されていないリンクを示します。

例 :

```
RSVP> list int

RSVP Interfaces:

If      IP address      b/w(K)  res'able  curr-res     state
0/Eth   5.0.27.2        10000   5000      0      Kbps  bwCtrl
2/PPP   5.0.45.2        0       1024      0      Kbps  notCnf
4/PPP   5.0.25.101      2048    1024      0      Kbps  bwCtrl
5/TKR   5.0.28.2        16000   8000      0      Kbps  bwCtrl
```

opwa このコマンドでは、RSVP インターフェースとその現在の OPWA 状況が表示されます。

例 :

```
RSVP>list opwa

OPWA running configuration
Network OPWA    CTL-LOAD
0       Y       Y
2       Y       Y
4       Y       Y
5       Y       Y
```

sender/receiver-records-in-sram

このコマンドでは、静的に構成された送信側と受信側の一覧表が表示されます。

例 :

```
RSVP> list sender

Following senders/receivers are defined in SRAM:
Rec.No   Type     DestAddr       Dest Port   Protocol   Src Addr        Src Port
1    Sender(PATH) 5.0.25.100      25         17         5.0.25.101      25
2    Receiv(RESV) 5.0.25.101      26         17         0.0.0.0         0
3    Receiv(RESV) 5.0.25.101      5006       17         0.0.0.0         0
```

system

このコマンドでは、RSVP システム・パラメーターの現在の実行値が表示されます。これらの値は、talk 5 のコマンドを使用して動的に変更されているものがあれば、SRAM 内の値とは異なります。

例 :

```
RSVP> list system

RSVP running configuration:
RSVP Status:                  Running
Current Existing Flows:       0
Current Existing Sessions:    0
Maximum RSVP Msg Size:        1500 (bytes)
Refresh Interval:             30 (sec)
Allowed Successive Msg Loss:  3 (frame)
Flow Life-Time:               158 (sec)
Refresh Slew Max:             30 (percent)
System resv Max:              unlimited
System current resv:          0 (kbps)
```

Reset

RSVP 構成のさまざまな性質をリセットする場合は、**reset** コマンドを使用します。**reset** コマンドでは、talk 5 を使用して動的に構成されたパラメーターがあればすべて上書きし、 talk 6 を使用して構成された最新の値を置き換えます。

構文 :

reset interface

queue-stat

rsvp

system-parameters

interface

SRAM に保管されている構成データで RSVP インターフェース・パラメーターを更新します。コマンドではプロンプトでインターフェース番号の入力を指示します。

このインターフェースでの予約は、次回の PATH と RESV の最新表示時に、資源の可用性に応じて、失われた上で再確立されます。予約によっては、帯域幅など、予約の更新に必要な資源が使用不能になっているため、失われてしまう恐れもあります。

queue-stat

RSVP 用として構成されているインターフェースすべてでフロー制御待ち行列がクリアされます。

rsvp ルーター上の RSVP を停止し、SRAM 内で使用可能になっていれば、RSVP を再始動します。

RSVP が停止すると、ルーター上の PATH メッセージと RESV メッセージはすべて終結処理されます。 RSVP が再始動すると、予約は、次回の PATH と RESV の最新表示時に、資源の可用性に応じて、再始動します。予約によっては、帯域幅など、予約の更新に必要な資源が使用不能になっているため、失われてしまう恐れもあります。

system-parameters

talk 6 で作成され、SRAM に保管されている構成データで、 RSVP システ

ム・パラメーターを更新します。RSVP システム・パラメーターは、 talk 6 **set** コマンドを使用して設定されるものです。

Send

IP PING メッセージと RSVP メッセージを動的に送信する場合は、 **send** コマンドを使用します。

構文 :

send data-packet
ip-ping
path
ptear
resv
rtear

data-packet

定義された IP フローでテスト・データを送信するためのコマンドです。ルーターの速度と資源の制限に応じて、毎秒複数のパケットが送信できます。10 番目のパケットが送信される度に、メッセージが表示されます。

例 :

```
RSVP>send data
IP Dest Address: [0.0.0.0]? 5.0.25.100
Destination UDP port: [1]? 100
IP Srce Address: [5.0.25.101]? 1
Source UDP port: [1]? 100
Number of pings per second: [1]?
UDP packet length: [56]?
RSVP send data 1 to 5.0.25.100 protocol 17 source port 100 dest port 100.
.........RSVP send data 11 to 5.0.25.100 protocol 17 source port 100 dest port
100.
.........RSVP send data 21 to 5.0.25.100 protocol 17 source port 100 dest port
100.
RSVP>
```

1 この IP フローを送信するルーターの IP アドレスです。

ip-ping

IP PING (ICMP エコー) メッセージを送信します。*プロトコルの構成と監視解説書 第 1 巻* の 『IP の構成と監視』 の章の **ping** コマンドを参照してください。

path RSVP *path* メッセージを、それ自体のためか、別のホストのプロキシーとしてかどちらかで送信します。このコマンドの入力形式は、 talk 6 **add sender** コマンドの場合と同じです。必要なパラメーターの説明については、 talk 6 **add sender** コマンドを参照してください。

省略時には、これらのメッセージは 30 秒ごとに送信されます。パスは、**send ptear** コマンドを使用して除去するか、RSVP をリセットしない限り、存在しています。

このコマンドでは、構成に送信側を動的に追加できます。talk 2 を使用して、パス最新表示の ELS トレースを表示させて見ることができます。

ptear RSVP *ptear* メッセージを、それ自体のためか、別のホストのプロキシーとしてかどちらかで送信します。**send ptear** コマンドを使用してパスを廃棄する

と、トラフィック・フローも予約も両方とも除去されます。このコマンドではプロンプトが出て、例えば、あて先アドレスと IP セッション・アドレスなど、パスを識別するパラメーターの入力を指示されます。要求されるパラメーターの説明については、talk 6 **add** コマンドを参照してください。

send ptear コマンドで指定されたパス状態が存在している必要があり、存在していなければ、 ELS エラー・メッセージが生成されます。talk 2 を使用して、このコマンドに関連する ELS メッセージを表示させて見ることができます。

resv RSVP *resv* メッセージを、それ自体のためか、別のホストのプロキシーとしてかどちらかで送信します。このコマンドではプロンプトが出て、例えば、あて先アドレスと IP セッション・アドレスなど、パスを識別するパラメーターの入力を指示されます。要求されるパラメーターの説明については、talk 6 **add** コマンドを参照してください。talk 2 を使用して、このコマンドに関連する ELS メッセージを表示させて見ることができます。これらのトレース・メッセージを表示させて見る場合は、talk 6 と talk 5 のどちらかのプロンプトでこれらのコマンドを使用して、メッセージを使用可能にする必要があります。

例 :

```
Config>event
ELS config>disp sub rsvp all
```

RSVP セッションを設定していない受信側にこのコマンドを試みると、`Inputting session does not exist` というメッセージが表示されます。既存の RSVP フローの表示には、 **show rsvp flow** コマンドを使用します。

例 :

```
RSVP>send resv
RESV requestor IP Address: [0.0.0.0]? 5.0.25.101
Session > IP Address: [5.0.25.101]?
Session > Port Number: [1]? 201
Session> Protocol Type (UDP/TCP): [UDP]?
Inputting session does not exist.
RSVP>
RSVP>show rsvp flow

Number of flows:        1

Num To (Session)    From            Prot DPrt  SPrt In-If Out-If Rsvd Nhop's
-------------------------------------------------------------------------------
1   5.0.25.101      5.0.25.100      UDP  26    26    4     6      N    0
RSVP>
RSVP>send resv
RESV requestor IP Address: [0.0.0.0]? 5.0.25.101 1
Session > IP Address: [5.0.25.101]? 2
Session > Port Number: [1]? 26
Session> Protocol Type (UDP/TCP): [UDP]?
Style> (WF, FF, SE): [FF]?
Need confirmation?(Yes or [No]):
Service Type: CTL-LOAD
Tspec> Peak Rate (in byte/sec) [250000]? 25000
Tspec> Average Rate (in byte/sec) [200000]? 20000
Tspec> Burst Size (in bytes) [2000]?
Tspec> Max. Pkt Size [1500]?
Tspec> Min Pkt Size [53]?

Existing Filters:
Filter 1 (sender-address : sender-port):  5.0.25.100:26

Make reservation to all senders?(Yes or [No]): Y
A new RESV message will be sent from 5.0.25.101:26 to 5.0.25.100:26
RESV message sent
RSVP>
RSVP>sh r flow

Number of flows:        1
```

```
Num To (Session)    From            Prot DPrt  SPrt In-If Out-If Rsvd Nhop's
------------------------------------------------------------------------------
1   5.0.25.101      5.0.25.100      UDP  26    26    4     6      Y 3    0
RSVP>

*t 2 4
43:56:28 RSVP.074: Send RESV refresh for session 5.0.25.101:26
43:56:28 RSVP.073: --RSVP send IP pkt to 5.0.25.100 on net 4, return code=0
```

1 リクエスターのアドレスは、IP ユニキャスト・アドレスである必要があります。

2 IP セッション・アドレスは、セッションのあて先アドレスであり、受信側の IP ユニキャスト・アドレスでも、受信側がメンバーになっているマルチキャスト・グループの IP マルチキャスト・アドレスでも構いません。

3 予約が行われた後は、フロー項目の *Rsvd* (予約済み) フィールドが N (No) から Y (Yes) に変わっています。この値が N では、フローは存在しますが、予約はありません。フローは、ベストエフォート QOS を使用して送信されています。

4 talk 2 ELS トレースによって、省略時に 30 秒ごとに送信されている予約最新表示メッセージが表示されます。

rtear RSVP *rsvtear* メッセージを、それ自体のためか、別のホストのプロキシーとしてかどちらかで送信します。このコマンドでは、 RSVP トラフィック・フローは切断されますが、送信側からのパスは廃棄されないので、IP トラフィック・フローはベストエフォート QOS で続けられます。このコマンドではプロンプトが出て、例えば、IP 受信側のあて先アドレスと IP セッション・アドレスなど、RSVP トラフィック・フローを識別するパラメーターの入力を指示されます。要求されるパラメーターの説明については、 talk 6 **add** コマンドを参照してください。

send rtear コマンドで指定された IP トラフィック・フローが存在している必要があり、存在していなければ、ELS エラー・メッセージが生成されます。talk 2 を使用して、このコマンドに関連する ELS メッセージを表示させて見ることができます。

Show

RSVP のさまざまな性質を表示させる場合は、**show** コマンドを使用します。

構文 :

show
- adspec
- classifier
- queue
- rsvp
  - flows
  - senders
  - sessions
  - reservations
  - requests

vc

adspec
すべてのフローの公示仕様 (adspec) を表示します。Adspec は OPWA の出力で、アクティブ RSVP セッション・パス上のすべてのリンクでそれぞれ予約されている資源についての情報が一覧表示されます。

classifier
パケット分類子の現行項目すべてが表示されます。

queue RSVP のソフトウェア待ち行列についての現行統計が表示されます。この対象になるのは、非 ATM リンクだけです。

rsvp 現行 RSVP 接続状況のさまざまな性質が表示されます。

flows アクティブ RSVP トラフィック・フローが表示されます。このコマンドの例については、talk 5 **send resv** コマンドの項の例を参照してください。

senders
RSVP 送信側が表示されます。送信側は構成されても、必ずしも起動されているとは限りません。

sessions
RSVP セッションが、フローを予約しているアクティブ・セッションと、存在していても現時点では予約のない非アクティブ・セッションの両方とも表示されます。

reservations
RSVP 予約が表示されます。

requests
RSVP 要求が表示されます。

vc 現在確立されていて、RSVP で予約されている ATM SVC が表示されます。

Stop-RSVP

ルーター内の RSVP を停止する場合は、 **stop-rsvp** コマンドを使用します。

構文 :

stop rsvp

第23章 SNMP の使用

この章では、SNMP 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。

- 『ネットワーク管理』
- 『SNMP 管理』

ネットワーク管理

ネットワーク管理については、*Planning and Setup Guide*を参照してください。

SNMP 管理

サーバーは、IBM NetView (AIX 用) および Nways Campus Manager プロダクトなど、ネットワーク管理プラットフォームおよびアプリケーションにつながるシンプル・ネットワーク・マネージメント・プロトコル (SNMP) インターフェースを提供します。

SNMP は、IP ネットワーク内での IP ホストの監視および管理に使用され、SNMP エージェントと呼ばれるソフトウェアを使用してネットワーク・ホストがサーバーの稼動パラメーターのいくつかを読み取って修正できるようにします。このようにして、SNMP は、IP コミュニティー用のネットワーク管理を確立します。

サーバー用に SNMP を構成する際には、次の点を考慮する必要があります。

コミュニティー
コミュニティーは、SNMP エージェントの管理情報ベース (MIB) 内の情報にアクセスすることを許されている SNMP 管理ステーションの IP アドレスをユーザーが定義できるようにします。MIB にアクセスする際に使用するためにコミュニティー名を定義してください。

認証 コミュニティー名は、無許可ユーザーが SNMP エージェントに関する情報を学習したり、その特性を修正したりできないようにするための認証方式として使用されます。

この方式では、1 つまたは複数の MIB データのセット (MIB ビューといいます) を定義し、アクセス権 (読み取り専用、読み取り/書き込み)、IP マスク、およびコミュニティー名を各 MIB ビューと関連付けることが必要です。IP マスクは、与えられた MIB ビューについてのアクセス要求を発信できる IP アドレスを設定し、コミュニティー名は、SNMP 要求が突き合わせなければならないパスワードとして機能します。コミュニティー名は、各 SNMP メッセージに組み込まれ、IBM 2210 SNMP エージェントによって検査されます。SNMP 要求は、正しいコミュニティー名を提供しない場合、IP マスクに一致しない場合、または割り当てられたアクセス権と矛盾するアクセスを試みた場合には拒否されます。

SNMP パスワード
snmp パスワードは、認証機能のユーザー・プロファイル・セクション内のパスワードまたは暗号化キーなどのセキュリティー上重要な MIB オブジェクト

の暗号化および認証に使用されます。SNMP パスワードをゼロ長のストリングに設定すると、セキュリティー上重要なデータはアクセスできないことが指示されます。SNMP パスワードを *clear* に設定した場合、データは、暗号化なしで SNMP でアクセスできます。 SNMP パスワードがそれ以外のストリングに設定されているときは、データは、 SNMP パスワードから派生したキーの使用による暗号化と認証によって検索できます。詳細については、MIB 定義を参照してください。

MIB サポート

MIB とは、管理情報へのアクセスが得られるバーチャル情報ストアのことです。 この情報は、ネットワーク管理ツールを使用してアクセスすることができ、場合によっては修正することもできる MIB オブジェクトとして定義されています。

IBM 2210 は、資源の監視および管理のために、標準 MIB およびエンタープライズ特定 MIB の包括的なセットを提供します。

次の WWW の URL の該当するリリース・ディレクトリーにアクセスすることにより、IBM 2210 MIB サポートについて記している readme ファイルが見つかります。

- **ftp://ftp.nways.raleigh.ibm.com/pub/netmgmt/2210/**

特定の MIB のコピーを受信するには、MIB の名前と一緒に **get** コマンドを入力します。例えば、**get ibm2210.mib** と入力します。このコマンドを使用すると、FTP サーバーへの接続元として使用したディレクトリー内に指定された MIB のコピーが入ります。

ftp サイトから、次の情報にアクセスできます。

- 標準 MIB
- エンタープライズ MIB
- SNMP 汎用トラップ
- エンタープライズ特定 MIB
- 設定可能な値

設定可能な値の場合を除き、サポートされている MIB 属性はすべて「読み取り専用」モードになっています。

トラップ・メッセージ

トラップ・メッセージとは、ルーター 再ロードまたはネットワーク障害など、ルーター またはネットワーク条件に応じて ルーター 内の SNMP エージェントから SNMP 管理プログラムまで送信された非送信請求メッセージです。

第24章 SNMP の構成と監視

この章では、SNMP の構成と監視コマンドについて説明します。この章には次の節が含まれています。

SNMP 構成環境へのアクセス

SNMP 構成環境へアクセスするには、Config> プロンプトで次のコマンドを入力します。

```
Config> protocol snmp
SNMP user configuring
SNMP Config>
```

SNMP 構成コマンド

この節では、SNMP 構成コマンドについて説明します。

表29 は、SNMP 構成コマンドをリストしています。SNMP 構成コマンドにより、SNMP エージェントとネットワーク管理ステーションの関係を定義するパラメーターを指定することができます。指定した情報は、IBM 2210 を再始動または再ロードした直後に有効になります。

SNMP 構成コマンドは、SNMP Config>プロンプトに入力してください。

表 29. SNMP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。xxxiiiページの『ヘルプの入手』 を参照してください。
Add	SNMP コミュニティーのリストにコミュニティーを追加するか、コミュニティーにマスク付きの IP アドレスを追加するか、または MIB ビューにサブツリーを追加します。
Delete	SNMP コミュニティーのリストからコミュニティーを除去するか、コミュニティーからマスク付きの IP アドレスを除去するか、または MIB ビューからサブツリーを除去します。
Enable/Disable	指定されたコミュニティーに関連する SNMP プロトコルおよびトラップを使用可能/使用不能にします。
List	現行のコミュニティーをそれらに関連するアクセス・モード、使用可能トラップ、IP アドレス、およびビューとともに表示します。すべてのビューおよびそれらに関連した MIB サブツリーも表示します。

表 29. SNMP 構成コマンドの要約 (続き)

コマンド	機能
Set	コミュニティーのアクセス・モードまたはビューを設定します。コミュニティーのアクセス・モードは次のうち 1 つです。 読み取りおよびトラップ生成 読み取り、書き込み、およびトラップ生成 トラップ生成のみ このコマンドは、トラップ UDP ポートの設定や、セキュリティー上重要なデータの暗号化および認証にも使用されます。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

表 30. SNMP 構成コマンド・オプションの要約

コマンド	パラメーター 1	パラメーター 2	パラメーター 3	パラメーター 4	省略時値
add	community	<comm_name>			None
	address	<comm_name>	<ipAddress>	<ipMask>	
	sub_tree	<view_text_name>	<oid>		
delete	community	<comm_name>			
	address	<comm_name>	<ipAddress>	<ipMask>	
	sub_tree	<view_text_name>	<oid>		
disable	snmp				
	trap	all	<comm_name>		
		cold_start	<comm_name>		
		warm_start	<comm_name>		
		link_down	<comm_name>		
		link_up	<comm_name>		
		auth_fail	<comm_name>		
		enterprise	<comm_name>		
enable	snmp				
	trap	all	<comm_name>		
		cold_start	<comm_name>		
		warm_start	<comm_name>		
		link_down	<comm_name>		
		link_up	<comm_name>		
		auth_fail	<comm_name>		
		enterprise	<comm_name>		
list	all				
	community	access			access
		traps			
		address			255.255.255.255
		view			all
	views				
set	community	access	read_trap	<comm_name>	
			write_read_trap	<comm_name>	
			trap_only	<comm_name>	

表 30. SNMP 構成コマンド・オプションの要約 (続き)

コマンド	パラメーター 1	パラメーター 2	パラメーター 3	パラメーター 4	省略時値
		view	<community>	all <view_text_name>	all
	trap_port password	<udpPort#>			
exit					

Add

add コマンドは、SNMP コミュニティーのリストにコミュニティー名を追加するか、コミュニティーにアドレスを追加するか、またはビューに MIB (サブツリー) の一部を割り当てるのに使用します。

構文:

add community
address
sub_tree

community

add community コマンドは、コミュニティーを作成するのに使用します。コミュニティーは、read_trap の省略時アクセス、すべてのビュー、すべてのトラップを使用不能およびすべての IP アドレスを許容を指定して作成されます。

注: add community コマンドでは、もはやアクセス・タイプまたはトラップ制御を選択することはできません。 既存の SNMP コミュニティーにアクセス・タイプを割り当てるには、set community access コマンドを使用し、トラップ制御では、 **enable trap** コマンドまたは **disable trap** コマンドを使用します。

community name パラメーターは、SNMP クライアントが使用するコミュニティー名を提供します。このコミュニティー名は、Community IP address パラメーターによって指定されたホストから装置内の管理情報ベース (MIB) にアクセスする際に使用されます。

有効値: 1 ～ 31 個の英数字からなるストリング。スペース、タブ、または <ESC> キー・シーケンスといった文字は受け入れられません。

省略時値: public

例: add community <community_name>

```
Community Name []?
```

Community Name　コミュニティーの名前 (最大 32 可視文字) を指定します。スペース、タブ、または <esc> キー・シーケンスといった文字は受け入れられません。

address

このボックスとの通信ができるようにする必要があるネットワーク内のネットワーク管理ステーションのアドレスをコミュニティー定義に追加するに

は、**add address** コマンドを使用します。 コミュニティーの名前およびネットワーク・アドレス (標準 a.b.c.d 表記による) を指定する必要があります。また、ネットマスクを指定して、個別ホスト (マスク = 255.255.255.255) とホストのネットワークのどちらかへのアクセスを制限することもできます。 2 つ以上のアドレスをコミュニティーに追加することができます。ただし、別のアドレスを追加したい場合は、その度にコマンドを入力します。

コミュニティーのアドレスを指定しなかった場合は、要求はどのホストからでも扱われます。

アドレスは、トラップを受信するホストも指定します。 アドレスが指定されない場合は、トラップは生成されません。

1. *community name* は、次の値をもちます。

   有効値: 1 〜 32 個の英数字からなるストリング。スペース、タブ、または <ESC> キー・シーケンスといった文字は受け入れられません。

   省略時値: なし

2. *IP address* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

3. また、*net mask* を指定して、個別ホスト (マスク = 255.255.255.255) とホストのネットワークのどちらかへのアクセスを制限することもできます。

   有効値: 0.0.0.0 〜 255.255.255.255

   省略時値: なし

例: add address <community_name> <ipAddress> <ipMask>

```
Community Name  []?
New Address [0.0.0.0]?
```

sub_tree

add sub_tree コマンドは、ビューに MIB の部分を追加したり、新しいビューを作成するのに使用します。省略時値は MIB 全体です。MIB ビューの管理には、**add sub_tree** コマンドを使用してください。<view_text_name> によって定義されたビューには複数のサブツリーを追加できます。新しい MIB ビューを作成するには、新しいビュー名を指定した **add sub_tree** コマンドを出してください。

注: ビューを有効にさせるには、**set community view** コマンドを使用して 1 つまたは複数のコミュニティーにビューを割り当てる必要があります。サブツリー定義は包括的です。つまり、指定されたサブツリー OID、および指定された OID より辞書編集上大きい OID はすべて、MIB ビューの一部とみなされます。

有効値:

- All - 指定されたコミュニティーにサポートされているすべての MIB ビューを割り当てます。
- View - 指定されたコミュニティーに指定の MIB ビューを割り当てます。

省略時値: All

MIB OID name は、sub_tree 用の MIB オブジェクト ID を指定するパラメーターです。これは、記号値ではなく、数値として入力する必要があります。

このパラメーターには、View name パラメーターで定義されたビュー内に組み込まれている MIB サブツリー名を入れます。指定された MIB サブツリーの子もすべて、ビューに組み込まれます。

例えば、MIB-II 内のシステム・グループへアクセスできるようにするビューを提供するためには、**1.3.6.1.2.1.1** を指定してください。

有効値:

<element1>.<element2>.<element3>... という形式のオブジェクト識別子。ここでは、次のようにします。

- 少なくとも 3 つの要素が必要です。
- 最大 49 個の要素を定義できます。
- element1 は 0、1、または 2 です。
- element2 は、1 ～ 40 の範囲の整数です。
- element3 およびそれ以降の要素は、1 から、符号なしバイト整数のサイズまでの整数です。

省略時値: なし

例: add sub_tree

```
View Name  []?
MIB OID name []?
```

View Name　ビューの名前 (最大 32 可視文字) を指定します。スペース、タブ、または <Esc> のキー・シーケンスのような文字は受け入れられません。

MIB OID　sub_tree 用の MIB オブジェクト ID を指定します。これは、記号値ではなく、小数点表記法による数値として入力する必要があります。

Delete

delete コマンドは、次のものを削除するのに使用します。

- 特定のアドレス
- コミュニティーおよびそのアドレスをすべて
- ビューからのサブツリー

構文:

delete　community
　　address
　　sub_tree

community

コミュニティーおよびその IP アドレスを除去します。コミュニティー名を提供する必要があります。

community name は、次の値をもちます。

有効値: 1 ～ 31 個の英数字からなるストリングスペース、タブ、または <ESC> キー・シーケンスといった文字は受け入れられません。

省略時値: public

このパラメーターは、SNMP クライアントが使用するコミュニティー名を提供します。このコミュニティー名は、Community IP address パラメーターによって指定されたホストから装置内の管理情報ベース (MIB) にアクセスする際に使用されます。

例: delete community <community_name>

address

コミュニティーからアドレスを除去します。 名前を提供する必要があります。

1. *community name* は、次の値をもちます。

   有効値: 1 〜 31 個の英数字からなるストリング。スペース、タブ、または <ESC> キー・シーケンスといった文字は受け入れられません。

   省略時値: public

   このパラメーターは、SNMP クライアントが使用するコミュニティー名を提供します。このコミュニティー名は、Community IP address パラメーターによって指定されたホストから装置内の管理情報ベース (MIB) にアクセスする際に使用されます。

2. *IP address* は、次の値をもちます。

   有効値: 任意の有効な IP アドレス

   省略時値: なし

3. また、*net mask* を指定して、個別ホスト (マスク = 255.255.255.255) とホストのネットワークのどちらかへのアクセスを制限することもできます。

   有効値: 0.0.0.0 〜 255.255.255.255

   省略時値: なし

例: delete address <comm_name> <ipAddress> <ipMask>

sub_tree

ビューから MIB または MIB の部分を除去します。 サブツリーの名前を提供する必要があります。 すべてのサブツリーが削除されると、MIB ビューも削除され、それについてのすべての参照が任意の関連する SNMP コミュニティーから除去されます。

1. 除去される*view name* (ビュー名) は、Community name パラメーターに定義されたコミュニティーが使用するビューを選択できるようにするパラメーターです。このビューは、このコミュニティーがアクセスできる MIB オブジェクトを判別します。ビューが指定されないと、コミュニティーは、ルーターの SNMP エージェントが認識しているすべてのオブジェクトにアクセスすることができます。

   コミュニティーがルーターの SNMP エージェントが管理する MIB 全体にアクセスできないようにすることに決めた場合には、このパラメーターを指定してください。

   このパラメーターは、View name パラメーターおよび MIB Subtree パラメーターを構成してからでないと、構成できません。

   有効値:

– All - 指定されたコミュニティーにサポートされているすべての MIB ビューを割り当てます。
– View - 指定されたコミュニティーに指定の MIB ビューを割り当てます。

省略時値: All

2. *MIB OID name* は、sub_tree 用の MIB オブジェクト ID を指定するパラメーターです。これは、記号値ではなく、数値として入力する必要があります。

このパラメーターには、View name パラメーターで定義されたビュー内に組み込まれている MIB サブツリー名を入れます。指定された MIB サブツリーの子もすべて、ビューに組み込まれます。

例えば、MIB-II 内のシステム・グループへアクセスできるようにするビューを提供するためには、**1.3.6.1.2.1.1** を指定してください。

有効値:

<element1>.<element2>.<element3>... という形式のオブジェクト識別子。ここでは、次のようにします。

– 少なくとも 3 つの要素が必要です。
– 最大 49 個の要素を定義できます。
– element1 は 0、1、または 2 です。
– element2 は、1 ～ 40 の範囲の整数です。
– element3 およびそれ以降の要素は、1 から、符号なしバイト整数のサイズまでの整数です。

省略時値: なし

例: `delete sub_tree <view_text_name> <oid>`

Disable

disable コマンドは、ルーター上で SNMP プロトコルまたは指定されたトラップを使用不能にするのに使用します。

構文:

disable snmp
trap

snmp SNMP を使用不能にします。

community name は、次の値をもちます。

有効値: 1 ～ 31 個の英数字からなるストリング。スペース、タブ、または <ESC> キー・シーケンスといった文字は受け入れられません。

省略時値: public

例: `disable snmp`

trap 指定されたトラップまたはすべてのトラップを使用不能にします。 以下のオプションからトラップ・タイプを指定する必要があります。

例: disable trap <trap_type> <community_name>

Trap Type	Description
all	指定されたコミュニティー内のすべてのトラップを使用不能にします。コミュニティー名をコマンド行の一部として指定してください。
cold_start	指定されたコミュニティーでコールド・スタート・トラップを使用不能にします。コールド・スタート・トラップ (0) は、送信ルーターが再初期化中であり、エージェントの構成またはプロトコル・エンティティーの実施を変更できることを意味します。コミュニティー名をコマンド行の一部として指定してください。
warm_start	指定されたコミュニティー内のウォーム・スタート・トラップを使用不能にします。ウォーム・スタート・トラップは、 伝送ルーターは再初期化中であるが、 構成またはプロトコル実装は変わらないことを意味します。コミュニティー名をコマンド行の一部として指定してください。
link_down	指定されたコミュニティー内の link_down トラップを使用不能にします。link_down トラップは、エージェントの構成内にある通信リンクの 1 つに障害が発生していることを認識します。 link_down トラップ -PDU には、影響を受けたリンクの ifIndex インスタンスの名前および値が、その変数バインディングの最初の要素として含まれます。
link_up	指定されたコミュニティー内の link_up トラップを使用不能にします。link_up トラップは、ネットワーク内の前に非アクティブであったリンクが起動状態になったのを認識します。link_up トラップ -PDU には、影響を受けたリンクの ifIndex インスタンスの名前および値が、その変数バインディングの最初の要素として含まれます。
auth_fail	指定されたコミュニティーについて認証障害トラップを使用不能にします。認証障害トラップは、SNMP 要求の送信側がこのボックスの SNMP エージェントに通信する適正な許可をもっていないことを示します。
enterprise	指定されたコミュニティー内のエンタープライズ特定トラップを使用不能にします。エンタープライズ特定トラップは、何らかのエンタープライズ特定事象が発生していることを示します。 特定トラップ・フィールドは発生した特定のトラップを識別します。 例えば、そのように構成されていると、ELS イベント・メッセージがエンタープライズ特定トラップで送信されます。

Enable

enable コマンドは、SNMP プロトコルまたはルーター上の指定トラップを使用可能にするのに使用します。

構文:

enable snmp

trap

snmp SNMP を使用可能にします。

例: enable snmp

trap 指定されたトラップまたはすべてのトラップを使用可能にします。 下に示したオプションからトラップ・タイプを指定する必要があります。

community name は、次の値をもちます。

有効値: 1 ～ 31 個の英数字からなるストリング

スペース、タブ、または <ESC> キー・シーケンスといった文字は受け入れられません。

省略時値: public

例: enable trap <trap_type> <community_name>

トラップのタイプ	説明
all	指定されたコミュニティー内のすべてのトラップを使用可能にします。コミュニティー名をコマンド行の一部として指定してください。
cold_start	指定されたコミュニティー内のコールド・スタート・トラップを使用可能にします。コールド・スタート・トラップ (0) は、送信ルーターが再初期化中であり、エージェントの構成またはプロトコル・エンティティーの実施を変更できることを意味します。コミュニティー名をコマンド行の一部として指定してください。
warm_start	指定されたコミュニティー内のウォーム・スタート・トラップを使用可能にします。ウォーム・スタート・トラップは、 伝送ルーターは再初期化中であるが、 構成またはプロトコル実装は変わらないことを意味します。コミュニティー名をコマンド行の一部として指定してください。
link_down	指定されたコミュニティー内の link_down トラップを使用可能にします。link_down トラップは、エージェントの構成内にある通信リンクの 1 つに障害が発生していることを認識します。 link_down トラップ -PDU には、影響を受けたリンクの ifIndex インスタンスの名前および値が、その変数バインディングの最初の要素として含まれます。
link_up	指定したコミュニティー内の link_up トラップを使用可能にします。link_up トラップは、ネットワーク内の前に非活動であったリンクが起動状態になったことを認識します。link_up トラップ -PDU には、影響のあったリンクの ifIndex インスタンスの名前および値が、その変数バインディングの最初の要素として含まれます。
auth_fail	指定されたコミュニティーについて認証障害トラップを使用可能にします。認証障害トラップは、SNMP 要求の送信側がこのボックスの SNMP エージェントに通信する適正な許可をもっていないことを示します。
enterprise	指定されたコミュニティー内のエンタープライズ特定トラップを使用可能にします。エンタープライズ特定トラップは、何らかのエンタープライズ特定イベントが発生していることを示します。 特定トラップ・フィールドは発生した特定のトラップを識別します。 例えば、そのように構成されていると、ELS イベント・メッセージがエンタープライズ特定トラップで送信されます。

List

list コマンドは、SNMP コミュニティー、アクセス・モード、トラップ、ネットワーク・アドレス、およびビューの現行構成を表示するのに使用します。

構文:

list all
community
views

list all

SNMP コミュニティーの現行構成をアクセス、トラップ、アドレス、およびビューについて表示します。オプションについて詳しくは、**list community** コマンドの説明の項を参照してください。

例: list all

```
SNMP Config>list all

   SNMP is enabled
   Trap UDP port: 162
   SRAM write is enabled

            Community Name                Access
   -------------------------------  -------------------
   oxnard                           Read, Write, Trap
   public                           Read, Trap


           Community Name             IP Address         IP Mask
   -------------------------------  ---------------  ---------------
   oxnard                           1.1.1.2          255.255.255.255
   public                           All              N/A


           Community Name                Enabled Traps
   -------------------------------  -------------------------------
   oxnard                           Link Down, Cold Restart
   public                           None


            Community Name                    View
   -------------------------------  -------------------------------
   oxnard                           mib2
   public                           All

             View Name                       Sub-Tree
   -------------------------------  -------------------------------
   mib2                             1.3.6.1.2

   Password is set. (security data flow encrypted)
```

list community *option*

SNMP コミュニティーの現行属性を表示します。 オプションは、Access、Traps、Address、View です。

オプション	説明
Access	コミュニティーのアクセス・モードを表示します。
Address	コミュニティーのネットワーク・アドレスを表示します。
Traps	コミュニティーについて生成されるトラップのタイプを表示します。
View	コミュニティーの MIB ビューを表示します。

list community access

例: list community access

```
           Community Name   Access
           public           Read, Write, Trap
           oxnard           Read, Trap
```

list community traps

例: list community traps

```
           Community Name   Enabled Traps
           public           Link Down, Cold Restart
           oxnard           NONE
```

list community address

例: list community address

```
Community Name   IP Address    IP Mask
public           All           N/A
oxnard           1.1.1.2       255.255.255.255
```

list community view

例: list community view

```
Community Name   View
public           All
oxnard           mib2
```

list views

指定された SNMP コミュニティーの現行ビューを表示します。

例: list views

```
View Name   Sub-Tree
mib2        1.3.6.1.2.1
```

Set

set コマンドは、コミュニティーに MIB ビューを割り当てたり、SNMP UDP トラップ・ポート番号を設定したり、あるいはコミュニティーのアクセス・モードを設定するのに使用します。

構文:

set community access

community view

trap_port

password

community access

set community access コマンドは、コミュニティーに 3 つのアクセス・タイプの 1 つを割り当てるのに使用します。コミュニティーの名前およびアクセス・タイプを指定する必要があります。

community name は、次の値をもちます。

有効値: 1 ～ 31 個の英数字からなるストリング

スペース、タブ、または <ESC> キー・シーケンスといった文字は受け入れられません。

省略時値: public

例: set community access <options> <comm_name>

オプション	説明
read_trap	指定されたコミュニティーに対する読み取りアクセスおよびトラップ生成を許可します。
write_read_trap	指定されたコミュニティーに対する書き込みおよび読み取りアクセス、およびトラップ生成アクセスを許可します。
trap_only	コミュニティーが使用されるのは、SNMP トラップの送信時だけであることを示します。

community view

set community view コマンドは、コミュニティーに MIB ビューを割り当てるのに使用します。

例: set community view <comm_name> <options>

オプション	説明
all	指定されたコミュニティーについてすべての MIB オブジェクトへのアクセスを可能にします。All は省略時値です。
view_text_name	指定されたコミュニティーに指定 MIB ビューを割り当てます。

trap_port

set trap_port コマンドは、トラップの送信先の UDP ポート番号 (省略時標準ポート 162 以外) を指定するのに使用します。省略時値は標準ポートです。

例: set trap_port <udpport#>

UDP Port Number	標準 UDP ポート以外のユーザー・データグラム・プロトコル・ポートを指定します (省略時値は # 162)。

password

set password コマンドは、MIB に定義されているセキュリティー上重要な MIB オブジェクトの暗号化および認証するためにパスワードを指定する場合に使用します。このパスワードをゼロ長のストリングに設定すると、セキュリティー上重要な MIB オブジェクトのアクセスまたは設定を許可しないことによって最大セキュリティーが提供されます。このパスワードを「clear」に設定すると、データを認証なしで流れるようにすることによって最小限のセキュリティーが与えられます。このパスワードを前述以外のストリングに設定すると、このパスワードで暗号化および認証が行われるセキュリティー上重要な MIB オブジェクトのアクセスおよび設定ができるようになります。

例:

```
(a) setting the password to a string of zero length:

        SNMP Config>set pa
        Password:
        Remove password? (Yes, No): y
        Password is set to NULL. (security data are not accessible)

    (b) setting the password to "clear":

        SNMP Config>set pa
        Password:
        to verify Enter password again:
        Password is set to "clear". (WARNING: security data flow in clear)

    (c) setting the password to "test":
        SNMP Config>set pa
        Password:
        to verify Enter password again:
        Password is set. (security data flow encrypted)
```

SNMPの監視

この節では、SNMP 監視コマンドについて説明します。

SNMP 監視環境へのアクセス

SNMP 監視環境にアクセスするためには、**+** (GWCON) プロンプトに次のコマンドを入力します。

```
+ protocol snmp
SNMP>
```

SNMP 監視コマンド

この節では、SNMP 監視コマンドについて説明します。

表31 は、SNMP 監視コマンドをリストしています。 SNMP 監視コマンドを使用すると、SNMP 構成のパラメーターを表示し、SNMP エージェントに関連するいくつかの統計を表示することができます。

実行時 SNMP パラメーターへの一時的変更は、監視を通じて行うことができます。変更は SNMP エージェントの操作に即時に影響を与えます。一時的変更を永続的にするには、SAVE コマンドを使用してください。元の SNMP 構成を復元する必要がある場合は、REVERT コマンドを使用してください。この機能により、構成を永続的に変更することなく、SNMP エージェントの行動を一時的に変更することができます。一時的変更が有効になるには、SNMP 監視プロセスを EXIT (終了) する必要があります。

SNMP 監視コマンドは、SNMP> プロンプトに入力してください。

表 31. SNMP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。xxxiiiページの『ヘルプの入手』 を参照してください。
Add	SNMP コミュニティーのリストにコミュニティーを追加するか、コミュニティーにマスク付きの IP アドレスを追加するか、または MIB ビューにサブツリーを追加します。
Delete	SNMP コミュニティーのリストからコミュニティーを除去したり、コミュニティーからマスク付きの IP アドレスを除去したり、あるいは MIB ビューからサブツリーを除去します。
Enable/Disable	指定されたコミュニティーに関連する SNMP プロトコルおよびトラップを使用可能/使用不能にします。これらのアクションは、SNMP 構成環境でしか許されません。
List	SNMP コミュニティー、ビュー、アクセス・モード、トラップ、およびネットワーク・アドレスの現行構成を表示します。
Revert	指定された変更を消去し、設定値を永続 SNMP 構成時の値に復元します。
Save	指定された変更を行ってから、SNMP 構成に永続的に保管します。
Set	コミュニティーのアクセス・モードまたはビューを設定します。コミュニティーのアクセス・モードは次のうち 1 つです。 • 読み取りおよびトラップ生成 • 読み取り、書き込み、およびトラップ生成 • トラップ生成のみ トラップ UDP ポートおよびパスワードの設定もできるようにします。追加情報については、488ページを参照してください。
Statistics	SNMP エージェントについて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。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

SNMP コミュニティーのリストにコミュニティー名を追加するか、コミュニティーにアドレスを追加するか、またはビューに MIB (サブツリー) の一部を割り当てる場合は、**add** コマンドを使用します。

add コマンドの使用についての説明は、 479ページの『Add』 を参照してください。

Delete

delete コマンドは、次のものを削除するのに使用します。

- 特定アドレス
- コミュニティーおよびそのすべてのアドレス
- ビューからのサブツリー

delete コマンドについての情報は、481ページの『Delete』を参照してください。

Disable

disable コマンドは、ルーター上で SNMP プロトコルまたは指定されたトラップを使用不能にするのに使用します。 このコマンドは、SNMP 構成環境でしか使用できません。

disable コマンドの使用については、483ページの『Disable』を参照してください。

Enable

enable コマンドは、SNMP プロトコルまたはルーター上の指定トラップを使用可能にするのに使用します。 このコマンドは、SNMP 構成環境でしか使用できません。

enable コマンドの使用については、484ページの『Enable』を参照してください。

List

list コマンドは、SNMP コミュニティー、ビュー、アクセス・モード、トラップ、およびネットワーク・アドレスの現行構成を表示するのに使用します。

構文:

list all

community

views

list all

SNMP コミュニティーの現行構成をアクセス、トラップ、アドレス、およびビューについて表示します。オプションについて詳しくは、**list community** コマンドの説明の項を参照してください。

list コマンドについては、485ページの『List』を参照してください。

list community option

指定された SNMP コミュニティーの現行属性を表示します。オプションは、Access、 Traps、Address、View です。

例: `list community option`

オプション	説明
Access	コミュニティーのアクセス・モードを表示します。
Address	コミュニティーのネットワーク・アドレスを表示します。
Traps	コミュニティーについて生成されるトラップのタイプを表示します。
View	コミュニティーの MIB ビューを表示します。

list community access

例: `list community access`

```
Community Name   Access
public           Read, Write, Trap
oxnard           Read, Trap
```

list community traps

例: `list community traps`

```
Community Name   Enabled Traps
public           Link Down, Cold Restart
oxnard           None
```

list community address

例: `list community address`

```
Community Name   IP Address   IP Mask
public           All          N/A
oxnard           1.1.1.2      255.255.255.255
```

list community view

例: `list community view`

```
Community Name   View
public           All
oxnard           mib2
```

list views

指定された SNMP コミュニティーの現行ビューを表示します。

例: `list views`

```
View Name   Sub-Tree
mib2        1.3.6.1.2.1
```

Revert

revert コマンドは、指定された変更を消去し、設定値を永続 SNMP 構成の値に復元するのに使用します。

Save

save コマンドは、指定された変更を永続的に保管するのに使用します。

Set

set コマンドの使用については、487ページの『Set』を参照してください。

Statistics

statistics コマンドは、SNMP エージェントについての統計を表示するのに使用します。

構文:

statistics

例: statistics

```
SNMP memory in use = 9416
```

第25章 DLSw フィーチャーの使用

本章では、データ・リンク交換 (DLSw) について説明し、データ・リンク交換 (DLSw) プロトコルの実装について解説します。 Config> プロンプトで加えた変更は、ただちに有効にはなりませんが、その後のルーターの再始動時に使用される SRAM 構成に加えられます。一時的だが即時に有効になる構成変更については、564 ページを参照してください。

2210では、システム・ネットワーク体系 (SNA) トラフィックおよびネットワーク基本入出力システム (NetBIOS) トラフィックを異種の広域ネットワーク内に統合することを可能にする、広範囲の機能を提供しています。

以下の節ではユーザーのルーターを DLSw 用に構成する方法を説明します。

- 『DLSw について』
- 496ページの『DLSw フィーチャーを使用する』
- 514ページの『DLSw をセットアップする』
- 520ページの『DLSw 構成の例』

DLSw について

DLSw は、 用の転送機構です。 LLC2、SDLC、および QLLC (X.25 上の SNA) の間のプロトコル変換が可能です。ルーターのブリッジング機能、スイッチ間プロトコル (SSP)、および TCP/IP に基づき、インターネットを介しての SNA トラフィックの信頼性の高いトランスポートを提供します。 DLSw は全部のルーティング機能は提供しませんが、データ・リンク・レイヤーでの交換を提供します。 LLC2 フレームをブリッジングするのではなく、DLSw はデータを TCP フレームにカプセル化し、その結果得られるメッセージを WAN リンクを通じてピア DLSw ルーターに転送して、意図されたエンド・ステーション・アドレスに送達します。

DLSw および ATM

数多くの ATM とフレーム・リレーとの相互作用製品によって、フレーム・リレー装置と ATM 装置の両方から構成されるネットワーク上でトラフィックの通信が可能になります。通常は、フレーム・リレー装置は T1 速度 (1.544 Mbps) で動作します。一方、ATM の速度は、それより 1 桁か 2 桁は高速です。 DLS は、この速度差を調整するという、重要な役割を果たすことができます。

DLS は、SNA トラフィックのブリッジングにおける選択肢の 1 つです。低速 T1 WAN リンクで接続された 2 つの高速構内ネットワークがあり、ブリッジングまたは DLS のどちらにするかを決定するとします。 ブリッジングの望ましくない副次作用は、すべてのブロードキャスト・トラフィックが T1 リンク上を転送されて、貴重な帯域幅を使用してしまうという点です。 一方、DLSw は、セッションをローカルで終端させ、ブロードキャスト・トラフィックには WAN を使用しません。このため、低速 WAN リンクをより有効に使用することができ、性能が向上します。

DLSw の動作

LLC2、SDLC、および QLLC はコネクション型プロトコルです。 DLSw は、これらにルーティング・プロトコルの動的特性を提供し、***しかも*** 終端間の信頼性と、効率的な通信のための制御フィーチャーを保持しています。

ブリッジング・ソリューションの問題

図43 は、WAN リンクを介して LLC2 フレームをブリッジする従来の手法を示しています。 このような従来の手法では、ネットワーク遅延が、WAN の場合は、LAN 上よりもはるかに頻繁に発生します。これらの遅延は、単純なネットワーク輻輳 (ふくそう)、回線速度がより遅いこと、またはその他の要因から生じます。 原因が何であれ、これらの遅延は、セッションがタイムアウトになり、データが意図されたあて先に到達しない確率を高めます。

また、LAN プロトコルは、LLC2 と同様、WAN より著しく短い再送/応答時間を使用します。 したがって、WAN リンクを介しての終端間接続は維持するのがきわめて困難であり、セッション・タイムアウトの確率がはるかに高くなります。

セッション・タイムアウトに加えて、データが WAN を横断している間に遅れると、重要な問題があります。 送信側のステーションは、遅れた (しかし、失われてはいない) データを再度送信することができます。これにより、LLC2 エンド・ステーションは重複するデータを受信することになります。 重複データは、受信側で LLC2 手順の混乱を生じさせることがあり、これは WAN リンクの非効率的使用につながります。

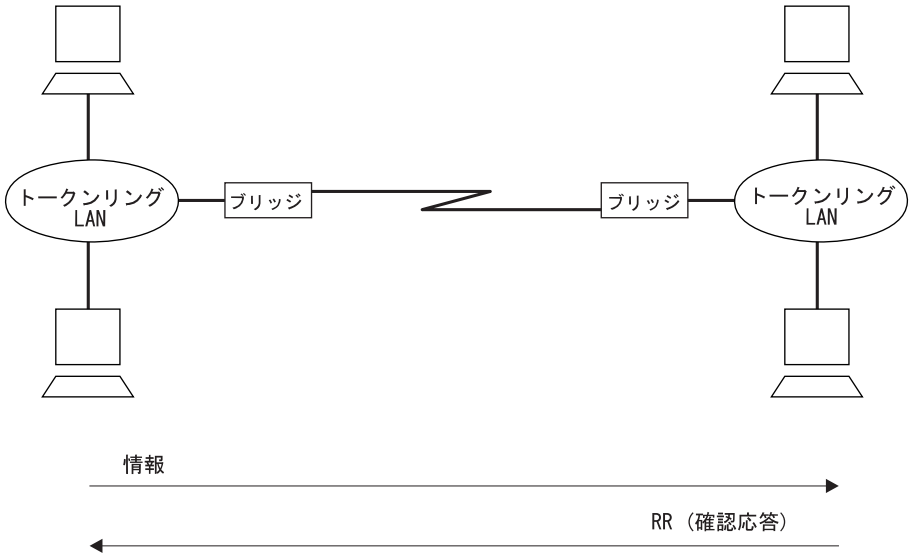


図 43. WAN リンクを介してのブリッジングの従来の手法

上の例は、終端間データ・リンク制御を含む、従来のブリッジングを示しています。 コネクションレス型プロトコルであるため、ブリッジングは、 WAN 上での LLC トラフィックの保全性の保証は行ないません。

プロトコル・スプーフ

セッション・タイムアウトの可能性を減らし、送信ステーションの終端間接続性の状態を維持するため、DLSw はローカル・ルーターで LLC2 接続を終了するか、あるいは『スプーフ』することによって動作します。 LLC2 フレームを受信すると、ルーターは送信側のステーションに確認を送信します。 この確認は、送信側に、前に伝送されたデータが受信されたことを知らせます。

この確認でステーションは再送しないようにします。 この時点以降は、データが到着することを確認するのは DLSw ソフトウェアの責任です。ソフトウェアはデータをルーティング可能な IP フレーム内にカプセル化することによって確認し、DLSw ピアに (TCP を介して) フレームを移送します。ピア DLSw ルーターは TCP ヘッダーをはぎ取り、データの予定された受信側のアドレスを判別し、そのエンド・ステーションとの新しい LLC2 接続を確立します。

図44 は、トークンリング・ネットワーク に接続された、2 つのピア・ルーター間の関係を示しています。

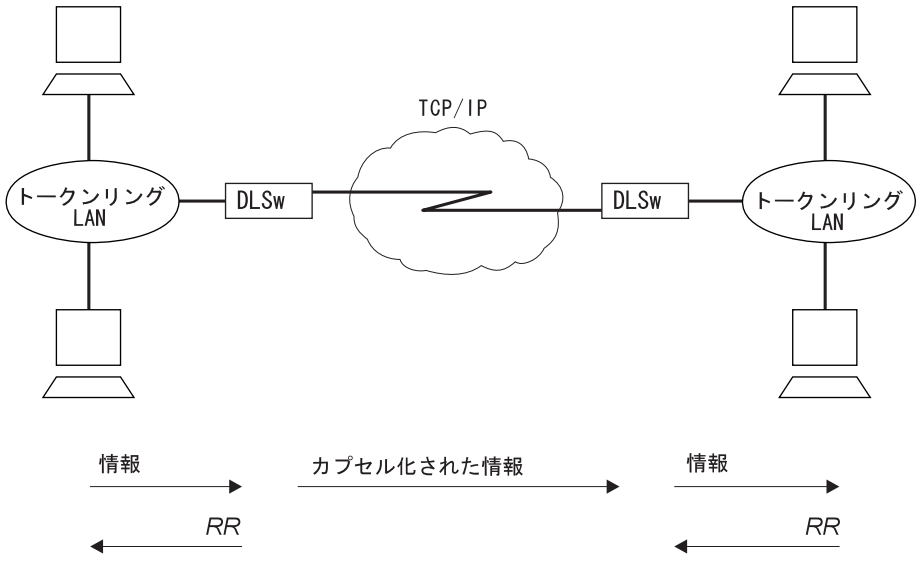


図 44. WAN を通じてのデータ・リンク交換

DLSw はルーターで LLC2 接続を終了します。 つまり、LLC2 接続は広域ネットワークをまたがりません。 これにより、セッション・タイムアウトおよびそうでなければ広域の区域リンクをまたがるであろう確認 (RR) は減少します。

DLSw の利点

DLSw は ローカル装置で DLC 接続を終了するので、(図44 参照)、SNA セッション・タイムアウトをなくし、共有回線での WAN オーバーヘッドを低減するのに、特に効果的です。プロトコルには主に次の利点があります。

- LLC2、SDLC、および QLLC の制御トラフィックをローカル装置で終了させることによって、セッション・タイムアウトの可能性を低減させる。

- 広域にわたって確認 (RR) を伝送する必要をなくすことによって、WAN ネットワーク・オーバーヘッドを削減する。 RR は各 DLSw ルーターにとってローカルな LAN に限定されます。
- DLSw と接続されたエンド・ステーションの間における、フロー制御と輻輳 (ふくそう) 制御、および探索パケットの同報通信制御が得られる。
- ソース・ルート・ブリッジングのホップ・カウントの限界が高くなる。
- LLC2、SDLC、および QLLC の間のプロトコル変換ができる。
- NetBIOS トラフィックをサポートする。

DLSw フィーチャーを使用する

以下の節では、さまざまな DLSw フィーチャーの使用について説明します。

- 『TCP 接続、近隣発見、およびマルチキャスト探索』
- 499ページの『LLC 装置サポート』
- 500ページの『SDLC 装置サポート』
- 504ページの『QLLC 装置サポート』
- 510ページの『APPN インターフェース・サポート』
- 511ページの『近隣優先順位フィーチャーを使用する』
- 512ページの『SNA トラフィックと NetBIOS トラフィックを平衡化する』

TCP 接続、近隣発見、およびマルチキャスト探索

DLSw は TCP を使用して、IP ネットワークを介してのエンド・ユーザー情報の信頼性の高い、順序付けられた送達を提供します。 DLSw メッセージ形式により、複数のエンド・ステーション・セッション、またはサーキットを単一の TCP トランスポート接続を介して搬送することができます。必要なエンド・ステーション接続性を可能にするために DLSw が可能などのルーターがそれらの間で TCP トランスポート接続をもつ必要があるかを構成する方法は 2 通りあります。

- 近隣ルーターの IP アドレスを各ペアのルーターの一方または両方で構成します。これは最も基本的な方式であり、すべての DLSw ルーター・ベンダーによってサポートされています。
- 各ルーターでマルチキャスト・グループ・メンバーシップを構成し、ルーターが相互の IP アドレスを動的に発見できるようにします。これはこの製品の DLSw の特別なフィーチャーで、近隣 IP アドレスを構成する負担を軽減します。

TCP 近隣を構成する

近隣 IP アドレスをルーターで構成するには、ルーターの近隣のそれぞれについて **add tcp** コマンドを一度使用してください。近隣関係にある 2 つのルーターのそれぞれが他方の IP アドレスを構成する必要はありません。1 つのルーターだけが他方のアドレスをもつ必要があり、他方のルーターは、非構成済み近隣からの動的 TCP 接続を受け入れるよう構成することができます。この行動を構成するには、**enable dynamic-neighbors** コマンドを使用し、これらの動的接続に使用されるパラメーターを構成するには、**set dynamic-tcp** コマンドを使用してください。動的 TCP

接続を使用可能にすることは、ハブに接続する新規のリモート事業所のルーターをセットアップするときに再構成したくない 『ハブ』・ルーターの場合に、特に便利です。

IP アドレスだけでなく、**add tcp** コマンドを使用すると、近隣と TCP 接続自体に関する多くのパラメーターが構成できます。 *Keepalive* パラメーターは、ユーザー・データのトラフィックがない場合に、TCP レイヤーがそのピア TCP レイヤーを時々ポーリングするかどうかを制御します。 Keepalive メッセージは、TCP 接続の障害についてよりタイムリーに通知することになりますが、WAN オーバーヘッドを増大させ、正常に再度ルーティングされていたと考えられる障害を報告することもあります。

NetBIOS SessionAlive Spoofing パラメーターは、NetBIOS SessionAlive フレームが DLSw ピアへ転送されるかどうかを制御します。このパラメーターは、ISDN リンク経由で DLSw ピアとの間に NetBIOS セッションを確立している場合に重要です。このパラメーターを使用可能、Keepalive パラメーターを使用不可に設定すると、DLSw ピア間にアイドル状態の NetBIOS セッションが確立されている場合に、DLSw パートナー間に DLSw トラフィックは発生しません。これによって、DLSw 上にアイドル状態の NetBIOS セッションを維持しながら、下層の ISDN 接続を終了させることができます。

connectivity setup type パラメーターは、DLSw が TCP 接続をいつ立ち上げ、ダウンさせるかを制御します。 一方または両方の近隣が CST を *active (能動)* に設定してある場合、DLSw はシステム始動時、およびシステムが立ち上がるまで定期的な間隔でシステムを立ち上げようと試みます。TCP 接続がいったん確立されると、 DLSw は、接続が失敗したときにはそれを元に戻そうとすることにより、接続を常時立ち上がった状態に保持しようとします。 両方の近隣が CST を *passive (受動)* に設定してある場合、DLSw は DLSw エンド・ステーション・セッションを実際に確立する必要がある場合のみ TCP 接続を立ち上げます。最後の DLSw セッションが終了し、構成可能な時間のうちに新規セッションが開始されない (*neighbor inactivity timer (近隣非活動タイマー)*) 場合、DLSw は TCP 接続を切断し、関連する内部資源を解放します。

近隣発見のためにグループを構成する

近隣ルーターの各ペアの一方または両方で近隣 IP アドレスを構成しないで済むように、DLSw をセットアップして、それが接続する必要のある近隣の IP アドレスを発見するために複数のマルチキャスト IP を使用するようにします。 各ルーターで **join-group** コマンドを使用して、ルーターを 1 つまたは複数の DLSw グループのメンバーにし、グループ内での役割を割り当てるようにします。 役割は、『クライアント』、『サーバー』、または 『ピア』 の場合があります。 DLSw はマルチキャスト IP を使用して、同じグループのメンバーであり、補完的な役割をもつすべての DLSw ルーターの IP アドレスを発見します (つまり、クライアントはグループ内のサーバーを発見し、その逆も同様、ピアは他のピアを発見します)。

DLSw は、各グループ内のその近隣の IP アドレスを確認するとき、グループ内のメンバーシップの 『接続性セットアップ・タイプ』 および各グループ近隣のそれを使用して、その近隣への TCP 接続をいつ立ち上げる必要があるかを判別します。 構成済みの個別の近隣の場合と同様に、どちらかの CST が *active* (アクティブ) である場合、DLSw は、発見された近隣への TCP 接続をできるだけ早く立ち上げ、接続を常時立ち上がった状態で保持しようとします。 両方の CST が *passive* (受動) である場

合、DLSw は、DLSw セッションを搬送する必要がある場合のみ TCP 接続を立ち上げ、*neighbor inactivity timer (近隣非活動タイマー)* を使用して、TCP 接続をそれが使用されていないときに切断します。

マルチキャスト探索およびフレーム転送

DLSw はマルチキャスト IP サービスを使用して、近隣ルーターの IP アドレスを発見する以上のことを行います。DLSw は同じサービスを使用して、エンド・ステーション資源 (例えば、MAC アドレスまたは NetBIOS 名) を探索する DLSw メッセージを転送し、NetBIOS データグラム・トラフィックを転送します。このフィーチャーは、DLSw ネットワークのスケーラビリティーを劇的に増大させます。というのは、すべての近隣への静的 TCP 接続は、探索およびデータグラム・メッセージを搬送する必要がないからです。また、DLSw は、各 TCP 接続で各同報通信メッセージの異なるコピーを送信する必要はありませんが、マルチキャスト IP 通信施設内で複写される単一のコピーを送信することができます。

探索およびフレーム転送のためにマルチキャスト IP を使用するには、**join-group** コマンドを出して、*connectivity setup type* を *passive* に設定してください。 DLSw は、他のグループのどのメンバーがマルチキャストが可能か、およびどれが単に近隣 IP アドレスを発見し、静的 TCP 接続を立ち上げるためにグループ・メンバーシップを使用しているかを自動的に判別します。 DLSw は、エンド・ステーション資源を探索し、NetBIOS データグラムを転送し、DLSw セッションを確立するときに、両方のタイプの近隣を同時に処理します。

join-group コマンドを発行する際には、2 つのアドレス指定方式のうちの 1 つを選択して、結合するグループを記述します。 前述したように、グループ ID および client/server/peer 機能を与える際には、ルーターは対応するマルチキャスト IP アドレスを構成し、この方式を使用する他の IBM ルーターと通信することができます。 使用されるマルチキャスト IP アドレスを直接指定し、各アドレスが読み取り、書き込み、またはその両方になることを選択することもできます。この方式を導入したのは、RFC 2166 をサポートし、 DLSw バージョン 2 に準拠する他の製品とのマルチキャスト相互運用性を可能にするためです。

与えられたルーターは、従来のグループのメンバーになり、DLSw バージョン 2 マルチキャスト・アドレスの読み書きを同時に行ないます。新しいマルチキャスト・アドレスも近隣発見に使用できますが、TCP を作成しようとするルーターの各ペアについて、一方のルーターは、他方のルーターが読み取っている書き込み可能アドレスに関して *active* (アクティブ) という *connectivity setup type* (接続性セットアップ・タイプ) をもつようにする必要があります。近隣発見を行っているかどうかに関係なく、マルチキャスト・アドレスを指定する場合は、グループ ID およびクライアント/サーバー/ピア・モデルを使用する場合よりも、さらに注意深い構成計画を行って確実に到達できるようにする必要があります。

エクスプローラー・トラフィックを削減する: DLSw 近隣間を転送されるエクスプローラー・トラフィックの量が非常に多い場合は、このエクスプローラー・トラフィックを削減する機能がいくつかあります。

DLSw オープン SAP
: 各 DLSw は、DLSw 機能交換を通じてその DLSw 近隣につながっているインターフェースでオープンになっているすべての SAP のリストを送信しま

す。DLSw 近隣は、この SAP リストを使用して、この DLSw に送信されるエクスプローラー・トラフィックを制限することができます。

DLSw MAC アドレス・リスト

各 DLSw は、ローカル MAC アドレス・リストを構成できます。このリストは、exclusive (排除) (この DLSw を介してアクセスできるすべての MAC アドレスを表します) または non-exclusive (非排除) (この DLSw を介してアクセスできる MAC アドレスの集合を表します) と定義されます。リスト内の各記入項目には、MAC アドレス・マスクおよび MAC アドレス値が含まれています。MAC アドレス・リスト全体および排除性のタイプは、DLSw 機能交換を通じてすべての DLSw 近隣に送信されます。DLSw 近隣は、この MAC リストを使用して、この DLSw に送信されるエクスプローラー・トラフィックを制限することができます。

MAC アドレス・リストは、NetBIOS 名前リストと同様に作用します。NetBIOS 名前リストについては、158ページの『NetBIOS 名前リスト』を参照してください。

DLSw MAC キャッシュ記入項目

DLSw は、特定の DLSw 近隣をもつ特定の MAC アドレスをマップする個々の MAC キャッシュ記入項目を構成できます。複数の MAC キャッシュ記入項目を使用して、複数の DLSw 近隣をもつ特定の MAC アドレスをマップできます。DLSw は、このリストをローカルで使用して、構成済み MAC アドレスについて構成された DLSw エクスプローラーが送信される先を制限します。

MAC アドレス・フィルター

ブリッジ・ネット・インターフェースについて構成された MAC アドレス・フィルターは、DLSw トラフィックに適用されます。ブリッジ・ネット上にある、これらのインバウンド MAC アドレス・フィルターを使用して、DLSw に与えられるトラフィックを制限できるため、DLSw パートナーに送信されるエクスプローラー・トラフィックを制限できます。MAC フィルターの詳細については、*ソフトウェア使用者の手引き*の『MAC フィルターの使用および構成』 と、『MAC フィルターの監視』を参照してください。

LLC 装置サポート

DLSw は、LAN およびリモート・ブリッジング WAN インターフェースを介してルーターに接続されている SNA および NetBIOS のエンド・ステーションをサポートします。 これらのエンド・ステーションおよびルーターは、両方とも ISO 8802-2 (IEEE 802.2) 標準論理リンク制御 (LLC) を実行して、データの順序付けおよび信頼性のある送達を提供します。 ルーターは現在、次のインターフェース・タイプを介してブリッジされた LLC トラフィックをサポートします。これらのインターフェース・タイプはすべて、DLSw と LLC エンド・ステーション間を流れるトラフィックに使用することができます。

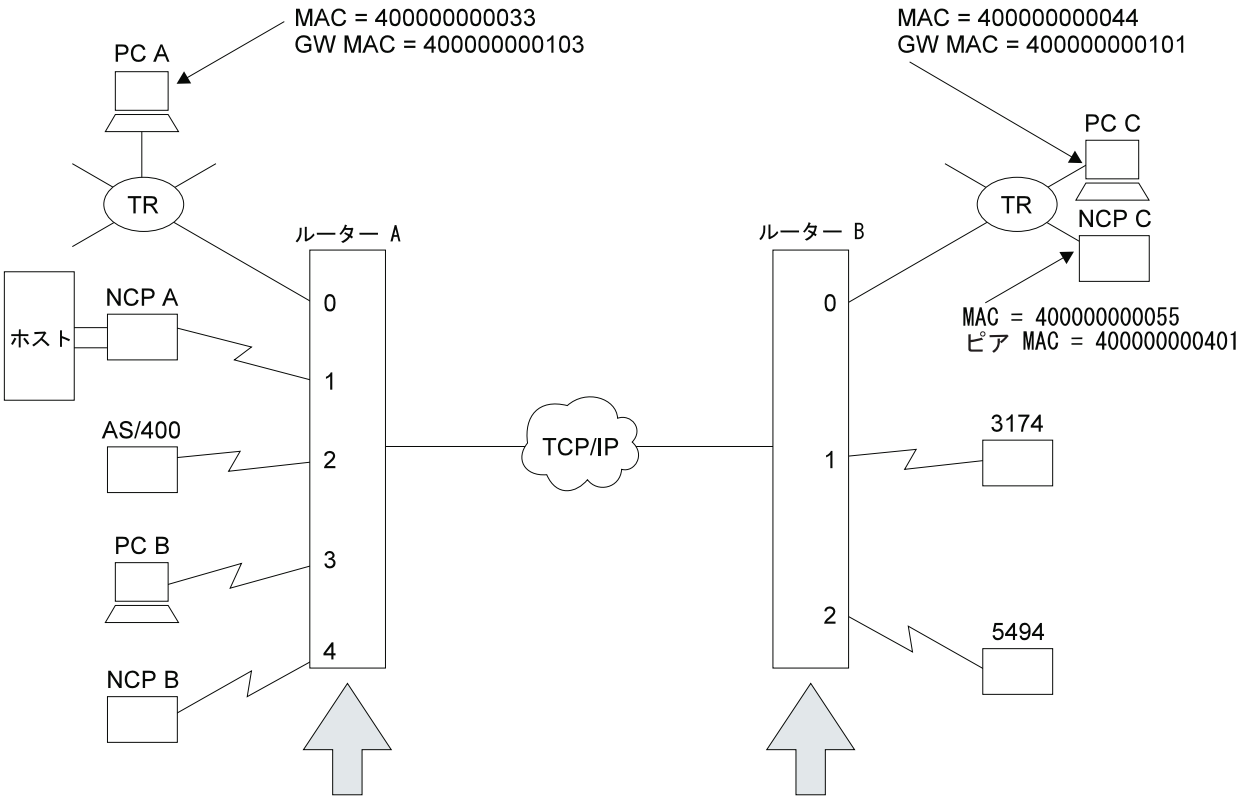
- トークンリング
- イーサネット/802.3
- ATM (LAN エミュレーション・クライアントとして)
- フレーム・リレー (RFC 1490 のブリッジされたフレーム形式を使用)

- PPP
- PPP または FR のフレームを使用するダイヤル・サーキット (例えば、ISDN)

DLSw は、ブリッジされたフレームで使用可能な MAC および SAP アドレスを使用するので、DLSw では個別の LLC エンド・ステーションについての情報は構成する必要がありません。 DLSw は、これらのエンド・ステーションによって送信される同報通信トラフィックを受信し、通常の LAN/ブリッジ同報通信方式を使用して、それらとの初期のコンタクトを行います。 ただし、DLSw が使用する予定のどのインターフェースについてもブリッジング・サポートを構成し、各インターフェース上で使用する SAP を DLSw 内で構成する必要があります。

SDLC 装置サポート

DLSw は SDLC エンド・ステーションをサポートします。これらのステーションは、SNA PU タイプ 2.0、2.1、4 (NCP-NCP トラフィック用)、または 4/5 (SNA 境界機能を実行するホストまたは NCP) にすることができます。ルーターは、SDLC インターフェース用に構成された役割に基づき、または SNA XID 折衝に基づき、基本または 2 次の SDLC リンク・ステーションの役割でサーブすることができます。基本の役割では、ルーターは同じ物理マルチポイント SDLC 回線上で異なる PU タイプの複数の SDLC 装置をサポートすることができます。 2 次の役割では、ルーターは単一の物理 SDLC インターフェース上で複数の SDLC 2 次ステーションを表すことができます。 ルーターは、2 次の役割で IBM 3174 グループ・ポーリング機能もサポートします。



インターフェース	SDLC アドレス	PU タイプ	発信元 MAC	あて先 MAC
1 (2 次)	01	2	400000000101	400000000044
	02	5	400000000102	4011111101C1
	03	5	400000000103	400000000033
	04	2	400000000104	400000000301
2(折衝可能)	01	2	400000000201	4011111102C1
3(折衝可能)	01	2	400000000301	000000000000
4(折衝可能)	01	4	400000000401	400000000055

インターフェース	SDLC アドレス	PU タイプ	発信元 MAC	あて先 MAC
1 (1 次)	C1	2	4011111101C1	000000000000
2(折衝可能)	C1	2	4011111102C1	400000000201

図 45. DLSw SDLC 構成の例

図45 は、DLSw によってサポートされる SDLC 構成のいくつかを図示し、SDLC および DLSw (MAC および SAP) アドレスの間でマップするのに必要な DLSw 構成のサブセットを示しています。図では、*ローカル* (単一のルーター内での) および *リモート* (2 つのルーターおよび IP ネットワークを介した) の両方の DLSw セッションを示しています。

以下の DLSw セッションが構成されます。

- NCP A から PC A、B、および C を経由して、3174 まで

  NCP A がこれらの 4 PU と通信できるようにするには、ルーター A は、各 PU についてインターフェース 1 で構成された 2 次リンク・ステーションをもつ必要があります。 このインターフェースは、SDLC で、2 次、全二重、およびポイントツーポイントとして構成される必要があります。 同じインターフェース上にいくつかの 2 次ステーションがある場合はいつも、非生産的なポーリングを減らすために、グループ・ポーリングをお勧めします。

  この例では、NCP A は、PC C に SDLC ステーション・アドレス 01 を介して、3174 にアドレス 02 を介して、PC A にアドレス 03 を介して、および PC B にアドレス 04 を介して通信します。 PC A および C のセッションは両方とも、そ

れぞれローカルおよびリモート構成で SDLC と LLC 間の変換を伴うことに注意してください。 PC B へのセッションはローカルの SDLC と SDLC 間のセッションです。(通常、これはありません。)

ルーター A で定義された 2 次リンク・ステーションの場合、PU タイプ 5 は、SDLC 装置がダウンストリーム PU2.0 装置に SNA BNN 機能を実行するホスト (ここでは、制御装置がフロントエンドです) であることを示しています。 PU タイプ 2 は、ここでは SDLC ホスト/FEP が DLSw ネットワーク内の別の T2.1 ノードと通信している T2.1 ノードとして働いていることを示しています。

- AS/400 から 5494 へ

  ここでは、これらの装置は T2.1 ノードとして機能し、それぞれのルーター上の SDLC リンクは折衝可能として構成されます (T2.1 ノードは固定した役割のリンクでもサポートされ、DLSw はそれに応じて役割折衝を制限します)。ステーションは、役割判別および SDLC アドレス解決を含む、完全な XID 折衝を実行します (同じリンク上のルーターおよびエンド・ステーションがそれぞれ異なる SDLC ステーション・アドレスを使って構成されている場合)。 リモートの SDLC-SDLC 構成では、2 つの異なる SDLC リンク上で使用される SDLC ステーション・アドレス間の関係はないことに注意してください。 リモートの SDLC と LLC 間のセッションは、T2.1 装置間でもサポートされています。

- NCP B から NCP C へ

  NCP B は PU タイプ 4 として構成され、この DLSw セッションが NCP 間で INN サブエリア・トラフィックは搬送するが、NCP から PU 2 装置へは BNN トラフィックを搬送しないことを示しています。 例ではリモートの SDLC と LLC 間のセッションを示していますが、同じもの同志の間のセッションもサポートされています。 DLSw INN 機能は、マルチリンク TG または NCP リモート・ロード/ダンプ機能はサポートしていません。

アドレス・マッピング

DLSw 構成では、単一バイトの SDLC ステーション・アドレスと、DLSw がそれによってエンド・ステーションを識別する、MAC アドレスおよび SAP の間でのマッピングを提供します。SDLC ステーション用の発信元 MAC アドレスは、残りの DLSw ネットワークへの SDLC 装置を表します。これは、装置から発信するフレームにとっては発信元アドレスであり、装置に着信するフレームにとってはあて先アドレスです。SDLC 装置が DLSw を通じて通信できるようにするためには、発信元 MAC アドレスが必要です。

あて先 MAC アドレスは、この SDLC 装置が通信を開始するときに接続される必要のある DLSw ネットワーク内のエンド・ステーションを指定します。常に新規セッションのターゲットであり、決してイニシエーターではない SDLC 装置は、ゼロのあて先 MAC アドレスをもつ必要があります。ルーターが 2 次リンク・ステーションとして構成される場合は、ホストのコネクト・アウトが成功するようにあて先 MAC アドレスを定義することが重要です。これは、2 次リンク・ステーションはコネクト・インするリモート DLSw エンド・ステーションの代わりにホストへのコンタクトを開始することはできず、ポーリングされるのを待つ必要があるからです。リモート DLSw エンド・ステーションがそれ自体で SDLC であり (例えば、501ページの図45のルーター B 上で 3174)、ローカル 2 次ステーションとペアになっている場合、リモート・ステーションは、ホストのコネクト・アウトへのこの依存性を反映して、ゼロのあて先 MAC アドレスをもっています。

DLSw 構成および SDLC 構成

SDLC インターフェースを介して DLSw を使用するには、DLSw 構成の一部としてアドレス・マッピングを構成し、SDLC 構成の一部としていくらかの情報も構成します。 SDLC では最小限、インターフェースを SDLC として設定し、リンクの役割などの他のインターフェース・レベルのパラメーターを構成する必要があります。SDLC インターフェース・パラメーターでは、インターフェースするすべての SDLC リンク・ステーションについて省略時値を提供しますが、ステーションについて固有の値をもちたい場合は、個別の SDLC ステーション情報を構成することができます。

アドレス・ペアの*インターフェース番号*、*SDLC ステーション・アドレス* は、DLSw のアドレス・マッピング情報を SDLC のステーション・レベル構成にリンクする共通のキーです。 ルーター・ソフトウェアは、初期設定時にこの関連付けを行います。DLSw がリンク・ステーションを初期設定しようとしてその SDLC ステーション・アドレスが DLSw が指定するインターフェース上で SDLC で構成されていない場合、SDLC はリンク・ステーションの定義を動的に作成し、そのインターフェースについて SDLC で定義されているパラメーターの省略時値を使用します。

SDLC リレー機能との関係

SDLC リレーとは、全体の SDLC フレームを IP パケット内にカプセル化するルーター機能です。次に、フレーム全体は同様に SDLC リレーをサポートする別のルーターにルーティングされます。あて先ルーターは IP ヘッダーを取り除いて、SDLC フレームを変更されない状態であて先 SDLC リンクに送達します。

この機能は、DLSw SDLC サポートとは次のように異なっています。

- SDLC リレーでは、ルーター内で稼働している SDLC リンク・ステーションはありません。制御フレーム (例えば、RR) は、IP ネットワークを横切って流れます。DLSw では、ルーターの SDLC サポートが SDLC 接続を終了します。 SDLC フレームからのデータだけが、IP ネットワークを横切って流れます。 その結果、DLSw はよりよい WAN 帯域幅使用率を提供することができ、WAN の遅延によるリンク・タイムアウトに影響されにくくなります。
- SDLC のデータおよび制御フレームは SDLC リレーを通じて透過に渡されるのに対し、DLSw はそれらの一部を解釈し、変更する必要があります。 DLSw が SDLC 接続を終了することに加えて、これは、特定の製品の構成および機能 (例えば、NCP 間のマルチリンク TG) が DLSw によってサポートされていないことを意味します。
- SDLC リレーは、通信する両方のエンド・ステーションのデータ・タイプが SDLC であることを必要とします。 DLSw は、プロトコル変換機能を提供するため、他方のエンド・ステーションのデータ・タイプは、LLC、SDLC、QLLC、および DLSw 製品でサポートされる任意のデータ・タイプでかまいません。
- DLSw は、APPN Implementers Workshop によって開発された標準であり、IETF RFC に文書化されています。 そのため、DLSw は多数のベンダーによってサポートされています。 SDLC リレーは現在、特定の IBM 製品および互換性のあるルーター製品でのみサポートされています。

次の場合には、DLSw を使用する必要があります。

- SDLC から LLC または QLLC へのプロトコル変換が必要な場合
- IP ネットワークの外側で流れる制御トラフィック (例えば、RR フレーム) を制限したい場合

次の場合には、SDLC リレーを使用する必要があります。

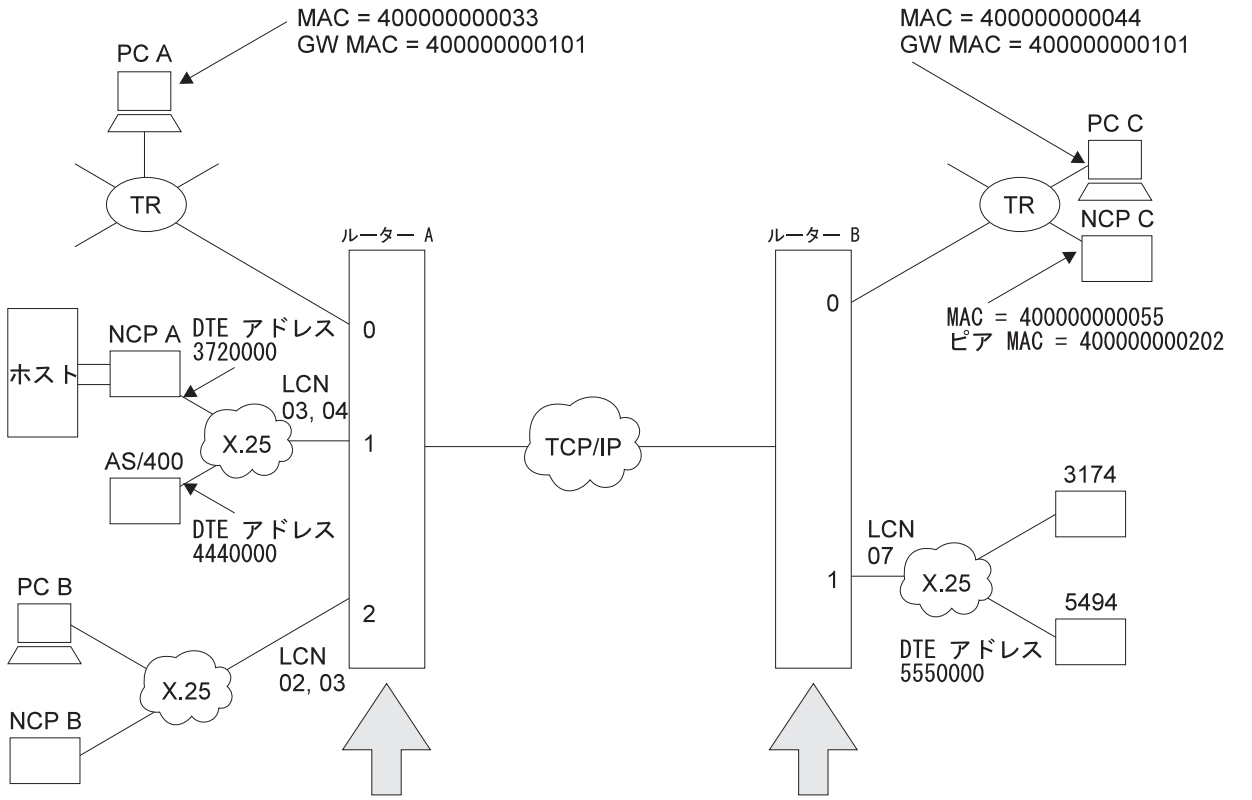
- 現在 DLSw によってサポートされていない、SDLC-SDLC 機能または構成の 1 つを必要とする場合

他の SDLC-SDLC 構成では、構成の容易さ、WAN 使用率、およびユーザーの現行のエンド・ステーション環境についてユーザーの要件を最もよく満たす機能を選択してください。 SDLC リレーについて詳しくは、 *ソフトウェア 使用者の手引き* を参照してください。

QLLC 装置サポート

QLLC は、X.25 のパケット・レイヤー・プロトコルより上位で働くプロトコルで、X.25 ネットワーク上の SNA 装置に SDLC と同様のステーションに見えます。QLLC は、バーチャル・サーキット (PVC または SVC) ごとに単一の SNA PU をサポートします。X.25 チャネル多重化により、X.25 ネットワークへの単一の物理インターフェースを通じて多くのバーチャル・サーキットまたは PU の接続機構に必要なものが提供されます。QLLC アーキテクチャーは、基本、2 次、および対等ステーションの役割を定義しますが、これらはエンド・ユーザー・データの伝送には影響を及ぼさないので、SDLC におけるほど重要ではありません。インターフェース上のすべてのバーチャル・サーキット用のデータは、平衡モードで働く単一の LAPB レイヤー 2 リンク接続機構を流れます。 リンクが接続されている間、どちらの側も常に送信する許可をもっています。

DLSw は QLLC エンド・ステーションをサポートします。これらのステーションは、SNA PU タイプ 2.0、2.1、4 (NCP-NCP トラフィック用)、または 4/5 (SNA 境界機能を実行するホストまたは NCP) にすることができます。エンド・ステーションは、構成済みの PVC、構成済みの SVC、または着信コールから生じる動的 SVC を介して接続することができます。ルーターは、X.25 インターフェース用に構成された役割に基づき、および SNA XID 折衝に基づき、基本または 2 次のいずれかの QLLC リンク・ステーションの役割となります。 異なる PU タイプが、同じ物理インターフェース上の異なるバーチャル・サーキット上で共存することができますが、インターフェースごとに単一のリンク・ステーションの役割だけがサポートされます。



インター フェース	VC タイプ	LCN/DTE アドレス	PU タイプ	発信元 MAC	あて先 MAC
1	PVC	03	5	400000000102	401111110101
(折衝可能)	PVC	04	5	400000000105	400000000201
	SVC	3720000	5	400000000101	000000000000
	SVC	4440000	2	400000000104	000000000000
2	PVC	02	2	400000000201	400000000105
(折衝可能)	PVC	03	4	400000000202	400000000055

着信コール用として使用可能にされたインターフェース
1

接続 ID	あて先 MAC
PCA	400000000033
PCC	400000000044

インター フェース	VC タイプ	LCN/DTE アドレス	PU タイプ	発信元 MAC	あて先 MAC
1 (1 次)	PVC	07	2	401111110101	400000000102

着信コール用として使用可能にされたインターフェース
1

接続 ID	あて先 MAC
AS400	400000000104

図 46. DLSw QLLC 構成の例

図46 は、DLSw によってサポートされる QLLC 構成のいくつかを図示し、QLLC および DLSw (MAC および SAP) アドレスの間でマップするのに必要な DLSw 構成のサブセットを示しています。 図では、*ローカル* (単一のルーター内での) および *リモート* (2 つのルーターおよび IP ネットワークを介した) の両方の DLSw セッションを示しています。 QLLC と SDLC の間のペアは示されていませんが、これらはローカルとリモートの両方の構成でサポートされます。

以下の DLSw セッションが構成されます。

- NCP A から PC A、B、および C を経由して、3174 まで

  NCP A は、2 つの PVC および 2 つの SVC (各バーチャル・サーキットは 1 つの PU を表しています) を介してルーター A 上のインターフェース 1 に接続されています。 PVC はインターフェース内で*論理チャネル番号* によってアドレス指定され、SVC は接続された X.25 装置の DTE アドレス (電話番号) によってアドレ

ス指定されます。 SDLC の場合と同様に、DLSw 構成は、これらの「固有の」DLC アドレス (LCN または DTE アドレス) を DLSw アドレス (MAC および SAP) にマップします。

この例では、NCP A は PVC 03 を介して 3174 (リモート QLLC-QLLC) に通信し、PVC 04 を介して PC B (ローカル QLLC-QLLC) と通信します。 これらの LCN は実際にはルーター A にローカルであり、NCP は X.25 ネットワークへのその対応する PVC について異なる LCN を使用することができます。ルーター A は、NCP A 用の DTE アドレス 3720000 とルーター A 上のインターフェース 1 用の DTE アドレスの間で 2 つの SVC を使用して、NCP A を PC C (リモート QLLC-LLC) および PC A (ローカル QLLC-LLC) と接続します。 ルーター A は NCP A からのコールを受け入れることができる必要があるので、DLSw への着信コールについてインターフェース 1 を使用可能にしてあります。 NCP A は、PC A および C に発信接続するために、以下で説明する*接続 ID* を使用します。

ルーター B では、PC C は LLC/LAN に接続されているので、構成されません。3174 はインターフェース 1 LCN 07 を介して接続されています。これは、ルーター A で使用されているインターフェースまたは LCN 番号とは関係がありません。

- AS/400 から 5494 へ

  NCP A に加えて、AS/400 はインターフェース 1 を介してルーター A にも接続されています。 SDLC とは異なり、所定のインターフェース上でのステーションの数を制限しても効率上の利点はありません。リンクの役割にかかわらず、リンク上に複数のステーションがあることができます。 役割が折衝可能であり、ステーションが T2.1 または PU4 ノードである場合、各ステーションは個別に折衝して、基本または 2 次になることができます。

  AS/400 はルーター A 内で構成されたあて先 MAC アドレスをもたないので、5494 に発信接続することはできません。5494 はルーター B では構成されないので、動的 SVC になります。 5494 は接続 ID を使用して、AS/400 に接続されたがっていることを示します。ルーター B は DLSw への着信コールについてインターフェース 1 を使用可能にしてあるので、5494 から呼び出しを受信することができます。

- NCP B から NCP C へ

  NCP B は PU タイプ 4 として構成され、この DLSw セッションが NCP 間で INN サブエリア・トラフィックは搬送するが、NCP から PU 2 装置へは BNN トラフィックを搬送しないことを示しています。 例でリモートの QLLC と LLC 間のセッションを示していますが、同じもの同志の間のセッションおよび SDLC に関係するセッションもサポートされています。 DLSw INN 機能は、マルチリンク TG または NCP リモート・ロード/ダンプ機能はサポートしていません。

アドレス・マッピング

DLSw では、DLSw ドメイン内のエンド・ステーション・エンティティーをアドレス指定するために使用される MAC/SAP ペア、および X.25 ドメイン内で使用される*インターフェース、LCN* (PVC) または *インターフェース、DTE アドレス* (SVC) ペアの間でのマッピングを提供します。 このマッピングは、接続確立時に行われますが、ルーターおよびエンド・ステーション製品で構成されたアドレス指定情報を使用します。

発信接続 (QLLC ステーションへ)

DLSw は、特定のターゲット MAC および SAP にアドレス指定された CUR_ex または CUR_cs メッセージを受信します。 DLSw はその QLLC エンド・ステーションの間で、その SMAC および SSAP (SAP は CUR_cs についてだけ検査されます) がこのターゲット MAC/SAP に一致するエンド・ステーションを探索します。 SMAC はルーター内で固有のため、一致は 1 つあるかまったくないかどちらかのはずです。

一致が見つかった場合、DLSw は、PVC については対応するインターフェースおよび LCN を使用し、SVC についてはインターフェースおよび電話番号を使用して、QLLC ステーションとの接続確立を開始します。 DLSw は、単一の QLLC ステーション (SVC) 定義を使用して同じ DTE アドレスへの複数の発信コールを行うことができます。これにより、最小限の構成の手間で、多くの DLSw 装置を同じあて先に接続することができます。

着信接続 (QLLC ステーションから)

PVC の場合、QLLC は、接続されたエンド・ステーションからサーキット確立を開始するフレームを受信します。 QLLC および DLSw は、その上でフレームが受信されたインターフェースおよび LCN を QLLC ステーション・リスト項目に突き合わせます。 LCN はインターフェース内で固有である必要があるため、一致は 1 つ見つかるか、まったく見つからないかどちらかです。一致がないか、項目に DMAC/DSAP が定義されていない場合、着信接続は失敗します。 それ以外の場合は、定義された DMAC/DSAP への接続が開始されます。 接続用の起点 MAC/SAP は、同じリスト項目からの SMAC/SSAP です。

SVC の場合、DLSw は、X.25 コーリング側アドレス、または受信された Call_Request パケットのコール・ユーザー・データ・フィールド内の*接続 ID* (バイト 4-11) を使用して MAC/SAP アドレスを引き出します。コーリング側アドレスが入手可能な場合、DLSw は最初にそれを、コールされた側のインターフェースについてそのすべての構成済みの SVC DTE アドレスと突き合わせて検査します。 DTE アドレスはインターフェース内で固有である必要があるため、一致は 1 つ見つかるか、まったく見つからないかどちらかです。 一致が見つかり、QLLC ステーション・リスト項目が非ゼロの DMAC/DSAP をもつ場合、DLSw はこの DMAC/DSAP を接続確立用のターゲット・アドレスとして使用します。接続用の起点 MAC/SAP は、同じリスト項目からの SMAC/SSAP です。

コーリング側アドレスが入手可能であるか、それがあるが DMAC/DSAP が定義されていない項目と一致するか、あるいはコールされたインターフェースについて定義された DTE アドレスに一致しない場合は、DLSw は Call_Request パケットに入れて受信された接続 ID (CID) が DLSw QLLC あて先レコード内で定義されたものに一致するかどうか検査します。CID は最大 8 文字までの EBCDIC 英数字ストリングとして解釈されます。

CID の一致がある場合、DLSw はあて先レコード内の関連した DMAC/DSAP をサーキット確立用のあて先アドレスとして使用します。コーリング側のアドレス一致 (DMAC/DSAP が定義されていない) もあった場合、DLSw は一致したステーション・リスト項目からの SMAC/SSAP を使用します。 その他の場合は、DLSw が SMAC および SSAP を動的に割り当てます。 SMAC の場合、DLSw は、グローバル DLSw 構成パラメーターの *QLLC base MAC address* および *Max dynamic addresses* によって

定義された範囲内で次に使用可能な (ラウンドロビン) MAC アドレスを選択します。動的に選択された SSAP は常に 0x04 です。

コーリング側アドレスまたは接続 ID の一致がない場合、DLSw はコールを行いません。CID は単一のコーリング側アドレスが複数のあて先へのコールを行うことができる唯一の方法です。

APPN および DLSw の両方は、同じコーリング側アドレスからの QLLC コールを受け入れることができます。 DLSw の方が受け入れるコールに制限が多いため、この呼び出しには最初にアクセスします。 DLSw がコーリング側または接続 ID の一致を見つけない場合、DLSw はコールをクリアせず、コールが APPN に提示されるようにします。

着信コールが受け入れられるためには、コーリング側アドレスまたは接続 ID のいずれかが DLSw に定義されている必要があります。これは主にアドレス・マッピングを提供するために必要であり、許可されない通話者からの着信コールを防ぐためのセキュリティーの要素も提供します。他の考えられるセキュリティー対策には、DLSw への着信コール用にインターフェースを使用可能にすること、および可能な動的発信元 MAC アドレスの数をゼロに設定することが含まれます。前者は、そのインターフェースでのすべての着信コールを、 DLSw で構成された DTE アドレスからのものでさえ、防止します。 後者は、構成されていない DTE アドレスからの動的着信コールのみを防止します。

X.25 コーリング側 (DTE アドレスや CID に関係なく) を DLSw が受け入れ、特定の DMAC と DSAP (ボックス 1 つに 1 つずつ) に突き合わせることができるようにするには、CID 値 ″ANYCALL″ と必要な DMAC および DSAP を使用して、 QLLC あて先レコードが構成できます。 DLSw は、SMAC および SSAP を動的に割り当てます。この機能が使用されると、DLSw はすべてのコールを受け入れます。APPN に対して示されるコールはなく、アドレス・マッピングと関連付けられたすべてのセキュリティー・フィーチャーがう回されます。

DLSw 構成および X.25 構成

所定の X.25 インターフェースを介して DLSw の QLLC サポートを使用するには、アドレス・マッピングを DLSw 構成の一部として構成する必要があり、次の情報も X.25 構成の一部として構成する必要があります。これらのステップの例については、518ページの『X.25 インターフェースを構成する』 を参照し、追加情報については、*ソフトウェア 使用者の手引き* の中の “X.25 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。

1. インターフェースが X.25 であるように構成し、その基本 X.25 インターフェース・パラメーターを構成します。
2. サポートされるプロトコルとして DLS を追加します。
3. DLSw が使用する PVC を構成し、それらを DLSw と関連付けます。
4. DLSw が使用する静的 SVC DTE アドレスを構成し、それらを DLSw と関連付けます。 これらは、DLSw で構成される同じアドレスです。動的に着信コールすることができる QLLC エンド・ステーションの DTE アドレスを構成する必要があります。

SDLC と異なり、X.25 には、DLSw で構成された情報に基づきリンク・ステーション (バーチャル・サーキット) 定義を動的に作成する機能はありません。

XTP 機能との関係

X.25 トランスポート・プロトコル (XTP) は、X.25 バーチャル・サーキットからパケットを受け取り、それらを TCP/IP を介して、同様に XTP をサポートする別のルーターに移送するルーター機能です。あて先ルーターは、次に XTP ヘッダー情報を除去し、パケットをあて先 X.25 バーチャル・サーキットへと送達します。

この機能は、次のように DLSw QLLC サポートと比較されます。

- 両方の機能は、TCP/IP を使用してピア・ルーター間で通信し、複数のバーチャル・サーキットからの情報 (または DLSw セッション) を単一の TCP 接続の上へと多重化することができます。
- 両方の機能で、ルーターは X.25 エンド・ステーションへのレイヤー 2 の LAPB およびレイヤー 3 のパケット・レイヤー接続を終了します。 LAPB 制御フレームは TCP/IP を横切って流れません。
- XTP は 2 つの X.25 エンド・ステーション間だけの通信をサポートします。 DLSw は、LLC (リモートからブリッジされているか、LAN 上の)、SDLC、QLLC、および DLSw 製品でサポートされる他のデータ・タイプ間でプロトコル変換を実行します。
- XTP は、パケット・レイヤーより上で稼働する LLC タイプ (例えば、QLLC または PAD) を識別しません。 両方の X.25 エンド・ステーションが同じ LLC タイプをサポートしている限り、それらは XTP を介して通信することができます。DLSw QLLC サポートは、 QLLC を実行する SNA エンド・ステーションとだけ通信することができます。
- XTP では、1 つの X.25 ネットワーク上のバーチャル・サーキット、対等ルーター、および別の X.25 ネットワーク上のバーチャル・サーキットの間で構成済みの関連付けがあります。 SVC の場合のみ、複数のピア・ルーターを定義して、1 次ルーターが使用可能でない場合に 2 次ルーターを通じて接続を立ち上げようとすることが可能ですが、 XTP は並列探索または接続確立試行を実行しません。それに対して、DLSw はバーチャル・サーキットを MAC および SAP アドレスにマップしてから、複数のピア間で完全に動的な探索を行い、あて先ステーションを見つけます。 DLSw マルチキャスト・サポートでは、探索される個別の対等 IP アドレスを構成することさえ必要ありません。
- XTP は、PVC を別の PVC にだけマップし、SVC を別の SVC にだけマップすることができます。 DLSw の QLLC と QLLC 間の構成では、PVC を SVC にマップすることが可能です。実際には、これは限られた価値しかありません。というのは、DLSw は、QLLC プロトコルが PVC 上でアクティブであるときはいつも SVC を立ち上げようとするからです。
- SVC を使用する XTP では、コールは、X.25 エンド・ステーションの DTE アドレスとの間で行われます。 X.25 スイッチまたはネットワーク加入は、ルーターが複数の DTE アドレスを表すことができるように構成する必要があります。DLSw では、コールは、エンド・ステーションからルーター・インターフェースの DTE アドレスに、およびその逆に行われます。

DLSw フィーチャーの使用

- DLSw は、APPN Implementers Workshop によって開発された標準であり、 IETF RFC に文書化されています。そのため、DLSw は多数のベンダーによってサポートされています。XTP は現在、特定の IBM 製品および互換性のあるルーター製品でのみサポートされています。

次の場合には、DLSw を使用する必要があります。

- QLLC から SDLC または LLC へのプロトコル変換が必要な場合
- あて先への複数の並行パスが必要な場合

次の場合は、XTP を使用する必要があります。

- X.25 を介して QLLC 以外のプロトコルを実行している場合

他の QLLC と QLLC 間の構成では、ユーザーのネットワークの要件に最もよく適合したプロトコルを選択してください。 XTP について詳しくは、*ソフトウェア 使用者の手引き* の中の「XTP の使用、構成、および監視」の章を参照してください。

APPN インターフェース・サポート

DLSw には、APPN の付いた内部インターフェースがあり、APPN をリモート DLSw ルーターに接続されたエンド・ステーションに接続します。 リモート・ルーターは APPN をサポートする必要はないので、それらが必要とするメモリーの量を減らすことができます。 図47 に示されるように、この内部インターフェースは、DLC 接続 (例えば、LAN を介しての LLC) を単一のソフトウェア・インターフェースに縮小することと等価です。

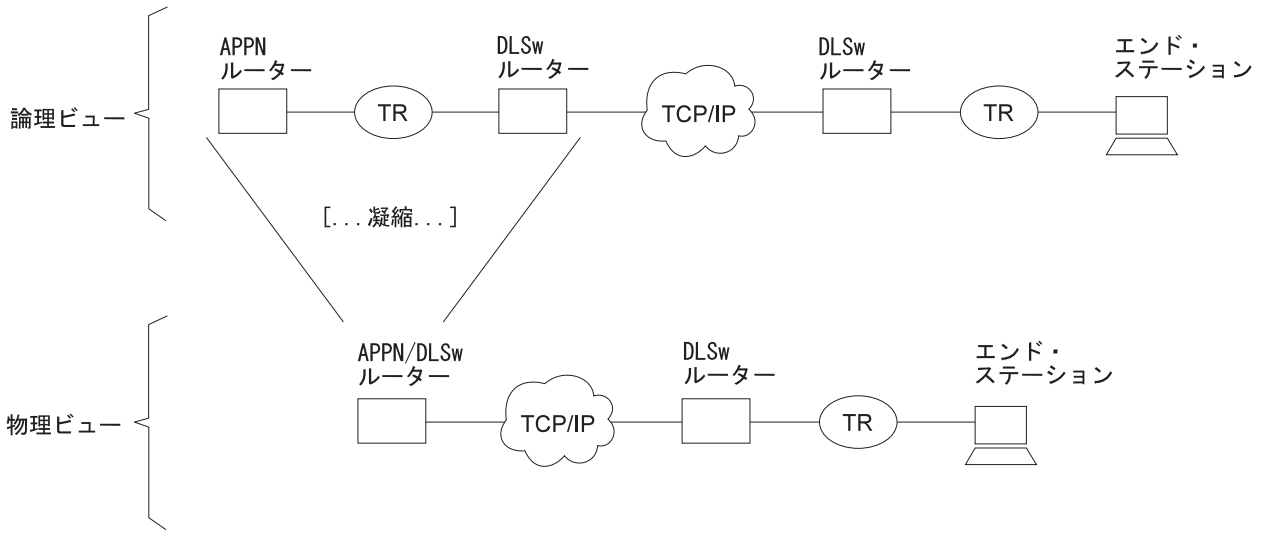


図 47. APPN と DLSw 間のソフトウェア・インターフェース

APPN は、DLSw ソフトウェア・インターフェースを使用して、APPN/DLSw ルーターにローカルに接続されたエンド・ステーションに到達することはできません。APPN は、その固有の DLC サポートを使用して、これらの装置と通信する必要があります。

APPN インターフェースをサポートするために追加の DLSw 構成は必要ありません。DLSw リモート・ルーターへの TCP Keepalive メッセージを使用可能にして、 DLSw

ポート上でのリンク・ステーションの喪失の検出ができるようにする必要があります。 DLSw バーチャル・インターフェースを使用して与えられたエンド・ステーションに到達するように APPN を構成する必要があります。 DLSw の使用による APPN のインプリメンテーションについては、 *プロトコルの構成と監視 解説書 第 2 巻* の APPN の構成に関する章を参照してください。

近隣優先順位フィーチャーを使用する

多くの DLSw ネットワーク構成では、あて先エンド・ステーションを DLSw ルーターにとってローカルにすることによって、起点 DLSw ルーターからあて先エンド・ステーションまで複数のパスが得られます。新しいサーキット用として DLSw ルーターが使用される追加の制御が得られるようにするには、各定義済み近隣に優先順位 (上位、中位、または下位) を割り当てることができます。 使用できる値は類似していますが、近隣優先順位は、512ページの『SNA トラフィックと NetBIOS トラフィックを平衡化する』で説明する SNA トラフィックと NetBIOS トラフィックの平衡化に関する優先順位と同じでは***ありません***。

近隣優先順位の場合は、**add tcp** コマンドまたは **join group** コマンドを使用して近隣を定義するときに、優先順位を割り当てます。 グループの優先順位は、グループ内で立ち上げられたすべてのトランスポート接続によって継承されます。

DLSw がサーキットの起点となり、あて先 MAC アドレスまたは NetBIOS 名が複数のリモート DLSw ルーターを経て到達可能であることが分かった場合は、DLSw は最上位の優先順位をもつ近隣の 1 つを通るサーキットを確立します。この最上位の優先順位を共有する複数のリモート・ルーターがある場合、DLSw は、それらのルーター間にサーキットを割り振る『ラウンドロビン』方式を使用します。

近隣優先順位を使用すれば、リモート・ルーター間に基本/バックアップ関係を確立することができます。 優先順位が上位のルーターが使用不能にならない限り、優先順位がそれより下位のルーターは使用されません。 さらに、ラウンドロビン方式によって優先順位が等しいルーター間の負荷平衡が得られます。

注:

1. 近隣が MAC アドレスに到達して求めることのできるキャッシュ情報を持たない MAC アドレスをあて先とするフレームが受信された場合は、SNA 探索メッセージがすべての DLSw 近隣に送信されます。この SNA 探索メッセージに対する応答が、『近隣優先順位待機タイマー』 によって指定された時間の間収集されます。この時間が経過すると、最上位の優先順位を持つ近隣からの応答による情報を用いて、MAC アドレス・キャッシュ項目が更新されます。 このような近隣の 1 つが選択されてこの SNA サーキットを扱うことになり、受信された元の SNA フレームに対する応答が送信されます。この MAC アドレスに関する以降の SNA サーキット要求は、優先順位が最上位のキャッシュ近隣の 1 つを使用して、サーキットを立ち上げます。
2. NetBIOS 名に関する現行のキャッシュ情報項目を持たない NetBIOS 名を宛先とする NetBIOS フレームが受信された場合は、NetBIOS をサポートするすべての DLSw 近隣に NetBIOS 探索メッセージが送信されます。 SNA の場合とは異なり、指定された時間の間応答が収集されてから、元の NetBIOS フレームに対する応答が送信されます。 エンド・ステーションのタイマーは、通常、ルーターでの待機遅延を認めません。

したがって、NetBIOS 探索メッセージに対する最初の応答が保管されます。 この近隣を使用してこの NetBIOS サーキットを立ち上げ、受信された元の NetBIOS フレームに対する応答が送信されます。 その一方で、NetBIOS 探索メッセージに対する以降の応答を使用して、NetBIOS 名前キャッシュを更新します。

- 優先順位が等しい近隣からの現行キャッシュ情報に対する応答が受信された場合は、キャッシュに追加されます。
- 優先順位が上位の近隣からの現行キャッシュ情報に対する応答が受信された場合は、現行キャッシュ情報は除去され、優先順位が上位の新しい近隣に関する情報が追加されます。
- 優先順位が下位の近隣からの現行キャッシュ情報に対する応答が受信された場合は、無視されます。 NetBIOS 名に関する以降の NetBIOS サーキット要求では、現行キャッシュの優先順位が最上位の近隣の 1 つを使用して、サーキットを立ち上げます。

すべての MAC アドレスに関して、または特定のセットの MAC アドレスに関して、近隣優先順位フィーチャーを使用不可にすることは可能です。すべての MAC アドレスに関して使用不可にする場合は、 *wait neighbor priority timer* を 0 に設定します。ある一組の MAC アドレスに関して使用不可にする場合は、MAC キャッシュ・エクスプローラー・オーバーライドを作成し、その *wait neighbor priority timer* を 0 に設定します。

近隣優先順位フィーチャーが使用不可にされていると、DSLw パートナー情報がその MAC アドレスについてキャッシュされることはありません。SNA と NetBIOS のエクスプローラーは、常に適用可能 DLSw パートナーすべてに送信され、最初に応答した DSLw パートナーを使用して、DLSw セッションを確立します (その優先順位に関係なく)。

SNA トラフィックと NetBIOS トラフィックを平衡化する

DLSw で NetBIOS トラフィックをサポートすることになったため、DLSw トランスポート接続内の SNA トラフィックと NetBIOS トラフィックの混合を制御する必要があります。この制御が行われないと、NetBIOS ファイル転送によって、対話式 SNA トラフィックが不当に長い間閉め出される傾向を生じます。特に、TCP 接続が比較的低速の WAN リンクで稼働している場合がそうです。 このトラフィック混合は、**set priority** コマンドの構成パラメーターを使用して制御することができます。 これらのパラメーターを使用すると、次のことを行うことができます。

- 輻輳 (ふくそう) 時に TCP 接続に伝送される各プロトコルのフレームの数の比率を確立する。
- 低速 WAN リンクが 1 つの大きいフレームで占められることがないように、NetBIOS の最大フレーム・サイズを確立する。

SNA フレーム数と NetBIOS フレーム数の比率を設定するには、各プロトコルごとに 4 つの優先順位値の 1 つ (重大、上位、中位、または下位) をグローバルに選択します。サーキットのセットアップ時に、ルーターは DLSw バージョン 1 (RFC 1795) のサーキット優先順位メカニズムを使用して、各新規サーキットごとに、サーキットが使用するプロトコルの値の優先順位の折衝を試みます。 サーキットを開始する DLSw ルーターが、使用するサーキット優先順位を選びます。ローカル DLSw ルーターがサーキットを開始する場合、それが選ぶサーキット優先順位は、構成済みの

サーキット優先順位の省略時値およびサーキット優先順位指定変更に基づくものです。リモート DLSw ルーターがサーキットを開始する場合には、ローカル DLSw ルーターは、それ自身は構成済みの省略時値および指定変更に基づいてサーキット優先順位を使用しなければならないが、リモート DLSw ルーターは、別の値を選んでもかまわないということをリモート DLSw ルーターに知らせます。いずれにせよ、確立された各サーキットごとに、そのサーキットの確立を開始したルーターによって、4 つの優先順位のうちの 1 つが割り当てられます。

TCP 輻輳 (ふくそう) 時には、ルーターは、4 つの待ち行列 (サーキット優先順位ごとに対応する待ち行列が 1 つずつある) の 1 つにフレーム (伝送するデータがあるサーキットからの) を入れます。 フレームは、各優先順位ごとに、待ち行列内では FIFO で待機します。 TCP 伝送プロセスを進めるために、ルーターは、『message allocation by priority』 パラメーターで指示されたフレーム数を各優先順位待ち行列から選択します。 省略時値は 4/3/2/1 であり、優先順位が重大の待ち行列から、多くとも 4 つのフレームが取り出され、次に優先順位が上位の待ち行列から、多くとも 3 つのフレームが取り出され、さらに以下同様であることを意味します。 待ち行列が空の場合は、その待ち行列の番はサイクルから省かれます。

大きい NetBIOS フレームが 1 つで長時間低速リンクを占有することがないようにするには、『NetBIOS maximum frame size』 パラメーターを使用して、単一の NetBIOS フレームのサイズに上限を設けることができます。 この値は、ソース・ルーティング MAC ヘッダー内の最大フレーム (LF) ビットを使用して、サーキット確立時に、両方の NetBIOS エンド・ステーションに渡されます。ソース・ルーティング NetBIOS エンド・ステーションでは、LF の値を監視し、指定された値より大きいフレームを生成しないようにする必要があります。

構成できる省略時サーキット優先順位は、次の 4 つがあります。

- 省略時 SNA エクスプローラー・トラフィック・サーキット優先順位
- 省略時 SNA セッション・トラフィック・サーキット優先順位
- 省略時 NetBIOS エクスプローラー・トラフィック・サーキット優先順位
- 省略時 NetBIOS セッション・トラフィック・サーキット優先順位

これらの異なる値により、異なる比率の SNA と NetBIOS、ならびにエクスプローラーとセッションのトラフィックを割り当てることができます。

一定のサーキット優先順位を特定のトラフィックに割り当てたい場合があります。例えば、一定の SNA MAC アドレスにあて先を指定されたトラフィックを、他のすべてのトラフィックよりも優先順位の高いものにした場合です。これは、サーキット優先順位指定変更 (**add priority**) コマンドを使用すると、行えます。こうすることで、エクスプローラーとセッション・サーキット優先順位を、特定の範囲の発信元 MAC アドレスと SAP、およびあて先 MAC アドレスと SAP に割り当てできます。これらのサーキット優先順位指定変更は、構成された順序で評価されます。サーキット優先順位は、最初に見つかったサーキット優先順位指定変更の一致にある値に設定されます。サーキット優先順位指定変更の一致が見つからない場合は、省略時のサーキット優先順位が使用されます。

DLSw をセットアップする

以下の項では DLSw に関するセットアップ手順を説明します。

- 『DLSw の構成要件』
- 『グローバル・バッファーの設定』
- 『DLSw 用の適応ソース・ルート・ブリッジング (ASRT) を構成する』
- 516ページの『DLSw 用のインターネット・プロトコル (IP) を構成する』
- 516ページの『DLSw 用の OSPF を構成する』
- 517ページの『SDLC インターフェースを構成する』
- 518ページの『X.25 インターフェースを構成する』
- 519ページの『DLSw を構成する』

さらに、DLSw 構成例を挙げ、注による説明を加えてあります (521ページの図48を参照)。

DLSw の構成要件

DLSw を使用するには、次のプロトコルを構成してください。それらは、ASRT、IP、および DLSw です。さらに、表32 にリストされているプロトコルを構成する必要がある場合があります。

表 32. DLSw 任意選択プロトコル

任意選択プロトコル	使用する場合
LLC2	省略時値でない LLC2 パラメーターを使用する必要がある場合
SDLC	SDLC を使用する装置に接続する場合
OSPF	動的ルーティングの場合または DLSw マルチキャスト・グループを使用する場合
X.25	QLLC を使用する装置に接続する場合

以下の各項では、これらの必須および任意選択のプロトコルを構成する方法をステップごとに説明します。

グローバル・バッファーの設定

DLSw を 4M DRAM 2210 で稼働する場合は、グローバル・パケット・バッファーの数を減らすことにより、DLSw により多くのメモリーを使えるようにする必要があります。 **set global** コマンドを `Config>` プロンプトで入力した上で、グローバル・パケット・バッファーの数 (4M DRAM 2210 の場合の推奨数は 50) を入力します。

DLSw 用の適応ソース・ルート・ブリッジング (ASRT) を構成する

DLSw ルーターは接続されたエンド・ステーションへのブリッジのようになっているので、ソース・ルート・ブリッジングを構成する必要があります。これは以下のステップに従って行ってください。

1. ASRT (適応ソース・ルート・ブリッジング) 構成プロセスに入る。Config> プロンプトから **protocol asrt** コマンドを使用してください。
2. **enable bridge** コマンドを使用してルーター上でブリッジングが発生するのを可能にする。 各ブリッジは各 DLSw 内で固有のブリッジ・アドレスをもつ必要があります。
3. **add port** コマンドを使ってブリッジ・ポートを追加する。 画面でインターフェース番号とポート番号を入力するようプロンプト指示されます。
   - ***トークンリング・インターフェースの場合:***

     トークンリングを通じて DLSw を稼働するには、指定したブリッジ・ポートにソース・ルート・ブリッジングのみがある必要があります。 したがって、透過ブリッジングは使用不能にする必要があります。 これは、**disable transparent** コマンドを使って行います。 次に、**enable source routing** コマンドを出して、ブリッジ・ポート用のソース・ルーティングをオンにします。
   - ***イーサネット・インターフェースの場合:***

     ブリッジ・ポートで透過ブリッジングを使用可能にするようにします。 **enable transparent** コマンドを出してください。
4. ***並行ブリッジングおよび DLSw***用にルーターを構成している場合:

   DLSw を使用しようとする SAP (サービス・アクセス・ポイント) に対してプロトコル・フィルターを作成します。 ルーターがブリッジング操作を行っており、かつ DLSw を介してパケットを転送している場合は、これを行うことが不可欠です。これを行わないと、ブリッジによって受信された DLSw パケットは DLSw によって転送され、ルーターによってブリッジされます。 考え方としては、DLSw パケットが DLSw ルーティングと並行して転送 (ブリッジ) されないようにすることです。

   SAP フィルターを作成する場合は、Config ASRT> プロンプトで **add protocol-filter dsap 4** コマンドを発行します。

   このコマンドに加えて、それが適用されるブリッジ・ポートを指定する必要があります。 このコマンドでは、DLSw 用に指定されたポートを除いて、DSAP が 4 のトラフィック をすべてフィルターするよう、ルーターに指示します。 (これは、ユーザーが DLSw トラフィック用に 4 の SAP を選択したと想定していることに注意してください。 これは DLSw 構成中に行うことです。)
5. **enable dls** コマンドを使用して DLSw を使用可能にする。 これによって、DLSw プロトコルが指定したブリッジ・ポートで使用可能になります。
6. ASRT 構成を検証する。 これを行う必要はありませんが、処理する前にブリッジ構成をチェックするのは良い考えです。 ASRT プロトコルの構成を検証するには、**list bridge** コマンドを使用してください。 次の例は、ASRT を構成した後の list bridge コマンドの結果を示しています。

```
          Source Routing Transparent Bridge Configuration
                ================================================
 Bridge:                 Enabled                 Bridge Behavior: Unknown
                    +----------------------------+
 -------------------| SOURCE ROUTING INFORMATION |------------------------------
                    +----------------------------+
Bridge Number:           01                      Segments:  1
Max ARE Hop Cnt:         14                      Max STE Hop cnt: 14
 1:N SRB:                 Not Active              Internal Segment:  0x000
LF-bit interpret:        Extended
                    +--------------------+
 -------------------| SR-TB INFORMATION |---------------------------------------
                    +--------------------+
SR-TB Conversion:        Disabled
```

```
TB-Virtual Segment:  0x000                        MTU of TB-Domain:  0
                    +-------------------------------------+
-------------------| SPANNING TREE PROTOCOL INFORMATION |-----------------------
                    +-------------------------------------+
Bridge Address:          Default                 Bridge Priority: 32768/0x8000
STP Participation:       IEEE802.1d
                    +--------------------------+
-------------------| TRANSLATION INFORMATION |---------------------------------
                    +--------------------------+
FA<=>GA Conversion:      Enabled                    UB-Encapsulation: Disabled
DLS for the bridge:      Enabled
                     +------------------+
 -------------------| PORT INFORMATION |----------------------------------------
                    +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP: Enabled
```

DLSw 用のインターネット・プロトコル (IP) を構成する

IP はローカル DLSw ルーターが他の DLSw ピアへの TCP 接続を形成できるように構成する必要があります。これを行うには、次のようにします。

1. Config> プロンプトから **protocol ip** コマンドを出すことにより IP 構成プロセスに入る。
2. ハードウェア・インターフェースに IP アドレスを割り当てる。他の DLSw ピアに接続するために使用しているハードウェア・インターフェースに IP アドレスを割り当てるには、**add address**コマンドを使用してください。
3. ***動的ルーティングを使用可能にする。*** ルーティング・プロトコルとして OSPF または RIP のいずれかを選択する必要があります。 OSPF は RIP より少ないネットワーク・オーバーヘッドを必要とするので、OSPF を使用するようお勧めします。
   - OSPF を使用可能にするには、『DLSw 用の OSPF を構成する』を参照してください。
   - RIP を使用可能にするには、IP Config> プロンプトで **enable RIP** を入力します。
4. 内部 IP アドレスを設定する。特定のインターフェースにではなくルーター全体に属するアドレスを設定するには、**set internal-ip-address**コマンドを使用してください。他の DLSw ピアへの TCP 接続を行うとき内部 IP アドレスがルーターにより使用されます。
   - RIP を使用している場合は、インターフェース・アドレスの 1 つを internal-ip-address として選択してください。
   - OSPF を使用している場合には、ネットワークで使用されているどのサブネットとも異なるサブネットをもつアドレスを選択してください。

DLSw 用の OSPF を構成する

ルーティング・プロトコルとしれ OSPF を使用したい場合は、次のようにしてそれを構成する必要があります。

1. *OSPF 構成プロセス*に入る。Config> プロンプトから **protocol ospf** コマンドを使用してください。
2. *ハードウェア・インターフェースに OSPF アドレスを割り当てる*。他の DLSw ピアに接続するために使用しているハードウェア・インターフェースに OSPF アドレスを割り当てるには、**set interface** コマンドを使用してください。

3. *動的ルーティングを使用可能にする。* **enable ospf** コマンドを使用して、ルーティングを使用可能にします。 DLSw グループ機能を使用する場合は、OSPF Config> プロンプトから OSPF ルーティング・プロトコルおよび OSPF マルチキャスト・ルーティングを使用可能にする必要があります。 OSPF 用のすべての省略時値は正常に働きます。 TCP 接続を明示的に定義するには、TCP 近隣を使用するのではなく、**join-group** コマンドを使用した後で OSPF およびマルチキャスト OSPF を使用可能にするだけで済みます。

SDLC インターフェースを構成する

SDLC 構成コマンドを使用すると、DLSw 構成プロセスの一環として、 SDLC インターフェース構成の作成や変更ができます。

注: SDLC が V.25bis 用のカプセル化機能である場合、物理リンク・パラメーターは、V.25bis レベルで構成する必要があるため、SDLC レベルで設定することはできません。この場合は、次の SDLC パラメーターは構成できません。

- Role (役割) - これは primary (基本) でなければなりません。
- Group (グループ) - グループ・ポーリング・アドレスは設定できません。
- Type (タイプ) - これは point-to-point (ポイントツーポイント) でなければなりません。
- Duplex (全二重)
- Idle state (アイドル状態)
- Clocking (刻時)
- Speed (速度)
- Cable (ケーブル)
- Encoding (符号化)
- Inter-frame delay (フレーム間遅延)

DLSw を通じて SDLC をサポートしようとする場合には、SDLC リンクを構成する必要があります。この項では、SDLC 構成コンソールにアクセスする方法を説明し、SDLC 関連コマンドについて解説します。

直接接続された SDLC 装置がある場合は、SDLC プロトコルを次のように構成してください。

1. データ・リンクを SDLC に設定する。Config> プロンプトで **set data-link SDLC** コマンドを使用して、シリアル・インターフェースに関するデータ・リンク・タイプを構成します。インターフェース番号を入力するようプロンプト指示されます。
2. SDLC 構成プロセスに入る。SDLC 構成プロセスに入るには、Config> プロンプトで **network** コマンドを使用してください。 インターフェース番号を入力するようプロンプト指示されます。
3. DLSw を構成する場合は、SDLC ステーションを追加すると、ソフトウェアはステーションに次の省略時値を割り当てます。
   - Maximum BTU はインターフェースによって許容可能な最大値です。
   - Tx および Rx ウィンドウは、Mod 8 の場合は 7、Mod 128 の場合は 127 です。

4. リンクの役割は省略時には 1 次に解釈されます。 必要な場合は、 **set link role** コマンドを使用してリンクの役割を 2 次または折衝可能に変更してください。
5. リンク上の 2 次ステーションについてグループ・ポーリングをセットアップすることができます。これを行うには、**set link group-poll** コマンドを使用してグループ・ポーリング・アドレスを設定し、**add station** および **set station group-inclusion** コマンドを使用して、ステーションをグループ・ポーリング・リストに組み込んでください。
6. リンク・クロック発信元 (任意選択) を設定する。モデム・エリミネーターを使用せずに直接 SDLC 装置に接続したい場合は、 DTE ケーブルおよびコマンド **set link clocking internal** を使用してください。
7. リンク速度 (任意選択) を設定する。内部クロックを使用する場合は、**set link speed** コマンドを使用して、この回線のクロック速度を選択します。

   注: SDLC を使用して PC から接続する場合は、PC の構成に一致するように、encoding (符号化) (NRZ/NRZI) および duplex (二重) (full/half) も設定する必要があります。
8. リンク・ケーブルを RS-232、X.21、V.35、または V.36 に設定する。
9. SDLC 構成を検証する。SDLC インターフェース構成を検証するには、**list link** コマンドを使用します。

X.25 インターフェースを構成する

QLLC 装置用の DLSwのサポートを使用したい場合は、X.25 インターフェースを使用してください。 以下のステップに従ってください。

1. インターフェースを X.25 になるように設定します。 `Config>` プロンプトで、**set data-link X25** コマンドを使用して、シリアル・インターフェースのタイプを設定します。 インターフェース番号を入力するようプロンプト指示されます。
2. X.25 構成プロセスに入るには、`Config>` プロンプトで **net** コマンドを使用します。 インターフェース番号を入力するようプロンプトが出されます。そうしたら、`X.25 Config>` プロンプトでコマンドを入力します。
3. **set address** コマンドを使用して、このインターフェース上のルーター DTE アドレスを定義します。
4. **set pvc** および **set svc** コマンドを使用して、PVC 用に使用される論理チャネル番号および SVC 用に使用可能な論理チャネル番号の範囲を定義します。 DLSw 構成で定義するどの PVC も、ここで定義する PVC 範囲内のチャネル番号をもつ必要があります。SVC の場合は、着信コールおよび発信コール用に使用可能なチャネルの数が、DLSw に発信または応答するものと予期する同時コールの数に十分であるようにする必要があります。
5. **add protocol** コマンドを使用して、「dls」をこのインターフェースで X.25 よりも上位で稼働するプロトコルとして追加します。 X.25 は、これが QLLC サポートを暗黙指定することを理解し、その値がこのインターフェース上のすべての DLSw バーチャル・サーキットに適用される一連の QLLC 操作パラメーターを入力するようプロンプト指示します。
6. **add pvc** コマンドを使用して、所定の PVC 論理チャネル番号を DLSw プロトコルと関連付けます。 これは、DLSw が使用するように構成されている、このインターフェース上の各 PVC (つまり、DLSw 構成内で行われる **add qllc station**

コマンドの対象となる各 PVC) について行う必要があります。論理チャネル番号は、このステーションについての DLSw 構成をこの X.25 PVC 定義と突き合わせるキーです。

7. **add address** コマンドを使用して、DLSw 構成で定義されるすべての PVC および SVC について X.25 DTE アドレスのリストを作成します。 DLSw は PVC について DTE アドレスを使用しないが、X.25 構成内ではそれが必要とされることに注意してください。DLSw に動的に着信コールすることができるが、DLSw 内で構成されていない QLLC エンド・ステーションの DTE アドレスを追加することは必要ありません。
8. X.25 への接続に必要とされる物理レイヤーまたは national personality 特性を設定します。 X.25 で構成可能なパラメーターについては、*ソフトウェア使用者の手引き*を参照してください。

DLSw を構成する

DLSw を構成する前に、Config> プロンプトで **list device** コマンドを入力して、異なる装置のインターフェース番号をリストしてください。

DLSw プロトコルを構成するには、次のように行います。

1. Config> プロンプトで、**protocol dls** コマンドを入力する。これで、DLSw config> プロンプトが表示されます。
2. DLSw config> プロンプトで、**enable dls** コマンドを入力して、ルーター内の DLSw を使用可能にする。
3. **set srb** コマンドを入力し、DLS ルーター用の SRB (ソース・ルート・ブリッジング) セグメント番号を指定する。

   SRB セグメント番号は、同じ LAN に接続されているすべての DLSw ルーターについて同じである必要があり、ソース・ルート・ブリッジ・ドメイン内で固有でなければなりません。ブリッジは、フレームが LAN 上で送信されるときに、この番号をルーティング情報フィールド (RIF) で使用します。 セグメント番号はループを防止するためのかぎです。
4. DLSw にスイッチさせたい各 SAP について **open-sap** コマンドを入力します。ルーターは、インターフェース番号を入力するようプロンプト指示します。 通常使用される SNA SAP (4、8、および C) をオープンするには、SNA を指定します。 少なくとも、SAP 0 および 4 をオープンします。NetBIOS SAP をオープンするには、NB または F0 を指定します。LNM SAP をオープンするには、LNM、または少なくとも 0 および F4 を指定します。
5. **add tcp** コマンドを使用して、構成したい各 DLSw ピアの IP アドレスを追加します。 ルーターに、構成済みでないピアからの接続を受け入れさせたい場合は、**enable-dynamic neighbor** コマンドを使用してください。 TCP 接続は、マルチキャスト OSPF および **join-group** コマンドを使用しても確立することができます。

   注: ルーターは、その対等ルーターが DLSw を実行する MRS ベースのプラットフォームである場合**のみ**、グループに参加することができます。 グループについて 1 つの DLSw ルーターを構成する場合は、グループ内のすべての DLSw ルーターで OSPF および MOSPF を使用可能にする必要があります。

6. DLSw 構成が SDLC をサポートするには、**add sdlc** コマンドを使用して、SDLC リンク・ステーションを追加する必要があります。
7. DLSw 構成が QLLC をサポートするには、 **add qllc station** コマンドを使って、QLLC リンク・ステーションを追加します。

   あるいは、動的 SVC をサポートしたい場合は、**enable qllc callin** コマンドを使って着信コール用に X.25 インターフェースを使用可能にし、**add qllc destination** コマンドを使って DLSw あて先を定義します。

DLSw 構成の例

次の DLSw 構成の例は、装置が他のどのプロトコルまたはデータ・リンク用にも構成されていないことを想定しています。この理由から、スクリプトは `Config>` ではなく、`Config (only)>` プロンプトから始まります。

サンプル・ダイアグラム

この例は 521ページの図48 に示される情報に基づいています。

構成しようとしている DLSw ルーター (図の R1) はその DLSw ピア (R2) に対し 1 つの LLC および 1 つの SDLC 接続をサポートします。 2 つのルーター間の TCP 接続はシリアル回線を介しています。

DLSw 用の R1 を構成するには、示された情報がすべて必要です。 この情報には次のものが含まれています。

- 内部 IP アドレス R1 および R2
- ルーター間の TCP 接続を維持するために使用される各ポートの IP アドレス
- トークンリングおよび SDLC 装置に割り当てられ、TCP 接続に使用されるインターフェース番号
- 接続された SDLC 装置の MAC アドレス
- 接続された QLLC 装置の MAC アドレス
- 接続されたトークンリング装置のソース・ルート・ブリッジ・セグメント番号

例は、構成手順の過程でこの情報が提供される場所を示しています。

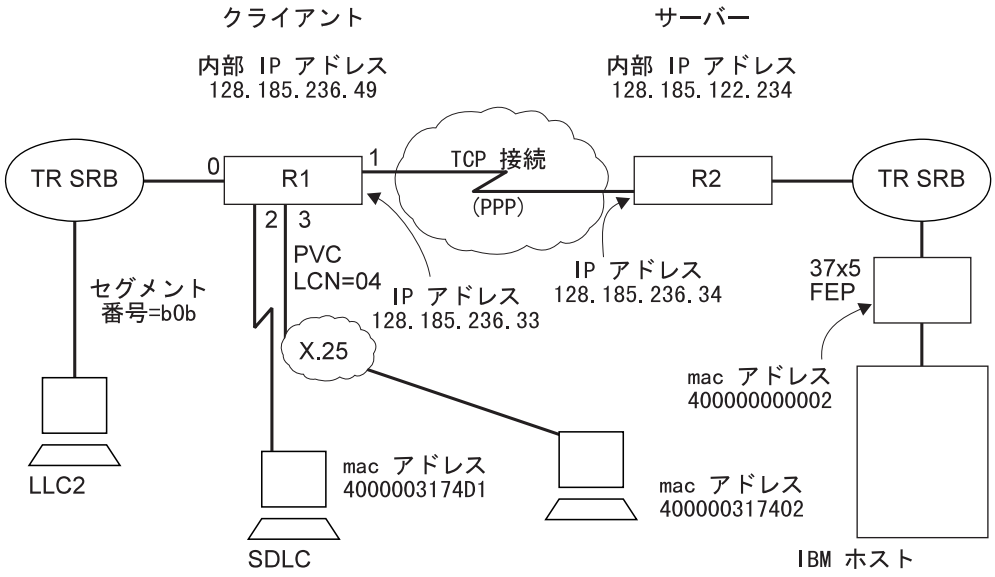


図 48. DLSw 構成用のサンプル・ダイアグラム

構成コマンドの例

この項では、次のものについての例を提供します。

- 『ステップ 1: 装置を追加する』
- 525ページの『ステップ 2: プロトコルを構成する』
- 529ページの『ステップ 3: プロトコル・フィルターを導入する』
- 530ページの『ステップ 4: DLSw を構成する』

ステップ 1: 装置を追加する

追加する装置は、トークンリング、SDLC、または QLLC です。透過型ブリッジ・ポートとしてイーサネットを追加することもできます。 図では、このサンプル DLSw 構成は、SDLC、LLC、および QLLC をサポートしているとします。 ただし、実際の構成では、これらのデータ・リンクの 1 つをサポートする必要があるだけです。

SDLC および QLLC の場合には、インターフェースは他のデータ・リンク (FR、X.25、および SDLC リレーなど) もサポートしているので、データ・リンクを明示的に設定する必要があります。

```
Config (only)>set data-link sdlc 2
Config (only)>set data-link x25 3
```

装置を追加した後、装置をリストして、それらが適正なルーター・インターフェースに割り当てられているか検証できます。

config> プロンプトに **list device** コマンドを入力して、構成済みの装置とそれぞれのインターフェース番号のリストを表示してください。

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

この **list** コマンドはトークンリング装置がインターフェース 5 に割り当てられていることを示していることに注意してください。

1. ***トークンリング装置を追加する***

   トークンリング・セットアップを構成します。 UTP ケーブルでは、通常、16 Mbps が使用されます。 これらの手順で示す **list** コマンドは、この時点でも、ルーターの構成中の他の時点でも必ずしも必要ではありません。

   ```
   Config (only)> network 5
   Token-Ring interface configuration

   TKR config>speed 16
   TKR config>media utp

   TKR config>list

   Token-Ring configuration:
   Packet size (INFO field): 2052
   Speed:                    16 Mb/sec
   Media:                    Unshielded
   RIF Aging Timer:          120
   Source Routing:           Enabled
   MAC Address:              000000000000
   IPX interface configuration record missing

   TKR config>exit
   ```

   WAN インターフェースを構成する。.最初のポート (インターフェース 1) は、WAN (TCP/IP) リンク用に使用されます。 WAN 用に選択したデータ・リンクは PPP です。 これはデータ・リンク用の省略時の選択です。 それ以外にフレーム・リレーおよび X.25 の選択が可能です。

   ```
   Config (only)>network 1
   Point-to-Point user configuration
   PPP Config>list hdlc
   Mode: Synchronous
   Encoding: NRZ
   Idle State: Flag
   Clocking: External
   Cable type: RS-232 DTE
   Speed (bps): 0

   Transmit Delay Counter: 0
   Lower DTR: Disabled
   ```

   ケーブル・タイプも設定する必要があります。 PPP の場合、ケーブル・タイプは **set hdlc cable** コマンドを使用して設定します。

   次に、必要があれば、シリアル・インターフェースに関して回線速度およびクロック・タイプを設定します。

   ```
   PPP Config>set hdlc clock internal
   Must also the line speed to a valid value
   Line speed (2400 to 2048000) [0]? 56000
   ```

   回線速度およびクロック・タイプを設定したら、**list hdlc** コマンドを使用して、下に示すように構成を検査することができます。

   ```
   PPP Config>list hdlc
   Mode: synchronous
   Encoding: NRZ
   Idle State: Flag
   ```

```
Clocking: Internal
Cable type: RS-232 DTE
Speed (bps): 56000

Transmit Delay Counter: 0
Lower DTR: Disabled

PPP Config>exit
```

2. ***SDLC 装置を追加する***

   SDLC をサポートするために DLSw を構成している場合、次のステップは SDLC を構成することです。 構成可能な項目の大部分は修正を必要としません。

   SDLC 構成にアクセスするには、**network** コマンドおよび SDLC 装置が割り当てられているインターフェースの番号 (この場合は 2) を使用します。

```
Config>network 2
SDLC user configuration
```

   SDLC を構成するときに追加する情報の大部分は、ハードウェアに関連しています。

   例は **list link** コマンドから開始しています。 **list** コマンドは構成を更新しませんが、現在 SDLC リンクに関連している値を示します。

   2210 を構成している場合は、次のようになります。

```
SDLC 2 Config>list link
Link configuration for: LINK_2   (ENABLED)

Role:         PRIMARY          Type:        POINT-TO-POINT
Duplex:       FULL             Modulo:      8
Idle state:   FLAG             Encoding:    NRZ
Clocking:     EXTERNAL         Frame Size:  2048
Speed:        0                Group Poll:  00
Cable:        RS-232 DTE

Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 sec
           RTS hold delay:     DISABLED
           Inter-frame delay:  DISABLED
           Inactivity timeout: 30.0 sec

Counters:  XID/TEST retry:  4
           SNRM retry:      6
           Poll retry:      10
```

   トークンリング装置を構成した場合と同じ要領で、SDLC 装置に関してクロック・タイプおよび回線速度を修正する必要があります。 外部モデム・エリミネーターを使用する場合は、これは不要です。

```
SDLC 2 Config>set link clock internal
Must also set the line speed to a valid value
Line speed (2400 to 2048000) [0]? 9600
SDLC 2 Config>exit
```

3. ***QLLC 装置を追加する***

   521ページの図48 に示されている QLLC ステーションをサポートするには、インターフェース 3 を X.25 になるように構成し、指定した PVC で DLSw 用 QLLC サポートをもつ必要があります。次の例は、X.25 以外のシリアル・インターフェースのスクラッチから開始します。次のサンプル構成は、PVC 上の DLSw 用の QLLC サポートを示しています。次のことを行ってください。

   a. list device コマンドを使用して、構成済みインターフェースのリストを入手する。

b. X.25 を構成するのに必要なシリアル・インターフェースを選択する。

c. そのインターフェース番号を記録し、set data-link コマンドでそれを使用して、インターフェース上に X.25 を構成する。

例では、X.25 はインターフェース 1 に構成されます。

```
Config>net
Network number [0]? 1
X.25 User Configuration

X.25 Config>li sum

X.25 Configuration Summary

Node Address:       <none>
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:           56000        Clocking:  Internal
MTU:              2048        Cable:     RS-232 DTE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC              low: 0    high: 0
Inbound          low: 0    high: 0
Two-Way          low: 1    high: 64
Outbound         low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400

X.25 Config>set addr
address [ ]? 3721111
X.25 Config>set pvc low 1
X.25 Config>set pvc high 4
X.25 Config>set svc low-two 5
X.25 Config>set svc high-two 64


X.25 Config>li sum

X.25 Configuration Summary

Node Address:       3721111
Max Calls Out:           4
Inter-Frame Delay:       0    Encoding:  NRZ
Speed:           56000        Clocking:  Internal
MTU:              2048        Cable:     RS-232 DTE
Lower DTR:   Disabled
Default Window:     2         SVC idle:  30 seconds
National Personality: GTE Telenet (DTE)
PVC              low: 1    high: 4
Inbound          low: 0    high: 0
Two-Way          low: 5    high: 64
Outbound         low: 0    high: 0
Throughput Class in bps Inbound:  2400
Throughput Class in bps Outbound: 2400

X.25 Config>li prot

X.25 protocol configuration

No protocols defined
X.25 Config>add prot
Protocol [IP]? dls
Idle timer [20]?
QLLC response timer [20]?
QLLC response count [10]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI  (2) SEC  (3) (PEER) [3]?
Non standard packet size [32]?
Packet window size [128]?
Max message size [256]?
Call User Data (in HEX) [0000000000000000]?


X.25 Config> li prot

X.25 protocol configuration

Prot         Window      Packet-size        Idle     Max     Station
```

```
Number       Size      Default Maximum      Time     VCs      Type
26 -> DLS     128        32      256         20       4       PEER

X.25 Config> li pvc

X.25 PVC configuration

No PVCs defined
X.25 Config>add pvc
Protocol [IP]? dls
Packet Channel [1]? 4
Destination X.25 Address [ ]? 4444
Window Size [2]?
Packet Size [128]?

X.25 Config> li pvc

X.25 PVC configuration

Prtcl        X.25_address     Window    Pkt_len   Pkt_chan
26 -> DLS    4444             2         128       4

X.25 Config> li add

X.25 address translation configuration

No address translations defined

X.25 Config> add addr
Protocol [IP]? dls
Enter an DLS address identifier (upto 12 chars) [ ]? Chicago
X.25 Address [ ]? 4444
X.25 Config> li addr

X.25 address translation configuration

IF #    Prot #       Protocol address -> X.25 address
1       26 -> DLS    Chicago          -> 4444
```

注: 論理チャネル番号 『4』 をもつ PVC 用に使用される DTE アドレス 『4444』 は、DLSw によっては使用されず、X.25 によってのみ構成情報を相関させるために使用されます。 同様に、DLSw プロトコル・アドレス (この例では、『Chicago』) は、DLSw には意味を持ちませんが、DLSw が使用することができるさまざまな DTE アドレスの参照を容易にするためだけのものです。 X.25 上で稼働する他のプロトコルとは異なり、DLSw アドレス変換は、DLSw 構成の一部として定義され、X.25 構成では定義されません。

ステップ 2: プロトコルを構成する

装置構成が完了したら、必要なプロトコルを構成する必要があります。 DLSw で稼働するためには、IP、OSPF (または RIP)、 ASRT、および DLSw プロトコルを構成する必要があります。

1. ***IP を構成する***

   この例は IP 構成で開始します。

   ```
   Config>protocol ip
   Internet protocol user configuration
   ```

   list all コマンドで省略時 IP 構成が表示されます。

   ```
   IP config>list all
   Interface addresses
   IP addresses for each interface:
      intf  0   192.1.1.3        255.255.255.0    Local wire broadcast, fill 1
      intf  1                                     IP disabled on this interface
      intf  2                                     IP disabled on this interface

   Routing

   Protocols
   BOOTP forwarding: disabled
   ```

```
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: enabled
BGP: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
     intf  0   192.1.1.3        Send net, subnet, static and default routes
                                Received RIP packets are ignored.
     intf  1                    IP & RIP are disabled on this interface
     intf  2                    IP & RIP are disabled on this interface

Accept RIP updates always for:
     [NONE]
```

この例では、最小限の IP 構成の作成を示します。 この重要なプロトコルの詳細については、237ページの『第14章 IP の使用』を参照してください。

- 最初に行うことは、インターネット・アドレスを追加し、IP トラフィックを実行する予定のインターフェースにそれを割り当てることです。

```
IP config>add address
Which net is this address for [0]? 1
New address [0.0.0.0]? 128.185.236.33
Address mask [255.255.0.0]?255.255.255.0
```

- 内部 IP アドレスを設定します。 これは、リモート DLSw ルーターが、ユーザーが構成しているルーターに接続するために使用するアドレスです。 RIP が IP 用に選択されたルーティング・プロトコルである場合、内部 IP アドレスは、インターフェース用に構成された IP アドレスに一致する必要があります。

```
IP config>set internal-ip-address 128.185.236.49
```

- その後 **list** コマンドを使用すると、新たに追加された情報が表示されます。

```
IP config>list all
Interface addresses
IP addresses for each interface:
   intf  0   192.1.1.3        255.255.255.0    Local wire broadcast, fill 1

   intf  1   128.185.236.33   255.255.0.0      Local wire broadcast, fill 1

   intf  2                                     IP disabled on this interface
Internal IP address: 128.185.236.49

Routing

Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: enabled
BGP: disabled
RIP: enabled
RIP default origination: disabled
  Per-interface address flags:
     intf  0   192.1.1.3        Send net, subnet, static and default routes
                                Received RIP packets are ignored.
     intf  1   128.185.236.33   Send net, subnet, static and default routes
                                Received RIP packets are ignored.
     intf  2                    IP & RIP are disabled on this interface

Accept RIP updates always for:
[NONE]

IP config>exit
```

2. ***OSPF または RIP を構成する***

この構成では、RIP ではなく、OSPF を使用します。 これらのルーティング・プロトコルのどちらも使用できます。 ただし、RIP を選択した場合は、DLSw のグループ機能は使用できません。

まず、**list** コマンドを入力します。このコマンドは省略時の OSPF 構成を表示します。 DLSw を稼働するにはこの構成を修正する必要があります。

```
Config>protocol ospf
Open SPF-Based Routing Protocol configuration console
OSPF Config>list all

             --Global configuration--
          OSPF Protocol:          Enabled
          # AS ext. routes:       1000
          Estimated # routers:    50
          External comparison:    Type 2
          AS boundary capability: Disabled
          Multicast forwarding:   Disabled

                  --Area configuration--
Area ID       AuType     Stub?   Default-cost Import-summaries?
0.0.0.0       0=None     No      N/A           N/A
```

- ここで、OSPF を使用可能にし、外部ルートおよび OSPF ルーターの数を見積もります。

  ```
  OSPF Config> enable ospf
  Estimated # external routes [0]? 100
  Estimated # OSPF routers [0]? 25
  ```

- この例では、DLSw のグループ機能を使用するので、下に示すようにマルチキャスト OSPF を使用可能にする必要があります。

  ```
  OSPF Config>enable multicast
  Inter-area multicasting enabled? [No]:
  ```

- OSPF を使用する各物理 IP インターフェースごとに **set interface** コマンドを出します。 この例では、バックボーンが OSPF 区域 (0.0.0.0) であると想定しています。 この時点では、IP インターフェースを 1 つだけ定義します。

  ```
  OSPF Config>set interface 128.185.236.33
  Attaches to area [0.0.0.0]?
  Retransmission Interval (in seconds) [5]?
  Transmission Delay (in seconds) [1]?
  Router Priority [1]?
  Hello Interval (in seconds) [10]?
  Dead Router Interval (in seconds) [40]?
  Type Of Service 0 cost [1]?
  Authentication Key [ ]?
  Retype Auth. Key [ ]?
  Forward multicast datagrams? [Yes]:
  Forward as data-link unicasts? [No]:
  IGMP polling interval (in seconds) [60]?
  IGMP timeout (in seconds) [180]?
  OSPF Config>
  ```

- 次の例では、OSPF が構成された後の OSPF 表示を示します。構成の中で何が変更されたか調べるために、この表示を先に示した省略時の OSPF 構成の表示と比較してください。

  ```
  OSPF Config>list all

         --Global configuration--
  OSPF Protocol:          Enabled
  # AS ext. routes:       100
  Estimated # routers:    25
  External comparison:    Type 2
  AS boundary capability: Disabled
  Multicast forwarding:   Enabled
  Inter-area multicast:   Disabled

                    --Area configuration--
  Area ID      AuType       Stub? Default-cost Import-summaries?
  0.0.0.0      0=None       No         N/A           N/A

                    --Interface configuration--
  IP address       Area     Cost  Rtrns  TrnsDly  Pri  Hello  Dead
  192.1.1.3        0.0.0.0     1      5       1     1     10    40
  ```

```
128.185.236.33   0.0.0.0     1      5       1     1     10    40

                                Multicast parameters
IP address    MCForward    DLUnicast    IGMPPoll    IGMPtimeout
192.1.1.3         On           Off          60           180
128.185.236.33    On           Off          60           180

OSPF Config>exit
```

3. ***ASRT を構成する***

   次に示すようにソース・ルート・ブリッジング用のルーターを構成し、ポートを使用可能にします。

   ```
   Config (only)>protocol asrt
   Adaptive Source Routing Transparent Bridge user configuration
   ASRT config>enable bridge
   ```

   - **list port** コマンドは、ポートが透過ブリッジングに省略時解釈されたことを示しています。 透過ブリッジングは、ユーザーの接続した装置がイーサネットの場合は必要なものですが、ユーザーの装置がトークンリングである場合には働きません。 ポート番号 1 はインターフェース 0 上のポート 0 であることに注意してください。言いかえると、ポート 1 はトークンリング用にセットアップした物理インターフェース用の論理ブリッジ・ポートです (521ページの図48を参照)。

     ```
     ASRT config>list port
     Port Id (dec)    : 128:01, (hex): 80-01
     Port State       : Enabled
     STP Participation: Enabled
     Port Supports    : Transparent Bridging Only
     Assoc Interface  : 0
     Path Cost        : 0
     ++++++++++++++++++++++++++++++++++++++++++
     ```

   - LLC データ・リンク(トークンリングなど) の DLSw は SRB (ソース・ルート・ブリッジング) を必要とします。この場合、最初に行うべきことは、ポート上で透過ブリッジングを使用不能にすることです。

     ```
     ASRT config>disable transparent
     Port Number [1]?

     ASRT config>enable source-routing
     ```

   - ここで、ポート用のセグメント番号を割り当てます。 トークンリングなどソース・ルート・ブリッジ装置を構成するときには、セグメント番号を割り当てるだけで済みます。この例では (521ページの図48を参照) **b0b** はトークンリング装置に割り当てられた 16 進数です。

     ```
     Port Number [1]?
     Segment Number for the port in hex(1 - FFF) [1]? b0b
     Bridge number in hex (1 - 9, A - F) [1]?
     ```

     次に、ブリッジ・ポートで DLSw を使用可能にします。

     ```
     ASRT config>enable dls
     ```

   これらのステップを完了した後、次に示すように DLSw を使用可能にします。 ブリッジ構成をリストすると、ASRT を正しく構成したか確認できます。

```
ASRT config>list bridge

          Source Routing Transparent Bridge Configuration
          ===============================================
Bridge:                 Enabled                 Bridge Behavior:
Unknown
                    +----------------------------+
------------------- | SOURCE ROUTING INFORMATION |-----------------------------
                    +----------------------------+
Bridge Number:           01                      Segments:  1
Max ARE Hop Cnt:         14                      Max STE Hop cnt: 14
1;N SRB:            Not Active              Internal Segment: 0x000
```

```
LF-bit interpret:        Extended

                    +-------------------+
-------------------| SR-TB INFORMATION |-------------------------------------
                    +-------------------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:  0x000                      MTU of TB-Domain:  0

                    +-----------------------------------+
-------------------| SPANNING TREE PROTOCOL INFORMATION |---------------------
                    +-----------------------------------+
Bridge Address:          Default                 Bridge Priority: 32768/0x8000
STP Participation:       IEEE802.1d

                    +-------------------------+
-------------------| TRANSLATION INFORMATION |--------------------------------
                    +-------------------------+
FA<=>GA Conversion:      Enabled                    UB-Encapsulation: Disabled
DLS for the bridge:      Enabled

                    +------------------+
-------------------| PORT INFORMATION |-------------------------------------
                    +------------------+
Number of ports added: 1
Port:   1      Interface:       0      Behavior:    SRB Only   STP: Enabled
```

ステップ 3: プロトコル・フィルターを導入する

これは DLSw を構成するときにしばしば無視される重要なステップです。

SAP (サービス・アクセス・ポイント) 04, 08, 0C でトラフィックを転送するのに、ブリッジングではなく DLSw を使用するので、ブリッジング・セットアップには特殊なプロトコル・フィルターを追加する必要があります。

注: ブリッジングを、DLSw に加えて、WAN リンクを介して構成する場合のみ、ここで説明するフィルターを導入する必要があります。 この例はそのような場合ではありません。 この例では、SAP フィルターを作成するための手順は、参考までに示してあります。

フィルターの目的は、ブリッジが、DLSw によってのみ扱われるべきパケットを他のポートで転送しないようにすることです。 DLSw およびブリッジング機能が同じパケットを転送するのは最適なことではありません。 これが発生する場合、競合状態が起こって、ネットワーク・パフォーマンスの低下を生じることがあります。

このコマンドは宛先 SAP が 4 のすべてのパケットに作用するフィルターを作成します。 その後出された **list** コマンドはフィルター特性を表示します。

```
ASRT config>add prot-filter dsap 4
Filter packets arriving on all ports?? [No]: yes

ASRT config>list prot-f dsap
Protocol Class: DSAP
Protocol Type : 04
Protocol State: FILTERED
Port Map      : 1
=========================
No ETHER type Filter Records Associated
No SNAP Filter Records Associated
```

必要なフィルターが適切な場所に用意されたら、ASRT 構成を終了します。

```
ASRT config>exit
```

ステップ 4: DLSw を構成する

最後のステップは、DLSw プロトコルを構成することです。 次の **list** コマンドは省略時値を示しています。

```
Config>protocol dls
DLSw protocol user configuration

DLSw config>list dls
DLSw is                                 DISABLED
LLC2 send Disconnect is                 ENABLED
Dynamic Neighbors is                    ENABLED
SRB Segment number                      000
MAC <-> IP mapping cache size           128
Max DLSw sessions                       1000
DLSw global memory allotment            141312
LLC per-session memory allotment        8192
SDLC per-session memory allotment       4096
QLLC per-session memory allotment       4096
NetBIOS UI-frame memory allotment       40960

Dynamic Neighbor Transmit Buffer Size   5120
Dynamic Neighbor Receive Buffer Size    5120
Dynamic Neighbor Maximum Segment Size   1024
Dynamic Neighbor Keep Alive             DISABLED
Dynamic Neighbor SessionAlive Spoofing  DISABLED
Dynamic Neighbor Priority               MEDIUM

QLLC base source MAC address            40514C430000
QLLC maximum dynamic addresses          64
Type of local MAC list                  NON-EXCLUSIVE
Use of local MAC list is                ENABLED
Use of remote MAC list is               ENABLED
```

DLSw を使用可能にし、SRB セグメント番号を設定します。 521ページの図48 に示すように、セグメント番号はトークンリング装置を指しています。

```
DLSw config>enable dls
DLSw config>set srb 020
```

DLSw グループおよび静的セッションを構成する: この例では、グループおよび構成された TCP セッションの両方を定義します。 DLSw を構成するには、これは不要です。ただし、近隣の DLSw ルーターに発信接続するためには、どちらか一方 (DLSw グループまたは構成された TCP セッションのどちらか) を定義する必要があります。着信接続するのに非構成済みのルーターが必要な場合は、**enable dynamic-neighbors** コマンドを出してください。

Join-Group コマンド: **join-group** コマンドを使用して、DLSw グループを作成します。各グループ・メンバーをクライアント/サーバーまたは Peer と指定します。Peer (ピア) は省略時値です。

ここで、**join-group** コマンドは R1 用に実行されます(521ページの図48 を参照)。つまり、この DLSw ルーターをグループ 1 内のクライアントとして指定します。このグループを結合するには、R2 をサーバーとして追加し、R2 で **join-group** コマンドを出す必要があります。

```
DLSw config>join
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]?
Client/Server or Peer Group Member(C/S/P)- [P]? c
Connectivity Setup Type (a/p) [p]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

```
DLSw config>list group

   Group#                  Xmit    Rcv      Max      Keep-    SessAlive
Mcast IP Addr Role    CST Bufsize Bufsize  Segsize  alive    Spoofing  Priority
------------- ------- --- ------- -------- -------- -------- --------- --------
Group  1      CLIENT   p    5120    5120     1024   DISABLED DISABLED  MEDIUM
```

Add TCP コマンド: **add TCP** コマンドを使用して、明示的に構成された DLSw 近隣を定義します。ここで追加する近隣 DLSw IP アドレスはピア DLSw ルーターの内部 IP アドレスです (521ページの図48では呼ばれています)。 R2 は R1 の近隣 IP アドレスを使って構成することもできます。あるいは、動的近隣を受け入れるように R2 を構成することができます。

```
DLSw config>add tcp
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.122.234
Connectivity Setup Type (a/p) [p]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable  NetBIOS SessionAlive Spoofing (E/D)[D]?
Neighbor Priority (H/M/L) [M]?

DLSw config>list tcp
                    Xmit    Rcv     Max      Keep-    SesAlive
Neighbor        CST Bufsize Bufsize Segsize  Alive    Spoofing Priority
--------------- --- ------- ------- -------  -------- -------- ---------
128.185.122.234  p     5120    5120    1024   DISABLED DISABLED MEDIUM
```

各 SDLC リンク・ステーションを定義する: 各 SDLC リンク・ステーションを定義する必要があります。

```
DLSw config>add sdlc
Interface # [0]? 2
SDLC Address or 'sw' (switched dial-in) [C1]?
Source MAC address [4000112402C1]? 4000003174d1
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000002
Destination SAP in hex [0]? 4
PU type (2/4/5) [2]?
XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xfffff) [0]? 00001
Poll with TEST (T) or SNRM (S) [T]?

DLSw config>li sdlc all
Net Addr   Status    Source SAP/MAC   Dest SAP/MAC      PU  Blk/Idnum  PollFrame
 2   C1    Enabled   04 4000003174D1  04 400000000002   2   017/00001  TEST
```

各 QLLC リンク・ステーションを定義する: 各 PVC および構成済みの SVC についてアドレス・マッピングを定義します。 構成例では、PVC に接続された 1 つの QLLC 装置があります。

```
DLSw config> add qllc sta
Interface # [0]? 3
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 4
Source MAC address [400000310101]? 400000317402
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000002
Destination SAP in hex [0]? 4
PU type (2/4/5) [2]?
XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xfffff) [0]? 00001
New QLLC station record added

DLSw config> li q st
If  P/S  LCN/DTE addr   E/D Source SAP/MAC   Dest SAP/MAC    PU Blk/IdNum
 3  PVC  4               E  04 400000317402  04 400000000002  2 017/00001
```

サービス・アクセス・ポイント (SAP) をオープンする: 次にすべきことは、各ブリッジング・インターフェースでサービス・アクセス・ポイント (SAP) をオープンすることです。

SAP 番号の 0、4、8、および C は、よく使用される SNA SAP です。 これらの SAP をオープンするには、下に示すように、**open-sap** コマンドで SNA オプションを使用します。 NetBIOS に関して SAP をオープンするには、NB オプションを選択します。 16 進数 を使用して、個別に SAP を入力することもできます。

```
DLSw config> open-sap
Interface #[1]?
Enter SAP in hex (range 0–FE), or one of the following:
   'SNA', 'NB', or LNM [4]? sna
SAP(s) 0 4 8 C opened on interface 1
DLSw config>
```

以下は、構成した後の DLSw 表示です。

```
DLSw config>list dls
DLSw is                                ENABLED
LLC2 send Disconnect is                ENABLED
Dynamic Neighbors is                   ENABLED
SRB Segment number                     020
MAC <-> IP mapping cache size          128
Max DLSw sessions                      1000
DLSw global memory allotment           141312
LLC per-session memory allotment       8192
SDLC per-session memory allotment      4096
QLLC per-session memory allotment      4096
NetBIOS UI-frame memory allotment      40960

Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor SessionAlive Spoofing DISABLED
Dynamic Neighbor Priority              MEDIUM

QLLC base source MAC address           40514C430000
QLLC maximum dynamic addresses         64
Type of local MAC list                 NON-EXCLUSIVE
Use of local MAC list is               ENABLED
Use of remote MAC list is              ENABLED
```

DLSw の構成を終えたら、DLSw 構成を終了し、ルーターを再始動します。

```
DLSw config>exit
Config (only)>restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

第26章 DLSw の構成と監視

この章では、データ・リンク交換プロトコルの構成用法および監視方法について説明します。この章には次の節が含まれています。

DLSw 構成環境へのアクセス

ルーターの構成を変更するには CONFIG プロセスを使用してください。 新しい構成はルーターが再始動されると有効になります。

構成プロセスを入力するには、OPCON (*) プロンプトで **talk 6** (または **t 6**) を入力します。 これにより、次の例に示すように CONFIG> プロンプトが出ます。

```
MOS Operator Control

* talk 6
Gateway user configuration

CONFIG>
```

CONFIG> プロンプトが即時に表示されない場合は、**Enter** キーを再び押します。

DLSw 構成コマンドはすべて、DLSconfig> プロンプトに入力します。このプロンプトにアクセスするには、次に示すように **protocol DLSw** コマンドを入力します。

```
Config>protocol dls
DLSw protocol user configuration
DLSw config>
```

事前構成の要件

構成手順を開始する前に、**config** プロンプトから **list device** コマンドを使用して、異なる装置のインターフェース番号をリストしてください。 さらに構成コマンドの説明が必要な場合には、この章で記述されている構成コマンドを参照してください。

重要な考慮事項

DLSw を実行する 4 MB DRAM 搭載の IBM 2210 の場合は、次のことが必要です。

- グローバル・バッファーの最大数は 50 に設定する必要があります。 こうすることによって、DLSw が効率的な実行に必要なメモリーを確保することができます。
- **set global-buffers** コマンドを `Config>` プロンプトから使用して、グローバル・バッファーの最大数を設定することができます。

DLSw 構成コマンド

この節では、DLSw 構成コマンドについて要約してから説明します。 DLSw 構成コマンドを使用すると、DLSw 構成の作成や変更ができます。 表33 は、各コマンドの要約を示しています。DLSw 構成コマンドはすべて、`DLSw Config>` プロンプトの後に入力してください。どのコマンドおよびそのパラメーターについても省略時値は、プロンプトの直後で大括弧に囲まれています。

ルーターの構成に加えられた変更は、即時有効にはなりませんが、ルーターの SRAM 構成が再始動された時点で、その一部となります。

表 33. DLSw 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	SDLC リンク・ステーション、TCP 近隣 IP アドレス、 QLLC ステーションやあて先、キャッシュ記入項目、MAC アドレス・リスト項目、サーキット優先順位指定変更、または MAC キャッシュ・エクスプローラー・オーバーライドを追加します。
Ban	境界アクセス・ノード (BAN) 構成プロンプトにアクセスして、BAN 構成コマンドが入力できるようにします。
Close-Sap	現在オープンされているサービス・アクセス・ポイント (SAP) をクローズします。DLSw は、LLC をサポートするインターフェース上での通信に SAP を使用します。
Delete	構成済み SDLC リンク・ステーション、TCP 接続、 QLLC ステーションやあて先、キャッシュ記入項目、MAC アドレス・リスト項目、サーキット優先順位指定変更、または MAC キャッシュ・エクスプローラー・オーバーライドを除去します。
Disable	DLSw プロトコル、SDLC リンク・ステーション、LLC 切断機能、動的近隣、QLLC ステーションもしくはインターフェース、またはローカルおよびリモート MAC アドレス・リストの使用を使用可能にします。
Enable	DLSw プロトコル、SDLC リンク・ステーション、LLC 切断機能、動的近隣、QLLC ステーションもしくはインターフェース、ローカルおよびリモート MAC アドレス・リストの使用、または IPv4 DLSw 優先ビット設定を使用可能にします。
Join-Group	DLSw 近隣が動的に相互を見つけられるようにします。
Leave-Group	指定した DLSw グループからルーターを除去します。

表 33. DLSw 構成コマンドの要約 (続き)

コマンド	機能
List	SDLC リンク・ステーション、SAP、サーキット優先順位、DLSw グループ、DLSw グローバル情報、QLLC あて先、ステーション、およびインターフェース、キャッシュ記入項目、または MAC アドレス・リスト項目についての情報を表示します。このコマンドによって、TCP 接続についての詳しい情報も得られます。
NetBIOS	NetBIOS 構成プロンプトへアクセスすることができます。
Open-SAP	DLSw が指定した SAP を介してデータを伝送できるようにします。DLSw は、LLC をサポートするインターフェース上での通信に SAP を使用します。
Set	LLC2 パラメーター、DLSw セッションの数、SRB セグメント番号、TCP バッファー・サイズ、メモリーの割り振り、プロトコル・タイマー、サーキット優先順位、動的近隣についてのパラメーター、QLLC 動作についてのパラメーター、および MAC アドレス・リスト関連のパラメーターを構成します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

SDLC リンク・ステーション、 TCP 近隣 IP アドレス、QLLC ステーションやあて先、キャッシュ記入項目、 MAC アドレス・リスト項目、サーキット優先順位指定変更、MAC キャッシュ・エクスプローラー・オーバーライドを構成する場合は、 **add** コマンドを使用します。

構文:

add cache-entry
explorer-override
mac-list
priority
qllc...
sdlc
tcp

cache-entry

構成済み MAC キャッシュ記入項目を追加します。このキャッシュ記入項目は、特定の MAC アドレスを特定の DLSw ピアにマップします。複数のキャッシュ記入項目を追加することにより、1 つの MAC アドレスを複数の DLSw ピアにマップすることができます。

例 : add cache-entry

```
Enter MAC Address [400000000000]? 10005a123456
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.122.234

MAC cache entry has been created.
```

explorer-override

MAC キャッシュ・エクスプローラー・オーバーライドを追加します。このオーバーライドによって、一組の MAC アドレスが異なる MAC キャッシュとエクスプローラー・フロー特性を所有できます。 MAC キャッシュ記入項目

が作成されると、エクスプローラー・オーバーライドの構成順に、そのリストが探索されます。一致が見つかると、最初に一致したエクスプローラー・オーバーライドからの MAC キャッシュとエクスプローラーの関連パラメーターが使用されます。一致が見つからなければ、 DLSw グローバル MAC キャッシュとエクスプローラーの関連値が使用されます。

例 : add explorer-override

```
Enter MAC address value [000000000000]?400031740000
Enter MAC address mask [FFFFFFFFFFFF]?ffffffff0000
Database age timeout (0-1000 secs. Decimal)[0.0]?0
Max wait timer ICANREACH (1-1000 secs. Decimal) [2.0?]
Neighbor priority wait timer (0,0-5.0 secs. Decimal) [2.0]?0
Time to delay sending test response (0.0-5.0 secs. Decimal) [0.0]?
Forwarding explorers (E/L/D) [E]?

Enter position in explorer override list to insert new entry ....
  Record number (0=add at end of list) [0]?
Explorer override record has been created.
```

MAC address value と MAC address mask

この 2 つのフィールドを結合すると、一組の MAC アドレスを表します。特定の値とマスクの構成済み MAC キャッシュ・エクスプローラー・オーバーライド・レコードを、特定の MAC アドレスとして使用する必要があるかどうか判別する場合は、次のアルゴリズムが使用されます。

```
if ((<specific MAC address>AND<override's mask>) == <override's value>)
match on explorer override is found; use override's value
```

Database age timeout

未使用 DLSw 項目を保留する時間の長さを指定します。 データベース項目は、あて先 MAC アドレスをそれらに到達できる DLSw ピアの組み合わせにマップします。

ゼロの値は、このデータベース内の項目が経過する必要がないことを指定します。これは、ダイヤル・インターフェースを介して近隣 TCP 接続を稼働するときに有用な場合がありますが、これは他のいくつかの DLSw 機能を使用不能にするので、一般的にはお勧めしません。

Max wait timer ICANREACH

前に伝送した CANUREACH に関して ICANREACH 応答を待つ時間の長さを指定します。

Neighbor priority wait timer

近隣の選択前、探索中に待つ時間の長さを指定します。これにより、たとえ ICANREACH メッセージによる応答は最初でなくても、優先順位が上位の近隣が選択されることができます。

値が 0 では、近隣優先順位フィーチャーが使用されないことを示します。MAC アドレスに関して DLSw ピア情報がキャッシュに入れられていることはありません。CANREACH が必ず送信され、ICANREACH を最初に送信した DLSw ピアが使用されます (その優先順位に関係なく)。

Delay sending TEST response

MAC アドレスの探索完了後、TEST 応答の送信前に待つ時間の長さ。これが役立つのは、DLSw ピアを経由して同じ MAC アドレスに到達

できる同じブリッジ LAN 上に、DLSw 2210 が 2 つある場合です。一方の DLSw 2210 を優先したければ、優先度の低い方の DLSw 2210 では、TEST 応答を遅らせることができます。

Forwarding explorers

エクスプローラーは、すべての適用対象 DLSw ピアに転送するのか、ローカル TCP 接続上にだけ転送するのか、まったく転送しないのかを指定します。

Position in explorer override list to insert new entry

最初に一致した MAC キャッシュ・エクスプローラー・オーバーライドの一致が使用されるので、エクスプローラー・オーバーライド記入項目が構成される順序が重要になります。このフィールドでは、この新規記入項目を現行オーバーライド・リストのどこに挿入するかを指定します。**list explorer-override** コマンドを使用して、現行エクスプローラー・オーバーライド・リストを表示させて見ることができます。このフィールドにゼロという値が指定されると、新規記入項目は、現行リストの終わりに追加されます。

mac-list

ローカル MAC アドレス・リスト記入項目を追加します。ローカル MAC アドレス・リストは、追加されたすべてのローカル MAC アドレス・リスト記入項目で構成されます。ローカル MAC アドレス・リストは、この DLSw を使用して到達可能な MAC アドレスの集合を示すために各 DLSw ピアに送信されます。

例: add mac-list

```
Enter MAC Address Value[400000000000]? 10005a000000
Enter MAC Address Mask [ffffff000000]?

MAC list entry has been created.

For the new entry to take effect, you must restart or commit the change using
     't 5': SET MAC LIST
```

Enter MAC Address Value and Enter MAC Address Mask

これら 2 つのフィールドは、結合されると、この DLSw を使用して到達可能な MAC アドレスの集合を表します。ピア DLSw でフレームが受信されると、これら 2 つのフィールドは、以下のアルゴリズムで使用されます。

```
if ( (<frame's destination MAC address> AND <MAC Address Mask>)
     == <MAC Address Value> )
match on MAC address list found; forward frame to this DLSw
```

priority

サーキット優先順位指定変更記入項目を追加します。DLSw セッションが確立されるときに、サーキット優先順位指定変更のリストは、構成された順序で探索されます。発信元 SAP 範囲と発信元 MAC アドレス範囲ならびにあて先 SAP 範囲とあて先 MAC アドレス範囲の一致が見つかった場合は、一致するサーキット優先順位指定変更記入項目のセッションとエクスプローラー優先順位が使用されます。どのサーキット優先順位指定変更記入項目とも一致が見つからない場合には、省略時サーキット優先順位値が使用されます。

例: add priority

```
Enter range of source SAPs .....
  Lower source sap value [0]?
  Upper source sap value [FE]?
```

```
Enter range of source MAC addresses .....
  Lower source MAC address [000000000000]?
  Upper source MAC address [FFFFFFFFFFFF]?

Enter range of destination SAPs .....
  Lower destination sap value [0]?
  Upper destination sap value [FE]? c

Enter range of destination MAC addresses .....
  Lower destination MAC address [000000000000]? 10005a000000
  Upper destination MAC address [FFFFFFFFFFFF]? 10005affffff

Enter desired circuit priorities .....
Priority for session traffic (C/H/M/L) [M]? c
Priority for explorer traffic (C/H/M/L) [M]? m

Enter position in circuit priority override list to insert new entry .....
  Record number (0=add at end of list) [0]?
Circuit priority override record has been created.
```

Lower source sap value

Upper source sap value

これら 2 つのフィールドは、結合されると、このサーキット優先順位指定変更に割り当てられた発信元 SAP の範囲を表します。送信元 SAP の値が重要でない場合は、発信元 SAP 値の全範囲 (小さい方の発信元値が 0 で、大きい方の発信元値が fe) を指定してください。

Lower source MAC address

Upper source MAC address

これら 2 つのフィールドは、結合されると、このサーキット優先順位指定変更に割り当てられた発信元 MAC アドレスの範囲を表します。発信元 MAC アドレスが重要でない場合は、発信元 MAC アドレス値の全範囲 (小さい方の発信元 MAC アドレスが 000000000000 で、大きい方の発信元 MAC アドレスが ffffffffffff) を指定してください。

Lower destination sap value

Upper destination sap value

これら 2 つのフィールドは、結合されると、このサーキット優先順位指定変更に割り当てられたあて先 SAP の範囲を表します。あて先 SAP の値が重要でない場合は、あて先 SAP 値の全範囲 (小さい方のあて先 SAP 値が 0 で、大きい方のあて先 SAP 値が fe) を指定してください。

Lower destination MAC address

Upper destination MAC address

これら 2 つのフィールドは、結合されると、このサーキット優先順位指定変更に割り当てられたあて先 MAC の範囲を表します。あて先 MAC の値が重要でない場合は、あて先 MAC 値の全範囲 (小さい方のあて先 MAC アドレスが 000000000000 で、大きい方のあて先 MAC アドレスが ffffffffffff) を指定してください。

Priority for session traffic

このサーキット優先順位指定変更記入項目の範囲の発信元 SAP、発信元 MAC アドレス、あて先 SAP、およびあて先 MAC アドレスに一致するすべてのセッション・トラフィックに割り当てるサーキット優先順位。

Priority for explorer traffic
このサーキット優先順位指定変更記入項目の範囲の発信元 SAP、発信元 MAC アドレス、あて先 SAP、およびあて先 MAC アドレスに一致するすべてのエクスプローラー・トラフィックに割り当てるサーキット優先順位。

Position in circuit priority override list to insert new entry
最初の突き合わせサーキット優先順位指定変更の一致が使用されるため、サーキット優先順位指定変更記入項目が構成される順序は重要です。このフィールドは、この新規記入項目を現行サーキット優先順位指定変更リストのどこに挿入するかを指定します。**list priority** コマンドを使用すると、現行サーキット優先順位指定変更リストが表示されます。このフィールドにゼロという値が指定されると、新規記入項目は、現行リストの終わりに追加されます。

qllc X.25 ネットワーク上の QLLC ステーション、または QLLC ステーション用の DLSw あて先についてのサポートを追加します。QLLC ステーションとは、X.25 インターフェースを通じてルーターに接続された QLLC 装置を表すローカル・リンク・ステーションです。QLLC あて先とは、DLSw ネットワーク内の装置を指すアドレス・マッピングです。 その装置は、サポートされる DLC タイプのどれかを介して近隣 DLSw ルーターに接続され、QLLC 装置自体ではないことがよくあります。

構文:

addqllc destination
station

例: add qllc destination

```
Enter the connection id (1-8 alphanumeric chars) [ ]? conn1
Destination MAC address [000000000000]? 400031740000
Destination SAP in hex [4]?
QLLC destination record added/updated
```

Connection id
着信する Call_Request パケット内のコール・ユーザー・データのバイト 4-11 に突き合わせされる英数字ストリング。多くの QLLC プロダクトでは、この値はパスワードとして構成されています。
重要: QLLC あて先レコードが「ANYCALL」で構成されている場合は、(DTE アドレスまたは接続 ID に関係なく) DLSw はすべてのコールを受け入れます。すべての着信コールを受け入れるときには、セキュリティー上の問題があることに注意してください。

Destination MAC address
着信 QLLC コールによって開始されるセッション用のターゲットとして使用される MAC アドレスで、そこでは Call_Request パケットは上記の connection id に一致します。

Destination SAP
同じタイプのセッションに使用されるターゲット SAP

例: add qllc station

```
Interface # [0]? 1
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 2
```

```
Source MAC address [400000310104]?
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400011112323
Destination SAP in hex [0]? 4
PU type (2/4/5) [2]?
XID0 block num in hex (0-0xfff) [0]?
XID0 id num in hex (0-0xfffff) [0]?
New QLLC station record added
```

Interface #

それによって QLLC 装置がルーターに接続されている X.25 インターフェースの番号

PVC or SVC

それによって QLLC 装置が接続されているバーチャル・サーキットのタイプ (permanent (パーマネント) または switched (スイッチド))

Logical channel number

PVC の場合、QLLC ステーションが加入している先の X.25 チャネル番号。このフィールドは SVC には適用されません。SVC は、動的に割り当てられたチャネル番号を使用します。

DTE address

SVC の場合、QLLC ステーションがそれによって X.25 ネットワークに知られている「電話番号」。これは、ルーターによって行われるコールの場合はコールされた側のアドレスであり、QLLC ステーションからのコールの場合はコーリング側アドレスです。このフィールドは PVC には適用されません。PVC は、固定論理チャネル番号によって固有に識別することができます。

Source MAC address

この QLLC ステーションを残りの DLSw ネットワークに表す媒体アクセス制御アドレス。 これは、QLLC ステーションによって開始される DLSw セッションの場合は起点アドレスであり、DLSw ネットワークの他の装置によって開始されるセッションの場合はターゲット・アドレスです。

このアドレスは各ステーションに必要とされ、ルーター内で構成された QLLC および SDLC 装置のすべての発信元 MAC アドレスの間で固有である必要があります。 信頼性があるように働くには、このアドレスは、DLSw ネットワーク内のすべてのエンド・ステーション MAC アドレスの間で固有である必要があります。 省略時値は、ネットワーク内で固有であるように構成されます。 このアドレスおよびすべての DLSw MAC アドレスは、非標準 (トークンリング) ビット配列形式で表されます。

Source SAP

発信元 MAC アドレスとペアにされたサービス・アクセス・ポイント・アドレス。これは同様に使用されます。

Destination MAC address

QLLC 装置が接続される DLSw ネットワーク内のステーションを表す媒体アクセス制御アドレス。PVC の場合、DLSw は、QLLC 装置が正常にコンタクトされるとすぐにこのターゲット・アドレスにセッションを開始しようとします。SVC の場合、DLSw は、QLLC 装置が着信コールを行うとすぐに、このターゲット・アドレスへのセッションを開始します。

このアドレスの指定は必須ではありません。これを構成しない場合、QLLC ステーションは DLSw セッションのターゲットにだけなることができ、起点にはなることはできません。

Destination SAP

あて先 MAC アドレスとペアにされたサービス・アクセス・ポイント・アドレス。これは同様に使用されます。DLSw があて先 MAC アドレスとあて先 SAP を DLSw をセッションのターゲットとして使用するには、これらは非ゼロである必要があります。

PU type

QLLC ステーションの SNA 物理装置タイプ。 これは、次の値の 1 つをもつことができます。

2 PU 2.0 または T2.1 ノード。 これは、XID_null ポーリングに応答して XID_1s を送信する装置を表すこともできます。

4 サブエリア SNA ルーティング機能を実行する中間 SNA 制御装置。 これらは一般に別の NCP への中間ネットワーク・ノード (INN) で IBM の NCP ソフトウェアを実行し、 PU 2 装置への NCP 境界機能接続用ではありません。

5 DLSw ネットワーク内の PU 2.0 装置への境界機能接続を行うホストまたはフロントエンド・プロセッサー搭載のホスト (例えば、NCP 搭載の 37xx)。ホストが DLSw ネットワーク内の T2.1 装置と接続を行う場合、ホスト自体を T2.1 装置として構成する (つまり、PU type=2, XID0 block/id num=0) ことは望ましいが、指定は必須ではありません。

XID0 block num

ルーターが QLLC ステーションに代わって XID_0 を作成するときに使用する XID ブロック番号フィールド。 このフィールドは、PU タイプが 2 である場合にのみ適用され、入力するようプロンプト指示されます。T2.1 装置およびそれ自体で XID_null ポーリングに応答することができる任意の PU 2.0 装置の場合、このフィールドの指定は任意であるため、ゼロのままにしてください。はっきりわからない場合は、すべての PU2.0 QLLC 装置についてこれを埋め込み、すべての T2.1 装置についてゼロのまま残すのが最も安全です。 非ゼロの場合、これは、リンク・ステーション用の IBM NCP 交換大ノード構成内の対応する PU アドレス・フィールドに一致する必要があります。

XID0 id num

XID0 ブロック番号フィールドに付随する XID 識別子番号フィールド。 これは同じ目的で使用され、同じ状態で必要とされます。

sdlc 与えられた SDLC シリアル・インターフェース上の構成に SDLC リンク・ステーションを明確に追加するには、SDLC 情報を追加します。 **sdlc** コマンドは、SDLC 回線上の各 2 次ステーションごとに一度ずつ使用する必要があります。

例: add sdlc

```
DLSw config>add sdlc
Interface # [0]? 2
SDLC Address or 'sw' (switched call-in) [C1]?
```

```
Source MAC address [4000112402C1]? 4000003174d1
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000002
Destination SAP in hex [0]? 4
PU type (2/4/5) [2]?
XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xfffff) [0]? 00001
Poll with TEST (T), SNRM (S), or DELAYED SNRM (D) [T]?
```

Interface #

それによって SDLC 装置がルーターに接続されている SDLC インターフェースの番号

SDLC Address

接続しているリンク・ステーションの SDLC アドレス。01 ～FE または 『sw』。『Sw』 は、これが交換 SDLC コールイン・サーキットであることを示します。

Source MAC address

この SDLC PU 用の MAC アドレス。この値は、DLSw ドメイン内の接続された SDLC ステーションを識別します。これは、このルーターに接続されている SDLC および QLLC ステーション間で固有でなければならず、すべての LAN、SDLC、および QLLC 間で固有でなければなりません。

Source SAP in hex

発信元 MAC アドレスとともに、DLSw ドメイン内の SDLC エンド・ステーションを表します。

Destination MAC Address

接続先のリモート・リンク・ステーションの MAC アドレス。 MAC アドレスは非標準ビット配列 (トークンリング) 形式で表されます。リモート・エンド・ステーションがイーサネット上にある場合でも、これが当てはまります。そのような場合には、ASRT 監視 **flip** コマンドを使用して MAC アドレスを切り替える上で役立ててください。

注: これが交換 SDLC コールイン・サーキットである (SDLC アドレスとして 『sw』 で示されている) 場合には、あて先アドレスは 0 という値をとれません。

Destination SAP in hex

リンク・ステーションが立ち上がるときに接続を自動的に試行している場合に使用される SAP を定義します。この SAP が 0 の場合は、リンク・ステーションは受動モードにあり、回線確立を開始することはありません。この場合は、あて先 MAC アドレスは無視されます。

注: これが交換 SDLC コールイン・サーキットである (SDLC アドレスとして 『sw』 で示されている) 場合には、あて先 SAP は 0 という値をとれません。

PU type

SDLC ステーションの SNA 物理装置タイプ。これは、次の値の 1 つをもつことができます。

2 PU 2.0 または T2.1 ノード

4 サブエリア SNA ルーティング機能を実行する中間 SNA 制御装置。一般にこれらは別の NCP への中間ネットワーク・ノード (INN) で IBM の NCP ソフトウェアを実行し、PU 2 装置への NCP 境界機能接続用ではありません。

5 DLSw ネットワーク内の PU 2.0 装置への境界機能接続を行う、フロントエンド・プロセッサーを搭載した、または搭載しないホスト (例えば、NCP 搭載の 37xx)。 ホストが DLSw ネットワーク内の T2.1 装置と接続を行う場合、ホスト自体を T2.1 装置として構成する (つまり、PU type=2, XID0 block/id num=0) ことが必要です。

注: ユーザーは、交換 SDLC コールイン・サーキットにこのパラメーターを設定することはできません。2.0 という PU タイプが想定されます。

XID0 block num

ルーターが SDLC ステーションに代わって XID_0 を作成するときに使用する XID ブロック番号フィールド。このフィールドは、PU タイプが 2 である場合のみ適用され、入力するようプロンプト指示されます。これは任意選択であり、T2.1 装置およびそれ自体で XID_null ポーリングに応答できる任意の PU 2.0 装置についてはゼロのまま残す必要があります。よくわからない場合は、すべての PU2.0 SDLC 装置についてこれを埋め込み、すべての T2.1 装置についてゼロのまま残すのが最も安全です。非ゼロの場合、これは、リンク・ステーション用の IBM NCP 交換大ノード構成内の対応する PU アドレス・フィールドに一致する必要があります。

注: 交換 SDLC コールイン・サーキットについてこのパラメーターを非ゼロ値に設定すると、構成済み情報は XID_0 に入れられます。交換 SDLC コールイン・サーキットの場合、構成済み XID_0 ブロック番号は、別に使用されます。ソフトウェアは、コールイン・ステーションが、必ず、それ固有の XID_0 を作成するものと想定します。このパラメーターが非ゼロ値に設定されると、ステーションの XID_0 は、構成済みの値で修正されます。このパラメーターがゼロ値に設定された場合、ステーションの XID_0 は修正されません。

XID0 id num

XID0 ブロック番号フィールドに付随する XID 識別子番号フィールド。これは同じ目的で使用され、同じ状態で必要とされます。

Poll type

SDLC 装置をポーリングする方法と時点を定義します。

TEST インターフェースがアクティブになった時点で、TEST フレームを使用して、 SDLC 装置をポーリングします。

SNRM インターフェースがアクティブになった時点で、SNRM フレームを使用して、 SDLC 装置をポーリングします。

DELAYED SNRM
DLSW セッションが確立され、インターフェースがアクティブになった時点で、 SNRM フレームを使用して、SDLC 装置をポーリングします。

tcp この DLSw が接続を行うことができる DLSw ピアの内部アドレスを追加します。

例: add tcp

```
Enter the DLSw neighbor IP Address [0.0.0.0]?
128.185.14.1
Connectivity setup type (a/p) [p]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal)  [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive? (E/D) - [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

Enter the DLSw neighbor IP Address
接続を行いたい先の IP ネットワーク内のリモート DLSw ピアの IP アドレスを示します。

Connectivity setup type
この DLSw への TCP 接続をルーター始動時に行う必要がある (Active) のか、あるいは必要に応じて行う (Passive) のかを示します。これらのオプションの概要については、496ページの『TCP 接続、近隣発見、およびマルチキャスト探索』を参照してください。

Transmit Buffer Size
パケット送信バッファーのサイズ (1024 ～ 32768)。 省略時値は 5120 です。

Receive Buffer Size
パケット受信バッファーのサイズ (1024 ～ 32768)。 省略時サイズは 5120 です。

Maximum Segment Size
TCP セグメントの最大サイズ (64 ～ 16384)。 省略時値は 1024 です。

Enable/Disable Keepalive (E/D)
DLSw に TCP 接続 Keepalive メッセージを送信させたいかどうかを示します。省略時値は D (Disable (使用不能)) です。

Enable/Disable NetBIOS SessionAlive Spoofing (E/D)
NetBIOS SessionAlive I フレームを廃棄したい (DLSw パートナーに転送しない) かどうかを指示します。省略時値は D (Disable (使用不能)) で、フレームを廃棄しないことを意味します。

Neighbor Priority
近隣優先順位を上位、中位、または下位に指定することができます。優先順位を異にする複数の近隣ルーターを経て到達可能なあて先ステーションの場合は、DLSw は、優先順位が最も上位の近隣を経てそのステーションに至るサーキットを確立しようと試みます。

BAN

ban コマンドは、境界アクセス・ノード (BAN) 構成プロンプトへアクセスするのに使用します。BAN コマンドは、BAN 構成プロンプト (BAN config>) で入力します。これらのコマンドのそれぞれの説明については、94ページの『BAN』を参照してください。

構文:

ban

Close-Sap

close-sap コマンドは、指定されたサービス・アクセス・ポイント (SAP) に関する DLSw 交換を使用不能にするのに使用します。 これらの SAP は、ネットワーク上で構成するために LLC が使用します。

構文:

close-sap

例: close-sap

```
Interface #[1]?
Enter SAP in hex (range 0–FE), or one of the following:
   'SNA', 'NB', or LNM [0]? sna
SAP(s) 0 4 8 C closed on interface 1
```

Interface #

open SAPによって使用されるインターフェース番号

Enter SAP

個別の SAP を16 進数で入力することもできれば、SNA、NB (NetBIOS)、または LNM (LAN ネットワーク管理プログラム) を入力することもできます。

SAP を 16 進数で入力する場合は、その範囲は 0 ～ FE であり、SAP は偶数であることが必要です。

SNA を入力した場合は、SAP 0、4、8、および C がクローズされます。

NB を入力する場合は、SAP F0 がクローズされます。

LNM を入力する場合は、SAP 0、2、D4、F2、F4、F8、および FC がクローズされます。

Delete

DLSw 構成から SDLC リンク・ステーション、 TCP 近隣 IP アドレス、QLLC ステーションやあて先、キャッシュ記入項目、 MAC アドレス項目、サーキット優先順位指定変更、MAC キャッシュ・エクスプローラー・オーバーライドを除去する場合は、**delete** コマンドを使用します。

構文:

delete cache-entry

explorer-override

mac-list

priority

qllc...

sdlc

tcp

cache-entry

構成済み MAC キャッシュ記入項目を削除します。

例: delete cache-entry

```
Enter mac cache record number [1]? 1
MAC cache entry has been deleted
```

mac cache record number

削除される MAC キャッシュ記入項目のレコード番号。レコード番号は、**list cache all** 構成コマンドを実行することによって判別できます。

explorer-override

MAC キャッシュ・エクスプローラー・オーバーライド記入項目を除去します。

例 : delete explorer-override

```
Enter explorer override record number [1]?
Explorer override record has been deleted.
```

Explorer override record number

除去される MAC キャッシュ・エクスプローラー・オーバーライド記入項目のレコード番号。レコード番号は、**list explorer-override** コマンドを *talk 6* で実行すれば、判別できます。

mac-list

ローカル MAC アドレス・リスト記入項目を削除します。

例: delete mac-list

```
Enter mac list record number [1]? 1
Local MAC list entry 10005A000000 / FFFFFF000000 has been deleted.

For the deletion to take effect, commit the change using
  't 5': SET MAC-LIST.
```

mac list record number

削除される MAC リスト項目のレコード番号。 レコード番号は、**list mac-list all** 構成コマンドを実行することによって判別できます。

priority

サーキット優先順位指定変更記入項目を削除します。

例: delete priority

```
Enter circuit priority override record number [1]? 1
Circuit priority override record has been deleted.
```

Circuit priority override record number

削除されるサーキット優先順位指定変更項目のレコード番号。レコード番号は、**list priority** 構成コマンドを実行することによって判別できます。

qllc X.25 ネットワーク上の QLLC ステーションについて、または QLLC ステーション用の DLSw あて先についてサポートを除去します。

構文:

delete qllc destination
station

例: del q destination

```
DLSw config>del qllc dest
Enter the connection id (1-8 alphanumeric chars) [ ]? conn1
QLLC Destination record deleted
```

例: del q station

```
DLSw config>del qllc st
Interface # [0]? 2
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 4
QLLC station record deleted
```

sdlc ルーターが再始動された時点で DLSw がサービスを提供できるステーションのリストから、指定された SDLC リンク・ステーションを除去します。

構文:

delete sdlc

例: delete sdlc

```
Interface # [0]? 1
            SDLC Address or 'sw' (switched dial-in) [C1]?
            Record deleted
```

Interface #
SDLC リンク・ステーションに接続するルーターのインターフェース番号

SDLC Address
削除するリモート・リンク・ステーションの SDLC アドレス。値は 01 ～ FE の範囲内のものか、交換 SDLC コールイン・サーキットの場合は 『sw』 です。

tcp TCP 接続を行うことのできる DLSw ピアの IP アドレス (*ip_address*) を除去します。

構文:

delete tcp *ip_address*

例: delete tcp

```
IP Address [0.0.0.0]? 128.185.14.1
```

Disable

disable コマンドは、DLSw プロトコル、SDLC リンク・ステーション、LLC 切断機能、 動的近隣、QLLC ステーションもしくはインターフェース、またはローカルおよびリモート MAC アドレス・リストの使用を使用不能にするのに使用します。

構文 :

disable dls

dynamic-neighbors

llc

mac-list

qllc...

sdlc

dls ブリッジング・ルーターがすべての DLSw 構成済みインターフェースを介して DLSw 機能を実行できないようにします。

例: disable dls

dynamic-neighbors
ルーターが、**add tcp** コマンドを使用して構成された DLSw 近隣の IP アドレス*以外*の IP アドレスから着信する DLSw TCP 接続を受け入れないようにします。

例: disable dy

llc ルーターが DISC LLC フレームを出すことにより LLC 接続を能動的に終了させないようにします。 その代わりに、ルーターは LLC 接続を受動的に終了させます。 これにより、LLC 接続はエンド・ステーションでリンク終了を検出します。IBM ホストは能動的および受動的な切断に異なる応答をします。

このコマンドは DLSw 内の LLC の交換機能に影響を与えません。 LLC 交換機能を停止するには、**close-sap** コマンドを使用します。

例: disable llc

mac-list
ローカルまたはリモート MAC アドレス・リストの使用を使用不能にします。

構文:

mac-list local

remote

例 : disable mac-list local

```
Use of local MAC list is  DISABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

例 : disable mac-list remote

```
Use of remote MAC list is  DISABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

qllc 『callin』 を指定すると、DLSw が指定された X.25 インターフェース上の着信 QLLC コールを受け入れないようにすることができます。 これは省略時の状態です。インターフェースは DLSw への着信コールを許可するように明確に使用可能にする必要があります。

『station』 を指定すると、構成済みの QLLC ステーションが DLSw セッションの起点またはターゲットでないようにすることができます。

構文:

qllc callin

station

例: dis q callin

```
Select the interface to be disabled for incoming QLLC calls:
Interface # [0]? 1
Interface 1 is now disabled for incoming QLLC
calls
```

例: dis q station

```
Interface # [0]? 1
PVC or SVC [PVC]?
Logical channel number (1-4095) [0] 2
This QLLC station has been marked disabled
```

sdlc 指定された SDLC リンク・ステーションへの DLSw 接続を防止します。

例: disable sdlc

```
Interface # [0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Record updated
```

Enable

enable コマンドは、DLSw プロトコル、SDLC リンク・ステーション、LLC 切断機能、 動的近隣、QLLC ステーションもしくはインターフェース、 またはローカルおよびリモート MAC アドレス・リストの使用を使用不能にするのに使用します。

構文:

enable dls

dynamic-neighbors

ipv4 dlsw precedence

llc

mac-list

qllc...

sdlc

dls ルーター上での DLSw 操作を使用可能にします。

例: enable dls

dynamic-neighbors

ルーターが、**add tcp** コマンドを使用して構成された近隣の IP アドレス以外の IP アドレスからの着信 DLSw TCP 接続を受け入れるよう設定します。これは省略時の状態です。

ipv4 dlsw precedence

IP バージョン 4 について IP 優先ビットを設定するようルーターを設定します。これらの優先ビットは、DLSw トラフィックの優先順位付けを行うためにルーターの BRS フィーチャーによって読み取られます。

例 :

```
enable IPv4 DLSw Precedence
IPv4 Precedence is now enabled.
```

llc TCP 接続が失われるときに、ルーターが LLC 接続を終了できるようにします。

mac-list
ローカルまたはリモート MAC アドレス・リストの使用を使用不能にします。

構文:

mac-list local
remote

例 : enable mac-list local

```
Use of local MAC list is  ENABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

例 : enable mac-list remote

```
Use of remote MAC list is  ENABLED

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

qllc 『callin』 を指定すると、DLSw は指定した X.25 インターフェース上の着信 QLLC コールを受信するようになります。

『station』 を指定すると、構成済みの QLLC ステーションが DLSw セッションの起点またはターゲットになるようにすることができます。 これは、各構成済み QLLC ステーションの省略時の状態です。

構文:

qllc callin
station

例: en q callin

```
Select the X.25 interface to be enabled for incoming QLLC calls:
Interface # [0]? 1
Interface 1 now enabled for incoming QLLC
calls
```

例: en q station

```
Interface # [0]? 1
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 2
This QLLC station has been marked enabled
```

sdlc 指定された SDLC リンク・ステーションへの DLSw 接続を使用可能にします。

例: enable sdlc

```
Interface # [0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Record updated
```

Join-Group

join-group コマンドは、DLSw 近隣が相互間の TCP セッションを動的に見つけ、作成することができるようにし、マルチキャスト探索およびフレーム転送を使用可能にするために使用します。 これらの機能の概要については、496ページの『TCP 接続、近隣発見、およびマルチキャスト探索』を参照してください。 このコマンドを使

用するためには、使用されている IP インターネットがマルチキャスト・ルーティングをサポートしているものでなければならないので、OSPF Config> プロンプトで OSPF および MOSPF を構成する必要があります。

DLSw ルーターをグループに追加するときに、ユーザーは、グループ識別のグループ ID を使用したいかどうかを選択する (ルーターが対応するマルチキャスト・アドレスを構成する場合) か、マルチキャスト・アドレスを自分で指定します。グループ ID モデルは、構成する方が簡単ですが、非 IBM DLSw バージョン 2 製品とのマルチキャスト接続が必要な場合は、自分でマルチキャスト・アドレスを指定する必要があります。ルーターは、同時に 2 つのスタイルのグループのメンバーである場合があります。

グループ ID モデルを使用して、最大 64 個のグループに参加できます。DLSw ルーターをグループに割り当てると、DLSw プロトコルは、マルチキャスト・アドレスを作成するために 2 つの アドレスのうちの 1 つをグループ番号に自動的に追加します。ルーターはマルチキャスト・アドレスを伝送して、他のグループ・メンバーに対してそれ自体を識別し、それらのメンバーにパケットを伝送します。 グループ番号に追加される 2 つのアドレスは、DLSw クライアントおよびピアの場合は 225.0.1.0 であり、DLSw サーバーの場合は 225.0.1.64 です。 例えば、グループ 2 内のクライアントのマルチキャスト・アドレスは 225.0.1.2 になります。

構文:

join-group

例 :

次の例は、省略時 [G] についてのものです。例の後に記載されている説明には、(G) と (M) の両方の情報が含まれています。

```
DLSw config>join
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]? 2
Client/Server or Peer Group Member(C/S/P)- [P]? c
Connectivity Setup Type (A/P/) [P]?
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

Group member or specific multicast address
ユーザーに代わってルーターにマルチキャスト・アドレスを作成させたいかどうか、あるいはマルチキャスト・アドレスを提供したいかどうかを選択します。

Multicast IP address
マルチキャスト IP アドレスは、224.0.10.0 ～ 224.0.10.191 の範囲内の、DLSw バージョン 2 準拠マルチキャスト IP アドレスで、DLSw エクスプローラー・トラフィックの送受信に使用されます。

Read Only , Write Only or Read Write
このパラメーターは、構成済みマルチキャスト IP アドレスをエクスプローラ

ー・トラフィックの受信専用に使用する (読み取り専用) か、エクスプローラー・トラフィックの送信と受信の両方に使用する (読み書き) かを指示します。

Group ID
このルーターを加えたいグループの番号

Client/Server or Peer Group Member
このルーターがグループ内で引き受ける必要のある役割。クライアントの場合は C、サーバーの場合は S、またはピアの場合は P

Connectivity setup type
ルーターがグループを Active (能動的) または Passive (受動的) メンバーのどちらとして結合する必要があるかを示します。 これは、496ページの『TCP 接続、近隣発見、およびマルチキャスト探索』で説明されたように TCP 接続が他のグループ・メンバーと確立される時期を制御します。

Transmit Buffer Size
パケット送信バッファーのサイズ (1024 ～ 32768)。 省略時値は 5120 です。

Receive Buffer Size
パケット受信バッファーのサイズ (1024 ～ 32768)。 省略時サイズは 5120 です。

Maximum Segment Size
TCP セグメントの最大サイズ (64 ～ 16384)。 省略時値は 1024 です。

Enable/Disable Keepalive
DLSw にこのグループ内で立ち上げられた接続上で TCP Keepalive メッセージを送信させたいかどうかを示します。省略時値は D (使用不能) です。

Enable/Disable NetBIOS SessionAlive Spoofing (E/D)
NetBIOS SessionAlive I フレームを廃棄したい (このグループと関連付けられた DLSw パートナーに転送しない) かどうかを指示します。 省略時値は D (Disable (使用不能)) で、フレームを廃棄しないことを意味します。

Neighbor Priority (H/M/L) [M]?
近隣優先順位を上位、中位、または下位に指定することができます。優先順位を異にする複数の近隣ルーターを経て到達可能なあて先エンド・ステーションの場合は、DLSw は、優先順位が最上位の近隣を経てそのエンド・ステーションに至るサーキットを確立しようと試みます。

Leave-Group

leave-group コマンドは、**join-group** コマンドを使用して構成されたグループからルーターを削除したり、構成済みマルチキャスト・アドレスの使用を停止するのに使用します。

Leave-group は、指定されたグループに属する既存の TCP 接続に影響を生じません。

構文:

leave-group

例: leave-group

```
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]? 2
```

List

list コマンドは、SDLC リンク・ステーション、サーキット優先順位、SAP、TCP 近隣、グループ、動的近隣、QLLC ステーション、あて先、インターフェース、キャッシュ記入項目、 MAC アドレス・リスト項目、サーキット優先順位指定変更、MAC キャッシュ・エクスプローラー・オーバーライドに関する DLSw 情報を表示させる場合に使用します。

構文 :

list
- cache
- dls
- explorer-override
- groups
- llc2
- mac-list
- open
- priority
- qllc...
- sdlc
- tcp
- timers

cache 構成済み MAC アドレス・キャッシュ記入項目をリストします。

構文:

cache all
- entry-number

cache all

例: cache all

```
Entry  Mac Address   IP Address
-----  ------------  ---------------
    1  10005A123456  128.185.236.49
    2  10005A789ABC  128.185.236.49
```

cache entry-number

例: cache entry-number

```
Enter mac cache record number [1]?

Entry  Mac Address   IP Address
-----  ------------  ---------------
    1  10005A123456  128.185.236.49
```

dls **enable** および **set** コマンドを使って構成された情報を表示します。

例: list dls

(**list dls** コマンドからの出力は、**list DLCglobal** コマンドからの出力と同じです。)

explorer-override

構成済み MAC キャッシュ・エクスプローラー・オーバーライドを表示します。

例 : list explorer-override

```
   Explorer      Explorer      DB Age    Wait ICR  Nbr Pri   TESTrsp  Forwarding
ID MAC Value     MAC Mask      Timeout   Timeout   Timeout   Delay    Explorers
-- ------------  ------------  --------  --------  --------  -------  ---------
 1 400031740000  FFFFFFFF0000  DISABLED    20      DISABLED  0.0      AllPartners
 2 10005A000000  FFFFFF000000   1200       20      2.0       0.0      NoPartner
```

groups

groups config コマンドを使って構成されたこの DLSw ピアについてのグループ情報を表示します。(詳細については、570ページの『List』を参照してください。)

llc2 **set llc2** コマンドを使って構成された LLC2 パラメーターを表示します (これらのパラメーターの詳細な説明については、**set llc2** コマンド560を参照してください)。これらのパラメーターはインターフェースごとに設定されます。 **set llc2**コマンドを使用して LLC2 パラメーターへの変更が行われなかった場合は、出力は生成されません。

例: list llc2

```
SAP             t1    t2    ti    n2    n3    tw    rw    nw    acc
 0               1     1    30     8     1     2     2     1     0
```

SAP SAP 番号

t1 応答タイマー

t2 Ack (確認) 受信タイマー

ti 非活動タイマー

n2 最大再試行値

n3 ACK を送信する前に受信された I フレームの数

tw 送信ウィンドウ

rw 受信ウィンドウ

nw Ww を増分するのに必要な ACK 数

acc 現行の LLC2 導入ではアクセス優先順位を使用していません。 したがって、このパラメーターは常に省略時値 0 に解釈されます。

mac-list

構成済み MAC アドレス・リスト項目をリストします。

構文:

mac all

entry-number

mac-list all

例: list mac-list all

```
Entry  Mac Value     Mac Mask
-----  ------------  ------------
    1  10005A000000  FFFFFF000000
    2  400031740000  FFFFFFFF0000
```

mac-list entry-number

例 : list mac-list entry-number

```
Enter mac list record number [1]?

Entry  Mac Value     Mac Mask
-----  ------------  ------------
    1  10005A000000  FFFFFF000000
```

open すべてのオープン SAP およびその関連インターフェースを表示します。

例: list open

```
Interface   SAP(s)
    0        0  4
    1        0  4  8  C
```

priority

SNA サーキットおよび NetBIOS サーキットに関して選択されたサーキット優先順位、さまざまなサーキット優先順位間の伝送比率、および NetBIOS に関して構成された最大フレーム・サイズをリストします。

```
DLSw config> list priority
Default priority for SNA DLSw session traffic is           MEDIUM
Default priority for NetBIOS DLSw session traffic is       MEDIUM
Default priority for SNA DLSw explorer traffic is          MEDIUM
Default priority for NetBIOS DLSw explorer traffic is      MEDIUM


Message allocation by C/H/M/L priority is   4/3/2/1
Maximum frame size for NetBIOS is           2052


    Source/  SAP      MAC Address                  Session   Explorer
ID  Dest     Range    Range                        Priority  Priority
--  -------  -------  ---------------------------  --------  --------
 1  Source:  00 - FE  000000000000 - FFFFFFFFFFFF  CRITICAL  MEDIUM
    Dest  :  00 - 0C  10005A000000 - 10005AFFFFFF
 2  Source:  04 - 04  400031740000 - 40003174FFFF  CRITICAL  MEDIUM
    Dest  :  00 - FE  000000000000 - FFFFFFFFFFFF
```

サーキット優先順位は、重大、上位、中位、または下位です。 ルーターは、割り当てた優先順位値を使用して、特定のタイプのトラフィックのバースト長さを選択的に制限します。例えば、4/3/2/1 のメッセージ割り振りを使って SNA トラフィックに Critical (重大) という優先順位を割り当て、NetBIOS に Medium (中位) の優先順位を割り当てた場合、ルーターは 2 つの NetBIOS フレームを処理する前に 4 つの SNA フレームを処理します。以下同様です。この例では、使用可能な帯域幅の 2/3 は SNA トラフィックに割り当てられています。 ルーターが指定された優先順位を使用して帯域幅を割り振る場合、ルーターはバイトではなく、フレームを数えます。

qllc... QLLC インターフェース、あて先、またはステーションをリストします。

構文:

qllc callin
destination
station

例: li q callin

```
Interfaces enabled for incoming QLLC calls to DLSw:
    1
```

例: li q destination

```
          Connection ID   Dest  SAP/MAC
            CHICAGO       04   400000112323
```

パラメーターの説明については、539 ページの **add qllc destination** コマンドを参照してください。

例: li q station

```
1f  P/S  LCN/DTE addr  E/D Source SAO/MAC   Dest Sap/MAC     PU Blk/IdNum
 1  PVC  2             E  04 400000310104  04 400011112323   2 000/00000
 1  PVC  4             E  04 400000317402  04 400000000002   2 017/00001
 1  SVC  3721111       E  04 400000310103  00 000000000000   2 000/00000
```

ここでリストされたパラメーターについては、539 ページで説明します。『E/D』 は、ステーションが **disable qllc station** コマンドを介して使用不能にされたかどうかを示します。

sdlc **add sdlc link station** コマンドを使って構成された SDLC リンク・ステーション情報を表示します。

注: 交換 SDLC コールイン・サーキットは、アドレス・フィールドの『FF(sw)』 によって示されます。

例: list sdlc all

```
Net  Addr    Status    Source SAP/MAC    Dest SAP/MAC     PU Blk/IdNum  PollType
2    C1    Enabled   04 4000003174D1   00 400000000002   2 000/00000   TEST
2    C2    Enabled   04 4000103D01C2   00 000000000000   4
2    C3    Enabled   04 4000103D01C2   00 000000000000   2 017/00001   SNRM
3    FF(sw)  Enabled   04 4000103d01d2   04 400000000003  2  017/00002
```

Net SDLC リンク・ステーションに接続するインターフェースの ID 番号。

Addr 接続するリンク・ステーションの SDLC アドレスで、01 ～ FE の範囲内のアドレス、あるいは交換 SDLC コールイン・サーキットの場合は 『FF(sw)』 です。

Status
リンク・ステーションの状態で、enabled (使用可能) または disabled (使用不能)

Source SAP/MAC
DLSw ドメインに接続された SDLC ステーションを表す LLC SAP アドレスおよび MAC アドレス

Dest SAP/MAC
SDLC ステーションが活動状態になった時点で、接続された SDLC ステーションがサーキット確立を開始する先のリモート・エンド・ステーションの LLC SAP アドレスおよび MAC アドレス

PU 接続された SDLC 装置の SNA PU タイプで、以下のとおりです。

2 PU 2.0 または T2.1 ノード

4 別の PU 4 への INN サブエリア・ルーティングを実行する PU 4 (つまり、NCP と NCP の間)

5 DLSw ネットワーク内の PU 2.0 装置への境界機能接続を行うホストまたはフロントエンド・プロセッサー搭載のホスト (例えば、NCP 搭載の 37xx)

Blk/IdNum
ルーターが、接続された SDLC 装置の代わりに XID0 を生成するのに使用する XID0 ブロック番号および ID 番号。 このフィールドは、PU タイプ 2 装置についてのみ表示されます。

PollType
ルーターが SDLC ステーションとの最初の接続を行う場合に使用する SDLC フレームのタイプで、TEST フレームか SNRM フレームか遅延 SNRMフレーム (DLSw セッションの確立後に初めて送信される SNRM フレーム) のどれか。このフィールドは、PU タイプ 2 装置についてのみ表示されます。

tcp 構成済みの DLSw TCP 近隣を表示します。 近隣は、**add tcp** コマンドを使って構成されました。

例: `list tcp`

```
                    Xmit    Rcv     Max      Keep-    SesAlive
Neighbor        CST Bufsize Bufsize Segsize Alive    Spoofing Priority
--------------- --- ------- ------- ------- -------- -------- --------
128.185.122.234  p     5120    5120    1024   DISABLED DISABLED MEDIUM
128.185.14.1     p    5120    5120    1024  DISABLED DISABLED
MEDIUM
```

Neighbor
TCP 近隣の IP アドレス

CST 接続性セットアップ・タイプで、Active (能動的) または Passive (受動的)

Xmit Bufsize
パケット送信バッファーのサイズ (1024 ～ 32768)。 省略時値は 5120 です。

Rcv Bufsize
パケット受信バッファーのサイズ (1024 ～ 32768)。 省略時値は 5120 です。

Max Segsize
TCP セグメントの最大サイズ (64 ～ 16384)。 省略時値は 1024 です。

Keepalive
Keepalive (キープアライブ) 機能の状態で、enabled (使用可能) または disabled (使用不能)

SesAlive Spoofing
NetBIOS SesAlive スプーフィング機能の状態で、enabled (使用可能) または disabled (使用不能)

Priority
選択プロセスでの近隣ルーターの優先順位。 近隣優先順位は、上位、中位、または下位です。

timers さまざまな活動を待機するためにユーザーが指定した時間

例: list timers

```
Database age timer                 1200  seconds
Max wait timer for ICANREACH       20    seconds
Wait timer for LLC test response   15    seconds
Wait timer for SDLC test response  15    seconds
QLLC session retry timer           20    seconds
Join Group Interval                900   seconds
Neighbor priority wait timer       2.0   seconds
Neighbor Inactivity Timer            5   minutes
Time to delay sending test resp.   0.0   seconds
```

追加情報については、**list timers** コマンドを参照してください。

NetBIOS

NetBIOS 構成プロンプトを表示します。

NetBIOS コマンドの説明については、174ページの『NetBIOS コマンド』を参照してください。

構文:

netbios

Open-Sap

DLSw に使用させたい (DLSw サーキットの発信元または着信先として) すべての SAP に関して **open-sap** コマンドを出します。 よく使用される SNA SAP 値は 00、04、08、および 0C です。これらすべての SAP は簡略記号 『SNA』 を使用して、一緒にオープンすることができます。 NetBIOS SAP は F0 であり、『NB』 と呼ぶことができます。 LAN ネットワーク管理プログラム機能に関連する SAP は集合的に 『LNM』 と呼ばれます。 DLSw が SNA または NetBIOS エンド・ステーションに到達する場合に経由するインターフェース、LNM、または LNM が管理しているブリッジ上で、選択するプロトコルに関して SAP をオープンします。

構文:

open-sap

例: open-sap

```
Interface #[1]?
Enter SAP in hex (range 0-FE), or one of the following:
  'SNA', 'NB', or LNM [4]? sna
SAP(s) 0 4 8 C opened on interface 1
```

Interface #

SAP をオープンしたいインターフェースの番号

Enter SAP in hex

個別の SAP を16 進数で入力することもできれば、SNA、NB (NetBIOS を表す)、または LNM (LAN ネットワーク管理プログラムを表す) を入力することもできます。

SAP を 16 進数で入力する場合は、その範囲は 0 ～ FE であり、SAP は偶数であることが必要です。 同じインターフェース上で前に SAP 0 をオープンしないで SAP 4、8、または C を入力した場合は、SAP 0 が自動的にオープンされます。

SNA を入力した場合は、SAP 0、4、8、および C がオープンされます。

NB を入力した場合は、SAP F0 がオープンされます。

LNM を入力した場合は、SAP 0、2、D4、F2、F4、F8、および FC がオープンされます。

Set

set コマンドは、MAC アドレスから IP アドレスへのマッピング・キャッシュのサイズ、LLC2 パラメーター、最大数の DLSw セッション、SRB セグメント番号、プロトコル・タイマー、TCP 受信バッファー・サイズ、 TCP 動的近隣、QLLC 動作についてのパラメーター、MAC アドレス・リスト関連パラメーター、およびサーキット優先順位の指定変更を構成するのに使用します。

構文:

set
- cache
- dynamic-tcp
- llc2
- mac-list
- maximum
- memory
- priority
- qllc
- srb
- timers

cache **set cache** コマンドでは、MAC アドレス・IP アドレス間マッピング・キャッシュのサイズを指定できます。

DLSw はこのキャッシュに保管されている情報を使用して、リモート・ステーションへのルートを発見します。 キャッシュが大きいほど、DLSw が既知の TCP/IP 近隣すべてに CANUREACH フレームを送信せずに必要なのリモート・ステーションを見つける可能性は高くなります。

とはいえ、このキャッシュ・サイズを大きく設定しすぎないようにする必要があります。 大きく設定しすぎると、ルーター上のメモリーが使い尽くされ、実際の DLSw セッションに必要なメモリーに食い込みます。その結果、ルーターで扱える DLSw セッションの数が減ることになります。

例: `set cache`

```
MAC  IP cache size (4 - 65535) [128]?
```

dynamic-tcp

動的近隣 TCP 接続 (つまり、**add tcp** コマンドによって定義されていない近隣から着信接続する TCP 接続) についてさまざまな TCP パラメーターを指定することができます。 DLSw がこれらの値を使用するのは、動的近隣が使用可能にされていない場合のみです。

例: `set dyn`

```
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

ここでリストされているパラメーターの説明については、544 ページの **add tcp** コマンドを参照してください。

llc2 特定の SAP について特定の LLC2 属性を構成できます。

例: set llc2

```
Enter SAP in hex (range 0-F0)  [0]?  04
Reply timer (T1) in sec. [1]?
Receive Ack timer (T2) in 100 millisec. [1]?
Inactivity Timer (Ti) in sec. [30]?
Transmit Window (Tw), 1-127, 0=default [2]?
Receive Window (Rw), 127 Max [2]?
Acks needed to increment Ww (Nw) [1]?
Max Retry value (N2) [8]?
Number I-frames received before sending ACK (N3) [1]?
```

Enter SAP in hex
調整したい SAP 番号。 値は 0 ～ FE の範囲です。

Reply timer (T1)
このタイマーは LLC2 ピアが他の LLC2 ピアから必要な確認または応答を受信しないときに時間満了になります。

Receive Ack timer (T2)
受信された I 形式のフレームに確認を送信するのに要する遅延で、単位はミリ秒。

Inactivity Timer (Ti)
このタイマーは、LLC が指定された時間の間にフレームを受信しないと、時間満了になります。このタイマーが時間満了になると、LLC2 ピアは、LLC2 ピアが応答するか N2 再試行カウントを超えるまで、RR を伝送します。省略時値は 30 秒です。

Transmit Window (Tw)
RR を受信する前に送信することができる I フレームの最大数。値は 1 ～ 127 の範囲です。 0 は Tw を省略時値に設定します。 省略時値は 2 です。

Receive Window (Rw)
LLC2 ピアがリモート・ホストから受信することができる無応答の順次に番号付けされた I フレームの最大数

Acks needed to increment Ww (Nw)
これは、動的ウィンドウ操作アルゴリズム作業に影響を及ぼします。エラー状態の後の確認の数を指定します。省略時値は 1 です。作業ウィンドウ (Ww) は、送信ウィンドウ (Tw) の動的に変化するシャドーです。LLC エラーが検出されると、作業ウィンドウ (Ww) は 1 にリセットされます。 'Acks needed to increment Ww' 値は、Ww を 1 だけ増分する前にステーションが受信する必要のある ack (確認) の数を指定します。 Ww は、Ww = Tw になるまで、このようにして引き続き増分されていきます。

Max Retry value (N2)

非活動タイマー (Ti) が時間満了になるときに LLC2 ピアが確認を受信せずに RR を伝送する最大回数

Number I-frames received before sending ACK (N3)

この値は T2 タイマーで、受信された I フレームへの確認トラフィックを減らすために使用されます。 このカウンターは指定した値に設定され、I フレームが受信されるたびに減分されます。 このカウンターが 0 に達するか、T2 タイマーが時間満了になると、確認が送信されます。

良好なパフォーマンスを保証するには、N3 をリモート LLC の Tw より小さい値に設定してください。 省略時値は 1 です。

mac-list

ローカル MAC アドレス・リストを排他的に修正します。

例: set mac-list

```
Local MAC list exclusivity (E=exclusive, N=non-exclusive) [N]? e

MAC list parameter set.

For the change to take effect, restart or commit the change using
  't 5' : 'SET MAC-LIST'.
```

Local MAC list exclusivity

ローカル MAC リストが exclusive (排除) (この DLSw を介してアクセスできるすべての MAC アドレスを表します) であるか、non-exclusive (非排除) (この DLSw を介してアクセスできる MAC アドレスの集合を表します) であるかを指示します。

maximum

DLSw プロトコルがサポートできる DLSw セッションの最大数を設定します。 これには SNA セッション (サーキット) と NetBIOS セッションの両方が含まれます。

例: set maximum

```
Maximum number of DLSw sessions (1-60000) [1000]?
```

memory

DLSw で使用可能なメモリーの合計量、および各 DLSw セッションごとに、また NetBIOS UI フレームで使用可能なメモリーの量を指定することができます。ルーターはセッションごとの値および UI フレームの場合の値を使用して、フロー制御アルゴリズムがデータ源に背圧を加えるのを開始/停止し、UI フレーム・トラフィックの廃棄を開始/停止する限界を設定します。

ルーターは現在、全体の DLSw 割り振り値を使用していないので、これはその省略時値のままにしておくことができます。 グローバル送信プールおよびグローバル受信プール (NetBIOS UI フレーム・プールではなく) を参照する DLS.161 メッセージは、いずれも無視することができます。 DLSw 歩調合せアルゴリズムは、これらの論理プールを使用するのではなく、物理メモリーの状況を使用して、公示するウィンドウ・サイズを決めます。

LLC、SDLC、および QLLC セッション割り振り値は、 LLC、SDLC、および QLLC 接続 装置から、それぞれ、 TCP へ流れるデータのバッファリングに関するサーキットあたりの (エンド・ステーション・ペア) 限界を提供します。ルーターがこれらの限界に到達すると、該当するエンド・ステーション

に RNR/RR を送信します。 セッションごとのプールの状態は、DLSw 監視コマンド **list dlsw memory** によって、活動セッションのリストの一部として見ることができます。

例: set memory

```
Number of bytes to allocate for DLSw (at least 2638)[140800]?
Number of bytes to allocate per LLC session [8192]?
Number of bytes to allocate per SDLC session [4096]?
Number of bytes to allocate per QLLC session [4096]?
Number of bytes to allocate for NetBIOS UI-frames [40960]?
```

NetBIOS UI フレーム割り振りは、DLSw が任意の一時点でバッファーできる UI フレーム (NetBIOS DATAGRAM、NAME_QUERY、ADD_NAME_QUERY などを含む) の数を制御します。 この限界に達すると、DLSw は受信した NetBIOS UI フレームを廃棄するので、起点エンド・ステーションによるその再送が必要です。 したがって、この限界を低く設定しすぎると、NetBIOS サーキット確立の試みが断続的に失敗する原因になりかねません。 ルーターは ELS メッセージ DLS.161 (グローバル NetBIOS UI フレーム・プールを参照する) を使用して、フレーム廃棄条件を報告します。

priority

SNA サーキットおよび NetBIOS サーキットに関して使用するサーキット優先順位の指定、ならびにこれらの優先順位*間* のトラフィック比率の指定を行うことができます。 **set priority** コマンドを使用して、サーキット優先順位を重大、上位、中位、または下位 (重大から下位に降順) として指定することができます。 ルーターはユーザーが割り当てた優先順位を使用して、近隣に伝送する特定のタイプのトラフィックのバースト長さを選択的に制限します。

この機能が働くのは、DLSw メッセージが TCP に送信される前に待ち行列で順番を待つ輻輳 (ふくそう) 時だけです。 例えば、SNA トラフィックに優先順位「重大」 (省略時解釈でメッセージ割り振り値 4 に対応する) を割り当てたとします。ついで NetBIOS セッションおよびエクスプローラー・トラフィックに優先順位「中位」 (メッセージ割り振り値 2 に対応する) を割り当てた場合は、ルーターは、SNA フレームを 4 つ伝送してから、NetBIOS フレームを 2 つ伝送します。 ルーターは、NetBIOS フレームを 2 つ処理すると、再度 SNA フレームを 4 つ処理し、以後についても同様です。 ユーザー割り当ての優先順位を使用して帯域幅を割り振る際に、ルーターはバイトではなくフレームを数えます。 また、特定のサーキットの優先順位は、サーキット立ち上げ時に、近隣ルーターと折衝されます。したがって、近隣ルーターは、ユーザーがこのルーターに関して指定した構成値に基づいた方針以外の方針を使用して、新しいサーキットの優先順位を確立する場合があります。 SNA および NetBIOS セッションならびにエクスプローラー・トラフィックに異なる優先順位を割り当てたい場合もあります。

set priority コマンドを使用すると、このルーターを経由するすべての NetBIOS サーキットに関する最大フレーム・サイズを設定することもできます。 NetBIOS エンド・ステーションには、許容されている最大のフレームを生成する傾向があり、その結果、低速リンク上の 1 つのフレームが数秒間にわたってそのリンクを占有するため、対話式 SNA トラフィックに悪影響をもたらすことになります。 このような影響を抑制するために、ルーターがソース・ルート・ブリッジング・メカニズムを使用して、NetBIOS エンド・ステ

ーションに信号を送る最大フレーム・サイズを小さい値に設定することができます。 ネットワーク内に NetBIOS を実行する透過型ブリッジ (TB) セグメントがある場合は、最大 NetBIOS フレーム・サイズは、少なくとも 1470 に設定します。

例: set priority

```
Default priority for SNA DLSw session traffic (C/H/M/L) [M]?
Default priority for NetBIOS DLSw session traffic (C/H/M/L) [M]?
Default priority for SNA DLSw explorer traffic (C/H/M/L) [M]?
Default priority for NetBIOS DLSw explorer traffic (C/H/M/L) [M]?
Message allocation by C/H/M/L priority (4 digits) [4/3/2/1]?
Maximum NetBIOS frame size (516, 1470, 2052, or 4399) [2052]? 516
```

qllc 着信する動的 QLLC コール用の起点 MAC アドレスとして使用される動的に割り当てられた MAC アドレスの範囲を指定することができます。

範囲についてのベース MAC アドレス 『X』、および動的アドレスの最大数 『N』 を提供することにより範囲を指定します。 DLSw は、X ～ X+(N-1) の範囲で MAC アドレスを選択します。

例: set qllc

```
QLLC base MAC address [40514C430000]?
Maximum QLLC dynamic addresses (0-max sess) [64]?
```

srb トークンリング・ネットワーク上で DLSw を識別するソース・ルーティング・ブリッジ (SRB) のセグメント番号を設定します。 セグメント番号は 3 桁の 16 進値として指定します。

例: set srb

```
Enter segment number hex (1-FFF) [5]?
```

timers DLSw プロトコル・タイマーを設定します。

例: set timers

```
DLSw config>set timers
Database age timeout (0-10000 secs. Decimal) [1200]? 480
Max wait timer ICANREACH (1-1000 secs. Decimal) [20]?
Wait timer LLC test response (1-1000 secs. Decimal) [15]?
Wait timer SDLC test response (1-1000 secs. Decimal) [15]?
QLLC session retry timer (1-1000 secs. Decimal) [20]?
Group join timer interval (1-60000 secs. Decimal) [900]? 180
Neighbor priority wait timer (0, 1.0-5.0 secs. Decimal) [2.0]?
Neighbor Inactivity Termination Timer (0-255 minutes) [5]?
Time to delay sending test response (0.0-5.0 secs. Decimal) [0.0]?
DLSw timer values have been
set.
```

Database age timeout

未使用 DLSw 項目を保留する時間の長さを指定します。データベース項目は、あて先 MAC アドレスをそれらに到達できる DLSw ピアの組み合わせにマップします。

ゼロの値は、このデータベース内の項目が経過する必要がないことを指定します。これは、ダイヤル・インターフェースを介して近隣 TCP 接続を稼働するときに有用な場合がありますが、これは他のいくつかの DLSw 機能を使用不能にするので、一般的にはお勧めしません。

Max wait timer

前に伝送した CANUREACH に関して ICANREACH 応答を待つ時間の長さを指定します。

Wait timer LLC test response
あきらめる前に LLC テスト応答を待つ時間の長さを指定します。

Wait timer SDLC test response
あきらめる前に SDLC テスト応答を待つ時間の長さを指定します。

QLLC session retry timer
DLSw セッションを開始するために QLLC ステーションに再び連絡を試みる前にルーターが待つ時間

Group join timer interval
グループ公示メッセージのクラスターを同報通信する前に、ルーターが待つ時間の量。 これは、グループ・ベースの DLSw 機能が中間のルーター障害から回復するのにかかる時間の長さに影響を与えることができ、マルチキャスト機能が働くのに必要なオーバーヘッドの量に影響を与えることができます。 この値は、DLSw の IP マルチキャスト機能を使用するのではなく TCP 接続を構成する場合は、使用されません。

Neighbor priority wait timer
近隣を選択する前に探索時に待つ時間の長さ。これにより、たとえ ICANREACH メッセージによる応答は最初でなくても、優先順位が上位の近隣が選択されることができます。

値が 0 では、近隣優先順位フィーチャーが使用されないことを示します。それぞれの MAC アドレスに関して DLSw ピア情報がキャッシュに入れられていることはありません。CANUREACH が必ず送信され、 ICANREACH を最初に送信した DLSw ピアが使用されます (その優先順位に関係なく)。

Inactive neighbor termination timer
DLSw が非アクティブ (ゼロ・セッション) の受動 TCP 接続をダウンさせるのに待つ時間。

Delay sending TEST response
MAC アドレスの探索完了後、TEST 応答の送信前に待つ時間の長さ。これが役立つのは、DLSw ピアを経由して同じ MAC アドレスに到達できる同じブリッジ LAN 上に、DLSw 2210 が 2 つある場合です。一方の DLSw 2210 を優先したければ、優先度の低い方の 2210 では、 TEST 応答を遅らせることができます。

DLSw 監視コマンド

この節では、DLSw 監視コマンドについて説明します。 これらのコマンドは即時に有効になりますが、ルーターの SRAM 構成の部分にはなりません。したがって、監視コマンドを使用すると、ルーターの構成にリアルタイムの変更を加えることができますが、こうして加えた変更は、ルーターを再始動すると、 SRAM 構成によって上書きされます。監視は以下のアクションから構成されます。

- 現在ルーターによって使用中のプロトコルおよびネットワーク・インターフェースを監視する。

- ルーターの活動およびパフォーマンスに関連する ELS (イベント・ログ・システム) メッセージを表示する。
- SRAM 構成に永続的に影響を与えずに、DLSw 構成に実時間変更を行う。

DLSw 監視環境へのアクセス

DLSw 監視環境 (GWCON プロセス) に入るには、下に挙げる例で示すように、**talk 5** (または **t 5**) を OPCON (*) プロンプトで入力し、**protocol dls** を GWCON (+) プロンプトで入力します。

```
MOS Operator Control

* talk 5
+ protocol dls
 DLS>
```

DLSw 監視コマンド

この節では、表34 にリストされている DLSw 監視コマンドについて説明します。データベースから情報を収集するには、これらのコマンドを使用してください。

表 34. DLSw 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。xxxiiiページの『ヘルプの入手』 を参照してください。
Add	現行構成に SDLC リンク・ステーション、TCP 近隣 IP アドレス、 QLLC ステーションやあて先、キャッシュ記入項目、MAC アドレス・リスト項目、サーキット優先順位指定変更、または MAC キャッシュ・エクスプローラー・オーバーライドを動的に追加します。
BAN	特定の BAN コンソール・コマンドを入力するために境界アクセス・ノード (BAN) コンソール・プロンプトにアクセスすることができます。詳しくは、65ページの『第4章 境界アクセス・ノード (BAN) フィーチャーの使用』 を参照してください。
Close-Sap	現在オープンされている LLC SAP を動的にクローズします。LLC インターフェースはネットワーク上で通信するために SAP を使用します。
Delete	SDLC リンク・ステーション、DLSw セッション、TCP 近隣 IP アドレス、QLLC ステーションやあて先、キャッシュ記入項目、MAC アドレス・リスト項目、サーキット優先順位指定変更、MAC キャッシュ・エクスプローラー・オーバーライドを動的に除去します。
Disable	LLC 交換機能、SDLC リンク・ステーション、動的近隣、QLLC ステーションもしくはインターフェース、またはローカルおよびリモート mac アドレス・リストの使用を動的に使用不能にします。
Enable	LLC 交換機能、SDLC リンク・ステーション、動的近隣、QLLC ステーションもしくはインターフェース、またはローカルおよびリモート mac アドレス・リストの使用を動的に使用可能にします。
Join-Group	ルーターを SRAM 構成とは異なる DLSw グループに動的に追加します。
Leave-Group	指定した DLSw グループからルーターを動的に除去します。
List	SDLC リンク・ステーション、SAP、サーキット優先順位、DLSw グループ、DLSw セッション、QLLC あて先、ステーション、およびインターフェースについてのセッション、キャッシュ記入項目、ならびに mac アドレス・リスト項目についての情報を表示します。このコマンドによって、TCP 機能、接続、および統計に関する詳細情報も得られます。

表 34. DLSw 監視コマンドの要約 (続き)

コマンド	機能
NetBIOS	NetBIOS サポート・プロンプトへアクセスすることができます。
Open-SAP	LLC SAP を動的にオープンします。
Set	LLC2 パラメーター、最大 DLSw セッション数、メモリー割り振り、プロトコル・タイマー、サーキット優先順位、動的近隣についてのパラメーター、QLLC 動作についてのパラメーター、または mac アドレス・リスト関連のパラメーターを動的に変更します。
Test	現行 MAC アドレス・キャッシュおよび MAC アドレス・リストに照らして特定の MAC アドレスをテストします。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、SRAM 構成に影響を及ぼさないで、SDLC リンク・ステーション、TCP 近隣 IP アドレス、QLLC ステーションやあて先、キャッシュ記入項目、 MAC アドレス・リスト項目、サーキット優先順位指定変更、MAC キャッシュ・エクスプローラー・オーバーライドを動的に構成する場合に使用します。

構文 :

add
- cache-entry
- explorer-override
- mac-list
- priority
- qllc...
- sdlc
- tcp

例およびフィールドの説明については、535ページの『Add』 の構成の章に記載されている **add** コマンドを参照してください。

BAN

ban コマンドは、BAN (境界アクセス・ノード) 監視プロンプトにアクセスするのに使用します。**ban** コマンドは、DLS> プロンプトから入力してください。

構文:

ban

BAN 監視プロンプトにアクセスすると、特定の監視コマンドの入力が開始できます。BAN 監視コマンドの説明については、65ページの『第4章 境界アクセス・ノード (BAN) フィーチャーの使用』を参照してください。

随時 DLSw> プロンプトに戻るには、**exit** コマンドを入力します。

Close-SAP

DLSw SRAM 構成に影響を及ぼすことなく、指定した SAP の DLSw の使用を動的に使用不能にするには、**close-sap** コマンドを使用してください。

構文:

close-sap

例: close-sap

```
Interface #[1]?
Enter SAP in hex (range 0-FE), or one of the following:
  'SNA', 'NB', or LNM [0]? 04
SAP(s) 4 closed on interface 1
```

(**close-sap** のパラメーターの説明については、545 ページで行っています。)

Delete

delete コマンドは、 DLSw SRAM 構成に影響を及ぼさないで、SDLC リンク・ステーション、 DLSw セッション、 TCP 近隣 IP アドレス、QLLC ステーションや着信先、キャッシュ記入項目、MAC アドレス・リスト項目、サーキット優先順位指定変更、または MAC キャッシュ・エクスプローラー・オーバーライドを動的に削除する場合に使用します。このコマンドの使用によって、既存のセッションもすべて終了します。

構文:

delete

- cache-entry
- dls
- explorer-override
- mac-list
- priority
- qllc...
- sdlc
- tcp

cache-entry

指定されたキャッシュ記入項目を削除します。

例: delete cache-entry

```
Enter MAC Address [400000000000]? 10005a123456
MAC 10005A123456 / IP address 128.185.122.234 configured cache entry deleted.
```

dls

現在アクティブな DLSw セッションを除去します。

例: delete dls

```
Session identifier [1]?
```

explorer-override

指定された MAC キャッシュ・エクスプローラー・オーバーライド記入項目を除去します。

例 : delete explorer-override

```
Enter explorer override record number [1]?
Explorer override record has been deleted.
```

mac-list

指定された mac アドレス・リスト項目を削除します。

例: delete mac-list

```
Enter mac list record number [1]?

Local MAC list entry 10005A000000 / FFFFFF000000 has been deleted.
```

priority

指定されたサーキット優先順位指定変更記入項目を削除します。

例: delete priority

```
Enter circuit priority override record number [1]?
Circuit priority override record has been deleted.
```

qllc QLLC あて先またはステーションについてのサポートを除去します。 現在アクティブなステーションを削除する場合、それを行う前に、DLSw はユーザーが接続をダウンさせたいと希望しているか確認します。あて先を削除することは既存の接続に影響を及ぼしません。

構文:

qllc destination

station

例: del q destination

```
Enter the connection id (1-8 alphanumeric chars) [ ]? conn1
QLLC Destination record deleted
```

例: del q station

```
Interface # [0]? 2
PVC or SVC [PVC]?
Logical channel number (1-4095) [0]? 4
QLLC station record deleted
```

sdlc SDLC リンク・ステーションの構成情報に影響を及ぼすことなく、現在アクティブな SDLC リンクをクローズします。

例: delete sdlc

```
Interface #[0]? 1
SDLC Address or 'sw' (switched dial-in) [C1]?
Link closed
```

Interface #

SDLC リンク・ステーションに接続するルーターのインターフェース番号

SDLC Address

削除するリモート・リンク・ステーションの SDLC アドレスで、01 ～ FE の範囲にあるか、あるいは交換 SDLC コールイン・サーキットの場合は 『sw』 です。

tcp TCP 接続が行われる先の DLSw ピアの IP アドレス (*ip_address*) を除去します。 TCP 接続はクローズされています。

例: delete tcp

```
IP Address [0.0.0.0]? 128.185.14.1
```

Disable

disable コマンドは、DLSw SRAM 構成に影響を与えずに、LLC 切断機能、DLSw プロトコル、 SDLC リンク・ステーション、動的近隣、QLLC ステーションまたはインターフェース、またはローカルおよびリモート MAC アドレス・リストの使用を動的に使用不能にするために使用します。***entire*** DLSw 機能を監視から使用不能にすることは、サポートされていません。

構文:

disable dynamic-neighbors
llc
mac-list
qllc...
sdlc

(**disable** コマンドのパラメーターを使用する例については、548 ページ以降に挙げてあります。)

Enable

enable コマンドは、DLSw SRAM 構成に影響を与えることなく、LLC 切断機能、SDLC リンク・ステーション、動的近隣、QLLC ステーションまたはインターフェース、またはローカルおよびリモート・アドレス・リストの使用を動的に使用可能にするために、使用します。

構文:

enable dynamic-neighbors
llc
mac-list
qllc...
sdlc

(**enable** コマンドのパラメーターを使用する例については、549 ページ以降に挙げてあります。)

Join-Group

join-group コマンドは、DLSw に、近隣発見、マルチキャスト検査、およびマルチキャスト・フレーム転送機能の実行を開始させるのに使用します。

追加情報および例については、493ページの『第25章 DLSw フィーチャーの使用』を参照してください。

構文:

join-group

Leave-Group

leave-group コマンドは、DLSw に、近隣発見、マルチキャスト検査、およびおよび指定されたグループ内でのもしくは指定のマルチキャスト・アドレスを使用したマルチキャスト・フレーム転送機能の実行を停止させるのに使用します。 この変更は、DLSw SRAM 構成に影響を与えずに行われます。**Leave-group** は、指定されたグループまたはマルチキャスト・アドレスで立ち上げられた既存の TCP 接続を終了します。追加情報および例については、493ページの『第25章 DLSw フィーチャーの使用』を参照してください。

構文:

leave-group

例 :

```
Configure group member (G) or specific multicast address (M) -  [G]?
Group ID (1-64 Decimal) [1]? 2
```

List

list コマンドは、SDLC リンク・ステーション、サーキット優先順位、SAP、TCP 近隣、グループ、動的近隣、QLLC ステーション、あて先とインターフェース、構成済みキャッシュ記入項目、MAC アドレス・リスト項目、MAC キャッシュ・エクスプローラー・オーバーライドに関する DLSw 情報を表示させる場合に使用します。

構文:

list dls...
explorer-override
groups...
llc2...
mac-list
priority...
qllc...
sdlc...
tcp...
timers

dls DLSw プロトコルに関係する情報を表示します。 DLSw パラメーターについてのオプション (global (グローバル)、memory (メモリー)、sessions (セッション)、および cache (キャッシュ)) は、以下およびこれ以降のページで説明されています。

Global
構成済みの一般 DLSw パラメーターの操作値を表示します。

Memory
構成済みの DLCメモリー情報および現行のメモリー使用を表示します。

Sessions
発信元、あて先、状態、フラグ、あて先 IP アドレス、およびセッション ID を含む、現行の DLCセッション情報を表示します。

cache DLSw MAC アドレス・キャッシュ内のアドレスをリストします。

dls global
DLS グローバル・パラメーター情報を表示します。

例: `list dls global`

```
DLSw is                                ENABLED
LLC2 send Disconnect is                ENABLED
Dynamic Neighbors is                   ENABLED
SRB Segment number                     020
MAC <-> IP mapping cache size          128
Max DLSw sessions                      1000
DLSw global memory allotment           141312
LLC per-session memory allotment       8192
SDLC per-session memory allotment      4096
QLLC per-session memory allotment      4096
NetBIOS UI-frame memory allotment      40960
Dynamic Neighbor Transmit Buffer Size  5120
Dynamic Neighbor Receive Buffer Size   5120
Dynamic Neighbor Maximum Segment Size  1024
Dynamic Neighbor Keep Alive            DISABLED
Dynamic Neighbor SessionAlive Spoofing DISABLED
Dynamic Neighbor Priority              MEDIUM
QLLC base source MAC address           40514C430000
QLLC maximum dynamic addresses         64
Type of local MAC list                 NON-EXCLUSIVE
Use of local MAC list is               ENABLED
Use of remote MAC list is              ENABLED
```

DLSw is
DLSw プロトコルの状況で、enabled (使用可能) または disabled (使用不能)

LLC2 send disconnect is
ルーターが TCP 接続が失われたときに LLC2 接続を終了させないようにする状況。 値は、enabled (使用可能) または disabled (使用不能) です。

Dynamic Neighbors
DLSw が、構成済みでない DLSw ルーターからの着信 TCP 接続の試みを受け入れている (つまり、**add tcp** コマンドを使用している) かどうかを示します。

SRB Segment number
RIF 内で DLSw を識別する SRB セグメント

MAC<->IP mapping cache size
MAC-IP マッピング・キャッシュのサイズを指定します。

Max DLSw Sessions
DLSw プロトコルがサポートできる DLSw セッション (SNA セッションと NetBIOS セッションの両方) の最大数

DLSw global memory allotment
DLSw が使用できるメモリーの最大容量

LLC per-session memory allotment
LLC DLSw セッションが使用できるメモリーの最大容量

SDLC per-session memory allotment
各 SDLC DLSw セッションが使用できるメモリーの最大容量

QLLC per-session memory allotment
各 QLLC DLSw セッションが使用できるメモリーの最大容量

NetBIOS UI-frame memory allotment
DLSw によって転送されるすべての NetBIOS UI フレーム用として使用できるメモリーの最大容量

Dynamic Neighbor Transmit Buffer Size
動的 TCP 接続用の TCP 送信バッファーのサイズ

Dynamic Neighbor Receive Buffer Size
動的 TCP 接続用の TCP 受信バッファーのサイズ

Dynamic Neighbor Maximum Segment Size
動的 TCP 接続用の最大 TCP セグメント・サイズ

Dynamic Neighbor Keep Alive
TCP Keepalive メッセージが新しい動的 TCP 接続上で送信されるかどうか。

Dynamic Neighbor NetBIOS SessionAlive Spoofing
NetBIOS SessionAlive I フレームが新しい動的 TCP 接続上に確立された DLSw ピアに転送されるかどうか。

Dynamic Neighbor Priority
すべての新しい動的 TCP 接続に使用される近隣優先順位

QLLC base source MAC address
動的着信 QLLC コール用の発信元 MAC アドレスとして使用される範囲内の最低の MAC アドレス (SVC)

QLLC maximum dynamic addresses
動的着信 QLLC コール用にいつでも使用できる動的発信元 MAC アドレスの最大数

dls sessions all
現行の dls セッション情報を表示します。

例: `list dls session all`

```
    Source            Destination      State       Flags  Dest. IP Addr Id
1. 400000000003 04  500000000003 04   Connected           128.185.236.51  2
```

Source
セッションの発信元 MAC アドレスおよび SAP。MAC アドレスは次の文字ストリングによって置き換えられ、これらのセッションを容易に識別できるようにします。

```
DLC Type        Characters      Content
  SDLC            1-5           "SDLC "
                  6-7           Interface number
                  8             "_"
                  9-10          SDLC station address
                  11-12         "  "
  QLLC            1-5           "QLLC "
                  6-7           Interface number
                  8             "P" for PVC, or "S" for SVC
                  9-12          LCN for PVC, or last 4 bytes of
                                     DTE address for SVC
  APPN            1-4           "APPN"
                  5-12          "        "
```

Destination
セッションのあて先 MAC アドレス

State セッションの状態。 表示できる状態には以下のものがあります。

DISCONECT
サーキットまたは接続が確立されていない初期状態を示します。

RSLV_PEND
ターゲット DLSw が SSP_STARTED 指示を待ち受けているか、SSP_START 要求の次に続くことを示します。

CIRC_PEND
あて先 DLSw が SSP_ICANREACH メッセージに対する SSP_REACHACK 応答を待ち受けていることを示します。

CIRC_EST
終端間サーキットが確立されたことを示します。

CIR_RSTRT
リセットを発信した DLSw がデータ・リンクの再始動および SSP_RESTART メッセージに対する SSP_RESTARTED 応答を待ち受けていることを示します。

CONN_PEND
起点 DLSw が SSP_CONTACT メッセージに対する SSP_CONTACTED 応答を待ち受けていることを示します。

CONT_PEND
ターゲット DLSw が SSP_CONTACT メッセージに対する SSP_CONTACTED 確認を待ち受けていることを示します。

CONNECTED
サーキットがコネクション型データ転送に備えて完全にアクティブであることを示します。

DISC_PEND
切断を発信した DLSw が SSP_HALT メッセージに対する SSP_HALTED 応答を待ち受けていることを示します。

HALT_PEND
リモート DLSw が SSP_HALT 要求に続く SSP_HALTED 指示を待ち受けていることを示します。

REST_PEND
ローカル DLSw が RESTART_DL を受信したが、まだ DL_RESTARTED を戻していないことを示します。

CIRC_STRT
ローカル DLSw が CANUREACH_cs を送信したが、まだ ICANREACH_cs を受信していないことを示します。

HLT_NOACK
ローカル DLSw が HALT_DL_NOACK を受信したが、リンク・ステーションのクローズを完了していないことを示します。

Flags フラグは次のいずれか 1 つになります。

A - CONTACT MSG PENDING (連絡メッセージ保留)

B - SAP RESOLVE PENDING (SAP 解決保留)

C - EXIT BUSY EXPECTED (終了使用中予期)

D - TCP BUSY (TCP 使用中)

E - DELETE PENDING (削除保留)

F - CIRCUIT INACTIVE (サーキット非活動)

Dest. IP Addr
リモート DLSw ピアの IP アドレス

Id セッションを識別するために使用される番号。 セッション ID を要求するコマンドにはこの番号を使用してください。

dls sessions appn

このルーター内の APPN を終点としてもつセッションについての dls セッション情報を表示します。

例: list dls sess appn

```
Source             Destination      State      Flags    Dest IP Addr    Id
-------------      --------------   ---------  -------  --------------  ----
1 APPN         04  400000000011 04  CONNECTED           187.7.239.11    0
2 APPN         04  400000000014 04  CONNECTED           142.7.245.14    1
```

dls sessions ban

BAN セッションについての現行の情報を表示します。

例: list dls session ban

```
BAN port number (user 0 for all ports) [0]?
No active sessions
```

dls sessions dest

あて先 MAC アドレス別の dls セッション情報を表示します。

例: list dls session dest

```
Destination MAC Address [40000000001]? 50000000003

Source              Destination       State       Flags  Dest. IP Addr  Id
1. 400000000003 04  500000000003 04   Connected           128.185.236.51  2
2. 400000000002 04  500000000003 04   Connected           128.185.236.52  3
```

dls sessions detail

詳しい dls セッション情報を表示します。

例: list dls session detail

```
                      Session Identifier [1]?

Source           Destination         State       Dest. IP Addr    Id
1. 400000000003 04  500000000003 04     Connected   128.185.236.512  2

                     Personality:      TARGET
                     XIDs sent:        2
                     XIDs rcvd:        0
                     Datagrams sent:   0
                     Datagrams rcvd:   0
                     Info frames sent: 15
                     Info frames rcvd: 0
                     RIF:              0620 0202 B0B 0
                     Local CID:        0136AF74:7E000021
                     Remote CID:       014AB030:7E000003
                     Priority:         MEDIUM
```

Personality
接続の ORIGINATOR (開始側) または TARGET (受信側)

XIDs sent XIDs rcvd
この DLSw ピアがリモート DLSw ピアに送受信した XID の総数

Datagrams sent Datagrams rcvd
この DLSw ピアがリモート DLSw ピアに送受信したデータグラムの総数

Info frames sent Info frames rcvd
この DLSw ピアが DLSw ピアに送受信した I フレームの総数

RIF LLC テスト・フレームの RIF に組み込まれている情報

Local CID
このルーターによって割り当てられた DLSw サーキット ID

Remote CID
近隣ルーターによって割り当てられた DLSw サーキット ID

Priority
このサーキットの開始時にこのサーキットに関して確立された DLSw サーキット優先順位

dls sessions ip

指定した TCP 接続近隣への dls セッションを表示します。

例: list dls session ip

```
Enter the DLS neighbor IP address [0.0.0.0]? 128.185.236.512

      Source        Destination      State      Dest. IP Addr     Id
1. 400000000003 04  500000000003 04  Connected  128.185.236.512   2
```

dls sessions nb

NetBIOS をサポートする現行活動サーキットについての情報をリストします。

例: list dls sessions nb

```
      Source        Destination      State      Dest. IP Addr     Id
1. 400000000003 F0  500000000003 F0  Connected  128.185.236.512   2
```

dls sessions range

表示したい dls セッションの範囲。この数は発信元 MAC アドレスの左に位置しています。

例: list dls session range

```
Start[1]?
Stop[1]?

   Source          Destination      State       Dest.  IP Addr    Id
1. 400000000003 04  500000000003 04  Connected   128.185.236.512   2
```

dls sessions src

発信元 MAC アドレス別のすべての dls セッション情報を表示します。

例: list dls session src

```
        Source MAC Address [400000000001]?

   Source        Destination      State       Flags Dest. IP Addr  Id
1. SDLC 04   400000000002 04      Connected     10.1.49.401        1
```

注: この例では、発信元 MAC アドレス 400000000001 が名前 『SDLC 04』にマップします。このコマンドのパラメーターとして必須の発信元 MAC アドレスが分からない場合は、**list SDLC config all** コマンドを入力して、この情報を入手します。

dls sessions state

指定した状態にあるすべての dls セッションを表示します。

例: list dls session state

```
                  DISCONECT = 0,  RSLV_PEND = 1
                  CIRC_PEND = 2,  CIRC_EST  = 3
                  CIR_RSTRT = 4,  CONN_PEND = 5
```

```
                          CONT_PEND = 6,  CONNECTED = 7
                          DISC_PEND = 8,  HALT_PEND = 9
                          REST_PEND = 10  WT_HALTNA = 11
                          CIRC_STRT = 12  HLT_NOACK = 13

                          Enter state value (0-10) [7]?

    Source            Destination      State       Flags  Dest. IP Addr Id
1. 400000000003 04  10005AF181A4 04  Connected          128.185.236.84  0
2. 400000000002 04  400000000088 04  Connected          128.185.236.84  1
```

list dls cache all

list dls cache all コマンドでは、 DLSw MAC アドレス・キャッシュ内の項目がリストされます。 このキャッシュには、最新の MAC アドレスから IP 近隣への変換のデータベースが含まれます。 キャッシュでは、MAC アドレス、キャッシュ内存続時間 (秒単位)、および近隣の IP アドレスが提供されます。

例: list dls cache all

```
       Mac Address   Entry Type  Secs to live      IP Address(es)   LFSize
   1.  10005A123456  PERMANENT   (not being timed) 128.185.236.84   0
   2.  10005A789ABC  STATIC      (not being timed) 128.185.236.84   0
   3.  10005AF1809B  DYNAMIC        810            128.185.236.84   2052
   4.  10005AF181A4  DYNAMIC        1170           128.185.236.84   2052
   5.  400000000088  DYNAMIC        1170           128.185.236.84   2052
```

dls cache config

DLSw 構成済み MAC キャッシュ記入項目を表示します。

例: list dls cache config

```
Mac Address   IP Address       Source     Last Mod
------------  ---------------  ---------  ---------
10005A123456  128.185.236.84   PERMANENT  UNCHANGED
10005A789ABC  128.185.236.84   STATIC     ADDED
```

list dls cache range

指定した範囲のキャッシュ項目についての情報を表示します。

例: list dls cache range

```
Start[1]?
Stop ]1]? 20
       Mac Address   Entry Type  Secs to live      IP Address(es)   LFSize
   1.  10005A123456  PERMANENT   (not being timed) 128.185.236.84   0
   2.  10005A789ABC  STATIC      (not being timed) 128.185.236.84   0
   3.  10005AF1809B  DYNAMIC        810            128.185.236.84   2052
   4.  10005AF181A4  DYNAMIC        1170           128.185.236.84   2052
   5.  400000000088  DYNAMIC        1170           128.185.236.84   2052
```

dls memory

このコマンドでは、すべての既存の DLSw セッションおよび各セッション別に使用されるメモリーの容量をリストします。

例: list dls memory

```
Total DLSw bytes requested:             153600
Global receive pool bytes granted:       92160
 Currently in use:                           0
Global transmit pool bytes granted:      61440
 Currently in use:                         232

NetBIOS UI-frame pool total bytes:       40960
 Currently in use:                           0


                                      Session    Initial  Current  Congest  DLC Xmits
Id Source           Destination        State      alloc   alloc    State     Queued
5. SDLC 04C1     04  400000000003  04  Connected   16384   16384    READY       0
6. 400000000003  04  0000c9001119  04  Connected   16384   16384    READY       0
```

『Currently in use』 フィールドは、現在 DLS によって割り振られているメモリーの総容量を示します。 これには、すべてのセッション割り振りおよび制御メッセージが含まれます。

『Congest State』 フィールドは、フロー制御についての情報を提供し、次のいずれかになります。

Ready セッションが輻輳 (ふくそう) していないことを示します。

Session
セッションがそのセッション割り振りの大半を使用しており、データ・リンクはフロー制御されていると考えられます。

Global
ルーター内のメモリーの不足からセッションが輻輳 (ふくそう) していることを示します。

Ses/gbl
セッション・メモリーおよびグローバル・メモリーの不足のため、セッションが輻輳 (ふくそう) していることを示します。

『DLC Xmits Queued』 フィールドには、 DLS 内で 待ち行列に入れられて LLC または SDLC への伝送を待機しているフレーム数に、接続されたエンド・ステーションによる確認を DLC 内で待ち行列に入れられて待ち受けているフレーム数を加えた合計数が示されます。

explorer-override
構成済み MAC キャッシュ・エクスプローラー・オーバーライドを一覧表示します。

例 : list explorer-override

```
   Explorer      Explorer      DB Age    Wait ICR  Nbr Pri   TESTrsp  Forwarding
ID MAC Value     MAC Mask      Timeout   Timeout   Timeout   Delay    Explorers
-- ------------  ------------  --------  --------  --------  -------  ---------
 1 400031740000  FFFFFFFF0000  DISABLED    20      DISABLED  0.0      AllPartners
 2 10005A000000  FFFFFF000000   1200       20      2.0       0.0      NoPartner
```

mac-list all
すべてのローカルおよびリモート MAC アドレス・リスト項目を表示します。

例: list mac-list all

```
MAC Value     MAC Mask      IP Address
------------  ------------  ---------------
10005AF17F23  FFFFFFFFFFFF  Local
10005AF1809B  FFFFFFFFFFFF  128.185.236.84
4000189E2000  FFFFFFFFF000  128.185.236.84
4000189E3000  FFFFFFFFF000  Local
```

mac-list config
ローカルで構成された MAC アドレス・リスト項目をすべて表示します。

例: list mac-list config

```
Entry  Mac Value     MAC Mask      Source     Last Mod
-----  ------------  ------------  ---------  ---------
    1  10005AF17F23  FFFFFFFFFFFF  STATIC     UNCHANGED
    2  4000189E3000  FFFFFFFFF000  STATIC     UNCHANGED
```

mac-list local
アクティブなローカル MAC アドレス・リスト項目をすべて表示します。

例: list mac-list local

```
LOCAL MAC List
Type of MAC List (active) ....... EXCLUSIVE
Type of MAC List (pending) ...... EXCLUSIVE


MAC Value     MAC Mask
------------  ------------
10005AF17F23  FFFFFFFFFFFF
4000189E3000  FFFFFFFFF000
```

mac-list remote

特定の DLSw ピアについてのアクティブなリモート MAC アドレス・リスト項目をすべて表示します。

例: list mac-list remote

```
          Enter the DLSw neighbor IP Address [0.0.0.0]?
128.185.236.84

Partner IP Address .............. 128.185.236.84
Type of MAC List ................ EXCLUSIVE
Use of remote MAC lists ......... ENABLED


MAC Value     MAC Mask
------------  ------------
10005AF1809B  FFFFFFFFFFFF
4000189E2000  FFFFFFFFF000
```

groups config

join-group コマンドを使って構成されたこの DLSw ピアについてのグループ情報を表示します。

例: list groups config

```
   Group#                    Xmit    Rcv     Max     Keep-    SesAlive
Mcast IP Addr   Role      CST Bufsize Bufsize Segsize Alive    Spoofing Priority
--------------- --------- --- ------- ------- ------- -------- -------- --------
224.0.10.0      READWRITE  p    5120    5120    1024  DISABLED DISABLED MEDIUM
Group  2        PEER       p    5120    5120    1024  DISABLED DISABLED MEDIUM
```

Group # / Mcast IP Addr

クライアント/サーバー/ピア・グループの場合は、グループの番号。DLSw バージョン 2 グループの場合には、マルチキャスト・アドレスは、読み書きの対象として構成されます。

Role

クライアント/サーバー/ピア・グループの場合は、このルーターがグループ内で引き受けるよう構成されている役割。DLSw バージョン 2 グループの場合には、構成済みのマルチキャスト・アドレスの読み取り/書き込み機能。つまり、読み取り専用、書き込み専用、または読み書きです。

CST

このルーターがグループ内で使用するよう構成されている接続性セットアップ・タイプ。Active (a) または Passive (p)。

Xmit Bufsize

パケット送信バッファーのサイズ (1024 ～ 32768)。 省略時値は 5120 です。

Rcv Bufsize

パケット受信バッファーのサイズ (1024 ～ 32768)。 省略時値は 5120 です。

Max Segsize

TCP セグメントの最大サイズ (64 ～ 16384)。 省略時値は 1024 です。

Keepalive

Keepalive 機能の状態、つまり、enabled (使用可能) または disabled (使用不能) を表示します。

SesAlive Spoofing

NetBIOS SessionAlive Spoofing 機能の状態、つまり、enabled (使用可能) または disabled (使用不能) を表示します。

Priority

選択プロセスでの近隣ルーターの優先順位を表示します。近隣優先順位は、上位、中位、または下位です。

groups statistics

ルーターの最後の再始動またはグループの作成以降のエクスプローラー・トラフィックについての DLSw グループの使用に対する統計を表示します。

例 : list groups stat

```
Group number    Data pkts   Data Bytes   Ctrl pkts   CURex pkts   NQex pkts
    or              Sent        Sent         Sent         Sent        Sent
Multicast IP@       Rcvd        Rcvd         Rcvd         Rcvd        Rcvd
-------------   ---------   ---------   ----------   ----------   ---------
Group 1                 0           0          116           24          10
                        0           0           25           10           2
224.0.10.0              0           0          224           33           0
                        0           0           21            8           0
```

llc2 open

LLC2 ピア間のインターフェース上で現在オープンしているすべての SAP についての情報を表示します。

例: list llc2 open

```
Interface   SAP(s)
    0        0  4
    1        0  4  8  C
```

llc2 SAP parameters

LLC2 パラメーター構成情報を表示します。 変更された構成だけが表示されます。 **set llc2** コマンドが使用されなかった場合は、出力は生成されません。

例: list llc2 sap parameters

```
SAP             t1    t2    ti    n2    n3    tw    rw    nw    acc
---             --    --    --    --    --    --    --    --    ---
 0               1     1    30     8     1     2     2     1     0
```

llc2 sessions all

すべての LLC2 セッションについての現行の情報を表示します。

例: list llc2 sessions all

```
   SAP   Int.   Remote Addr    Local Addr    State      RIF
1. 04    6     400000000003   500000000003  CONTACTED  0620 0202 B0B0
```

State llc セッションの状態。 表示できる状態には以下のものがあります。

DISCONNECTED

データ・リンク制御構造が存在するが、データ・リンクが確立されていないことを示します。

CONNECT_PEND

接続保留状態に入るのは、NULL SAP へのテスト・コマンド・フレームが受信されるとき、またはDLS からの DLC_START_DL コマンドが受信されるときです。

RESOLVE_PEND
解決保留状態に入るのは、DLC_RESOLVE_C コマンドが DLS に送信されたときです。

CONNECTED
これは、DLS クラウドを介して LLC タイプ 1 のレベルのサービスが使用可能な定常状態です。 この状態に入るのは、DLC_RESOLVE_R コマンドが DLS から受信されるとき、または TEST 応答フレームがネットワークから受信されるときです。

CONTACT_PEND
この状態に入るのは、送信または受信された SABME への応答が未解決の場合です。

CONTACTED
これは、伝送された SABME への UA 応答が受信されたとき、または受信された SABME に UA が以前に伝送されていたときに入る定常状態です。 この状態では、LLC2 情報フレームは DLS クラウドを介して交換されます。

DISCONNECT_PENDING
この状態に入るのは、DISC コマンドが伝送または受信されたとき、または DLC_HALT が DLS から受信されたときです。

llc2 sessions ban
BAN 機能に関係する LLC2 セッションについての現行の情報を表示します。

llc2 sessions nb
NetBIOS プロトコル・トラフィックを搬送する LLC2 セッションについての現行の情報を表示します。

llc2 sessions range
選択された範囲の LLC2 セッションについて現行の情報を表示します。

例: `list llc2 sessions range`

```
Start[1]?
Stop[1]?
              SAP   Int.   Remote Addr   Local Addr    State      RIF
           1. 04    6      400000000003  500000000003  Contacted  0620 0202 B0B0
```

priority
DLSw サーキット優先順位情報を表示します。

例: `list priority`

```
Default priority for SNA DLSw session traffic is           HIGH
Default priority for NetBIOS DLSw session traffic is       MEDIUM
Default priority for SNA DLSw explorer traffic is          MEDIUM
Default priority for NetBIOS DLSw explorer traffic is      LOW

Message allocation by C/H/M/L priority is   4/3/2/1
Maximum frame size for NetBIOS is           516

    Source/  SAP      MAC Address                  Session   Explorer
ID  Dest     Range    Range                        Priority  Priority
--  -------  -------  ---------------------------  --------  --------
 1  Source:  00 - FE  000000000000 - FFFFFFFFFFFF  CRITICAL  MEDIUM
    Dest  :  00 - 0C  10005A000000 - 10005AFFFFFF
 2  Source:  04 - 04  400031740000 - 40003174FFFF  CRITICAL  MEDIUM
    Dest  :  00 - FE  000000000000 - FFFFFFFFFFFF
```

qllc... 使用可能にされている QLLC インターフェース、あて先、またはステーションをリストします。

構文:

qllc callin

destinations

sessions

stations

例: li qllc callin

```
           Interfaces enabled for incoming QLLC calls to DLSw:
   1
```

例: li qllc dest

```
Connection ID   Dest  SAP/MAC           Hits
  CHICAGO       04   400000112323         0
```

この表示の構成可能なフィールドの説明については、493ページの『第25章 DLSw フィーチャーの使用』 の **add qllc** コマンドを参照してください。 *Hits* フィールドは、DLSw が着信 QLLC Call_Request パケット内の接続 ID とこの接続 ID の間の合致を使用した回数を示します。

例: li qllc sess

```
If  P/S  LCN/DTE addr    Source SAP/MAC   Dest SAP/MAC      Type   State
 4  PVC  4               04 400000310401  00 000000000000   PERM   NET_DOWN
 4  SVC  3721111         04 400000310402  00 000000000000   STAT   NET_DOWN
    2 Circuits    1 PVC   1 SVC       1 Permanent   1 Static   0 Dynamic
```

この表示の構成可能なフィールドの説明については、493ページの『第25章 DLSw フィーチャーの使用』 の **add qllc** コマンドを参照してください。

Type フィールドは以下の値をもちます。

PERM (Permanent)
このステーションの定義は、ルーターが最後に始動されたときにルーター構成の一部でした。

STAT (Static)
このステーション定義は、ルーターが最後に始動された後にユーザーが DLSw 監視機能のもとで追加しました。

DYNM (Dynamic)
DLSw は、このステーション定義を、着信コールの結果として、または単一のリモート DTE アドレスへの複数の発信コールを行う必要から、動的に作成しました。

セッション・リストの下部の要約行は、現在存在する各タイプのセッションの数を示します。

State フィールドは、QLLC の視点からの DLSw 接続の状態を示します。 これらの状態は、**list dls sess** コマンドのもとで表示されるメイン DLS 状態とは異なり、QLLC インターフェースで何が起こっているかについての情報を追加します。 可能な値は次のとおりです。

NET_DOWN
X.25 インターフェースは現在ダウンしています。

PLC_DOWN
X.25 パケット・レイヤーは現在ダウンしています。

DISCONNECTED
この状態およびそれ以降のすべての状態について、X.25 インターフェースおよびパケット・レイヤーは立ち上がっています。 この状態では、DLSw はエンド・ステーションが接続の確立を開始するのを待っています。

XID_POLL
DLSw は、最初に装置にコンタクトしようとして、または失われた接続を回復しようとして、QXID (XID_null) を使って QLLC エンド・ステーションをポーリングしています。

SETMODE_POLL
DLSw は、最初に装置にコンタクトしようとして、または失われた接続を回復しようとして、QSM を使って QLLC エンド・ステーションをポーリングしています。

SENT_EX
DLSw は QLLC エンド・ステーションから連絡を受け、DLSw ネットワーク内の該当するあて先を探索しています。

CS_PEND
DLSw の探索は満足され、サーキット開始要求が開始されました (CUR_cs を送信しました)。

CALL_REQ_PEND
DLSw は QLLC エンド・ステーションへのコール・リクエストを行い、コールが正常に応答されるか調べるために待っています。

ESTABLISHED
DLSw サーキットは 『サーキットが確立された』 状態にあります。これは、SNA XID の送信または受信用に使用可能です。

CONTACT_PEND
DLSw は QSM を QLLC エンド・ステーションに送信し、QUA を待ち受けています。

CONNECTED
DLSw サーキットは完全に立ち上がり、I フレームのエンド・ユーザー・データを搬送することができます。

DISC_PEND
DLSw は QLLC ステーションにサーキット切断を要求し、確認を待ち受けています。

RESET_PEND
DLSw は QLLC ステーションに PVC リセットまたは SVC 切断コールを要求し、確認を待ち受けています。

例: `li qllc sta`

```
If  P/S  LCN/DTE addr   E/D Source SAP/MAC   Dest SAP/MAC    PU Blk/IdNum  Type
 1  PVC  2              E  04 400000310104  04 400011112323  2 000/00000  PERM
 1  SVC  3721111        E  04 400000310103  00 000000000000  2 000/00000  PERM
 1  PVC  4              E  04 400000317402  04 400000000002  2 017/00001  PERM
```

この表示の構成可能なフィールドの説明については、493ページの『第25章 DLSw フィーチャーの使用』 の **add qllc** コマンドを参照してください。 『E/D』 フィールドは、ステーションが現在使用可能にされているかどうかを示します。 『Type』 フィールドは、上で **list qllc sessions** コマンドについて説明されたのと同じ値をもっています。

sdlc config

SDLC に接続された PU について構成済みのパラメーターを表示します。

例: list sdlc config

```
    Interface #, or 'ALL' [0]? all

Net  Addr    Status    Source SAP/MAC    Dest SAP/MAC      PU  Blk/Idnum  PollType
1    C1      Enabled   04 4000103D01C1   00000000000000    2   000/00000  TEST
1    C2      Enabled   04 4000103D01C2   00000000000000    2   000/00000  SNRM
3    FF(sw)  Enabled   04 4000103D01D2   04 400000000003   2   000/00000  TEST
```

sdlc sessions

ルーター内のすべての SDLC dls セッションについての情報を表示します。

例: list sdlc sessions

```
       Net  Address   Source SAP/MAC    Dest SAP/MAC     PU    OutQ   State
  1.   1    C1        04 4000103D01C1   00 000000000000  2      0    NET_DOWN
  2.   1    C2        04 4000103D01C2   00 000000000000  2      0    NET_DOWN
```

DLSw および SDLC は完全な XID 折衝を行う能力をもっているので、接続された SDLC リンク・ステーションが、ルーターで構成された SDLC ステーション・アドレスとは異なるアドレスにリンクを設定することが可能です。これが起こる場合、2 つの SDLC ステーション・アドレスは、この表示の 『Addr』 欄のもとで xx(yy) の形式を使用して示されます。 この形式では、 xx はこのルーターで構成されたステーション・アドレスであり、すべての構成コマンドおよび監視コマンドでもこのリンク・ステーションを指すために使用されています。接続された SDLC 装置によって設定された現行の操作可能なアドレスは、右側の括弧の中で示された値 yy です。

tcp capabilities

パートナー DLSw ルーターから機能交換メッセージで受信した情報を表示します。

例: list tcp capabilities

```
Enter the DLSw neighbor IP Address [0.0.0.0]? 128.185.236.84
Vendor ID:                  10005A
Vendor product version:     IBM 2210 Nways MRS 5765-B86 Feature 5045 V3 R2
Initial pacing window:      12
Preferred TCP connections:  1
Supported SAPs:             00 04 08 0C F0
MAC List Exclusivity:       Complete List
MAC List:                   08005ACEEA1C [FFFFFFFFFFFF]
                            4000189E2000 [FFFFFFFFF000]
NetBIOS Exclusivity:        (not supplied)
NetBIOS Name List:          (none supplied)
Multicast Version:          01
IBM CST:                    Passive Transport
IBM Multicast:              Available
IBM Capex Correlator:       19660
```

Vendor ID

近隣 DLSw のベンダーの IEEE 組織固有識別子 (OUI)。 IBM の OUI は X'10005A' です。

Vendor version
近隣 DLSw がそれ自体を記述するために送信したテキスト・ストリング。 『(not available)』 では、近隣実施がそのようなストリングを送信しなかった場合を示します。

Initial pacing window
この DLSw が、新しいサーキットごとに初期歩調合わせ認可を受信した時点で、近隣 DLSw に送信することができる歩調合せ SSP メッセージの数。

Preferred TCP connections
この近隣が持ちたい TCP 接続の数 (1 または 2)。 IBM 2210 では、要求された数に調整し、近隣が要求すれば、その近隣とは全二重 TCP 接続を 1 つだけ持ちます。

Supported SAPs
近隣 DLSw がその LAN インターフェース上でオープンしているか、または自動的にオープンするか、またはその接続 SDLC ステーションを表す SAP のリスト。

MAC List Exclusivity
この近隣によって送信された MAC アドレス・リストが、その近隣にローカルである MAC アドレスの完全なリストまたは部分的なリストとして見なされるかどうかを示します。 『(not supplied)』 という応答は、この近隣が MAC アドレス・リストをその機能の一部として送信しなかったことを意味します。

MAC List
この近隣がその MAC アドレス・リストに入れて送信した MAC リスト値およびマスクをすべて表示します。『(none supplied)』 という応答は、この近隣が MAC アドレス・リストをその機能の一部として送信しなかったことを意味します。

NetBIOS Exclusivity
この近隣によって送信された NetBIOS 名前リストが、その近隣にローカルである NetBIOS 名の完全なリストまたは部分的なリストとして見なされるかどうかを示します。 『(not supplied)』 という応答は、この近隣が NetBIOS 名前リストをその機能の一部として送信しなかったことを意味します。

NetBIOS Name List
この近隣がその NetBIOS 名前リストに入れて送信したすべての NetBIOS 名前修飾子を表示します。 『(none supplied)』 という応答は、この近隣が NetBIOS 名前リストをその機能の一部として送信しなかったことを意味します。

Multicast Version
この近隣が AIW 標準によって定義されたとおりにサポートしているマルチキャストのバージョンを指示します。*(not supplied)* という応答は、この近隣が マルチキャスト・バージョンをその機能の一部として送信しなかったことを意味します。

IBM CST
この近隣が構成した IBM 接続セットアップ・タイプ (CST) を指示し

ます。*(not supplied)* という応答は、この近隣が IBM CST をその機能の一部として送信しなかったことを意味します。

IBM Multicast
特定の IBM Multicast 機能がこの近隣で使用可能になっているかどうかを指示します。*(not supplied)* という応答は、この近隣が IBM Multicast をその機能の一部として送信しなかったことを示します。

IBM Capex Correlator
この近隣から最後に受信された IBM Capex Correlator の値を指示します。 *(not supplied)* という応答は、この近隣が IBM Capex Correlator をその機能の一部として送信しなかったことを示します。

tcp config

ピア DLSw ルーターへのすべての構成済みの TCP 接続についての構成パラメーターを表示します。

例: `list tcp config`

```
                        Xmit    Rcv     Max      Keep-    SesAlive
Neighbor        CST Bufsize Bufsize Segsize Alive    Spoofing Priority
--------------- --- ------- ------- ------- -------- -------- --------
128.185.236.84   p    5120    5120    1024  DISABLED DISABLED MEDIUM
```

tcp sessions

ピア DLSw ルーターへのすべての既知の TCP セッションの状況を表示します。

例: `list tcp sessions`

```
   Group   IP Address      Conn State     CST  Version  Active Sess Sess Creates
   ------- --------------- -------------- ---  -------- ----------- ------------
1          128.185.236.49  ESTABLISHED     p   AIW V1R0      2           4
```

Group 近隣が発見されたグループ (該当する場合)

IP Address
DLSw に関して使用された近隣 IP アドレス

Conn State
この近隣へのトランスポート接続 (1 つまたは 2 つの TCP 接続で構成されるもの) の状態。 有効値は、次のものです。

DOWN
TCP セッションは確立されません。機能は交換されません (受動パートナーのみ)。

CAPEX FAILED
機能の交換を試みますが、失敗しました。TCP セッションはダウンしています。

Unicasting
TCP セッションは確立されません。機能は正常に交換されました (受動パートナーのみ) (DLSw エクスプローラー・トラフィックについて作動可能)。

PENDING R/W
この 2210 は、近隣との TCP セッションの確立を試みました。

RD EST/WR PEND
近隣とこの 2210 の間の TCP セッションはアクティブですが、この 2210 と近隣の間の TCP セッションはアクティブではありません。

RD EST/WR PEND
この 2210 と近隣の間の TCP セッションはアクティブですが、近隣とこの 2210 の間の TCP セッションはアクティブではありません。

CAPEX PENDING
TCP セッションは確立されています。機能の交換中です。

ESTABLISHED
TCP セッションが確立されました。機能は交換済みです (DLSw セッションについての使用は作動可能)。

CLOSING
TCP セッションがダウンします。

RECONNECT WAIT
TCP セッションは確立されていません。TCP セッションの再確立を試みるためにタイマーが満了するのを待機しています。

CST 現行の接続性セットアップ・タイプで、次のものがあります。

```
a - active (能動) としてローカルで構成済みです
p - passive (受動) としてローカルで構成済みです
A - passive (受動) としてローカルで構成済みですが、近隣要件により
    アクティブ・モードで動作中です
D - ローカルに構成されてはいませんが、動的近隣 TCP 接続です
```

Version
近隣の DLSw プロトコルのレベル。 AIW 標準準拠ルーターを表す AIW VnRm、AIW 前 V1R0 実施を表す RFC1434+、または UNKNOWN のいずれか 1 つ

Active Sess
このトランスポート接続上の活動 (状態は任意) DLSw セッション (サーキット) の現在数

Sess Creates
ルーターの最後の再始動またはこのトランスポート接続の 『add tcp』 以後に、CIRC_EST 状態に入ったことのある DLSw セッション (サーキット) の合計数

tcp statistics
ルーターの最後の再始動またはこのトランスポート接続の 『add tcp』 以後の TCP トランスポート接続の使用に関する統計を表示します。

例: `list tcp statistics`

```
Enter the DLSw neighbor IP Address -0.0.0.0-?
192.1.1.3
                                  Transmitted          Received
                                  -----------          -----------
 Data Messages                         214                 231
 Data Bytes                         372997              413259
 Control Messages                       16                  34

 CanYouReach Explorer Messages           0                   0
```

```
ICanReach Explorer Messages                0                   0
NameQuery Explorer Messages                1                   2
NameRecognized Explorer Messages           2                   1
```

timers さまざまな活動を待機するためにユーザーが指定した時間。

例: `list timers`

```
Database age timer                1200  seconds
Max wait timer for ICANREACH      20    seconds
Wait timer for LLC test response  15    seconds
Wait timer for SDLC test response 15    seconds
QLLC session retry timer          20    seconds
Join Group Interval               900   seconds
Neighbor priority wait timer      2.0   seconds
Neighbor Inactivity Timer           5   minutes
Time to delay sending test resp.  0.0
seconds
```

Database age timer
参照されない MAC アドレスと IP アドレス間のデータベース項目を保留する時間。ゼロは、このデータベース内の項目が時間を指定されていないことを示します。

Max wait timer for ICANREACH
セッションが立ち上がらないことを判断する前にルーターが CANUREACH メッセージへの応答を待つ時間

Wait timer for LLC test response
LLC テスト・フレームを再送する前にルーターが LLC テスト応答を待つ時間

Wait timer for SDLC test response
DLSw セッションを開始するために SDLC ステーションに再びコンタクトを試みる前にルーターが待つ時間

QLLC session retry timer
DLSw セッションを開始するために QLLC ステーションに再びコンタクトを試みる前にルーターが待つ時間

Join Group Interval
DLSw グループ公示同報通信間の時間

Neighbor priority wait timer
所定のセッション確立の試みの間に近隣を選択する前に DLSw が待つ時間

Neighbor Inactivity Timer
DLSw が非アクティブ (ゼロ・セッション) の受動 TCP 接続をダウンさせるのに待つ時間

Delay sending TEST response
MAC アドレスの探索完了後、TEST 応答の送信前に待つ時間の長さ

NetBIOS

NetBIOS 監視プロンプトを表示します。

構文:

netbios

例: `netbios`

```
NetBIOS Support User Configuration
NetBIOS config>
```

NetBIOS コマンドの説明については、171ページの『第8章 NetBIOS の構成と監視』を参照してください。

Open-Sap

DLSw SRAM 構成に影響を及ぼすことなく、指定したサービス・アクセス・ポイント (SAP) の DLSw 交換を動的に使用可能にするには、**open-sap** コマンドを使用してください。

構文:

open-sap

例: **open-sap**

(追加情報および **open-sap** パラメーターの説明については、558ページの『Open-Sap』を参照してください。)

Set

set コマンドは、DLSw SRAM 構成に影響を及ぼすことなく、LLC2 パラメーター、最大数の DLSw セッション、プロトコル・タイマー、TCP 動的近隣、QLLC 操作用のパラメーター、MAC アドレス・リスト関連パラメーター、およびサーキット優先順位パラメーターを動的に変更するために使用します。

構文:

set dynamic-tcp
llc2
mac-list
memory
priority
qllc
timers

dynamic-tcp

動的近隣 TCP 接続 (つまり、**add tcp** コマンドでは定義されていない近隣から着信接続する TCP 接続) に関するさまざまな TCP パラメーターが指定できます。 DLSw がこれらの値を使用するのは、動的近隣が使用可能にされていない場合のみです。

構文: dynamic-tcp

例: **set dyn**

```
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
Enable/Disable Keepalive (E/D) [D]?
Enable/Disable NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
```

これらのパラメーターの説明については、493ページの『第25章 DLSw フィーチャーの使用』の **add tcp** コマンドを参照してください。

llc2 特定の SAP について特定の LLC2 属性を構成できます。

例: set llc2

(**set llc2** コマンドの例については、560 ページに挙げてあります。)

mac-list

ローカル MAC アドレスを排他的に設定できるようにします。また、このコマンドでは、次の監視コマンドによって以前に行った変更をすべてコミットすることもできます。

- enable mac-list local
- enable mac-list remote
- disable mac-list local
- disable mac-list remote
- add mac-list
- delete mac-list
- set mac-list

このコマンドの結果として、新しい実行時機能は、新しい情報を通信するためにすべての DLSw ピアに送信されます。

構文: mac-list

例: set mac-list

```
Local MAC list exclusivity (E=exclusive, N=non-exclusive) [N]? e

MAC list parameter set.

For the change to take effect, commit the change (next question).

The next question allows you to commit
any of the following changes (permanent and temporary):
  - changes made using ENABLE MAC-LIST LOCAL
  - changes made using ENABLE MAC-LIST REMOTE
  - changes made using DISABLE MAC-LIST LOCAL
  - changes made using DISABLE MAC-LIST REMOTE
  - changes made using ADD MAC-LIST
  - changes made using DELETE MAC-LIST
  - changes made using SET MAC-LIST

Would you like to commit the MAC list changes? [No]: y

Use of local MAC list remains    ENABLED.
Use of remote MAC list remains    ENABLED.
Type of local MAC list has changed from NON-EXCLUSIVE to EXCLUSIVE    .
Entry added temporarily:   08005ACEE5D9 / FFFFFFFFFFFF.
Entry added temporarily:   4000189E3000 / FFFFFFFFF000.
Would you still like to commit the MAC list changes? [No]: y


MAC address list changes have been committed.
```

memory

このコマンドでは、DLSw に割り振られるメモリーの合計量と、それぞれの DLSw セッションに割り振られるメモリーの合計量が動的に指定できます。

例: set memory

(**set memory** コマンドの例については、561 ページに挙げてあります。)

priority

SNA サーキットおよび NetBIOS サーキットに関して使用するためのサーキ

ット優先順位を指定することができます。 サーキット優先順位は、Critical (重大)、High (上位)、Medium (中位)、または Low (下位) (重大から下位への降順) に構成することができます。

また、このコマンドを使用すると、それぞれのサーキット優先順位に関するトランスポート送信数の比率の構成と、NetBIOS 用として使用する最大フレーム・サイズの設定もできます。ネットワークに透過型ブリッジ (TB) セグメントがある場合は、最大 NetBIOS フレーム・サイズとして少なくとも 1470 を使用します。

例: set priority

set priority コマンドの詳細については、562を参照してください。

qllc 着信する動的 QLLC コールから生じる DLSw セッション用の起点 MAC アドレスとして使用される動的に割り当てられた MAC アドレスの範囲を指定することができます。

範囲についてのベース MAC アドレス 『X』、および動的アドレスの最大数 『N』 を提供することにより範囲を指定します。 DLSw は、X 〜 X+(N-1) の範囲で MAC アドレスを選択します。

構文:

qllc

例: set qllc

```
DLSw
config>set qllc
QLLC base MAC address [40514C430000]?
Maximum QLLC dynamic addresses (0-max sess) [64]?
```

timers DLSw プロトコル・タイマーを設定します。

例: set timers

set timers コマンドの例については、563 ページに挙げてあります。

Test

test コマンドは、現在アクティブな MAC アドレス・キャッシュおよび MAC アドレス・リストに照らしてテストを実行するのに使用します。

構文:

test cache
mac-list

cache 特定の MAC アドレスについてあて先を指定されているフレームを現行キャッシュおよび DLSw ピア情報に基づいて転送する方法を判別できるようにします。

構文: cache

例: test cache

```
MAC address to be tested [000000000000]? 10005af1809b
Enter largest frame size to perform test against [2052]?
Destination MAC address being tested .... 10005AF1809B
```

```
MAC cache entry found:
  Entry type = DYNAMIC

Handling of SNA explorer SSP messages ....
  Explorer SSP message not sent (information found locally).

Handling of SNA circuit setup SSP messages ....
  Circuit Setup SSP message would be forwarded to 128.185.236.84

Handling of NetBIOS explorer SSP messages ....
  Explorer SSP message would be broadcast.
  How explorer destined for this MAC address is forwarded to DLSw partners
.....
    Send to all partners with non-exclusive mac address lists.
  There are currently no DLSw partners to forward the explorer to.

Handling of NetBIOS circuit setup SSP messages ....
  No currently known transport that can support circuit setup for given lfsize.
```

mac-list

与えられた MAC アドレスを、現在アクティブな MAC アドレス・リスト項目 (ローカルおよびリモート) すべてと突き合わせできるようにします。これは、MAC アドレス・リスト競合問題を解決する際に役立ちます。

構文: mac-list

例: test mac-list

```
MAC address to be tested [000000000000]?
10005af1809b

Destination MAC address being tested .... 10005AF1809B


MAC address value  MAC address mask   IP Address
-----------------  -----------------  ---------------
10005AF1809B       FFFFFFFFFFFF       128.185.236.84
```

第27章 ARP の使用

この章では、ルーター上でアドレス解決プロトコル (ARP) と逆アドレス解決プロトコル (逆 ARP) を使用する方法について説明します。この章には次の節が含まれています。

- 『ARP の概要』
- 595ページの『逆 ARP の概要』
- 595ページの『ATM を介したクラシカル IP および ARP (RFC 1577)』
- 608ページの『ATM を介した IPX および ARP の概要 (RFC 1483)』
- 609ページの『ATM を介したブリッジングの概要 (RFC 1483)』
- 602ページの『クラシカル IP 冗長の概要』
- 604ページの『分散 ARP サーバーの概要』

注: 装置のソフトウェア・ロードに非同期転送モード (ATM) が含まれていない場合、ATM に関連するコマンドは無効であり、 ARP 構成およびコンソール・プロンプトで表示されません。

ARP の概要

ARP プロトコルは、ネットワーク・レイヤー・アドレスを ATM アドレスや物理媒体アクセス制御 (MAC) アドレスに動的にマップする下位レベル・プロトコルです。あて先システムのネットワーク・レイヤー・アドレスだけが分かれば、ARP では、同じネットワーク・セグメント内であて先ホストの ATM アドレスや MAC アドレスを見つけます。

例えば、ルーターがその LAN の 1 つに接続されたホストをあて先とする IP パケットを受信します。パケットには 32 ビットの IP あて先アドレスしか入っていません。データ・リンク・レイヤー・ヘッダーを構成するために、ルーターは着信先ホストの物理 MAC アドレスを獲得します。その上で、ルーターはそのアドレスを 32 ビットの IP アドレスにマップします。 この機能を*アドレス解決* と呼びます。594ページの図49 に ARP の動作を図示してあります。

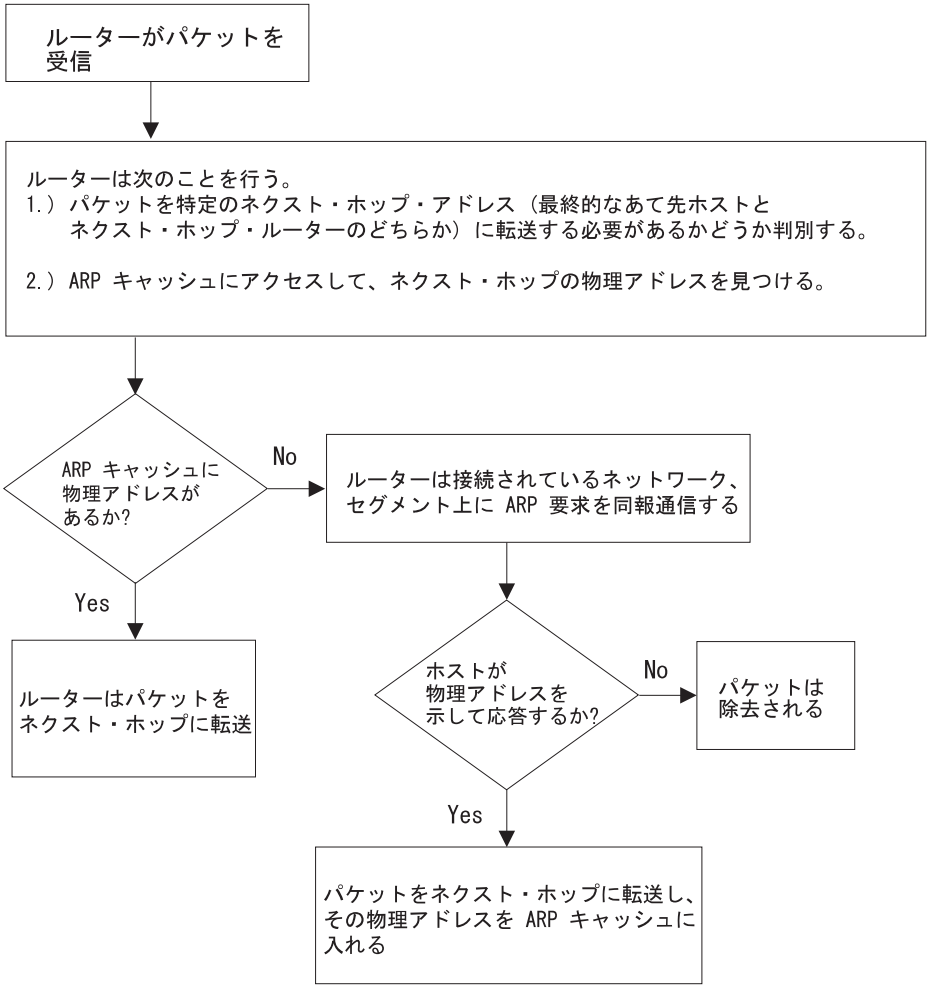


図 49. ARP アドレス解決同報通信

ルーターがネットワーク・レイヤー・アドレスを物理アドレスに変換する場合、ルーターは ARP (変換) キャッシュへアクセスします。 ARP キャッシュには、そのネットワーク・レイヤー・アドレスに対応する物理 MAC アドレスが入っています。 アドレスが欠落している場合は、正しい物理 MAC アドレスを見つけるために、ルーターは接続されたネットワーク・セグメントにあるすべてのホストに ARP 要求を同報通信します。 正しい物理 MAC アドレスをもつノードがルーターに応答します。 そこで、ルーターはそのノードにパケットを送信し、その物理 MAC アドレスを将来の使用に備えて変換キャッシュに入力します。

RFC 1577 の ATM を介したクラシカル IP & ARP は、597ページの『クラシカル IP 構成要素』 で説明されるように異なるパケット形式を使い、 ARP サーバーとして知られるエンティティーを追加することにより、ARP プロトコルを拡張します。

逆 ARP の概要

逆 ARP は、RFC 1293 に記述されているもので、フレーム・リレー・ネットワーク用として作成されました。このプロトコルでは、フレーム・リレー・ネットワーク上のルーターが、アドレス解決用に ARP パケットを同報通信する必要をなくすことにより非常に効率的にトラフィックを減らす方法で、他のルーターのプロトコル・アドレスを学習する方式を定義します。逆 ARP では、サーキットがアクティブになりしだい、逆 ARP 要求パケットをハードウェア・アドレス (フレーム・リレー・サーキットの場合は、サーキット識別子が、フレーム・リレーでハードウェア・アドレスに相当するものであり、ATM の場合は、ATM アドレスが交換されます) に送信して、プロトコル・アドレスを検出します。リモート・ルーターはそのプロトコル・アドレスを使って応答し、その結果得られたマッピングが ARP キャッシュ内に保管されます。

ATM では、逆 ARP パケットは、発信元およびあて先の可変サイズの ATM アドレスを扱うように拡張されました。 逆 ARP によって学習されたアドレスは、ARP によって学習されたアドレスと同様に経過時間切れになります。

逆 ARP によって学習されたプロトコル・アドレス対ハードウェア・アドレス項目は、ARP 最新表示タイマーが満了した時点でタイムアウトになりません。 フレーム・リレー・サーキットが故障した時を除いて、マッピングが経過時間切れになることはありません。 つまり、ARP キャッシュを更新するために、ルーターはどの逆 ARP 同報通信も伝送する必要がないことを意味します。ただし、他の (リモート) ルーターがそのプロトコル・アドレスを変更するときには、ルーターは項目への更新を許可します。

ARP と逆 ARP の両方をサポートすることによって、フレーム・リレーを介する他のベンダーのルーターとのルーターの相互運用性が、プロトコル・アドレスとハードウェア・アドレスのマッピングに関して大いに強化されます。 他のフレーム・リレーに接続されたルーターが逆 ARP をサポートしている場合には、上述したようにマッピングは動的に学習されます。 接続されたルーターが逆 ARP をサポートしていないが、フレーム・リレー上で『従来の』 ARP をサポートしている場合には、マッピングはまだ ARP 交換を使用して動的に学習することもできます (594ページの図49を参照してください。)

必要な場合は、フレーム・リレーの構成コマンド **add protocol-address** を使用して、他のルーターのプロトコル・アドレスを手動で構成することができます。追加情報については、 *ソフトウェア 使用者の手引き* の中の フレーム・リレー・インターフェースの構成と監視 の章を参照してください。

ATM を介したクラシカル IP および ARP (RFC 1577)

The Internet Engineering Task Force (IETF) は、RFC 1577 の 『ATM を介したクラシカル IP & ARP』 で ATM インターフェースを介して IP トラフィックを送信するための解決法を標準化しました。 この文書は、 IETF の ATM を介した IP の作業グループによって作成され、 ATM 通信施設を IP にとって透過に保つよう努めています。 今日 LAN または WAN 環境で稼働するほとんどのアプリケーションは、

機能に差がありませんが、『クラシカル IP の利点』 に説明するように、それらの効率とスループットの利得はかなり大きい場合があります。

RFC 2225 では、RFC 1577 を拡張して、クライアント登録メカニズムを変更し、複数の ATM ARP サーバーの場合が考慮されています。2210 では、 RFC 1577 と 2225 の両方の振る舞いをサポートします。

ATM を介したクラシカル IP および ARP の追加情報、ならびに論理および物理ネットワーク構成を示す図については、*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* を参照してください。

クラシカル IP (CIP) の論理 IP サブネット (LIS)

クラシカル IP (CIP) では、IP ステーションは論理 IP サブネット (LIS) にグループ化されています。クラシカル IP サーバーおよびクライアントは、*ソフトウェア使用者の手引き*の『LAN エミュレーション・サービス (LES) の使用および構成』の章で説明されているように、LAN エミュレーションのサーバーおよびクライアントが LAN エミュレーション・サービスに定義されるのに似た方法でこれらのサブネットを、サポートするよう定義されています。

多くの構成コマンドについて、LAN エミュレーションのクライアントおよびサーバーについての質問と同様の質問に答えるようプロンプト指示されます。 例えば、ATM アドレス ESI およびセレクターを要求する質問は、ユーザーがクラシカル IP または LAN エミュレーションを構成しているかどうか類似した方法で尋ねられます。

これらの構成のそれぞれは、クライアント定義に基づいています。クライアントはインターフェース番号 (ATM のみ) および IP アドレスとして定義されます。

最も単純な形では、IP はサーバーをもたず、その*自動的に* 割り当てられた ATM アドレスにコンタクトするサーバーにのみ話すことができます。 PVC が割り当てられた場合には、それが操作可能になります。

ATM の詳細については、 *ソフトウェア使用者の手引き*の『ATM の使用、構成、および監視』の章を参照してください。

クラシカル IP の利点

クラシカル IP には従来の IP と比べていくつかの利点があります。

- ATM によって提供されるより高速の回線速度
- 利用可能な帯域幅のより効率的な使用

  クラシカル IP は、例えば LAN (これには、発信元とあて先の MAC アドレスが含まれます) よりフレーム指示バイトが少なくて済むので、オーバーヘッドにより少ない帯域幅が使用され、データにより多くの帯域幅が使用されます。
- ARP フレームの解決には、同報通信トラフィックは必要とされません。

  同報通信環境では、ARP トラフィックはすべてのステーションに悪影響を及ぼすことがあります。 クラシカル IP では、ARP トラフィックは、情報を要求する ARP サーバーおよびクライアントにのみ影響を及ぼします。 サブネット上の他のすべてのステーションは、このトラフィックによって影響を受けません。

- 独立会話チャネル

  IP がトークンリングまたはイーサネットなどの共用媒体を介して使用される場合は、2 つのステーション間で伝送されるフレームは、同じ物理ネットワーク上の他のステーションがメッセージを送信できないようにします。 これは、トラフィックが非同報通信である場合でも当てはまります。 クラシカル IP では、独立チャネルは、会話をもつホスト間で確立されます。 これらのチャネルは、会話が他の会話から影響されないようにするトラフィック・パラメーターを使って確立することができます。

- ステーションを追加、削除、移動、または変更するための方法がより単純

  ATM を介した LAN エミュレーションについて説明された、移動、追加、削除などの同じ利点は、CIP 論理 IP サブネット (LIS) にも当てはまります。 *ソフトウェア使用者の手引き*の『ATM の使用、構成、および監視』の章を参照してください。

  LIS 内のメンバーシップは物理ロケーションに基づいていません。 論理的に関連するステーションは、同じ LIS にグループ化することができます。 クライアントは ARP サーバーを使って容易に登録することができるので、追加および変更はささいなことになります。 削除は、ARP サーバーがその項目を経過時間切れにすると自然に発生します。

  LIS のすべてのメンバーがクラシカル IP モデルをサポートする必要があるのに対し、2210 は CIP 論理 IP サブネット (LIS) およびエミュレートされた LAN サブネットの間で容易にルートすることができます。 装置によっては、 CIP に、より高機能なものと、LAN エミュレーションに、より高機能なものがあります。2210 には柔軟性があるので、ユーザーはその装置を最も効率的な場所に置くことができます。

クラシカル IP 構成要素

論理 IP サブネットには、それがイーサネット、トークンリング、またはフレーム・リレーのどれであれ、通常の IP サブネットのすべての特性が含まれています。 ただし、ATM は非同報通信多重アクセス (NBMA) ネットワークであるので、アドレスを解決するための既存の同報通信の方法は実行できません。 アドレス指定の問題を解決するため、RFC 1577 では、登録/要求手順を説明し、ARP サーバーおよび ARP クライアントの概念を紹介しています。

1 つの LIS につき、ARP サービスが 1 つ定義されます。ARP サービスは、1 つの LIS につき 1 台の ARP サーバーまたはいくつかの分散 ARP サーバーの場合があります。サービスは、IP アドレスから ATM アドレスへの変換を保持します。 これにより、CIP クライアントは、着信 VCC を受信し、適切な情報をクライアントに照会することにより、登録することができます。 ARP サービスは、クライアントによって要求された IP アドレスに対応する ATM アドレスについての ATMARP 要求にも応答します。 最後に、ARP サーバーは、ARP 項目を経過させ、着信 VCC を管理することにより、そのテーブルを管理し、更新します。

クライアントは、常にコールを行うエンティティーです。クライアントは、IML するときに、ARP サーバーにコールを行い、ARP サーバーに登録します。 クライアントによってサーバーに行われたコールは、制御チャネルと呼ばれます。クライアントが LIS 上の別のクライアントに伝送するトラフィックをもっている場合、クライアントは ARP サーバーに ARP 要求をターゲット IP アドレスを指定して送信します。

サーバーは、応答 (サーバーがそのテーブル内に情報をもっている場合) または NAK (情報が入手できない場合) のいずれかを送り返します。クライアントはこの ATM アドレスを使用して、ターゲット・クライアントにコールを行います (この呼び出しはデータ・チャネルと呼ばれます)。コールが確立されると、IP データグラムはリンクをいつでも横断することができます。

CIP モデル内では、次の 2 つの形式の要求/応答があります。それらは ATM ARP 要求/応答 (ARP と呼ばれます)、および InATMARP 要求/応答です。 InATMARP は、じかに得た情報を収集しているものと見なすことができます。 つまり、InATMARP は、VCC の他方の端を照会して、その IP アドレスおよび ATM アドレスを調べるのに使用されます。 また、InATMARP は他方の端にそれがだれであるか (その IP アドレスおよび ATM アドレス) も知らせます。 ATMARP は、代理情報と見なすことができます。 CIP クライアントは、ATMARP を ARP サーバーに送信して、指定された IP アドレスに対応する ATM アドレスを見つけます。サーバーは、要求された情報で応答するか、情報が入手できない場合は NAK で応答します。 ただし、RFC はすべてのクライアントおよびサーバーが ARP および InATMARP に適切な応答で応答するよう要求しています。

RFC 2225 クライアントでは、ソースとターゲットのプロトコル・アドレスを同じ値に設定した ARP 要求を送信して、ARP サーバーに登録します。クライアントがこの要求に対する ARP 応答を受信すると、この登録プロセスは、正常に完了されます。

各 LIS ごとに、装置はクライアントのみとして現れるか、その LIS 上のクライアントおよび ARP サーバーの両方として現れることができます。 装置は、ARP サーバーのみをサポートすることはしません。これは、各 ARP サーバーが IP アドレスを含むべきだとする RFC 1577 の勧告に反するからです。

ATM バーチャル・インターフェースの追加情報については、*ソフトウェア使用者の手引き*を参照してください。

タイムアウトおよび最新表示

CIP クライアントおよび ARP サーバーは両方とも、それぞれの ARP 項目の経年処理を行います。 ARP 項目用のタイマーが満了すると、その項目は削除されます。ARP 項目が時間切れになったときにトラフィックが流れている場合、そのトラフィックは新規の ARP 項目が作成されるまで、しばらく停止します。 サービスが中断されるのを避けるため、装置は自動最新表示オプションを提供します。 このオプションにより、クライアントは ARP 要求を ARP サーバーに伝送するか、肯定の InATMARP 応答を ARP 項目が満了になるしばらく前にターゲット・クライアントに伝送することができます。 ターゲットが応答する場合、ARP 項目のタイマーがリセットされます。 ターゲットが応答しない場合は、項目が削除されます。 ARP サーバーは、そのテーブル内で項目が経過時間切れになる前に、InATMARP メッセージを自動的に送信します。 クライアントおよび ARP サーバーは、省略時にはそれぞれ 5 分および 20 分の経過時間に解釈されます。 これらの時間は、各 LIS (クライアントまたはクライアント/サーバーのペア) について構成可能です。

注:

1. ARP 項目は、そのクライアントから ARP または InARP が受信された場合には、必ず更新されます。

2. **Auto-refresh** の省略時値は、クライアントについては *No*、サーバーについては *Yes* です。

RFC 2227 クライアントは、その固有の IP アドレスに関する ARP 要求を送信して、15 分ごとに ARP サーバーに再登録する必要があります。最新表示時間は構成可能ですが、RFC 2225 には、15 分を再登録間隔とする旨が規定されています。

RFC 2225 サーバーでは、InARPs を使用してクライアント項目を最新表示する必要はありません。再登録は、クライアントの責任で行うことです。サーバー **auto-refresh** が RFC 1577 クライアントと互換性があるように、その省略時値は *Yes* のままです。LIS に RFC 2225 クライアントしかない場合は、**auto-refresh** は、サーバー上で *No* に設定できます。

IP アドレスおよび CIP 構成要素

IP アドレスは IP ルーティングへのキーです。 装置を構成するとき、IP アドレスをインターフェース (ATM ポート) に追加すると、自動的に CIP クライアントが作成されます。 クライアントは、ATM ARP クライアント情報を追加することにより、さらに定義されますが、クライアントを作成するのは IP アドレスの追加によってです。

各サーバーは IP アドレスを含んでいるので、クライアントも暗黙に含んでいます。サーバーを構成しているとき、IP アドレスを構成し、自動的にクライアントを作成する必要があります。 必要なデータベースが次に作成され、着信要求をサービスするために保持されます。

構成された IP アドレスは、装置がルーターとして働くことを必ずしも意味しません。ルーターとして働くためには、OSPF などのより高水準のルーティング・プロトコルを構成する必要があります。 ただし、装置が複数のサブネットに接続されている場合、およびパケットが、1 つのサブネットから、接続された他のサブネットの 1 つにあるステーションにあてて送信される場合、装置はルーティング・プロトコルを構成させずにそのパケットを転送します。 さらに、パケットがその装置に送信されるが、パケットのあて先がその装置ではなく、あて先が発信元と同じサブネット上にある場合、装置は発信元に ICMP あて先変更メッセージを送信し、パケットを適切なホストに転送します。

CIP 構成要素の ATM アドレス

各クライアントは固有の ATM アドレスを受信します。 前述したように、 NSAP アドレスのみがサポートされます。 終端システム識別子 (ESI) およびセレクターは、構成する人が選択するか、初期設定時に自動的に生成することができます。 装置が LIS 上でクライアントのみとして構成されている場合には、ESI またはセレクターの構成は必要とされません (自動生成を使用するようお勧めします)。 装置がクライアント/サーバーのペアとして構成される場合には、ユーザー自身のセレクター、および必要な場合は ESI を指定するよう強くお勧めします。 (ESI の省略時値は、固有の、焼き付けられた 6 バイトの値であることに注意してください。)そのサーバーについて特定の ATM アドレスが毎回出てくるように、この情報を指定したい場合があります。 このサーバーに接続したいクライアントは、サーバーの ATM アドレスが変わらないものであることを当てにすることができます。

特定の LIS についてサーバー/クライアントのペアが構成されている場合には、サーバーとクライアントの両方が同じ ATM アドレスを使用します。 各 CIP クライアント用の ATM アドレス (ESI とセレクターの組み合わせ) は固有である必要があります。

バーチャル・チャネル・コネクション (VCC)

バーチャル・チャネル・コネクション (VCC) は、データ伝送用の最も低い共通の標準です。 これは動的に作成することができるか (この場合、VCC はスイッチド・バーチャル・サーキット (SVC) です)、あるいは ATM スイッチおよびエンド・ステーションでパーマネント・バーチャル・サーキット (PVC) として構成することができます。

SVC は、接続を確立するのに、コールのセットアップまたは信号プロトコルを必要とします。SVC のセットアップは、電話呼び出しを行うのに似ています。ユーザーは電話番号をダイヤルし、応答通話者と通信する前に電話が応答されるのを待ちます。どちらかの端が電話を切る場合、コーラーは再び話す前に番号をリダイヤルする必要があります。ATM SVC についても同じことが言えます。ホストは、20 バイトの ATM アドレス (電話番号に似ています) の付いたセットアップ・メッセージを発信し、他の端が接続するのを待ちます。 どちらのホストもチャネルを切断することができます。

他方、PVC は信号プロトコルを必要としません。 UNI の突き合わせレベルも必要でありません。 それらは静的であり、初期設定時から電源を落とすまでホストに使用可能です。 ホストは、接続を 『セットアップ』 するのに何のアクションも取る必要がありません。 そのようになっているので、PVC は SVC より単純で、一般的に高い信頼性をもちます。

装置の実施するクラシカル IP は、PVC と SVC の両方をサポートしています。SVC は、クラシカル IP コードによって実行されるアドレス解決プロセスおよびそれに続く呼び出しセットアップによって自動的に生成することができるか、あるいは SVC はユーザーによって明示的に構成することができます。 自動 SVC は、送信する IP トラフィックについて要求されるように、ARP サブシステムによって立ち上げられ、破棄されます。 構成済みの SVC は、初期設定時に立ち上げられ、無限に立ち上がった状態で保持されます。 構成済みの SVC が接続しない場合、装置は電源が切られるまで、定期的に接続の再試行を継続します。

PVC および構成済みの SVC は、ARP サーバー定義を必要としません。 つまり、LIS は、構成済みの情報によってのみ相互に接続されるホストから構成することもできます。 任意選択で、構成済みの PVC または SVC の着信 IP アドレスも同様に構成することができます。 IP アドレスが構成されていない場合、InATMARP パケットを使用して、VCC の反対側の端にどの IP アドレスがあるか判別することができます。どのサイズのネットワークでも、手動構成の量は困難なものとなります。 SVC が自動的に生成されると、構成済みの情報の量が激減し、ホストを追加したり移動する上で最大限の柔軟性が提供されます。

自動的に生成された VCC は、ARP サーバーの援助がないと存在できません。 各クライアントは、ARP サーバーの ATM アドレスを使って構成する必要があります。初期設定の直後に、クライアントは ARP サーバーへの接続を試みます。 この接続は、制御チャネルと呼ばれます。 制御チャネルの主な使用は、ATMARP および

InATMARP の要求および応答を送信するためです。ただし、ARP サーバーがクライアントでもある場合は、制御チャネルは IP データを送信するのにも使用することができます。 1 つのホストから別のホストにデータを送信するために生成された自動 VCC は、データ・チャネルと呼ばれます。

制御チャネルとデータ・チャネルの両方の属性は、ユーザーのニーズに従って調整することができます。 装置の CIP 構成では、ピーク・セル速度、保持セル速度、最大 SDU サイズ、および装置によってセットアップされる制御チャネルおよびデータ・チャネルの他の特性の構成を行うことができます。 ユーザーは、さまざまな ATM 接続機構の帯域幅の不一致によって生じる問題を避けるために、着信コールのセル速度を制限するよう選択することもできます。

クラシカル IP 用の主な構成パラメーター

CIP は単純であるため、必須指定の構成パラメーターはごくわずかです。クライアント専用の場合には、次の 3 つの情報が必要です。

1. IP アドレスおよびサブネット・マスク。 (**add address**)
2. ARP サーバー (または分散 ARP サーバー) の ATM アドレス。 (**add arp-server**)
3. ARP クライアントの構成、ならびにそのクライアントがサーバーでもあるかどうかを尋ねられたときに *No* と応答すること。

IP アドレスおよびサブネット・マスクは、クライアントが IP データグラムを送受信できるようにその固有な IP 識別子をクライアントに与える必要があります。この CIP クライアントが属しているサブネットも定義されます。ARP サーバーの ATM アドレスは、ARP サーバーとの制御チャネルを確立するために、初期設定時に クライアントが使用します。

与えられた 1 つの LIS について、複数の ARP サーバーをバックアップ目的で定義することができます。基本 ARP サーバーが故障した場合、クライアントは、単一点障害を避けるためにバックアップ ARP サーバーに切り替えることができます。クライアントは、基本 ARP サーバーがサービスを再開するとすぐに、その基本 ARP サーバーに切り替え直すことができます。与えられた LIS の基本 ARP サーバーとして、最初の構成済み ARP サーバー ATM アドレスが選択されます。基本 ARP サーバーは、`ARP Config>` コマンド・プロンプトから **reorder** コマンドを使用して変更できます。

サーバーの構成も同様に単純です。 本質的には、サーバーは、固定した、既知の ATM アドレスを使って定義する必要があり、どの LIS にサービスを行っているかを知っている必要があります。 サーバーの構成には、次のものが必要です。

1. IP アドレスおよびサブネット・マスク。 (**add address**)
2. このクライアントがサーバーでもあるかどうかについての質問に 『Yes』 と答えること。(**add atm-arp-client-configuration**)
3. サーバーの ATM アドレスについて明示的なセレクターを指定すること (内部的に割り当てられたセレクターを使用したい場合は、『no』 と答えること)。 (**add atm-arp-client-configuration**)

IP アドレスおよびサブネット・マスクは、サーバーにそれがどの LIS にサーブしているかを知らせます。 IP アドレスは、サーバーに IP アクセスも与え、必要な場合

は (暗黙クライアントを通じて) ルーティング情報も与えます。 『add atm-client-configuration』 では、特に質問 2 および 3 が尋ねられます。質問 2 は、その LIS についてサーバー機能を使用可能にするために必要です。 質問 3 は、サーバーに予測可能な ATM アドレスを与えるために使用されます。

アドレスを入力する方法

アドレスが (1) IP アドレスを表しているか、(2) ATM アドレス、MAC アドレス、またはルート記述子を表しているかに応じて、アドレスを入力するには次の 2 通りの方法があります。

1. IP アドレス

   IP アドレスは、ドット 10進形式で入力され、4 バイトのフィールドは、ピリオド (.) によって分離された 4 つの 10 進数 (0 ～ 255) によって表されます。

2. ATM または MAC アドレスあるいはルート記述子

   ATM アドレス、MAC アドレス、およびルート記述子は、16 進文字のストリングとして入力され、バイトの間に任意選択の分離文字がある場合とない場合があります。 有効な分離文字はダッシュ (-)、ピリオド (.)、またはコロン (:) です。

   これは、ATM、LAN エミュレーション、および ATM を介したクラシカル IP & ARP について入力されたアドレスに適用されます。

IP Address の例:

```
01.255.01.00
```

ATM アドレス、MAC アドレス、またはルート記述子の例:

```
A1FF010203
```

または

```
A1-FF-01-02-03
```

または

```
A1.FF.01.02.03
```

または

```
39.84.0F.00.00.00.00.00.00.00.00.00.03.10.00.5A.00.DE.AD.C8
```

または

```
A1:FF:01:02:03
```

または、以下の場合もあります。

```
A1-FF.01:0203
```

クラシカル IP 冗長の概要

ARP サーバー冗長には、2 つの装置があります。1 つは基本 ARP サーバーとして機能し、もう 1 つは基本のバックアップとして機能します。クラシカル IP 冗長により、ユーザーは、基本サーバーとして行動する装置と、2 次サーバー (バックアップ・サーバー) として行動する装置を構成内で指定できます。このタイプの冗長性では、基本サーバーは、与えられた LIS についてサービスとルーティングを行うよう構成さ

れます。基本が故障すると、バックアップが、基本の ATM アドレスを使用して登録し、ARP サーバーとして引き継ぎます。バックアップは、冗長省略時 IP ゲートウェイとしても行動することができるため、その LIS についてのサーバーおよびルーターとして引き継ぎます。したがって、すべてが作動可能な場合、基本は LIS 上に 2 つの IP アドレス (クライアント IP アドレスとゲートウェイ IP アドレス) をもち、バックアップは LIS 上に単一のクライアント IP アドレスをもちます。基本サーバーは故障すると、LIS 上での表示が明白に停止され、バックアップが LIS 上に IP アドレスを 2 つもつようになります (その元のクライアント IP アドレスと、新たに取得した冗長省略時 IP ゲートウェイ・アドレス)。バックアップは、(基本の ATM アドレスを引き継ぐことにより) その LIS について ARP サーバーの役割を果たすものと想定されます。

ARP サーバー冗長構成により、ユーザーは、基本として機能する装置と、2 次として機能する装置を制御することができます。これにより、ユーザーが ARP サーバー上での負荷の平衡を効率よく取れる一方で、バックアップが提供されます。例えば、ある装置を 6 つの LIS の基本 ARP サーバーとし、別の 6 つの LIS の 2 次サーバーとしたいとします。また、1 つの 2 次装置を最初の 6 つの LIS の 2 次にし、他の 6 つの LIS の基本としたいとします。結果として生じる構成には 12 の LIS があり、6 つは一方の装置がサーバーとしての機能を果たし、他の 6 つはもう一方の装置がサーバーとしての機能を果たすことになります。どちらかの装置が故障すると、もう一方の装置が 12 個の LIS すべてについてサーバーの役割を引き継ぎます。

ATM エンドポイントと関連付けられた ATM アドレスが 2 つになることに注意してください。ATM アドレスの 1 つは、実際の ATM アドレスであり、もう一方は、特別な冗長 ATM アドレスで、これを冗長アドレスと呼びます。冗長アドレスは、必ず、登録されます。冗長チャネルは、基本と 2 次の冗長アドレスの間に設定されます。冗長アドレスは、冗長活動専用に使用されます。実際のアドレスは、IP 情報の交換に使用されます。

ARP サーバー冗長では、基本として構成された場合、基本エンティティーはその実際の ATM アドレスを正常に登録できるまで、*常に*登録を試みます。基本は、また、2 次に対して冗長チャネルについてのコールを行おうとします。

注:

1. ARP サーバー冗長では、LIS 上のクライアントが、複数の IP アドレスを単一の VCC と関連付けられることが必要です。
2. 基本とバックアップは、同じ ATM スイッチに接続する必要があります。

非分散 ARP サーバー LIS の ARP 冗長構成プロセスについて、以下のステップで説明します。

1. 一方の装置上に ARP クライアント/サーバーのペアを構成する。これが、基本 ARP サーバーになります。
2. もう一方の装置だけに ARP クライアントを構成する。これにより、バックアップ ARP サーバー機能が提供されます。
3. 基本 ARP クライアント/サーバーのペアおよびバックアップ ARPサーバー機能を提供する ARP クライアント (両方の IP アドレスは同じ LIS 上になければなりません) に対して異なる ATM アドレスと異なる IP アドレスを使用する。

注: 詳細については、635ページの『ARP 構成の例』に記載されている構成の例を参照してください。

ARP サーバー冗長により、1577 クライアントについてのバックアップ・サーバーの機能が提供されます。 2225 クライアントでは、バックアップ ARP サーバーへの切り替えができるため、 ARP サーバー冗長は必要ありません。

分散 ARP サーバーの概要

分散 ARP サーバーを使用して、ARP サーバーが故障した場合に LIS との接続性を保持することができます。1 つの LIS あたり必要な数の分散サーバーを定義することができます (通常、3 〜 4 つあれば足ります)。分散サーバーは、ATM ネットワーク内の任意の場所に配置できます。分散サーバーは、メッシュする必要はありませんが、互いを結ぶなんらかの通信パスが必要です。

分散 ARP サーバーの利点として、これ以外に、ATM ARP サービス負荷を多数の装置に分散できるため、大型の LIS をさらに効率よく扱えるということがあります。

同じ LIS 上の分散 ARP サーバーは、次のものを使用して構成する必要があります。

- 同じサーバー・グループ ID (SGID)
- 他のサーバーが ARP データベース情報を交換するためにこのサーバーに接続するのに使用できる ATM アドレスを作成するために使用される ESI/セレクターのペア
- 分散 ARP サーバーが同期を試みる直接接続サーバー (DCS) の ATM アドレス

分散 ARP サーバーは、IETF 草案「サーバー・キャッシュ同期プロトコル (SCSP) - NBMA」 に準拠しています。SCSP は、ATM ネットワークにサーバー・データベースを分散するための汎用プロトコルです。

ATM ARP クライアントは、ARP サーバーへの接続が作動可能でないときを認識できる必要があり、代替サーバーへ切り替えられることも必要です。 RFC 2225 準拠のクライアントは、この要件に適合します。

分散 ARP サーバーの例

605ページの図50 では、1 つの LIS 上に 2 つの ARP サーバーが定義されています。これらの ARP サーバーは、互いの ARP データベースを複写できるように構成されています。各装置の SCSP は、他方の ARP サーバーの SCSP ATM アドレスで構成されています。ARP サーバーは、データベース情報を交換できるように、プライベート・セッションを確立します。装置内の SCSP は、同じ装置内の ARP サーバーと対話して、キャッシュ変更を入手して報告します。

ATM ARP クライアントは、2 つの ARP サーバーをもつように構成されており、一方のサーバーが基本サーバーとして機能し、もう一方は故障の際のバックアップとして機能します。クライアントは、基本サーバーとの接続がなくなると、バックアップに登録します。バックアップは、全 ARP 解決データベースをもち、クライアントに ARP 解決サービスを提供するようになります。

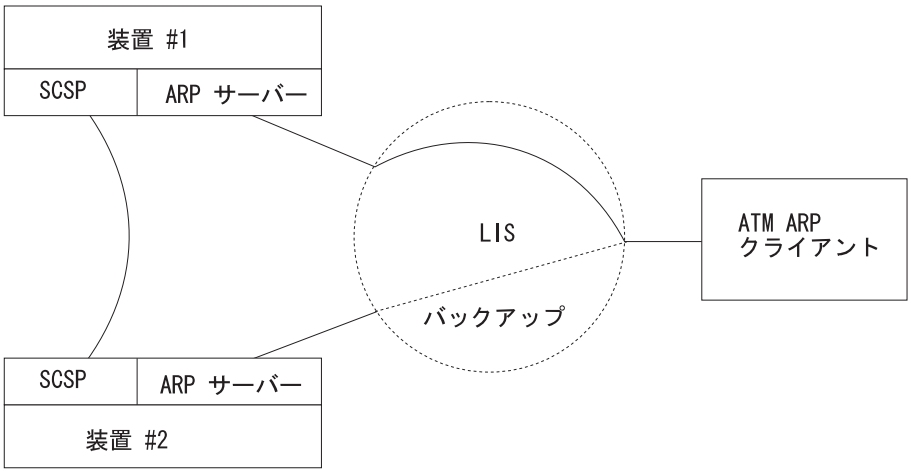


図 50. 単純な分散 ARP サーバー構成

606ページの図51 では、1 つの LIS 上に 3 つの ARP サーバーが構成されています。装置 1 は、1 つの直接接続サーバー (DCS) で構成され、装置 2 は 2 つの DCS で構成され、装置 3 は 1 つの DCS で構成されています。

クライアント 1 は、その ARP サーバーとして装置 1 で構成されています。クライアント 2 は、その基本サーバーとして装置 3 で、また、そのバックアップとして装置 2 で構成されています。この構成では、クライアント 1 は、クライアント 2 が装置 3 に登録されている場合でもクライアント 2 のアドレスを装置 1 から入手できます。同様に、クライアント 2 は、クライアント 1 のアドレスを装置 3 から入手できます。

装置 3 が故障した場合、クライアント 2 は、接続性を失うことなく、ARP サービスについて装置 2 に切り替わることができます。装置 1 が故障した場合には、クライアント 1 は、バックアップ ARP サーバーが構成されていないため、結局、LIS との接続性を失います。装置 2 が故障すると、冗長性は失われます。この構成が全冗長性を保存するためには、装置を全体メッシュにする必要があります。

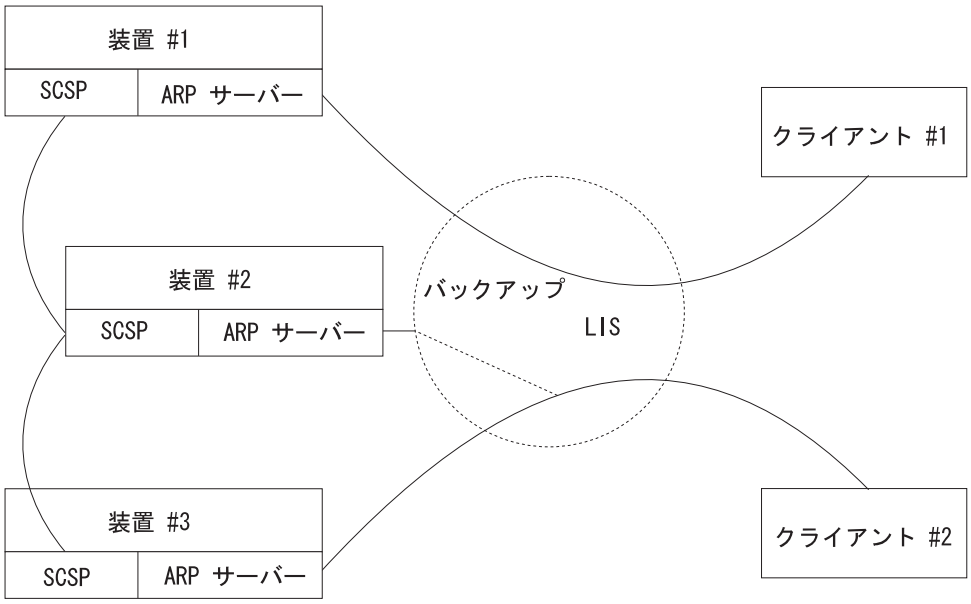


図 51. 3 つの ARP サーバーのある分散構成

ピア冗長

分散 ARP サーバーを使用すると、RFC 2225 クライアントに対する代替 ARP サーバー・サポートが得られます。 ARP サーバー冗長により、ユーザーは、RFC 1577 クライアントについてバックアップ ARP サーバーを定義することができます。 冗長機能と分散 ARP サーバー機能を、同じ装置上で定義できます。この構成では、基本とバックアップの両方が、SCSP が使用可能なサーバーとして定義されます。 両方が動作しているときは、全 ARP データベースが使用可能な状態の ARP サーバーとして行動します。 基本が故障すると、バックアップは、基本の ATM アドレスを引き継ぎます (自分自身のアドレスも保持します)。 さらに、バックアップが故障した場合には、基本はバックアップの ATM アドレスを引き継ぐことができるため、その 1577 クライアントをサポートします。

注: 基本とバックアップの両方を、同じ ATM スイッチに接続する必要があります。
.

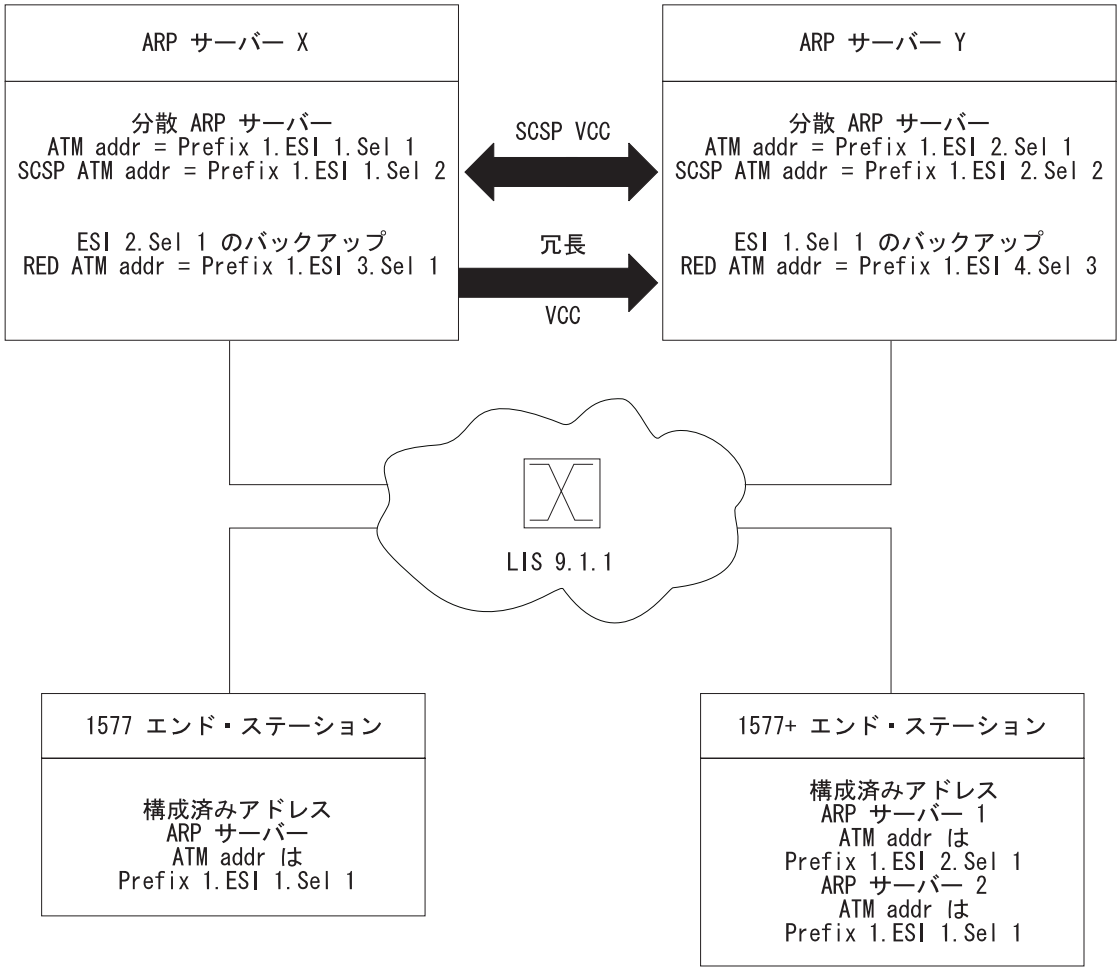


図 52. RFC 1577 および 2225 クライアントをもつ ARP サーバー構成

サーバーは、冗長サーバーと分散サーバーの両方として構成できます。 図52 では、LIS 9.1.1 用に分散 ATMARP サーバーが使用されます。 サーバー X とサーバー Y は両方とも、LIS 9.1.1 上の ATMARP の異なるセットに積極的にサーバーとして機能しています。サーバー X は、RFC 1577 準拠のクライアントにサービスを提供し、サーバー Y は、2225 クライアントによって最初に選択されています。 2 つの ARP サーバーのデータベースは、SCSP プロトコルによって同期化されます。サーバー Y に障害が起こった場合は、2225 は、ATMARP サーバー ATM アドレスのリスト上の次の項目を使用し、サーバー X に接続します。

1577 準拠クライアントに ARP サーバー冗長を提供するために、サーバー X は ATM アドレス Prefix 1.ESI 1.Sel 1 の基本 ARP サーバーとして指定され、サーバー Y は ATM アドレス Prefix 1.ESI 1.Sel 1 のバックアップ ARP サーバーとして指定するされています。基本およびバックアップ ARP サーバーにより、冗長サポートが提供されます。サーバー X が故障して、サーバー Y が引き継いだ場合、サーバー Y は、他の ATM アドレスに加えて ATM アドレス Prefix 1.ESI 1.Sel 1 を登録します。したがって、サーバー Y は、ATM アドレス Prefix 1.ESI 1.Sel 1 と ATM アドレス Prefix 1.ESI 2.Sel 1 を同時に表します。その後、サーバー X が回復し、サーバー Y

への VCC を再確立すると、サーバー Y は、サーバー X が LIS についてのアクティブな ARP サーバーとしてのその役割を再開できるように、ATM アドレス Prefix 1.ESI 1.Sel 1 の登録を解除します。

ピア冗長は、冗長性のために構成された分散 ARP サーバー間に冗長チャネルが存在するかどうかによって異なります。 大きい方の冗長 ESI をもつ ATM クライアントまたはサーバーが、パートナーとの冗長チャネルを開始します。この例では、ESI 3 は ESI 4 より大きいため、サーバー X が、サーバー Y に対する冗長チャネルについてのコールを開始します。

ピア冗長を構成する

ARP サーバー冗長について新しい構成を作成する際に、ATM クラシカル IP クライアントが分散 ARP サーバーとして構成されている場合にはピア冗長が自動的に確立されます。

以前のリリースから既存の構成が使用される場合には、ピア冗長が自動的に作成されることはありません。この場合には、ピア冗長を使用可能にするために、**change redundancy** コマンドを使用して、分散 ARP サーバーのそれぞれに対してパートナー・サーバー ESI とセレクターを提供し、構成を装置に書き込んでください。そうすると、ピア冗長は、冗長 ARP サーバーが分散 ARP サーバーである限り、使用可能になります。

クライアントの分散 ARP サーバーが与えられた IP アドレスについてクライアント構成を変更することによって使用不能にされ、しかも冗長構成がある場合には、ピア冗長は使用不能になります。分散 ARP サービスが使用不能であると、冗長構成が正しいかどうかを検査するようプロンプト指示されます。

ATM を介した IPX および ARP の概要 (RFC 1483)

2210 は、ATM を介して IPX トラフィックを搬送するのに RFC 1483 によって指定された LLC/SNAP カプセル化を使用します。 2210 (および ATM 上での RFC 1483 LLC/SNAP カプセル化をサポートするその他のルーター) は、手動で構成された RFC 1483 接続を介して全体メッシュまたは部分的なメッシュで相互に接続することができます。PVC および構成済みの SVC の両方がサポートされます。 ただし、IPX ルーターへの SVC は IPX 専用にする必要があります。それらは、IP などの他のプロトコルと共用することはできません。

クラシカル IP の場合と同様に、サーバー品質特性は、ピーク速度および保持速度などの VCC トラフィック・パラメーターを構成することによって指定することができ、複数のサーキットを単一の ATM インターフェース上で構成することができます。

2210 は、ATM インターフェースごとに単一の IPX ネットワークをサポートします。これは、IPX を明示的に構成する必要のある各インターフェースごとに単一の ATM ARP クライアントを意味します。したがって、ATM インターフェース上の相互に接続されたすべてのルーターは同じ IPX ネットワークの部分である必要があります。

IPX ATM アドレスは、RFC 1483 カプセル化 (これにはクラシカル IP 構成要素が含まれています) を使用するすべての構成要素間で固有でなければなりません。IPX

ATM アドレスの ESI およびセレクターの部分は、クラシカル IP の ATM アドレスと同様に構成されます。2210 が SVC を開始していない場合には、コーリング・ルーターで構成することのできる固定したアドレスを提供するためには、現行の構成で少なくともセレクターが明示的に指定されている必要があります。

IPX プロトコル・アドレスには、次の 2 つの部分があります。

- 4 バイトのネットワーク番号、および
- 6 バイトのホスト番号 (またはホスト ID)

ネットワーク番号は IPX ルーティング・ドメイン内で固有である必要があり、ホスト番号は与えられたネットワーク内で固有である必要があります。IPX ホスト番号は (2210 によって) 関連する ATM アドレスの ESI 構成要素に設定されます。ESI は、ユーザーによって明示的に構成されない場合は、ATM インターフェース・ハードウェアに焼き付けられた MAC アドレスに省略時解釈されます。

あて先 IPX ホスト番号は、VCC 構成時に指定するか、InATMARP を介して動的に学習することができます。InATMARP をサポートしていないあて先ルーターの IPX ホスト番号は手動で構成する必要があります。InATMARP は、接続されたルーターの IPX ホスト番号についての 2210 の知識を定期的に最新表示するためにも使用されます。

部分メッシュで相互接続され、同じ ATM インターフェース上で中間ルーティングを提供するルーターは、ATM インターフェース上で IPX 水平分割を使用不能にする必要があります。これにより、RIP および SAP は、相互接続されたルーターに、使用可能なすべてのルートおよびサービスについて正しく知らせることができるようになります。 全体のメッシュで相互接続されたルーターは、水平分割を使用不能にする必要はありません。

ATM バーチャル・インターフェース機能を使用すると、IPX は、1 つの ATM インターフェースにつき 1 つのアドレスという制限がなくなります。いくつかの ATM バーチャル・インターフェースを 1 つの物理 ATM インターフェース上に定義することができ、各 ATM バーチャル・インターフェースに IPX アドレスを 1 つ構成できます。

ATM バーチャル・インターフェースの追加情報については、*ソフトウェア使用者の手引き*を参照してください。

ATM を介したブリッジングの概要 (RFC 1483)

ブリッジングは ARP サポートを使用しませんが、固有のATM に対してブリッジングを実施すると、いくつかの内部構造を ARP と共用することになります。この関係では、ブリッジ・ポートの ATM クライアントとチャネル・レコードを表示したり、修正することができます (クライアント・レコードのみ)。これらのレコードの追加や削除は、ATM インターフェース上でブリッジ・ポートが追加または削除されたときに自動的に行われることに注意してください。

ATM に対するブリッジングの RFC 1483 サポートについて詳しくは、60ページの『ブリッジングについての RFC 1483 サポート』を参照してください。

第28章 ARP の構成と監視

この章では、 ARP プロトコル活動の構成と監視方法、ならびに ARP 監視コマンドの使用方法について説明します。 この章には次の節が含まれています。

ARP 構成環境へのアクセス

ARP 構成環境にアクセスする方法についての説明は、 *ソフトウェア 使用者の手引き* の中の “はじめに” を参照してください。

ARP *構成* プロセスにアクセスするには、次の手順を使用してください。

1. OPCON プロンプトで、**talk 6** を入力します (このコマンドについて詳しくは、 *ソフトウェア 使用者の手引き* の中の “OPCON プロセス” を参照してください)。 例えば、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>`) が端末で表示されます。最初に構成を入力したときにプロンプトが表示されない場合は、**Return** を再び押します。
2. CONFIG プロンプトで **prot arp** コマンドを入力して、`ARP Config>` プロンプトを出します。

ARP および逆 ARP の構成コマンド

この節では、 非 ATM ネットワーク用の ARP 構成コマンド 612ページの表35 は、ARP 構成コマンドをリストします。 ARP 構成コマンドには、`ARP config>` コマンドでアクセスできます。

注: これらのコマンドは、ATM インターフェース上でクラシカル IP、IPX、および ブリッジング用に ARP を構成するために使用するものではありません。 しかし、これらのコマンドを使用して、ATM LAN エミュレーション・クライアント用に ARP を構成することができます。

表 35. 非 ATM ネットワーク用の ARP 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add Entry	MAC アドレス変換項目を追加します。
Change Entry	MAC アドレス変換項目を変更します。
Delete Entry	MAC アドレス変換項目を削除します。
Disable Auto-refresh	ARP 自動最新表示を使用不能にします。
Enable Auto-refresh	ARP 自動最新表示を使用可能にします。
List	SRAM 内の ARP 構成データをリストします。
Set	使用法を設定し、タイムアウト値を最新表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add Entry

add entry コマンドは、『静的プロトコルからハードウェア・アドレスへのマッピング』 項目を追加するのに使用します。このコマンドは、現在、IP アドレス用にのみサポートされています。

構文 :

add entry *ifc# prot-type prot-addr MAC-addr*

ifc#
有効値: 任意の定義済みインターフェース

省略時値: 0

prot-type
有効値: ARP がサポートする任意のプロトコル

省略時値: IP

prot-addr
有効値: 任意の有効な IP アドレス

省略時値: 0

MAC-addr
有効値: 任意の有効な MAC アドレス

省略時値: なし

例: add entry

```
Interface Number [0]?
Protocol [IP]?
IP Address [0.0.0.0]?
Mac Address []?
```

Change Entry

change entry コマンドは、『静的プロトコルからハードウェア・アドレスへのマッピング』 項目を変更するのに使用します。このコマンドは、現在、IP アドレス用にのみサポートされています。 ハードウェア・アドレス・パラメーター (MAC-addr) は、変更されるノードのアドレスでなければなりません。

構文 :

change entry *ifc# prot-type prot-addr MAC-addr*

ifc# **有効値**: 任意の定義済みインターフェース

省略時値: 0

prot-type

有効値: ARP がサポートする任意のプロトコル

省略時値: IP

prot-addr

有効値: 任意の有効な IP マスク

省略時値: なし

MAC-addr

有効値: 任意の有効な MAC アドレス

省略時値: なし

例: change entry

```
Interface Number [0]?
Protocol [IP]?
IP Address [0.0.0.0]?
Mac Address []?
```

Delete Entry

delete entry コマンドは、『静的プロトコルからハードウェア・アドレスへのマッピング』 項目を削除するのに使用します。このコマンドは、現在、IP アドレス用にのみサポートされています。

構文 :

delete entry *ifc# prot-type prot-addr*

ifc# **有効値**: 任意の定義済みインターフェース

省略時値: 0

prot-type

有効値: *IP* または *IPX*

省略時値: IP

prot-addr

有効値: 任意の有効な IP アドレス

省略時値: 0.0.0.0

例: delete entry

```
Interface Number [0]?
Protocol [IP]?
IP Address [0.0.0.0]?
```

Disable Auto-Refresh

disable auto-refresh コマンドは、自動最新表示機能を使用不能にするのに使用します。自動最新表示機能とは、最新表示タイマーが時間切れになる前に、ルーターが変換キャッシュ内の項目に基づいて ARP 要求を送信する機能です。要求は、同報通信の代わりに現行の変換キャッシュ内のハードウェア・アドレスに直接送信されます。 自動最新表示が使用不能にされている場合は、'プリエンプティブ' ARP 要求は行われず、最新表示タイマーが時間切れになり、ARP 変換がテーブルから除去されます。あて先プロトコル・アドレスへの次のプロトコル・パケットにより、新規の ARP 要求がネットワーク上で同報通信されます。

構文 :

disable auto-refresh

例: `disable auto-refresh`

Enable Auto-Refresh

enable auto-refresh コマンドは、自動最新表示機能を使用可能にするのに使用します。自動最新表示機能とは、最新表示タイマーが時間切れになる前に、ルーターが変換キャッシュ内の項目に基づいて ARP 要求を送信する機能です。要求は、同報通信の代わりに現行の変換キャッシュ内のハードウェア・アドレスに直接送信されます。

自動最新表示を使用可能にすると、項目がそれらの使用法とは無関係にキャッシュ内で保持されます。多数のノードをもつネットワークでは、これによりキャッシュ内に過剰な数の項目が入ることになり、ルーターの性能に悪影響を及ぼすおそれがあります。ただし、ノードの数が少ないネットワークでは、このオプションは同報通信 ARP トラフィックを減らすのに便利です。

構文 :

enable auto-refresh

例: `enable auto-refresh`

List

list コマンドは、SRAM に保管されているとおりのルーターの ARP 構成の内容を表示するのに使用します。 list コマンドは、最新表示および使用法のタイマーについて現行のタイムアウト設定値を表示します。

構文 :

list all
config
entry

all ARP 構成に続いてすべての ARP 項目をリストします。

例: `list all`

```
ARP configuration:

Refresh Timeout: 5 minutes
Auto Refresh: disabled

Mac address translation configuration
IF #           Prot #         Protocol --> Mac Address
 0                0           2.2.2.1 --> 0000C90932EF
```

config 異なる ARP パラメーターについての構成をリストします。

例: `list config`

```
ARP configuration:

Refresh Timeout: 5 minutes
Auto refresh: disabled
```

entry SRAM 内の ARP 項目をリストします。

例: `list entry`

```
Mac address translation configuration

IF #           Prot #         Protocol --> Mac Address
 0                0           2.2.2.1 --> 0000C90932EF
```

Set

set コマンドは、ARP 構成パラメーターを設定するのに使用します。

構文 :

set refresh-timer

refresh-timer *minutes*

最新表示タイマーのタイムアウト値を変更します。 最新表示タイマーのタイムアウト値を変更するには、タイムアウト値を分単位で入力してください。設定値がゼロ (0) だと、最新表示タイマーはオフ (使用不能) にされます。

このタイマーは、ARP 変換キャッシュ項目が自動最新表示が使用可能にされている間に最新表示される時期、または自動最新表示が使用不能にされている間に消去される時期を判別するために使用されます。タイマーを使用不能にすると、項目は、新規に学習されたアドレス変換が項目を除去するまで、項目が ARP **clear** 監視コマンドを使って手動でクリアされるまで、あるいはルーターが再始動されるまで、保持されます。

有効値: 0 ～ 65535 の範囲内の整数の分数

省略時値: 5 分

例: `set refresh-timer 3`

ATM を介した ARP の構成コマンド

この節では、ATM を介した ARP の構成コマンドについて説明します。これらのコマンドは次のものに適用されます。

- ATM を介したクラシカル IP & ARP
- ATM を介した IPX
- 1483 ブリッジング

コマンドは、`ARP Config>` プロンプトに入力します。

ARP テーブル項目への影響

これらのコマンドは、ATM を介した ARP 用に ARP 項目が常駐する物理 ATM インターフェースにのみ適用されます。これらのコマンドは、非 ATM インターフェースには影響しません。

表 36. ATM を介した ARP の構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
List	すべて (現行の ATM を介した ARP の構成) をリストするか、ARP サーバー (IP についてのみ) をリストするか、あるいは pvc-atm-arp-entries および redundancy をリストします。
Add	arp-server、atm-arp-client-configuration、 pvc-atm-arp-entry、svc-atm-arp-entry、または redundancy を追加します。
Change	atm-arp-client-configuration または redundancy を変更します。
Delete	arp-server、atm-arp-client-configuration、 pvc-atm-arp-entry、svc-atm-arp-entry、または redundancy を削除します。
Disable	ARP 項目が自動的に更新されないように、**auto-refresh** を使用不能にします。
Enable	ARP 項目が自動的に更新されるように、**auto-refresh** を使用可能にします。
Set	ARP 項目を経年処理するよう **refresh-timer** を設定します。
Reorder	与えられた ARP サーバー・リストから基本 ARP サーバーを選択します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、arp-server、atm-arp-client-configuration、svc-atm-arp-entry、または redundancy を追加するのに使用します。

構文 :

add arp-server
atm-arp-client-configuration
pvc-atm-arp-entry
svc-atm-arp-entry
redundancy

arp-server private-nsapa *local-client-IP-address private-NSAP-address*

指定されたクライアントに arp-server を追加したり、ARP サーバーに直接接続サーバー (DCS) を追加したりします。

IP アドレスがクライアント専用の場合、NSAP アドレスは、リモート・サーバーのアドレスです。1 つのクライアントにつき、複数のリモート・サーバーを追加できます。初期設定時に、指定した CIP クライアントが ARP サーバーにコールを行い、それを ATM への IP アドレスを解決するためのメカニズムとして使用します。

IP アドレスがサーバーである場合、NSAP アドレスは、分散 ARP サーバーの DCS のアドレスです。このアドレスは、DCS の SCSP ATM アドレス (クライアント ATM アドレスではなく) に一致するものでなければなりません。**t 5** の下にある SCSP> コマンド・プロンプトで **List Server-Groups** 監視コマンドを使用して、サーバーの SCSP ATM アドレスを判別してください。追加情報については、651ページの『第29章 サーバー・キャッシュ同期プロトコル (SCSP) の監視』を参照してください。

local-client-IP-address

この値は、クライアントまたはサーバーの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

省略時値: なし

private-nsap-address

このフィールドは、UNI バージョン 3.0 および 3.1 で指定されたアドレス指定形式である私設ネットワーク指定アクセス・ポイント・アドレスです。DCS を構成する場合、この値は、DCS の ATM アドレスです。

nsapa の最初のバイトは、アドレス形式を次のように定義します。

最初のバイト	NSAP アドレス形式仕様
0x39	DCC ATM 形式
0x47	ICD ATM 形式
0x45	E.164 ATM 形式

注: この設定値は、クライアントの (IP アドレス/ポート番号) ペアに対応します。

省略時値: なし

例:

```
ARP config> add arp-server private-nsapa
Local Client IP Address [0.0.0.0]? 2.2.3.100
Private NSAP Address: Specify 40 digits
ATM Address []? 39840f000000000000000000000410005a3345f3a0
```

atm-arp-client-configuration

atm-arp-client-configuration を追加します。

このクライアントまたはサーバーによってセットアップされ、受信される VCC の特性、最新表示タイムアウトおよび自動最新表示の設定値、このクライアントの ATM アドレスがどのように判別されるか、分散 ARP サービス・パラメーター、さらにこのクライアントが扱うことのできるフレーム・サイズを提供するようプロンプト指示されます。

注: ゼロに等しい帯域幅またはセル・パラメーターは、ATM インターフェースの回線速度として扱われます。

IP についての例:

ATM を介した ARP の構成コマンド (Talk 6)

```
ARP config> add atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]?
Client IP Address [0.0.0.0]? 1.1.1.2
This client is also a server? [Yes] yes
Refresh timeout (in minutes) [20]?
Enable auto-refresh? [Yes]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) 222222222222
  (  4) 121212121212
  (  5) AAAAAAAAAAAA
Select ESI [1]?2
Use internally assigned selector? [Yes]: no
Selector Only, Page 00..FF [00] ? 11
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
Participate in Server Synchronization [No]? yes
Server Group ID [1]?
Do you want to accept sessions from non-configured DCSs [Yes]?
Hello Interval [3]
Dead Factor [3]?
(  1) Use burned in ESI
(  2) 111111111111
(  3) 222222222222
(  4) 121212121212
(  5) AAAAAAAAAAAA
Server Synchronization ESI [2]?
Server Synchronization selector, Range 00..FF [00]? 12
Server Synchronization Max SDU size (bytes) [9188]?
Re-registration time with Arp Server (in minutes) [15]?


To enable or change multicast support,
please issue the ADD or CHANGE MULTICAST-SUPPORT command.
```

IPX についての例:

```
ARP config> add atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? IPX
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [Yes]:
  (  1) Use burned in ESI
Select ESI [1]?
Use internally assigned selector? [Yes]:
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
```

ブリッジングについての例:

```
ARP config> add atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? ASRT
Clients for this protocol can only be changed here.
Additions must be done under ASRT Config by adding a port.
```

Interface Number

割り当てられたインターフェース番号

有効値: 装置上の任意のインターフェース

省略時値: 0

Protocol

有効値*IP*、*IPX*、または *ASRT*

省略時値: IP

Client IP Address
クライアントの IP アドレス (IP のみ)。これは、**p IP** コマンドを使用して構成されたアドレスに一致するものでなければなりません。

注: この値は、SCSP プロトコルで LSID のためにも使用されます。

有効値: 任意の有効な IP アドレス

省略時値: 0.0.0.0

This client is also a server
Yes または No。no の場合は、クライアントはサーバーではありません。(IP のみ)

Refresh timeout (in minutes)
最新表示タイムアウト値の分数。ARP 項目は、更新されない場合に、この数の分数が経過した後で経時タイムアウトします。

有効値: 0 〜 65535 の範囲内の整数の分数

省略時値: 5 分

Enable auto-refresh
YES または NO

No の場合は、ARP 項目は、自動的に更新されません。

省略時値: クライアントの場合は No、サーバーの場合は Yes

Refresh by InAtmArp
YES または NO

YES の場合で、自動最新表示が使用可能にされている場合は、リモート・ホストの存在を確認するため、InAtmArp 要求が定期的に伝送されます。

NO の場合、および自動更新が使用可能になっている場合には、ARP 項目を再確認するために AtmArp 要求が ARP サーバーに伝送されます。

省略時値: クライアントの場合は No、サーバーの場合は Yes

Select ESI
全般的に監視される MAC アドレスまたは ATM インターフェース構成の下で構成された MAC アドレスを ATM アドレスのエンド・システム識別子コンポーネントとして使用すべきかどうかを指定します。この質問の前に、選択を行う有効な ESI のリストが示されます。

有効値 この質問の前に示されるメニューにリストされている値のいずれか。 **Add ESI** ATM ネットワーク構成コマンドを使用して ESI アドレスとして定義されている任意の 12 個の 16 進数字

省略時値 1 (焼き付け)

Use internally assigned selector
内部的に割り当てられたセレクターを使用します。

有効値: Yes または No

省略時値: Yes

Selector

これは、クライアントの ATM アドレスの最後のバイトです。

有効値: 以前に使用されたことがなく、しかも装置について定義された範囲内にある任意の、単一オクテット値

省略時値: 0

Validate PCR for best effort VCCs

TRUE または FALSE。真である場合、信号化された転送 PCR が最大予約帯域幅またはアダプターの速度を超えると、ベストエフォート VCC は拒否されます。偽である場合は、信号化されたピーク・セル速度にかかわらず、ベストエフォート PCR は拒否されます。

Maximum Reserved Bandwidth for incoming VCCs (Kbps)

着信 VCC について許容最大の保持セル速度 (SCR) を定義します。着信コールで SCR が指定されていない場合には、このパラメーターが許容最大のピーク・セル速度 (PCR) を定義します。それより高い速度を指定するトラフィック・パラメーターで受信されたコールは解放されます。このパラメーターは、前方および後方のセル速度パラメーターの両方に適用されます。このパラメーターによって課される制約は、ベストエフォート・コネクションに適用され (『PCR 妥当性検査』 が yes の場合)、着信コールで PCR と比較されます。

有効値: 0 ～ 回線速度までの範囲内の整数 Kbps。0 を入力すると、パラメーターは、回線速度に設定されます。

省略時値: なし

Use Best Effort Service for Control VCCs

コントロール VCC と関係付けられるトラフィック特性のタイプを指定します。帯域幅はベストエフォート・トラフィック用に予約されていません。

有効値: *Best Effort* または *Reserved Bandwidth*

省略時値: Best Effort

Peak Cell Rate of outbound control VCCs (Kbps)

コントロール VCC 用のピーク・セル速度 (PCR) トラフィック・パラメーターを指定します。この PCR 値はベストエフォートおよび予約帯域幅 VCC の両方の前方および後方の PCR 値の両方に使用されます。

有効値: 0 ～ 回線速度までの範囲内の整数 Kbps。0 を入力すると、パラメーターは、回線速度に設定されます。

省略時値:

- best effort の場合、省略時値は max data rate です。
- reserved の場合、省略時値はありません。

Sustained Cell Rate of outbound control VCCs (Kbps)

所定の ATM 装置ですべての VCC によって予約された帯域幅を指定します。 (保持セル速度は予約帯域幅と見なすことができます。) こ

のパラメーターは、コントロール VCC についてベストエフォート・サービスが選択されていない場合のみ適用されます。

有効値: 0 ～ コントロール VCC PCR までの範囲内の整数 Kbps。0 を入力すると、パラメーターは、回線速度に設定されます。

省略時値: なし

Use Best Effort Server for Data VCCs
Yes または No。データ VCC に関連付けられたトラフィック特性のタイプを指定します。帯域幅はベストエフォート・トラフィック用に予約されていません。

Peak Cell Rate of outbound Data VCCs (Kbps)
データ VCC 用のピーク・セル速度 (PCR) トラフィック・パラメーターを指定します。この PCR 値はベストエフォートおよび予約帯域幅 VCC の両方の前方および後方の PCR 値の両方に使用されます。

有効値: 0 ～ コントロール VCC PCR までの範囲内の整数 Kbps。0 を入力すると、パラメーターは、回線速度に設定されます。

省略時値: 0

Sustained Cell Rate of outbound Data VCCs (Kbps)
データ VCC についての保持セル速度 (SCR) トラフィック・パラメーターを指定します。(保持セル速度は予約帯域幅と見なすことができます。) このパラメーターは、データ VCC についてベストエフォート・サーバーが選択されていない場合のみ適用されます。

有効値: データ VCC についての 0 ～ PCR 値までの範囲内の整数 Kbps。0 を入力すると、パラメーターは、回線速度に設定されます。

省略時値: なし

Max SDU size (bytes)
このクライアント・アドレスからコールが行われるときに指定される最大 SDU サイズを指定します。これは、着信コールを検査するためにも使用されます。このパラメーターは、物理 ATM インターフェース (ポート) についての最大 SDU サイズより大きい値に設定することはできません。

有効値: 72 ～ 最大インターフェース SDU までの範囲内の整数

省略時値: 9188

Participate in Server Synchronization
このサーバーが常駐する LIS の ARP データベースを分散するかどうかを指定します。

有効値: Yes または No

省略時値: No

Server Group ID
このサーバー・グループを識別するための値を指定します。この値は、ATM ネットワーク内のすべてのサーバー・グループ (ATMARP プロトコル・タイプ) について固有なものでなければなりません。こ

の値は、このサーバー・グループ (この LIS 内の) 内にあるすべてのサーバーについて使用する必要があります。

有効値: 0 ～ 65535

省略時値: 1

Accept sessions from non-configured DCS

このローカル・サーバーが、明示的に構成されていない DCS からの接続を受け入れるべきかどうかを指定します。

有効値: Yes または No

省略時値: Yes

Hello Interval

このローカル・サーバーについてのハロー・メッセージの送信間の時間を秒数で指定します。

有効値: 0 ～ 65535

省略時値: 3

Dead Factor

直接接続サーバー (DCS) がこのサーバーはダウンしたものとみなした後のハロー間隔の倍数を指定します。

有効値: 0 ～ 65535

省略時値: 3

SCSP ESI

汎用管理 MAC アドレスと ATM インターフェース構成下で構成された MAC アドレスのどちらを SCSP ATM アドレスのエンド・システム識別子構成要素として使用するかを指定します。この質問の前に、選択を行う有効な ESI のリストが示されます。

有効値 この質問の前に示されるメニューにリストされている値のいずれか。 **Add ESI** ATM ネットワーク構成コマンドを使用して ESI アドレスとして定義されている任意の 12 個の 16 進数字。

省略時値 クライアント/サーバーの ESI

SCSP Selector

この SCSP ローカル・サーバーと関連付けられるセレクターを指定します。 ***SCSP ESI*** が省略時値として ARP サーバーの ESI をとる場合、このセレクター値は、ARP サーバー・セレクターとは別のものでなければなりません。

これは、このローカル・サーバーの ATM アドレスの最後のバイトです。

注: SCSP ATM アドレスは、同じインターフェース上の CIP クライアント間で共用できます。 ATM アドレスは、1483 ATM LLC を使用する他のプロトコルとも共用できます。*ソフトウェア使用者の手引き*の『ATM の使用および構成』というタイトルの章を参照してください。SCSP ATM アドレスは、IP、IPX、または ASRT クライアントでは共用できません。

有効値: 以前に使用されたことがなく、しかも装置について定義された範囲内にある任意の有効なセレクター

省略時値: 0

Re-registration time with Arp Server (in minutes)

クライアントから ARP サーバーへの登録要求の時間間隔を指定します。

有効値: 0 〜 65535 の範囲内の整数

省略時値: 15

pvc-atm-arp-entry

PVC を追加し、あて先プロトコル・アドレスが指定されていない場合は任意選択で永続 ARP 項目を作成します。バーチャル ATM インターフェースの場合には、AVI が存在する実際の ATM インターフェースの構成およびその実際の ATM インターフェース上に構成されているその他すべての AVI を検査してください。新しい PVC トラフィックを既存の PVC のトラフィックと特に共用したい場合を除き、新しい PVC には新しい VPI/VCI ペアが必要です。

IP についての例:

```
ARP config> add pvc-atm-arp-entry
Interface Number [0]?
Protocol [IP]?
Local client IP address [0.0.0.0]? 2.2.3.100
Specify destination protocol address? [Yes]: no
Permanent Virtual Circuit VPI, Range 00..FF [00]?
Permanent Virtual Circuit VCI, Range 0000..FFFF [0000]? 0029
```

IPX についての例:

```
ARP config> add pvc-atm-arp-entry
Interface Number [0]?
Protocol [IP]? IPX
Specify destination protocol address? [Yes]: no
Permanent Virtual Circuit VPI, Range 00..FF [00]?
Permanent Virtual Circuit VCI, Range 0000..FFFF [0000]? 0037
```

ブリッジングについての例:

```
ARP config> add pvc-atm-arp-entry
Interface Number [0]?
Protocol [IP]? ASRT
Channels for this protocol must be added under ASRT Config by adding
a port.
```

interface number

有効値: 割り当てられたインターフェースの番号

省略時値: 0

protocol

有効値*IP*、*IPX*、*ASRT*

省略時値: IP

local client IP address

IP の場合は必須。このアドレスは、この PVC をクライアントと関連付けます。

有効値: 任意の有効な IP アドレス

省略時値: 0.0.0.0

destination protocol address

有効値: 任意の有効な IP アドレス (IPX の場合は、任意の 6 バイトの IPX ホスト番号)。

省略時値: 0.0.0.0

permanent virtual circuit VPI

有効値: 0 ～ 255 の範囲内の任意の有効値

省略時値: 0

permanent virtual circuit VCI

有効値: 0 ～ 65535 の範囲内の任意の有効値

省略時値: 0

svc-atm-arp-entry

SVC を追加し、任意選択で永続 ARP 項目を作成します。

IP についての例:

```
ARP config> add svc-atm-arp-entry
Interface Number [0]?
Protocol [IP]?
Local client IP address [0.0.0.0]? 2.2.3.100
Specify destination protocol address? [Yes]: no
Destination ATM Address []? 39840f000000000000000000000210005a00dead03
```

IPX についての例:

```
ARP config> add svc-atm-arp-entry
Interface Number [0]?
Protocol [IP]? IPX
Specify destination protocol address? [Yes]: no
Destination ATM Address []? 39840f000000000000000000000210005a00dead03
```

ブリッジングについての例:

```
ARP config> add svc-atm-arp-entry
Interface Number [0]?
Protocol [IP]? ASRT
Channels for this protocol must be added under ASRT Config by adding
a port.
```

interface number

有効値: 割り当てられたインターフェースの番号

省略時値: 0

protocol

有効値 *IP*、 *IPX*、または *ASRT*

省略時値: IP

local client IP address

IP の場合は必須。このアドレスは、この SVC をクライアントと関連付けます。

有効値: 任意の有効な IP アドレス

省略時値: 0.0.0.0

destination protocol address

有効値: 任意の有効な IP アドレス。IPX の場合は、任意の 6 バイトの IPX ホスト番号

省略時値: 0.0.0.0

destination ATM address

有効値: 任意の有効な ATM アドレス

省略時値: なし

Redundancy

このコマンドは、冗長構成を追加するのに使用します。

ARP サーバー冗長の例

```
ARP config>add red
Interface Number [0]?
Protocol [IP]?
Local client IP Address [0.0.0.0]? 1.1.1.1
Note: Local Redundancy ESI must be different from the Primary Server ESI
     (1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAAA
  (  4) BBBBBBBBBBBB
Select Local Redundancy ESI [1]? 3
Local Redundancy selector, Range 00..FF [00]? aa
Partner's (Redundancy) ATM Address, 40 Hex digits
 [0000000000000000000000000000000000000000]?
39840f000000000000000000001bbbbbbbbbbbbb  1
Redundancy default IP Gateway also ? [No]: yes
If Yes, Redundancy default IP Gateway protocol address [0.0.0.0]? 1.1.1.3
ARP config>
---------- Backup Server (client) -----------------
ARP config>add red
Interface Number [0]?
Protocol [IP]?
Local client IP Address [0.0.0.0]? 1.1.1.2
Note: Local Redundancy ESI must be different from the Primary Server ESI
     (1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAAA
  (  4) BBBBBBBBBBBB
Select Local Redundancy ESI [1]? 4
Local Redundancy selector, Range 00..FF [00]? bb
Partner's (Redundancy) ATM Address, 40 Hex digits
 [0000000000000000000000000000000000000000]?
 39840f000000000000000000001aaaaaaaaaaaaa  1
     (1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAAA
  (  4) BBBBBBBBBBBB
Partner Server ESI [1]? 2
Partner Server selector, Range 00..FF [00]? 11
Redundancy default IP Gateway also ? [No]: yes
If Yes, Redundancy default IP Gateway protocol address [0.0.0.0]? 1.1.1.3
ARP config>exit
Config>
```

注: 1 この入力は、直前の行になければなりません。ここでは、形式設定の理由から、分離した行に示されています。

Interface Number

割り当てられたインターフェース番号

Protocol

IP

Local Client IP Address

この冗長構成をクライアントと関連付けます。

有効値 任意の IP アドレス

省略時値 0.0.0.0

Select Redundancy ESI

全般的に監視される MAC アドレスまたは ATM インターフェース構成の下で構成された MAC アドレスを CIPC または CIPC ATM アドレスのエンド・システム識別子コンポーネントとして使用すべきかどうかを指定します。この質問の前に、選択を行う有効な ESI のリストが示されます。

有効値 冗長 ESI は、must be 基本 ARP クライアント/サーバー機能 ESI のすべてと異なっている必要があります。

省略時値: 1

Choose Redundancy Selector

Redundancy ATM address (冗長 ATM アドレス) のセレクター・バイトを識別します。

有効値: 以前に使用されたことがなく、しかも装置について定義された範囲内にある任意の、単一オクテット値

省略時値 00

Partner's (Redundancy) ATM Address

Redundancy ARP Server (冗長 ARP サーバー) の ATM アドレスを指定します。

有効値 有効なのは、プライベート NSAP アドレスだけです。最初のバイト (Authority and Format Identifier (権限および形式識別子)) には、次の値が含まれている必要があります。

39 -- データ国別コード ATM 形式

47 --- 国際コード指定機能 ATM 形式

45 -- E.164 ATM 形式

省略時値: なし

Partner Server ESI

パートナーの実際の ATM アドレスの ESI コンポーネントを指定します。

有効値 この質問の前に示されるメニューにリストされている有効なサーバー ESI

省略時値: 1

Partner Server Selector

パートナーの実際の ATM アドレスのセレクター・コンポーネントを指定します。

有効値 サーバー・セレクターについて定義された値

省略時値 00

Redundancy's default IP gateway also?

この ARP エンティティーがLIS についての省略時ゲートウェイ冗長サポートの規定に参加するかどうかを指定します。

省略時値: No

Redundancy's default IP gateway address

この LIS についての冗長省略時ゲートウェイの IP アドレスを指定します。これは、ルーターをそれぞれの省略時ルーターとして使用するホストで構成された IP アドレスです。

省略時値: 0.0.0.0

Change

change コマンドは、ATM-ARP 構成を変更するのに使用します。

構文 :

change entry
atm-arp-client-configuration
redundancy
multicast-support

atm-arp-client-configuration

atm-arp-client-configuration を変更します。

Change パラメーターについては、617ページを参照してください。

IP についての例:

```
ARP config> change atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]?
Client IP Address [0.0.0.0]? 1.1.1.2
This client is also a server? [Yes] yes
Refresh timeout (in minutes) [20]?
Enable auto-refresh? [Yes]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) 222222222222
  (  4) 121212121212
  (  5) AAAAAAAAAAAA
Select ESI [1]?2
Use internally assigned selector? [Yes]: no
Selector Only, Page 00..FF [00] ? 11
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
Participate in Server Synchronization [No]? yes
Server Group ID [1]?
Do you want to accept sessions from non-configured DCSs [yes]?
Hello Interval [3]
Dead Factor [3]?
(  1) Use burned in ESI
(  2) 111111111111
(  3) 222222222222
(  4) 121212121212
(  5) AAAAAAAAAAAA
Server Synchronization ESI [2]?
Server Synchronization selector, Range 00..FF [00]? 12
Server Synchronization Max SDU size (bytes) [9188]?
Re-registration time with Arp Server (in minutes) [15]?


To enable or change multicast support,

please issue the ADD or CHANGE MULTICAST-SUPPORT command.
```

IPX についての例:

ATM を介した ARP の構成コマンド (Talk 6)

```
ARP config> change atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? IPX
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [Yes]:
  (  1) Use burned in ESI
Select ESI [1]?
Use internally assigned selector? [No]:
Selector Only, Range 00..FF [00]? 20
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
```

ATM インターフェースには 1 つだけの IPX ATM-ARP クライアント構成レコードが存在するので、プロトコル・アドレスを入力するようにプロンプト指示されません。

ブリッジングについての例:

```
ARP config>
change atm-arp-client-configuration
Interface Number [0]?
 Protocol [IP]? asrt
 Client Address (Port Number) [0]? 2    1
     (1) Use burned in ESI
 Select ESI [1]?
 Use internally assigned selector? [No]:
 Selector Only, Range 00..FF [0A]?
 Validate PCR for best effort VCCs? [No]:
 Use Best Effort Service for Data VCCs? [Yes]:
 Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
 Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
 Max SDU size (bytes) [9188]?
```

注: 1 ブリッジングの場合、プロトコル・アドレスではなく、ポート番号を入力するようプロンプト指示されます。

また、特定のポートについて SVC サポートを使用している場合は、対応するクライアントに内部的に割り当てられたセレクターを使用しないでください。セレクターは、このクライアントの ATM アドレスがもう一方の終端での構成について明確に認識されるように、ユーザーが指定する必要があります。

このコマンドは、トラフィック・パラメーターに省略時値以外の値を使用したい場合にのみ使用してください。

redundancy

クライアントの冗長構成を変更します。

変更できるパラメーターの説明については、625ページを参照してください。

Delete

delete コマンドは、arp-server、atm-arp-client-configuration、pvc-atm-arp-entry、または svc-atm-arp-entry を削除するのに使用します。

構文 :

delete arp-server

atm-arp-client-configuration

pvc-atm-arp-entry

svc-atm-arp-entry

redundancy

mars-server

arp-server

arp-server または DCS を削除します。

arp-server のアドレスを指定してください。この質問の前に、選択を行う有効な arp-servers または DCS のリストが示されます。

有効値 この質問の前に示されるメニューにリストされている値のいずれか

省略時値: 0

IP についての例:

```
ARP config> del arp-server

ATM Arp Remote Server List:
   IP Address      Number       Address / Sub Address
        1.1.1.1     [ 1]       39.84.0F.00.00.00.00.00.00.00.00.02.
                                          11.11.11.11.11.11.11
        1.1.1.1     [ 2]       39.84.0F.00.00.00.00.00.00.00.00.03.
                                         AA.AA.AA.AA.AA.AA.AA

Number of the IP Address/Arp Server pair to be deleted
Default of 0 will delete nothing [0]? 1
```

atm-arp-client-configuration

クライアントの atm-arp-client-configuration を削除します。

インターフェース番号、プロトコル、およびクライアント IP アドレスを指定してください。

interface number

有効値: 任意の定義済みインターフェース

省略時値: 0

protocol

有効値*IP*、*IPX*、**または** *ASRT*

省略時値: IP

client IP address

有効値: 任意の有効な IP アドレス

省略時値: 1.1.1.100

IP についての例:

```
ARP config> del atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]?
Client IP Address [1.1.1.100]? 2.2.3.100
ATM ARP Client Config record deleted
```

IPX についての例:

```
ARP config> del atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? IPX
ATM ARP Client Config record deleted
```

ATM を介した ARP の構成コマンド (Talk 6)

ATM インターフェースには 1 つだけの IPX ATM-ARP クライアント構成レコードが存在するので、プロトコル・アドレスを入力するようにプロンプト指示されません。

フィールドの説明については、IP についての前の例を参照してください。

ブリッジングについての例:

```
ARP config> del atm-arp-client-configuration
Interface Number [0]?
Protocol [IP]? ASRT
Clients for this protocol can only be changed here.
Deletions must be done under ASRT Config by deleting a port.
```

pvc-atm-arp entry

pvc-atm-arp-entry を削除します。

削除したい pvc-atm-arp-entry についての項目番号を指定してください。

IP および IPX についての例:

```
ARP config> del pvc

ATM Arp Permanent Virtual Circuit Definitions
No. IF# Prot# P/S     Protocol     -> VPI / VCI
1    0    0    P         0.0.0.0   ->  00 / 0029
2    0    7    P 00.00.00.00.00.00 ->  00 / 0037
Which Arp entry do you want to delete [0]? 1
ATM Arp entry 1 being deleted
```

No. 1 は IP PVC であり、 No. 2 は IPX PVC です。

ブリッジングについての例:

```
    ARP config>
del pvc
    ATM Arp Permanent Virtual Circuit Definitions
    No. IF# Prot# P/S     Protocol     -> VPI / VCI    (Client Address)
    1    0   23    P                    ->   0 / 87     (Port: 1)
    Which Arp entry do you want to delete [0]? 1
    Channels for this protocol must be deleted under ASRT Config by
    deleting a port.
```

svc-atm-arp-entry

svc-atm-arp-entry を削除します。

削除したい svc-atm-arp-entry についての項目番号を指定してください。

IP および IPX についての例:

```
    ARP config> del svc
   ATM Arp Switched Virtual Circuit Definitions
    No. IF# Prot# P/S     Protocol     -> Destination ATM Address
    1    0    0    S         0.0.0.0   ->
                        39.84.0F.00.00.00.00.00.00.00.00.00.02.10.00.5A.00.DE.AD.03
    2    0    7    P 00.00.00.00.00.00 ->
                     39.84.0F.00.00.00.00.00.00.00.00.00.02.11.00.B7.38.AA.BB.12
    Which Arp entry do you want to delete [0]? 1
    ATM Arp entry 1 being deleted
```

No. 1 は IP SVC であり、 No. 2 は IPX SVC です。

ブリッジングについての例:

```
   ARP config>del svc
   ATM Arp Switched Virtual Circuit Definitions
   No. IF        Prot    P/S     Protocol     -> Destination ATM Address (Client)
   2    0   23    S                     -> 39.11.22.33.44.55.66.77.88.99.00.11.22
                                       33.44.55.66.77.88.99 (Port: 2)
Which Arp entry do you want to delete [0]? 2
Channels for this protocol must be deleted under ASRT Config by deleting a port.
```

redundancy

クライアントの冗長構成を削除します。

Disable

disable コマンドは、ARP 項目の auto-refresh を使用不能にするのに使用します。

auto-refresh 構成値は、atm-arp-client 構成での *auto-refresh* の設定により指定変更されます。atm-arp-client 構成パラメーターについては、617ページを参照してください。

構文 :

disable auto-refresh

auto-refresh

ARP 項目の auto-refresh を使用不能にします。

有効値: Yes または No

省略時値: クライアントの場合は Yes、サーバーの場合は No

Enable

enable コマンドは、ARP 項目の auto-refresh を使用可能にするのに使用します。

auto-refresh 構成値は、atm-arp-client 構成での *auto-refresh* の設定により指定変更されます。atm-arp-client 構成パラメーターについては、617ページを参照してください。

構文 :

enable auto-refresh

auto-refresh

ARP 項目の auto-refresh を使用可能にします。

有効値: Yes または No

省略時値: クライアントの場合は No、サーバーの場合は Yes

List

list コマンドは、SRAM に保管されているとおりのルーターの ARP 構成の内容を表示するのに使用します。また、list コマンドは、最新表示および使用法のタイマーについて現行の設定値も表示します。

構文 :

list entry
all
arp-servers
atm-arp-client-configuration
pvc-atm-arp-entry
svc-atm-arp-entry
redundancy
mars-servers

all ARP 構成に続いてすべての ARP 項目をリストします。

例: list all

```
ARP config> list all
ARP configuration:

Refresh timeout: 5 minutes
Auto refresh: disabled

Mac address translation configuration

No arp entries defined

ATM Arp Server List:
  IP Address      Number       Address / Sub Address
 1.1.1.1     [ 1]       39.84.0F.00.00.00.00.00.00.00.00.00.02.
                                    11.11.11.11.11.11.11.11
 1.1.1.1     [ 2]       39.84.0F.00.00.00.00.00.00.00.00.00.03.
                                    AA.AA.AA.AA.AA.AA.AA.AA
```

arp-servers

arp-servers をリストします。これがクライアント専用の構成である場合、この出力は、構成済みの ARP サーバーをリストします。これが分散 ARP サーバー構成の場合には、構成済みの直接接続サーバーがリストされます。分散 ARP サーバー間の通信の説明については、604ページの『分散 ARP サーバーの概要』を参照してください。

```
ARP config> list arp-servers

ATM Arp Remote Server List:
   IP Address      Number       Address / Sub Address
        1.1.1.1     [ 1]       39.84.0F.00.00.00.00.00.00.00.00.00.02.
                                          11.11.11.11.11.11.11.11
        1.1.1.1     [ 2]       39.84.0F.00.00.00.00.00.00.00.00.00.03.
                                          AA.AA.AA.AA.AA.AA.AA.AA
```

atm-arp-client-configuration

atm-arp-client-configuration をリストします。

```
ARP config> list atm

ATM Arp Clients:

-------------------------------------------------

If: 0  Prot: 0  Addr: 1.1.1.2          ESI: 11.11.11.11.11.11  Sel: 11
Server: yes  Refresh T/O: 20   AutoRefr: yes   By InArp: yes  Validate PCR: no
Use Best Effort: yes/yes  (Control/Data)   Max B/W(kbps):      0
Cell Rate(kbps):  Peak:      0/     0      Sustained:      0/     0
Max SDU(bytes):   9188
Server Synchronization: yes  SGID: 1       Secure DCSs: no
Hello Interval: 3    Dead Factor: 3
Server Synchronization ESI: 11.11.11.11.11.11   Selector: 12
Server Synchronization Max SDU(bytes):   9188
Arp Server Re-registration time in (minutes): 15
Multicast Support: no    Broadcast Support: no
```

フィールド記述については、617ページを参照してください。

redundancy

冗長構成およびゲートウェイ状況をリストします。

```
ARP config>list red


ATMARP Clients with Redundancy Configured
-----------------------------------------

If:  0    Prot: IP    Addr: 1.1.1.2
Red. ESI: bb.bb.bb.bb.bb.bb   Red. SEL: bb   Pri/Secy: Secondary
Partner's (Red.) ATM Address:  39.84.0F.00.00.00.00.00.00.00.00.01.aa.aa.aa.aa.aa.aa.aa
Partner Server ESI: BB.BB.BB.BB.BB.BB Partner Server SEL: AA
Redundancy Default IP Gateway Address: 1.1.1.3
-----------------------------------------
```

```
ARP config>list red


ATMARP Clients with Redundancy Configured
-----------------------------------------

If:  0    Prot: IP    Addr: 2.2.2.2
Red. ESI: aa.aa.aa.aa.aa.aa  Red. SEL: aa   Pri/Secy: Primary
Partner's (Red.) ATM Address:  39.84.0F.00.00.00.00.00.00.00.00.01.bb.bb.bb.bb.bb.bb.bb
Partner Server ESI: BB.BB.BB.BB.BB.BB Partner Server SEL: AA
Redundancy Default IP Gateway Address: 1.1.1.3
-----------------------------------------
```

If: インターフェース番号

Prot: IP

Addr: IP アドレス

Red. ESI:
冗長 ATM アドレスの ESI 部分を識別します。

Burned In - ATM アダプターの全般的に監視される MAC アドレスを冗長 ATM アドレスのエンド・システム識別子 (ESI) 部分として使用する必要があることを指定します。

Locally administrated - 冗長 ATM アドレスの ESI コンポーネントとして使用すべきローカルに監視されるエンド・システム識別子を識別します。

Red. SEL:
冗長 ATM アドレスのセレクター部分を識別します。

Peer Redundancy/Primary/Secondary
クライアント/サーバーの役割を識別します。

基本の場合、クライアント/サーバーは、その冗長 ATM アドレスから 2 次の冗長 ATM アドレスへのコールを行います。

2 次の場合には、このクライアント/サーバーは、冗長 VCC が確立されている限りアイドル状態になります。

ピアの場合、高位の冗長 ATM アドレスをもつサーバーが呼び出しを行います。

Partner's (Red.) ATM Address:
パートナー・クライアント/サーバーについての冗長 ATM アドレスを指定します。

Partner Server ESI:
ARP サーバーが故障した場合にパートナー ARP サーバー ATM アドレスの ESI コンポーネントとして使用されるローカルに監視される ESI を識別します。

Partner Server SEL:
パートナー・ルーターで構成されたパートナー・サーバー ESI およびセレクターのセレクター部分を識別します。

Redundancy Default IP Gateway Address:
省略時 IP ゲートウェイ・アドレスを指定します。これは、この ARP サーバーによってサービスを受けるクライアント内で構成された省略時ゲートウェイ・アドレスです。このアドレスが定義されると、ARP サーバーは、1 つのサブネットから別のサブネットまでのルーティング機能を提供できます。

pvc-atm-arp-entry

ARP PVC をリストします。

```
ARP config> list pvc
ATM Arp Permanent Virtual Circuit Definitions
No. IF# Prot# P/S     Protocol     -> VPI / VCI
1    0    0    P         0.0.0.0   ->  00 / 0029
2    0   23    P                   ->  00 / 0068
```

No. VCC 番号

IF# インターフェース番号

Prot# プロトコル番号 (Prot# 0 = IP、7 = IPX、23=ASRT)

P/S: P は PVC を、S は SVC を表します

Protocol

IP アドレス (protocol が IPX である場合は IPX ホスト番号)

VPI/VCI

定義されたチャネルの 10 進値

svc-atm-arp-entry

ARP SVC をリストします。

```
ARP config> list svc

ATM Arp Switched Virtual Circuit Definitions


No. IF# Prot# P/S     Protocol     -> Destination ATM Address
2    0    0    S         0.0.0.0   ->
                    39.84.0F.00.00.00.00.00.00.00.00.00.02.10.00.5A.00.DE.AD.03
```

No VCC 番号

IF# インターフェース番号

Prot# プロトコル番号 (Prot# 0 = IP、7 = IPX、23=ASRT)

P/S: P は PVC を、S は SVC を表します

Protocol

IP アドレス (protocol が IPX である場合は IPX ホスト番号)

Destination ATM Address

あて先 ATM アドレス

Reorder

reorder コマンドは、ARP サーバーのリストから基本 ARP サーバーを選択するのに使用します。このコマンドは、クライアントにのみ有用です。

構文 :

reorder arp

例: reorder arp

```
    ATM Arp Remote Server List:
       IP Address      Number       Address / Sub Address
            1.1.1.1     [ 1]       39.84.0F.00.00.00.00.00.00.00.00.00.02.
                                                 11.11.11.11.11.11.11.11
            1.1.1.1     [ 2]       39.84.0F.00.00.00.00.00.00.00.00.00.03.
                                                 AA.AA.AA.AA.AA.AA.AA.AA
Number of the IP Address/Arp Server ATM Address pair to be made Primary
Default of 1 will change nothing [1]?
```

Set

Set コマンドは、最新表示タイマー値を (分数で) 設定します。ARP 項目は、更新されない場合に、この数の分数が経過した後で経時タイムアウトします。

構文 :

set refresh-timer

refresh-timer

ARP 項目の経時タイマーに値を指定します。

有効値: 0 〜 65535 の範囲内の整数の分数

省略時値: 5

ARP 構成の例

構成の例では、その構成についての完全な一連のイベントを示します。

非分散 ARP サーバー LIS 内の ARP サーバー冗長構成

パートナーの構成

以下の例は、ARP サーバー冗長についての ARP サーバーの構成を示します。

注:

1. 物理 ATM 装置を追加します
2. ローカルで監視される ESI を追加します
3. サーバーに使用される IP アドレスを追加します
4. ARP 構成を開始します
5. ATM ARP クライアントを定義します
6. ARP サーバーを定義します
7. ローカルで監視される ESI を使用します
8. IP アドレス 1.1.1.1 の冗長構成を開始します

```
Config (only)>add device atm        1
Device Slot #(0-3) [0]?
Adding CHARM ATM Adapter device in slot 0  port 1 as interface #0
Use "net 0" to configure CHARM ATM Adapter parameters
Config (only)>net
Network number [0]?
ATM user configuration
ATM Config>int
ATM interface configuration
ATM Interface Config>add esi   2
ESI in 00.00.00.00.00.00 form []? 11.11.11.11.11.11
ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? aa.aa.aa.aa.aa.aa
ATM Interface Config>exit
ATM Config>exit
Config (only)>p ip
Internet protocol user configuration
IP config>add addr    3
Which net is this address for [0]?
New address [0.0.0.0]? 1.1.1.1
Address mask [255.0.0.0]?
IP config>exit
```

ATM を介した ARP の構成コマンド (Talk 6)

```
Config (only)>p arp   4 .
ARP user configuration
ARP config>add atm   5
Interface Number [0]?
Protocol [IP]?
Client IP Address [0.0.0.0]? 1.1.1.1
This client is also a server? [No]: yes   6
Refresh timeout (in minutes) [20]?
Enable auto-refresh? [Yes]:
Refresh by InAtmArp? [Yes]:
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAAA
Select ESI [1]? 2      7
Use internally assigned selector? [Yes]: n
Selector Only, Range 00..FF [00]? 11
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Max SDU size (bytes) [9188]?
Participate in Server Synchronization [N]?
Re-registration time with Arp Server (in minutes) [15]?
ARP config>add red      8
Interface Number [0]?
Protocol [IP]?
Local client IP Address [0.0.0.0]? 1.1.1.1
Note: Local Redundancy ESI must be different from the Primary Server ESI
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) AAAAAAAAAAAA
Select Local Redundancy ESI [1]? 3
Local Redundancy selector, Range 00..FF [00]? aa
Partner's (Redundancy) ATM Address, 40 Hex digits
[0000000000000000000000000000000000000000]?
39.84.0F.00.00.00.00.00.00.00.00.01.bb.bb.bb.bb.bb.bb.bb

Redundancy default IP Gateway also ? [Yes]:
If Yes, Redundancy default IP Gateway protocol address [0.0.0.0]? 1.1.1.3
ARP config>exit
Config (only)>reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
  EXIT, reload requested
```

パートナーの構成

以下の例は、ARP サーバー冗長についてのパートナーの構成を示します。

注:

1 物理 ATM 装置を追加します

2 ローカルで監視される ESI を追加します

3 ARP 構成を開始します

4 これはクライアント定義です

5 2 次の場合は、クライアントとしてのみ定義します (分散 ARP サーバー LIS でない場合)。分散 ARP サーバーの場合は、パートナーを分散 ARP サーバー LIS として定義できます。

6 ローカルで監視される ESI を使用します

7 ARP サーバーを定義します

8 IP アドレス 1.1.1.2 の冗長構成を開始します

9 2 次を定義します。

```
Config (only)>add device atm  1
Device Slot #(0-3) [0]?
Adding CHARM ATM Adapter device in slot 0  port 1 as interface #0
Use "net 0" to configure CHARM ATM Adapter parameters
Config (only)>net
Network number [0]?
ATM user configuration
ATM Config>int
ATM interface configuration
ATM Interface Config>add esi
ESI in 00.00.00.00.00.00 form []? 11.11.11.11.11.11
ATM Interface Config>add esi  2
ESI in 00.00.00.00.00.00 form []? bb.bb.bb.bb.bb.bb
ATM Interface Config>exit
ATM Config>exit
Config (only)>p ip
Internet protocol user configuration
IP config>add addr
Which net is this address for [0]?
New address [0.0.0.0]? 1.1.1.2
Address mask [255.0.0.0]?
IP config>exit

Config (only)>p arp  3
ARP user configuration
ARP config>add atm   4
Interface Number [0]?
Protocol [IP]?
Client IP Address [0.0.0.0]? 1.1.1.2
This client is also a server? [No]: no   5
Refresh timeout (in minutes) [5]?
Enable auto-refresh? [no]:
Refresh by InAtmArp? [no]:
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) BBBBBBBBBBBB
Select ESI [1]? 1  6
Use internally assigned selector? [Yes]: y
Validate PCR for best effort VCCs? [No]:
Maximum Reserved Bandwidth for incoming VCCs (Kbps) [0]?
Use Best Effort Server for Control VCCs? [Yes]:
Peak Cell Rate of outbound control VCCs (Kbps) [0]?
Sustained Cell Rate of outbound control VCCs (Kbps) [0]?
Use Best Effort Server for Data VCCs? [Yes]:
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?
Participate in Server Synchronization  (Y or N) [N]?    N
Max SDU size (bytes) [9188]?
Re-registration time with Arp Server (in minutes) [15]?
ARP config> add arp-server private-nsapa 7
Local Client IP Address [0.0.0.0]? 1.1.1.2
Private NSAP Address: Specify 40 digits
ATM Address []? 39840F000000000000000000000111111111111111
ARP config>add red  8
Interface Number [0]?
Protocol [IP]?
Local client IP Address [0.0.0.0]? 1.1.1.2
Note: Local Redundancy ESI must be different from the Primary Server ESI
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) BBBBBBBBBBBB
Select Local Redundancy ESI [1]? 3
Local Redundancy selector, Range 00..FF [00]? bb
Partner's (Redundancy) ATM Address, 40 Hex digits
[0000000000000000000000000000000000000000]?
39.84.0F.00.00.00.00.00.00.00.00.01.aa.aa.aa.aa.aa.aa.aa    9
  (  1) Use burned in ESI
  (  2) 111111111111
  (  3) BBBBBBBBBBBB
Select Partner Server ESI [1]? 2
Partner selector, Range 00..FF [00]? 11
Redundancy default IP Gateway also ? Yes
If Yes, Redundancy default IP Gateway protocol address [0.0.0.0]? 1.1.1.3
ARP config>exit
Config (only)>reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
  EXIT, reload requested
```

ATM を介した ARP の構成コマンド (Talk 6)

注:

1. 分散 ARP サーバー LIS では、パートナーは両方とも分散 ARP サーバーです。
2. ARP サーバー冗長の構成は、分散 ARP サーバーのプロセスは、非分散 ARP サーバーの場合と同じです。

ARP 監視環境にアクセスする

ARP 監視コマンドにアクセスするには、以下の手順を使用します。このプロセスでは、ARP *監視* プロセスにアクセスできます。

1. OPCON プロンプトで、**talk 5** を入力します。 (このコマンドについて詳しくは、*ソフトウェア 使用者の手引き* の中の “OPCON プロセス” を参照してください)。例えば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、GWCON プロンプト (+) が端末で表示されます。最初に構成を入力したときにプロンプトが表示されない場合は、**Return** を再び押します。
2. + プロンプトで、**protocol arp** コマンドを入力して、ARP> プロンプトを出します。

   例 :

   ```
   + prot arp
   ARP>
   ```

非 ATM ネットワーク用の ARP 監視コマンド

この節では、非 ATM ネットワーク用の ARP 監視コマンドについて説明します ARP 構成コマンドには、ARP> コマンドでアクセスできます。

注: 装置のソフトウェア・ロードに非同期転送モード (ATM) が含まれていない場合、ATM に関連するコマンドは無効であり、ARP 構成と監視プロンプトで表示されません。

表37 はコマンドを示しています。

表 37. 非 ATM ネットワーク用の ARP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Clear	指定したインターフェースのキャッシュをクリアします。
Dump	指定したインターフェースのキャッシュを表示します。
Hardware	ARP で構成された各ネットワークをリストします。
Ping	装置と指定されたエンド・ステーションの間の接続性を検査します。
Protocol	ARP で構成された各プロトコルをリストします。
Statistics	ARP 情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Clear

clear コマンドは、与えられたネットワーク・インターフェースについて ARP キャッシュをフラッシュするのに使用します。 **clear** コマンドを使用すると、正しくないトランザクションを削除させることができます。

特定のインターフェースをクリアするには、コマンドの一部としてインターフェースまたはネットワークの番号を入力してください。インターフェース番号を入手するには、CONFIG **list devices** コマンドを使用します。

構文 :

clear *interface#*

例: clear 1

Dump

dump コマンドは、与えられたネットワーク/プロトコルの組み合わせについて ARP キャッシュを表示するのに使用します。特定のインターフェースの ARP キャッシュを表示するには、コマンドの一部としてインターフェースまたはネットワークの番号を入力してください。インターフェース番号を入手するには、CONFIG **list devices** コマンドを使用します。

そのネットワーク上に複数のプロトコルがある場合は、プロトコル番号も与える必要があります。これにより、監視はそのデータベースに保管されたハードウェア・アドレス対プロトコルのマップを表示します。指定されたインターフェース上で ARP が 1 つだけのプロトコルを使用している場合には、プロトコル番号の指定は任意です。プロトコル番号を入手するには、CONFIG **protocol** コマンドを使用してください。

dump コマンド画面では、各マッピングごとにハードウェア・アドレス、プロトコル・アドレス、および最新表示タイマー・パラメーターが表示されます。

構文 :

dump *interface# protocol#*

例: dump 2 ip

```
Hardware Address    IP Address      Refresh
02-07-01-00-00-01   192.9.1.2       Permanent
a1-b2-c3-4d-5e-6f   128.185.214.36  5
100                 128.185.123.51  Not Aging
16                  128.185.214.38  Not Aging
```

指定できるタイマー・パラメーターには、次のものがあります。

Permanent
ハードウェア・アドレスとプロトコル・アドレス間の静的に構成されたマッピング (ARP **add entry** コマンド、フレーム・リレー **add protocol** コマンド、または X25 **add address** コマンドを使用して入力されます)。これらの項目は経過時間切れになることがなく、動的に学習されたマッピングによって上書きされることはありません。

minutes to expire
このマッピングが経過時間切れにより満了するまで、またはこのマッピングが最新表示されるまで (自動最新表示が使用可能にされている場合) の分数。このパラメーターは数値として表されます。

Not Aging
逆 ARP を通じて学習された固定した SVC または PVC のマッピング。これが経過時間切れを始めるのは、サーキットがダウンした時だけです。マッピングは新しく学習されたアドレスによって上書きすることができ、 ARP **clear** 監視コマンドによってクリアすることができます。

Hardware

hardware コマンドは、ARP で登録済みのネットワークを表示するのに使用します。**hardware** コマンドでは、ARP で登録済みのネットワークがそれぞれリストされ、各ネットワークのハードウェア・アドレス空間 (ハードウェア AS) およびローカル・アドレスが表示されます。

構文 :

hardware

例: hardware

```
   Network       Hardware AS    Hardware Address

   1 FR/0          000F           1023
   5 TKR/0         0006           00:00:C9:09:32:EF
   8 Eth/0         0001           AA-00-04-00-26-14
   9 IPPN/0        2048           128.185.214.38
  10 BDG/0         0001           00-00-93-90-4C-F7
```

注: IPPN 項目は、ハードウェア・アドレス・フィールドが IP トンネルの IP アドレスを示す IP トンネル伝送を指しています。

Ping

ping コマンドは、与えられたあて先にルーターが ICMP エコー要求を送信するようにさせるのに使用します。**ping** コマンドの詳細については、325ページの『Ping』を参照してください。

Protocol

protocol コマンドは、ARP に登録したアドレスをもつプロトコルを (ネットワーク別に) 表示するのに使用します。 このコマンドは、ネットワーク・プロトコル名、プロトコル番号、プロトコル・アドレス空間 (16 進数)、およびローカル・プロトコル・アドレスを表示します。

構文 :

protocol

例: protocol

```
Network  Protocol (num)  AS    Protocol Address(es)
5 TKR/0  IP       (00)   800    128.185.209.38
6 TKR/1  IP       (00)   800    10.1.181.38
8 Eth/0  IP       (00)   800    128.185.221.38
8 Eth/0  AP2      (22)   80F3   221/38
```

注: SR 項目とは、ソース・ルーティングを指しています - MAC アドレスを示すためにプロトコル・アドレスが使用されます。実 RIF 項目を表示するには、トークンリングの **dump** コマンドを使用してください。

Statistics

statistics コマンドは、ARP モジュールの操作に関するさまざまな統計を表示するのに使用します。

構文 :

statistics

例: statistics

```
ARP input packet overflows
Net   Count
 PPP/0  0
 PPP/1  0
 TKR/0  0
IPPN/0  0
 BDG/0  0

ARP cache meters
Net Prot  Max Cur Cnt    Alloc  Refresh: Tot  Failure  TMOs: Refresh
0   0     1   1   1       17             0        0               13
0  22     1   0   0        6             0        0                6
1   0     1   1   2       27             0        0               25
1  16     3   3   7      291             0        0                0
2   0     1   0   0        2             0        0                2
2  16     1   0   0        1             0        0                0
8   0     1   1   1       11             0        0               10
```

ARP input packet overflows	ARP レイヤーが使用中であったために入力時に廃棄された ARP パケットの数を表すカウンターを表示します。示されるカウントはネットワーク・インターフェース別です。
ARP cache meters	ARP キャッシュの操作に関するさまざまなメーターから構成されます。示されるカウントは、すべてプロトコル別、インターフェース別です。
Net	インターフェース番号を表示します。
Prot	プロトコル番号を表示します。
Max	全時間を通じて最大長のハッシュ・チェーンを表示します。
Cur	現行の最大長のハッシュ・チェーンを表示します。
Cnt	現在アクティブな項目のカウントを表示します。
Alloc	作成された項目のカウントを表示します。
Rfrsh:Tot	このネットワークのインターフェースおよびプロトコルに送信された最新表示要求の数を表示します。
Fail	内部資源が使用できないために自動最新表示の試行が失敗した回数を表示します。このカウントは、項目が更新されたかどうかとは無関係です。
TMOs:Rfrsh	最新表示タイマーのタイムアウトにより削除された項目のカウントを表示します。

ATM を介した ARP 監視コマンド

この節では、ATM を介した ARP (CIP) 構成コマンドについて説明します。ここでは、次のものについての監視コマンドについて説明します。

- ATM を介したクラシカル IP & ARP
- ATM を介した IPX
- 1483 ブリッジング

ATM を介した IPX についての監視コマンドは、本質的にはクラシカル IP および ARP 用の監視コマンドと同じです。主な違いは、プロトコル・アドレスの形式です。

- IP 用のプロトコル・アドレスはドット 10 進表記の 4 バイトのフィールドとして指定されます。
- IPX 用のプロトコル・アドレスは 16 進文字の 6 バイトのフィールドとして指定されます。

注: ATM を介した IPX 用の **ping** コマンドは、クラシカル IP および ARP 用に使用されるものとは異なっています。IPX バージョンの **ping** コマンドは IPX 監視で使用できます。ARP 構成コマンドには、ARP> コマンドでアクセスできます。表38 はコマンドを示しています。

さらに詳しい情報は、595ページの『ATM を介したクラシカル IP および ARP (RFC 1577)』および 608ページの『ATM を介した IPX および ARP の概要 (RFC 1483)』を参照してください。ATM を介した ARP の追加情報、ならびに論理および物理ネットワーク構成を示す図については、*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* を参照してください。

ブリッジングでは ARP を使用しないため、監視は、ブリッジ・ポートと関連付けられたチャネルの状況を検査するためだけに使用されます。また、ブリッジングではプロトコル・アドレスも使用しないため、対応する (ローカル) ポートのポート番号だけがチャネルと共に表示されます。

表 38. ATM を介した ARP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Delete	活動チャネルを即時にダウンさせます。状態によっては、新規チャネルを古いチャネルに取って代わるように立ち上げることができる場合とできない場合があります。
Display	単一の ATM インターフェースに関連付けられたすべてのチャネル (VCC) を表示します。
Dump	データグラムを送信するためにどの ATM チャネルが使用されているかを示し、それらの対応する IP アドレスを示します。
Hardware	ARP で構成された各ネットワークをリストします。
Ping	装置と指定されたエンド・ステーションの間の接続性を検査します。
Protocol	ARP で構成された各プロトコルをリストします。
Redundancy-State	Redundancy で構成された IP クライアントを表示します

表 38. ATM を介した ARP 監視コマンドの要約 (続き)

コマンド	機能
Statistics	すべてのネットワーク・インターフェースを通じての ARP コード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。 xxxivページの『下位レベル環境の終了』 を参照してください。

Delete

活動チャネルを即時にダウンさせるには、**delete** コマンドを使用してください。状態によっては、新規チャネルを古いチャネルに取って代わるように立ち上げることができる場合とできない場合があります。

活動チャネル・リストから特定のチャネルを削除してください。このオプションを呼び出すときは細心の注意を払う必要があります。VPI/VCI によって指定されたチャネルは、それが活動チャネル・リストで見つかる場合には、削除されます。削除する前に、チャネルは通常の停止原因コードを使って解放されます。この特定のチャネルに依存するすべての ARP 項目も削除されます。

構文 :

delete

例: delete

```
ARP> del 0
VPI, Range 00..FF [00]?
VCI, Range 0000..FFFF [0000]? 0020
Channel found and deleted
```

Display

display コマンドは、単一の ATM インターフェースに関連付けられたすべてのチャネル (VCC) を表示するのに使用します。

構文 :

display

例: display

```
ARP> display 0
Active Channel List : Net 0
   P/S FLAGS LIST  VPI/VCI    FwdPcr    FwdScr     MaxSDUsz Control P2P
  0) S   80    01   00/0020  155000000 155000000      9188      T     T
         Tgt Addr. 39.84.0F.00.00.00.00.00.00.00.00.02.10.00.5A.00.DE.AD.02
         Client Address (owner): 1.1.1.100
         Target Protocol Addresses: 1.1.1.2
New Channel List : Net 0
PVC Channel List : Net 0
   P/S FLAGS LIST  VPI/VCI    FwdPcr    FwdScr     MaxSDUsz Control P2P
  1) P   80    03   00/0085  155000000 155000000      9188      F     T
         Tgt Addr:
         Client Address (owner): 3.5.5.5
         Target Protocol Addresses: 3.4.4.4
```

P/S P はこのチャネルが PVC であることを意味します。S はこのチャネルが SVC であることを意味します。

List 内部で使用するためのもの

Flags 内部で使用するためのもの

ATM を介した ARP 監視コマンド (Talk 5)

VPI/VCI
使用中のチャネルのバーチャル・パス識別子およびバーチャル・チャネル識別子

FwdPcr
ビット/秒で示したピーク・セル速度

FwdScr
ビット/秒で示した保持セル速度

MaxSDUsz
このチャネル用の最大 SDU サイズ。このインターフェースで送信または受信されるすべてのパケットは、このサイズから、RFC 1483 で使用される 8 バイトのヘッダー接頭部を差し引いたもの以下である必要があります。

Control
これが制御チャネル (ARP サーバーへのチャネル) である場合は T。これがデータ・チャネル (別のクライアントへのチャネル) である場合は F

P2P このチャネルがポイントツーポイントである場合は T。このチャネルがポイントとマルチポイント間である場合は F

Active Channel List
これらのチャネルはリモート・ユーザーとの真の接続です。データは、示されたトラフィック・パラメーターを使ってこれらの接続を介して流れることができます。

New Channel List
これらのチャネルは、他の端に接続されるプロセスにあります。チャネルが活動リストに移動されるまで、データはチャネルを介して流れることはできません。

PVC Channel List
これらは、PVC として固有に構成されたチャネルです。 これらは、データ・チャネル構成で定義されたようにデータ・チャネル用のクライアント特性をもっています。

Client Address
この VCC に接続されたローカル・クライアントのプロトコル・アドレスです。

Target Protocol Address
この VCC に接続されたリモート・クライアントのプロトコル・アドレスです。

Dump

dump コマンドは、データグラムの送信に使用されている ATM チャネルを示したり、それらの対応する IP アドレスを示すのに使用します。

このテーブルは、クラシカル IP を稼働する物理 ATM ネットワークの全体の ARP テーブルを示しています。ハードウェア・アドレスは、活動チャネルについての結果として得られる VCC 識別子 (VPI/VCI) です。つまり、 IP アドレスに送信されたすべてのトラフィックは、関連付けられたチャネル (ハードウェア・アドレスのもとでリストされています) から伝送されます。

注: チャネルの他の端のホストがそれ自体のアドレスを付けて要求または応答のいずれかを送信する場合、最新表示時間はその最大値に自動的にリセットされます。

構文 :

dump

例: dump

```
 ARP>du 0
Hardware Address  IP Address          Refresh      Origin Srvrid   Seq number
  0/0               1.1.1.1           19               1.1.1.1      868997267
  0/0               1.1.1.2           permanent        1.1.1.2      868997028
  0/0               1.1.1.3           permanent        1.1.1.2      868997028
  0/35              1.1.1.5           20               1.1.1.2      868997042
```

最新表示のもとでは、指定された時間は ARP 項目が経過時間切れになるおおよその時間 (分単位) です。自動最新表示がオンにされる場合には、 ARP 要求または InATMARP 要求が、時間切れになる 30 秒前に送信されます。応答が時間切れになる前に受信される場合、最新表示時間がリセットされ、 ARP 項目が残ります。応答が受信されないか、自動最新表示がオフにされる場合、 ARP 項目は時間切れになると削除されます。この項目は必要に応じて再作成されます。

以下は、有効な最新表示状態です。

Hardware Address
ARP に登録されたハードウェア・アドレスを指定します。Hardware Address の下に 『0/0』 が示された場合、この ARP 項目についてオープンなチャネルはありません。

Refresh States

- Refresh の下に 『resolve only』 と示されている場合には、この ARP 項目は、与えられた IP アドレスの ATM アドレスを解決する目的のためだけに存在しています。これらの項目は、ARP サーバーへの登録 (2225 登録) で使用されます。
- Refresh の下に 『not aging』 が示された場合、項目は無期限に残ります。

Origin Server Id
このキャッシュ項目を発信したサーバーの DCS ID (IBM プロダクトの IP アドレス)。クライアントが複数のサーバーに登録している場合は、そのクライアントの IP アドレスに複数のキャッシュ項目ができることが考えられます。クライアントが登録する各サーバーごとに項目は 1 つありますが、それぞれ、異なる起点 ID をもちます。

Seq. Number
対応する SCSP キャッシュ項目の現在の順序番号 (10 進数)。この番号は、この特定のキャッシュ項目のサーバー・グループにあるすべてのサーバーについて一致する必要があります。

Hardware

hardware コマンドは、構成済みの各 IP クライアントに関連付けられたすべての ATM アドレスをリストするのに使用します。

ATM を介した ARP 監視コマンド (Talk 5)

構文 :

hardware

例: hardware

```
ARP> hardware
    Network         Hardware AS     Hardware Address
    0 ATM/0         0013            39.84.0F.00.00.00.00.00.00.00.00.00.01.
                                    10.00.5A.00.DE.AD.C8  (IP 1.1.1.100)
    1 IPPN/0        0800            1.1.1.100
```

Network:

物理ネットワーク番号

Hardware AS:

このネットワークを分類するために ARP パケットで使用されるハードウェア・タイプ。 ATM を介した ARP では、AS タイプは 0x13 (10進数の 19) です。

Hardware Address:

ハードウェア・アドレス。一般には、このアドレスは他のネットワークでは MAC アドレスですが、ATM では、このアドレスは特定のクライアントに関連付けられた ATM アドレスです。例では、IP クライアント 1.1.1.100 は、対応する ATM アドレス 39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.C8 をコールすることによりアクセスされます。

Ping

ping コマンドは、装置と指定されたエンド・ステーション間の接続性を検査するのに使用します。

Ping は、他のネットワークを介して働くのと同様に働きます。これは、毎秒 1 つの ICMP エコー要求を送信し、対応する応答の統計を表示します。要求の中の発信元アドレスには、あて先のサブネットに最も近く一致するクライアントのアドレスが含まれていることに注意してください。

構文 :

ping

例: ping

```
ARP> ping 1.1.1.2
PING 1.1.1.100 -> 1.1.1.2: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 1.1.1.2: icmp_seq=0. ttl=64. time=19. ms
56 data bytes from 1.1.1.2: icmp_seq=1. ttl=64. time=11. ms

----1.1.1.2 PING Statistics----
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 11/15/19 ms
```

Protocol

protocol コマンドは、各ネットワーク・インターフェースですべてのクライアント・アドレスをリストするのに使用します。これは、他のインターフェースの場合とま

ったく同様です。ATM インターフェースの場合、プロトコル・アドレスのリストは、このインターフェースで構成されるすべての CIP クライアントです。

構文 :

protocol

例: protocol

```
ARP> protocol
Network  Protocol (num)  AS     Protocol Address(es)
0 ATM/0  IP       ( 0)   0800   1.1.1.100
```

Redundancy-State

redundancy-state コマンドは、redundancy で登録された IP クライアントを表示するのに使用します。

構文 :

redundancy-state

以下の例は、冗長チャネルが非アクティブの場合に基本 ARP サーバー上の冗長監視セクションを示します。

```
CGW Operator monitoring
+p arp
ARP>red
Network number  [0]?
Protocol [IP]
If: 0 Prot: IP  Clients configured with Redundancy
------------------------------------------------------------
Addr: 1.1.1.1   Place Redundancy Call: Yes  Real Esi: Up  Red. Esi: Up  Red. Chnl: Down
                    FLAGS: Real Client: C8  Red. Client: C8 RedFlags: C0
                    Red. Channel: 0/0
                     Red. Channel: Source ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.AA.AA.AA.AA.AA.AA.AA
                     Red. Channel: Target ATM address
39.84.0F.00.00.00.00.00.00.00.00.00.01.BB.BB.BB.BB.BB.BB.BB
                     Redundancy Status: Active
 Redundancy default IP Gateway protocol address: 1.1.1.3
```

以下の例は、冗長チャネルがアクティブの場合に基本サーバー上の冗長監視セクションを示します。

```
CGW Operator monitoring
+p arp
 ARP>red
 Network number  [0]?
 Protocol [IP]?
 If: 0 Prot: IP  Clients configured with Redundancy
 ------------------------------------------------------------
 Addr: 1.1.1.1   Place Redundancy Call: Yes  Real Esi: Up  Red. Esi: Up  Red. Chnl: Up
                     FLAGS: Real Client: C8  Red. Client: C8 RedFlags: D0
                     Red. Channel: (VPI/VCI)  0/32
                     Red. Channel: Source ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.AA.AA.AA.AA.AA.AA.AA
                     Red. Channel: Target ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.BB.BB.BB.BB.BB.BB.BB
                     Redundancy Status: Active
 Redundancy default IP Gateway protocol address: 1.1.1.3
 ------------------------------------------------------------
```

以下の例は、冗長チャネルが非アクティブで、しかもパートナーがバックアップ ARP サーバーとして行動している場合にパートナー上の冗長監視セクションを示します。

ATM を介した ARP 監視コマンド (Talk 5)

```
ARP>red
 Network number  [0]?
 Protocol [IP]?
 If: 0 Prot: IP  Clients configured with Redundancy
 ---------------------------------------------------------
 Addr: 1.1.1.2   Place Redundancy Call: No  Real Esi: Up  Red. Esi: Up  Red. Chnl: Down
                     FLAGS: Real Client: C8  Red. Client: C8 RedFlags: 80
                     Red. Channel: 0/0
                    Red. Channel: Source ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.BB.BB.BB.BB.BB.BB.BB
                     Red. Channel: Target ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.AA.AA.AA.AA.AA.AA.AA
                     Redundancy Status: Active
 Partner Server ESI: 11.11.11.11.11.11, Partner Server SEL: 11, In backup Server mode
 Redundancy default IP Gateway Protocol address: 1.1.1.3
 -------------------------------------------
```

以下の例は、冗長チャネルがアクティブで、しかも 2 次がクライアントとして活動し、バックアップ ARP サーバー・モードでない (基本 ARP サーバーはアクティブであるため) 場合に 2 次上の冗長監視セクションを示します。

```
ARP>red
Network number  [0]?
 Protocol [IP]?
 If: 0 Prot: IP  Clients configured with Redundancy
 ---------------------------------------------------------
Addr: 1.1.1.2   Place Redundancy Call: No  Real Esi: Down  Red. Esi: Up  Red. Chnl: Up
                     FLAGS: Real Client: C0  Red. Client: C8 RedFlags: 90
                     Red. Channel: (VPI/VCI)  0/32
                     Red. Channel: Source ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.BB.BB.BB.BB.BB.BB.BB
                    Red. Channel: Target ATM address
 39.84.0F.00.00.00.00.00.00.00.00.00.01.AA.AA.AA.AA.AA.AA.AA
                     Redundancy Status: Inactive, not trying ...
 Partner Server ESI: 11.11.11.11.11.11, Partner Server SEL: 11, Acting as a Client
 Redundancy default IP Gateway Protocol address: 1.1.1.3
 -------------------------------------------
 ARP>exit
```

以下のフィールドは、冗長監視から表示されます。

If: インターフェース番号を指定します。

Prot: プロトコルを指定します。

Addr: クライアントの IP アドレスを指定します。

Place Redundancy Call
クライアントが冗長コールを開始するかどうかを指示します。608参照してください。

Real ESI:
実際の ESI の状態を指示します。状態が起動中の場合、クライアントの ATM アドレスは、スイッチに正常に登録されます。状態がダウンの場合は、クライアントがその ATM アドレスをスイッチに登録しようとしても失敗します。

Red. ESI:
冗長 ESI の状態を指示します。状態が起動中の場合、冗長チャネル ATM アドレスは、スイッチに正常に登録されます。状態がダウンの場合は、冗長チャネル ATM アドレスは、スイッチに正常に登録されていません。

Red. Chnl:
冗長チャネルの状態を指示します。状態が起動中の場合、冗長チャネルは、基本と 2 次との間でセットアップされます。状態がダウンの場合は、冗長チャネルは、基本と 2 次との間でセットアップされません。

Red Channel
冗長チャネルの VPI/VCI を指示します。

Red. Channel Source ATM address:
発信元冗長チャネルの ATM アドレスを識別します。

Red. Channel Target ATM address:
ターゲット冗長チャネルの ATM アドレスを識別します。

Redundancy Status:
redundancy (冗長性) の状態を識別します。

Active ARP サービスを提供します。

Inactive
ARP サービスを提供しません。

Partner Server ESI:
パートナー ARP サーバーが故障した場合にパートナー ARP サーバー ATM アドレスの ESI コンポーネントとして使用されるローカルに監視される ESI を識別します。

Partner Server SEL:
パートナー装置上で構成された ESI およびセレクターのセレクター部分を識別します。このフィールドは、バックアップまたはピア ARP サーバーについてのみ表示されます。

Redundancy Default IP Gateway Address:
省略時 IP ゲートウェイ・アドレスを指定します。これは、この ARP サーバーによってサービスを受けるクライアント内で構成された省略時ゲートウェイ・アドレスです。このアドレスが定義されると、ARP サーバーは、1 つのサブネットから別のサブネットまでのルーティング機能を提供できます。

Statistics

statistics コマンドは、すべてのネットワーク・インターフェースを介しての ARP コードの統計を表示するのに使用します。これらの統計は、641ページの『Statistics』で説明されているように、他のどのインターフェースを介しての ARP コマンドの統計とも同じです。

構文 :

statistics

例: statistics

```
ARP> statistics

    ARP input packet overflows
        Net   Count
       ATM/0  0
      IPPN/0  0
       BDG/0  0

    ARP cache meters
    Net Prot  Max Cur Cnt    Alloc  Refresh: Tot  Failure  TMOs: Refresh
      0   0     1   1   1        1             0        0              0
```

ATM を介した ARP 監視コマンド (Talk 5)

第29章 サーバー・キャッシュ同期プロトコル (SCSP) の監視

サーバー同期の状態を監視するには、SCSP 監視機能を使用します。

SCSP 監視環境へのアクセス

SCSP 監視コマンドにアクセスするには、以下の手順を使用してください。このプロセスでは、SCSP *監視* プロセスにアクセスできます。

1. OPCON プロンプトで、**talk 5** を入力します (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』を参照してください)。例えば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、GWCON プロンプト (+) が端末で表示されます。最初に構成を入力したときにプロンプトが表示されない場合は、**Return** を再び押します。

2. + プロンプトで、**protocol scsp** コマンドを入力して、SCSP プロンプトを出します。

   例 :

   ```
   + prot scsp
   SCSP>
   ```

SCSP 監視コマンド

この節では、SCSP 監視コマンドについて説明します。SCSP 構成コマンドには、SCSP> コマンドでアクセスできます。 表39 はコマンドを示しています。

表 39. SCSP 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
List	SCSP 監視情報をリストします。
Statistics	直接接続サーバーについて SCSP 統計を表示します。
Dump	サーバー・グループについて SCSP キャッシュのダンプをとります。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

List

List コマンドは、サーバー同期の状態に関する情報を表示するのに使用します。特定のコマンドの後に ? を入力して、そのオプションをリストすることもできます。

構文 :

list dcs . . .

server-groups . . .

dcs *interface sgid*

サーバー・グループ内のすべての DCS をリストします。

interface

DCS が定義されるインターフェース番号を指定します。

sgid この DCS のサーバー・グループ識別子を指定します。

例 :

```
SCSP>li dcs
Network number [0]?
Server Group ID [0]?
      DCS Id      HFSM State  CAFSM State  M/S  CRL Len  ReTran Len
 03.04.02.00   Bidirectional      Aligned   S         0           0
```

DCS Id

DCS (VCC のもう一方の終端にある) の 16 進識別子

HFSM State

この DCS セッションについてのハロー有限状態機械の状態。考えられる状態は、次のものです。

Down_Inop

DCS までのチャネルがダウンしています。

Down DCS までのチャネルはダウンしていますが、オープンが進行中です。

Waiting

ローカル・サーバー (LS) は DCS にすでにハロー・メッセージを送信しており、応答を待機中です。

Unidirectional

LS はすでに DCS からハロー・メッセージを受信していますが、このローカル・サーバーをまだ認識していません。

Bidirectional

LS および直接接続サーバーは、互いに認識します。これは、正常な状態です。

CAFSM State

この DCS セッションについてのキャッシュ調整有限状態機械の状態。考えられる状態は、次のものです。

Down キャッシュ調整は、まだ始まっていません。

MS_Neg

LS と DCS は、マスター/スレーブ状況について折衝中です。

Summarize

LS と DCS は、キャッシュ要約情報を交換中です。

Update

LS と DCS は、完全キャッシュ要約情報を交換中です。

Aligned

LS と DCS は、同期化されます。これは、正常な状態です。

M/S この LS のマスター (M) または 2 次 (S) 状況を指示します。これ

は、CAFSM が Summarize (要約)、Update (更新)、または Aligned (調整された) 状態にある場合にのみ有効です。

CRL Len
キャッシュ長要求リスト長。これは、Update (更新) 状態のときに送信されるために残っているキャッシュ更新レコードの数です。

ReTran Len
ReTransmit リスト長。これは、DCS による確認応答を受けるために残っているキャッシュ更新レコードの数です。

server-groups *interface*
すべてのサーバー・グループに関する情報をリストします。

interface
ネットワーク・インターフェース番号

例 :

```
SCSP config> list ser
Network number [0]?
       SGID  Protocol      LSID  DCSs  ATM Addr
          1    ATMARP  04040100     0  39.84.0F.00.00.00.00.00.00.00.00.01.
                                       11.11.11.11.11.11.01
          0    ATMARP  03040100     1  39.84.0F.00.00.00.00.00.00.00.00.01.
                                       11.11.11.11.11.11.01
```

sgid Server Group Identifier (サーバー・グループ識別子)。これは、このサーバー・グループ内のサーバーの構成済み識別子です (LIS)。

Protocol
交換されるデータベースのタイプ

lsid ローカル・サーバー識別子の 16 進値。これは、サーバー・グループ内でこのサーバーを識別します。ATMARP の場合、これは、クライアントの IP アドレスです。

DCS このローカル・サーバーと関連付けられた直接接続サーバーの数

ATM address
このローカル・サーバーの ATM アドレス。DCS は、このアドレスを使用して、このローカル・サーバーとの接続をセットアップする必要があります。

Statistics

このコマンドは、直接接続サーバーの統計を表示するのに使用します。

Statistics コマンドは、サーバー同期の状態に関する情報を表示するのに使用します。特定のコマンドの後に ? を入力して、そのオプションをリストすることもできます。

構文 :

statistics *interface server-group dcs-id*

interface
DCS が定義されるインターフェース番号を指定します。

有効値: 任意の定義済みインターフェース

省略時値: 0

server-group

この DCS のサーバー・グループを指定します。

有効値: 0 ～ 65535

省略時値: 0

dcs-id DCS (VCC のもう一方の終端にある) の 16 進識別子を指定します。

有効値:

省略時値: 0

例 :

```
SCSP>stat 0 0
DCS ID (hex) [0]?
DCS with that ID not found, listing all DCS's.
-------------------------------------------
DCS ID: 03.04.02.00
HFSM State: Bidirectional   DCS Hello Interval(sec): 3   DCS Dead Factor: 3
CAFSM State: Aligned  Master/Slave: S   CA seq: 33D35204   CSUS seq: 33D351F1
Cache Summary List sent?: yes   Cache Summary List ACKed?: yes
Cache Request List Size: 0   Cache ReTransmit List Size: 0   Age(sec): 302
ATM Addr: 39.84.0F.00.00.00.00.00.00.00.00.00.04.12.12.12.12.12.12.01
VPI: 0  VCI: 32  Missed Hello Msgs: 0   RID doesn't match LSID: 0
Short Messages: 0   Sequence Mismatches: 0
```

DCS Id

652 ページを参照してください。

HFSM State

652 ページを参照してください。

CAFSM State

652 ページを参照してください。

Hello Interval

DCS がハロー・メッセージを送信する、秒単位の間隔

DCS Dead Factor

この DCS がダウンしたと見なされた後でハロー・メッセージを受信せずに引き渡さなければならないハロー間隔の数

Master/Slave

652 ページを参照してください。

CA Seq

現在のキャッシュ調整メッセージの順序番号

CSUS Seq

現在のキャッシュ状態更新送信請求メッセージの順序番号

Cache Summary List Sent?

キャッシュ要約リストが (キャッシュ調整状態中に) DCS に完全に伝送済みである場合には Yes

Cache Summary List Acked?

キャッシュ要約リストが (キャッシュ調整状態中に) 確認応答済みである場合には Yes

Cache Request List size
652 ページを参照してください。

Cache ReTransmit List size
652 ページを参照してください。

Age この DCS が初期化されてからの秒数

VPI, VCI
DCS に対する VCC のバーチャル・パス識別子とバーチャル・チャネル識別子

Missed Hello Msgs
双方向状態のときに脱落したハロー・メッセージの数

RID doesn't match LSID
メッセージ内の受信 ID が LS の LSID に一致しない場合に受信されたメッセージの数

Short Messages
形式の正しくない (短過ぎる) SCSP メッセージの数

Sequence Mismatches
順序番号プロトコル違反の数

Dump

Dump コマンドは、サーバー・グループについて SCSP キャッシュのダンプをとるのに使用します。

構文 :

dump *interface server-group*

interface
DCS が定義されるインターフェース番号を指定します。

有効値: 任意の定義済みインターフェース

省略時値: 0

server-group
この DCS のサーバー・グループを指定します。

有効値: 0 〜 65535

省略時値: 0

例 :

```
SCSP> dump 0 0
Next key to assign = 33D351F1
Key          Origin ID             Seq. No.   Age   Paddr
03.04.02.00  03.04.02.00           869487085    0   03.04.02.00
03.04.01.00  03.04.01.00           869487090    0   03.04.01.00
SCSP>
```

Key このキャッシュ記入項目の 16 進キャッシュ・キー値。ATM ARP の場合、これは、サーバーの IP アドレス (16 進数) に相当します。

Origin ID
このキャッシュ記入項目の発信元であるサーバーの 16 進 DCS ID。ATM ARP の場合、これは、サーバーの IP アドレスに相当します。

Age この記入項目が一致するサーバー・キャッシュ記入項目なしで存在している分数。20 分経過すると、この記入項目は、経年処理されます。

Paddr このキャッシュ記入項目の対応するプロトコル・アドレス。これがブランクの場合、対応するサーバー・キャッシュ記入項目 (例えば、ATM ARP キャッシュ記入項目) はありません。

第30章 IPX の使用

この章では、2210 で IPX プロトコルを使用する方法を説明します。この章には次の節が含まれています。

IPX の概要

IBM による IPX の実施によって、ルーターは Novell NetWare インターネットワーク・ルーターとして機能することができます。これには次の 3 つの特性があります。

- 以前の Novell NetWare バージョン環境すべてとの互換性
- NetWare ファイル・サーバー内のブリッジング機能に独立型 NetWare ブリッジを加えたものとの互換性
- Novell NetBIOS エミュレーターのサポート

IPX アドレス指定

以下の各項で IPX アドレス指定について説明します。

ネットワーク番号

IPX ネットワーク番号では、インターネットワーク内の特定のネットワークの場所を指定します。郵便で使用している市区町村丁目番地のような、複数の部分からなるアドレスが使用できます。例えば、IPX ではネットワーク番号 (市区町村)、ホスト番号 (丁目)、およびソケット番号 (番地) を参照します。 これらのアドレスによって、異なるネットワーク上の 2 つのエンティティー間の通信が可能になります。

ホスト番号

各 IPX サーキットには、それぞれ 6 バイトのホスト (ノード) 番号が必要です。

トークンリングイーサネットのサーキットでは、そのハードウェア MAC アドレスをホスト番号として使用し、これは変更できません。

シリアル回線にはハードウェア MAC アドレスがないので、固有のホスト番号を指定する必要があります。 IPXWAN では、構成済みノード ID の後に x'0000' を続けて使用します。

ATM サーキットでは、そのエンド・システム識別子 (ESI) をホスト番号として使用します。 ESI が構成されていない場合は、組み込み ESI が使用されます。

IPX サーキット

IPX ルーティング・ソフトウェアでは、単一の IPX 同報通信サーキットと、1 つまたは複数の IPXWAN ポイント・ポイント・サーキットと、その両方のタイプのサーキットの組み合わせのどれかとして、ネットワーク・インターフェースをモデル化しています。サーキット上で使用されるカプセル化のタイプ、IPX アドレス指定、ルーティング・プロトコルは、下位 DLC と、IPX サーキットが同報通信と IPXWAN ポイント・ポイントのどちらとして構成されているかに応じて決まります。

IPX 同報通信サーキットには、次のような特性があります。

- LAN インターフェース上で使用される。
- IPXWAN が構成されていなければ、WAN インターフェース上で使用される。
- 各インターフェースごとに単一 IPX 同報通信サーキット 1 つに制限される。
- ゼロ以外の IPX ネットワーク番号が割り当てられる必要がある。
- LAN では、ネットワーク・インターフェースの MAC アドレスをサーキットの IPX ノード番号として使用する。
- WAN では、構成済み IPX ホスト番号をサーキットの IPX ノード番号として使用する。
- RIP/SAP と静的ルートおよびサービスのコンカレント使用ができる。

IPXWAN ポイント・ポイント・サーキットには、次のような特性があります。

- WAN インターフェース上だけに限って使用できる。
- 各インターフェースごとに単一 IPXWAN ポイント・ポイント・サーキット 1 つに制限されなくてもよい場合がある。
- IPXWAN を使用してパラメーターを交渉する。
- IPX ネットワークを必要としない場合がある。
- IPXWAN ノード ID の後に 0000 を続けたものを、サーキットの IPX ノード番号として使用する。
- 単一の交渉されたルーティング・タイプに制限される。

以下の各項では、サポートされているネットワーク・インターフェースのタイプごとに、それぞれのモデル化について説明します。

LAN (トークンリング、イーサネット、ATM LAN エミュレーション)

IPX ルーティング・ソフトウェアでは、単一の IPX 同報通信サーキットとして LAN インターフェースをモデル化しています。

サーキットには、固有の非ゼロ IPX ネットワーク番号が割り当てられる必要があります。

ネットワーク・インターフェースの MAC アドレスが、サーキットの IPX ノード番号として使用されます。

RIP や SAP の更新など、同報通信パケットの受信と送信には、LAN 全ステーション・アドレス (x'FFFFFFFFFFFF') が使用されます。

該当するタイプの LAN インターフェースでは、通常のカプセル化タイプがサポートされます。

IPX 最大パケット・サイズは、インターフェース用として構成されている MTU を基にして決めます。

トークンリング・インターフェースの場合は、ソース・ルーティングをインターフェース上で使用可能にすれば、IPX 転送元がソース・ルート・ブリッジを通してエンド・ステーション (および、その他のルーター）に到達できるようにすることができます。

次のルーティング・タイプのどれでも、サーキット上ですべて使用できます。

- 静的ルート/サービス
- RIP/SAP (番号制)

ネイティブ ATM

IPX ルーティング・ソフトウェアでは、単一の IPX 同報通信サーキットとして ATM インターフェースをモデル化しています。したがって、ユーザーが ATM ネットワーク上のルーターとの相互接続を定義している ATM PVC と SVC は、 IPX ルーティング・ソフトウェアからは透過的です。

サーキットには、固有の IPX 非ゼロ・ネットワーク番号が割り当てられる必要があります。

ATM アドレスの ESI 構成要素が、サーキットの IPX ノード番号として使用されます。ATM インターフェースに対応する IPX ATM ARP クライアントで ESI が構成されていない場合は、組み込み ESI が使用されます。

LAN 全ステーション・アドレス (x'FFFFFFFFFFFF') が、IPX 同報通信アドレスとして使用されます。同報通信アドレスにアドレス指定されたパケットは、下位 ATM DLC によって、インターフェース上のすべての VC 上に送信されます。

IPX 最大パケット・サイズは、インターフェース用として構成されている MTU を基にして決めます。

下位 ATM DLC では、ATM InARP を使用して、あて先 IPX ノード・アドレスを該当する ATM VC にマップします。オプションですが、 VC が ATM InArp をサポートしないルーターに接続されている場合は、あて先 IPX ノード・アドレスが静的に構成できます。

全メッシュ以外の ATM トポロジーをサポートするために、サーキット上で水平分割を使用不可にできます。こうすれば、RIP と SAP がインターフェース上のすべての VC に情報を伝送して、同じインターフェース上の VC 間の中間ルーティングが行われるようにすることができます。

全メッシュ ATM トポロジーでは、水平分割を使用不可にする必要はありません。

次のルーティング・タイプのどれでも、サーキット上ですべて使用できます。

- 静的ルート/サービス
- RIP/SAP (番号制)

ポイント・ポイント・プロトコル (PPP)

IPX ルーティング・ソフトウェアでは、単一の IPXWAN ポイント・ポイント・サーキットとして PPP インターフェースをモデル化しています。

IPX 最大パケット・サイズは、下位 PPP DLC によって交渉された MTU を基にして決めます。

IPX 同報通信サーキット: 同報通信サーキットとして構成されたときは、サーキットには、固有の非ゼロ・ネットワーク番号が割り当てられる必要があります。

PPP インターフェースに対応する MAC アドレスはないので、構成済みホスト番号がサーキットの IPX ノード番号として使用されます。

次のルーティング・タイプのどれでも、サーキット上ですべて使用できます。

- 静的ルート/サービス
- RIP/SAP (番号制)

IPXWAN ポイント・ポイント・サーキット: IPXWAN ポイント・ポイント・サーキットとして構成されたときは、IPXWAN を使用して、ルーティング・パラメーターを交渉します。

IPXWAN 番号制 RIP ルーティング・タイプでは、固有の非ゼロ・ネットワーク番号がサーキットに割り当てられることが必要です。それ以外の IPXWAN ルーティング・タイプ (非番号制 RIP、静的ルーティング) では、ネットワーク番号は必要ありません (値 0)。

PPP インターフェースに対応する MAC アドレスはないので、IPXWAN ノード ID の後に 0000 を続けたものがサーキットの IPX ノード番号として使用されます。

サーキット上で交渉されるルーティング・タイプは構成可能です。静的ルーティングが使用可能にされていると、他のルーティング・タイプが交渉されることはありません。下に挙げてあるそれ以外のタイプはどれもが、すべて使用可能にでき、単一ルーティング・タイプに至るまで、優先順位の降順に交渉されます。

- 非番号制 RIP/SAP
- 番号制 RIP/SAP

フレーム・リレー

IPX ルーティング・ソフトウェアでは、次のサーキットとしてフレーム・リレーをモデル化しています。

- 単一の IPX 同報通信サーキットか
- 1 つまたは複数を一組とする IPXWAN ポイント・ポイント・サーキットか
- 両方の組み合わせ

IPX 最大パケット・サイズは、インターフェース用として構成されている MTU を基にして決めます。

下位フレーム・リレー DLC では、InARP を使用して、あて先 IPX ノード・アドレスを該当するフレーム・リレー・バーチャル・サーキットにマップします。オプシ

ョンですが、VC が InArp をサポートしないルーターに接続されている場合は、あて先 IPX ノード・アドレスが静的に構成できます。

IPX 同報通信サーキット: IPXWAN ポイント・ポイント・サーキットとして構成されていない、フレーム・リレー・インターフェース上のバーチャル・サーキットは、すべてが一括してグループ化され、固有の非ゼロ・ネットワーク番号の割り当てを必要とする単一の IPX 同報通信サーキットとしてモデル化されます。したがって、ユーザーがフレーム・リレー・ネットワーク上のルーターとの相互接続を定義している下位バーチャル・サーキットは、IPX ルーティング・ソフトウェアからは透過的です。

フレーム・リレー・インターフェースに対応する MAC アドレスはないので、構成済みホスト番号がサーキットの IPX ノード番号として使用されます。

LAN 全ステーション・アドレス (x'FFFFFFFFFFFF') が、サーキット上の IPX 同報通信アドレスとして使用されます。同報通信アドレスにアドレス指定されたパケットは、下位フレーム・リレー DLC によって、IPX 同報通信サーキット内のすべての VC 上に送信されます。このフレーム・リレー・プロトコル同報通信機能は、次のフレーム・リレー構成オプションを使用可能にすることで起動します。

- プロトコル同報通信
- マルチキャスト・エミュレーション

全メッシュ以外のフレーム・リレー・トポロジーをサポートするために、 IPX 同報通信サーキット上で水平分割を使用不可にできます。こうすれば、 RIP と SAP が IPX 同報通信サーキット内のすべてのバーチャル・サーキットに情報を伝送して、同じ IPX 同報通信サーキット内のバーチャル・サーキット間の中間ルーティングが行われるようにすることができます。

全メッシュ・フレーム・リレー・トポロジーでは、水平分割を使用不可にする必要はありません。

次のルーティング・タイプのどれでも、サーキット上ですべて使用できます。

- 静的ルート/サービス
- RIP/SAP (番号制)

IPXWAN ポイント・ポイント・サーキット: IPX は、個々のフレーム・リレー PVC を通る (SVC はサポートされない) IPXWAN ポイント・ポイント・サーキットとして動作するように構成できます。 IPXWAN を使用して、ルーティング・パラメーターを交渉します。

IPXWAN 番号制 RIP ルーティング・タイプでは、固有の非ゼロ・ネットワーク番号がサーキットに割り当てられることが必要です。それ以外の IPXWAN ルーティング・タイプ (非番号制 RIP、静的ルーティング) では、ネットワーク番号は必要ありません (値 0)。

フレーム・リレー・インターフェースに対応する MAC アドレスはないので、IPXWAN ノード ID の後に 0000 を続けたものがサーキットの IPX ノード番号として使用されます。

サーキット上で交渉されるルーティング・タイプは構成可能です。静的ルーティングが使用可能にされていると、他のルーティング・タイプが交渉されることはあり

ません。下に挙げてあるそれ以外のタイプはどれもが、すべて使用可能にでき、単一ルーティング・タイプに至るまで、優先順位の降順に交渉されます。

- 非番号制 RIP/SAP
- 番号制 RIP/SAP

X.25

IPX ルーティング・ソフトウェアでは、単一の IPX 同報通信サーキットとして X.25 インターフェースをモデル化しています。したがって、ユーザーが X.25 ネットワーク上のルーターとの相互接続を定義している下位 VC は、 IPX ルーティング・ソフトウェアからは透過的です。

サーキットには、固有の IPX 非ゼロ・ネットワーク番号が割り当てられる必要があります。

X.25 インターフェースに対応する MAC アドレスはないので、構成済みホスト番号がサーキットの IPX ノード番号として使用されます。

LAN 全ステーション・アドレス (x'FFFFFFFFFFFF') が、サーキット上の IPX 同報通信アドレスとして使用されます。同報通信アドレスにアドレス指定されたパケットは、下位 X.25 DLC によって、IPX 同報通信サーキット内のすべてのあて先 X.25 アドレスに送信されます。

IPX 最大パケット・サイズは、インターフェース用として構成されている MTU を基にして決めます。

全メッシュ以外の X.25 トポロジーをサポートするために、IPX 同報通信サーキット上で水平分割を使用不可にできます。こうすれば、RIP と SAP が IPX 同報通信サーキット内のすべてのあて先 X.25 アドレスに情報を伝送して、同じ IPX 同報通信サーキット内の VC 間の中間ルーティングが行われるようにすることができます。

全メッシュ X.25 トポロジーでは、水平分割を使用不可にする必要はありません。

次のルーティング・タイプのどれでも、サーキット上ですべて使用できます。

- 静的ルート/サービス
- RIP/SAP (番号制)

あて先 IPX ノード・アドレスがすべてのあて先 X.25 アドレスについて静的に構成される必要がありますが、これは X.25 DLC では InArp をサポートしないからです。

IPX の構成

この節では IPX の初期構成の方法を説明します。以下の各項で、設定できる任意指定パラメーターについて説明します。

1. 下に示すようにして、IPX 構成プロンプトを表示します。

```
* talk 6
Config> protocol ipx
IPX protocol user configuration
IPX config>
```

2. IPX をグローバルに使用可能にします。

```
IPX config> enable ipx
```

3. 同報通信サーキットを WAN または LAN に追加したり、 IPXWAN サーキットを WAN に追加したりします。

```
IPX Config>add broadcast-circuit
Which interface [0]? 1
IPX circuit number[3]? 5
IPX network number in hex
('0' is only allowed on IPXWAN unnumbered circuits) [1]? 01

IPX Config>add ipxwan-circuit
Which interface [0]? 2
IPX circuit number[4]? 6
IPX network number in hex
('0' is only allowed on IPXWAN unnumbered circuits) [1]? 40
Frame Relay PVC circuit number [16]? 18
```

   注: IPX ネットワーク番号 0 が有効なのは、 IPXWAN 非番号制 RIP 回線か静的ルーティング回線の場合だけです。 IPX ネットワーク番号 FFFFFFFF は、IPX ネットワーク番号として有効な番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX 省略時ルート用として予約されていて、IPX ネットワーク番号として使用できない場合があります。

4. IPX がシリアル・インターフェースを通して稼働できるようにした場合は、固有のホスト番号をルーターに割り当てます。

```
IPX config>set host-number
Host number for serial lines (in hex) []? 2
```

5. オプションですが、イーサネット、トークンリングまたは ATM LAN エミュレーション・クライアントのフレーム・タイプを変更します。イーサネット、トークンリングまたは ATM LAN エミュレーション・クライアント以外のサーキットについては、フレーム・タイプを設定する必要はありません。使用可能なフレーム・タイプの説明については、 695ページの『Frame』 を参照してください。

   省略時カプセル化形式は、次のとおりです。

   - イーサネット - Ethernet_8023
   - トークンリング - Token-ring MSB

   frame コマンドを、次のように使用します。

```
IPX config> frame ethernet_8023
IPX circuit number [1]? 2
```

6. オプションですが、省略時値を使用したくない IPXWAN パラメーターがあれば変更します。

```
IPX config> set ipxwan
IPX circuit number [1]? 3
Routing type ('u'=Unnumbered, 'r'=RIP, 'b'=Both, 's'=Static) [u] r
Connection Timeout (in sec) [60]? 90
Retry timer (in sec) [60]? 45
```

任意選択の構成作業

ユーザーが調整できる任意選択の設定値は以下の節で説明されています。

- 664ページの『IPX RIP ネットワーク・テーブルのサイズを指定する』
- 664ページの『RIP 更新間隔を指定する』
- 665ページの『IPX SAP サービス・テーブルのサイズを指定する』
- 665ページの『SAP 更新間隔を指定する』

IPX RIP ネットワーク・テーブルのサイズを指定する

IPX RIP ネットワーク・テーブルには各 IPX ネットワークについての情報が含まれています。省略時テーブル・サイズは 32 です。 テーブル・サイズは 1 ～ 2048 の範囲で構成することができます。ただし、ルーターにはメモリーの制限により最大のテーブル・サイズが使用されない場合があります。

```
IPX config>set maximum networks
New Network table size [32]? 32
```

RIP 更新間隔を指定する

IPX では RIP を使用して、ルーティング・テーブル内のルートを維持します。ルートはパケットがたどるパスを示します。 RIP 更新間隔で、ルーターがそのサーキットにルーティング情報テーブルを同報通信する頻度が決まります。また、RIP 項目が経過時間切れ前に留まる時間の長さも決まります。

有効な項目は、RIP 更新間隔の 3 倍の期間、ルーティング・テーブル内に留まり、ルーターは、更新間隔ごとに一度、その RIP テーブルを同報通信します。

例えば、省略時間隔は 1 分ですから、この場合は、有効な項目がテーブル内に留まるのは 3 分間です。 この時間の経過後、RIP 更新によって項目が再生されない場合は、ルートは無限大というホップ・カウント (16) がマーク付けされた上で、削除されます。 60 秒ごとに、ルーターは、対応するサーキットにその RIP テーブルを同報通信します。

RIP 間隔は 1 ～ 1440 分 (24 時間) の範囲で構成できます。RIP 間隔を大きくすると、WAN 回線およびダイヤル回線のトラフィックが減少します。また、要求時ダイヤル・サーキットの頻繁なダイヤルアウトも防止します。

注: 完全な RIP 公示は更新間隔によって制御されますが、その一方でルーターはネットワーク・トポロジーの変更を学習すると、即時に伝送します。

RIP 間隔は Novell ファイル・サーバーでは構成不能です。

```
IPX config>set rip-update-interval
IPX circuit number [1]? 2
RIP timer value(minutes) [1]? 2
```

IPX SAP サービス・テーブルのサイズを指定する

IPX サービス公示プロトコル (SAP) サービス・テーブルは、ファイル・サーバーなどの NetWare サービスを見つけるのに使用する分散データベースです。サービスは、2 バイトの数値タイプと 47 文字の名前で固有に識別されます。各サービス提供者は、それぞれサービスを公示し、サービス・タイプ、名前、およびアドレスを指定します。ルーターはこの情報をテーブルに累積し、他のルーターに送信します。省略時テーブル・サイズは 32 です。

テーブル・サイズは 1 ～ 2048 の範囲で構成できます。ただし、ルーターのメモリー制約によって最大テーブル・サイズの使用を防止することができます。

```
IPX config>set maximum services
New Service table size [32]? 32
```

SAP 更新間隔を指定する

IPX サービス公示プロトコル (SAP) 間隔を使用して、サーキット単位で IPX SAP 更新間の時間が構成できます。同一ネットワーク上のルーター・サーキットは、すべてが同じ SAP 間隔を使用する必要があります。この間隔によって、テーブル情報の経過時間切れ時間とルーター・インターフェースへの同報通信間の間隔が、両方とも決まります。

有効な項目は、SAP 更新間隔の 3 倍の期間、SAP サービス・テーブル内に留まり、ルーターは、更新間隔ごとに一度、その SAP サービス・テーブルを同報通信します。

SAP 間隔は 1 ～ 1440 分 (24 時間) の範囲で構成できます。SAP 間隔を大きくすると、WAN 回線およびダイヤル回線のトラフィックが減少します。また、要求時ダイヤル・サーキットの頻繁なダイヤルアウトも防止します。

注: 完全な SAP 公示はこの間隔によって制御されますが、その一方でルーターはネットワーク・トポロジーの変更を学習すると即時に伝送します。

SAP 間隔は Novell ファイル・サーバーでは構成不能です。

```
IPX config>set sap-update
IPX circuit number [1]? 2
SAP timer value(minutes) [1]? 4
```

IPX キープアライブおよび逐次化パケット・フィルター

キープアライブおよび逐次化パケットがダイヤル・オンデマンド・リンクを継続的に活動化するのを避けるため、またはダイヤル・オンデマンド・リンクを介してのトラフィックを最小化するために、IPX を構成することができます。

例えば、666ページの図53 では、Novell クライアントが Novell サーバーにログインしてからアイドルのまま留まる場合は、サーバーはクライアントに定期的にキープアライブ要求を送信し、クライアントはキープアライブ応答で応答します。キープアライブ・フィルターにより、ルーターはキープアライブ・テーブルに最初のキープアライブ応答を入力しから、応答を転送するようになります。その後、ルーターは WAN リンクを介してのクライアント/サーバー接続についてキープアライブ・トラ

フィックを転送しません。代わりに、ルーター A はサーバーから受信するキープアライブ要求に応答し、ルーター B は Novell クライアントにキープアライブ要求を送信します。

キープアライブ・フィルターは、ルーターが WAN リンクを介して NetWare 逐次化パケットを転送しないようにします。

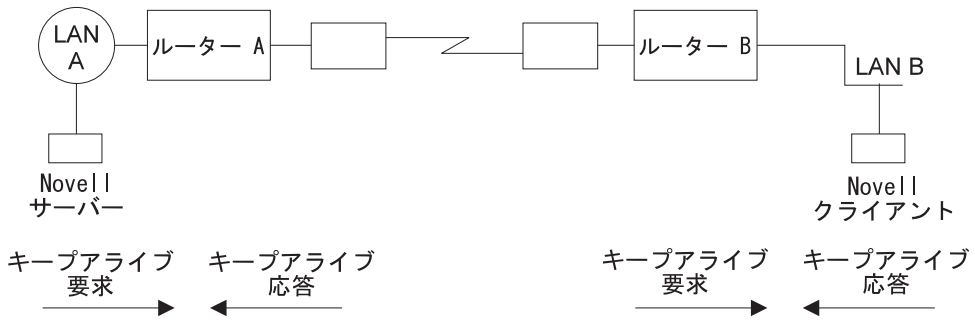


図 53. キープアライブ・フィルター

キープアライブ・フィルターをセットアップするには、それをダイヤル・サーキットで使用可能にしてください。

```
IPX Config> enable keepalive-filtering
IPX circuit number [1]? 5
```

複数ルートを構成する

IPX が同一のあて先ネットワークに関して複数のルーティング項目を保持するように構成することができます。このフィーチャーの利点は、ルートが故障した場合に、代替ルートが即時使用される点にあります。ルーターは RIP 同報通信を待つ (この場合は、新しいルートを学習するのに、数秒ないし 1 分を要する可能性があります) 必要がありません。ルーターはルーティング・テーブル内に等コスト・パスのみを保管します。

各あて先ごとにルーティング・テーブルに保管するルートの最大数を構成するには、次のコマンドを使用します。範囲は 1 ～ 64 です。省略時値は 1 です。

```
IPX config>set maximum routes-per-destination
New maximum number of routes per destination net [1]? 4
```

ルーティング・テーブルに保持される項目の合計数を設定するには、次のコマンドを使用します。範囲は 1 ～ 4096 です。省略時値は 32 です。項目の数は少なくとも RIP ネットワーク・テーブルと同じサイズになるように設定します。(RIP ネットワーク・テーブルの構成は、この章で説明している **set maximum networks** コマンドを使用して行います。)

```
IPX config>
set maximum total-route-entries
New route table size [32]? 40
```

静的ルートを構成する

静的ルートは、あて先ネットワーク番号ごとに構成できます。各静的ルートは、それぞれサーキットに対応付けられ、IPX がサーキット上で起動されると、ルーティン

グ・テーブルにインストールされます。IPX がサーキット上で停止したり、サーキット自体がダウンしたり、あて先ネットワークへの動的確認ルートが確認されたりすると、静的ルートはルーティング・テーブルから除去されます。 (RIP により) 動的に確認されたルートは、必ず、静的ルートを指定変更します。 IPX がサーキット上で再起動されたり、サーキット自体がアップ状態に戻ったり、あて先ネットワークへの RIP ルートがすべて失われたりすると、静的ルートがルーティング・テーブルに再インストールされます。

静的ルートは、RIP が使用不能になっており、あて先ネットワークまでのルートが静的に構成されているダイヤル・オンデマンド・サーキットでは特に有用です。

静的ルーティングは、単独でも RIP との組み合わせでも、サーキット上で使用できます。ただし、静的ルーティングが IPXWAN サーキット上で使用可能にされている場合だけは例外です。この場合、静的ルーティングは、IPXWAN によって折衝される唯一のルーティング・タイプです。

静的ルートは、水平分割および適用可能なフィルターがあれば、RIP によって公示されます。

あて先ネットワークごとに複数の静的ルートが構成されるときは、RIP ルートを選ぶのに使用されたのと同じ規則を使用して、ルーティング・テーブルに入れる静的ルートが決められます。同じあて先ネットワークまでの複数の静的ルートが等コストである場合は、ルーティング・テーブルに入れられます。あて先ごとの構成済みルートまでは、ルーティング・テーブルに同時に保管できます。

次の例は、IPX 静的ルートの構成方法を示しています。

```
IPX Config> disable rip
IPX circuit number [1]? 2

IPX Config> enable route-static

IPX Config> add route-static
IPX net address: (1-fffffffe) [1]? 30
IPX circuit number [1]? 2
Next-hop address, in hex [] ? 400000003000
Ticks: (0-30000) [0]? 4
Hops: (0-14) [0]? 4
```

静的サービスを構成する

静的サービスは、サービス・タイプまたは名前のペアごとに構成できます。各静的サービスは、それぞれが 1 つのサーキットに対応付けられ、IPX がそのサーキット上で起動されると、SAP サービス・テーブルにインストールされ、そのサービスのネットワークへのルートが (静的ルートと RIP 公示のどちらかによって) 認識されます。IPX がサーキット上で停止したり、サーキット自体がダウンしたり、サービスのネットワークへのルートが失われたり、同じサービスが動的に確認されたりすると、静的サービスは SAP テーブルから除去されます。サーバーのネットワークまでのルートが認識されている限り、 IPX がインターフェース上で再起動されたり、インターフェース自体がアップ状態に戻ったり、SAP 確認のサービスが失われたりすると、静的サービスは、サービス・テーブルに再インストールされます。 (SAP を使用して) 動的に確認されたサービスは、必ず、静的サービスを指定変更します。

静的サービスは、SAP が使用不能になっており、サービスが静的に構成されているダイヤル・オンデマンド・サーキットでは特に有用です。

静的サービスは、単独でも RIP/SAP との組み合わせでも、サーキット上で使用できます。ただし、静的ルーティングが IPXWAN サーキット上で使用可能にされている場合だけは例外です。この場合、静的ルーティングは、IPXWAN によって折衝される唯一のルーティング・タイプです。

静的サービスは、水平分割および適用可能なフィルターがあれば、SAP によって公示されます。

名前またはタイプごとに複数の静的サービスが構成されるときには、SAP ルートを選ぶのに使用されたのと同じ規則を使用して、ルーティング・テーブルに入れる SAP サービスが決められます。等コストの静的サービスが構成されている場合は、サーバーのネットワークへの現行ルートと同じサーキット上に定義されている静的サービスが、サービス・テーブルにインストールされます。

次の例は、IPX 静的サービスの構成方法を示しています。

```
IPX Config> disable sap
IPX circuit number [1]? 2

IPX Config> enable sap-static

IPX Config> add sap-static
Sap type: (0-ffff) [4]?
Sap name: []? FILE_SERVER01
IPX circuit number [1]? 2
IPX net address: (1-fffffffe) [1]? 30
IPX node address, in hex: []? 400000202000
IPX socket: (0-ffff) [451]?
Hops: (0-14) [0]? 4
```

RIP 省略時ルートを構成する

省略時ルートは、特別な場合の静的ルートです。省略時ルートは、未知のあて先ネットワークのネクスト・ホップとして、最後の手段として使用されます。

省略時ルートは、RIP が使用不能になっているときに、ダイヤル・オンデマンド・サーキット上で特に有用です。ダイヤル・オンデマンド・サーキット上に省略時ルートを構成すると、クライアントは、各あて先ごとに静的ルートを構成しなくても、サーキットの反対側のあて先ネットワークまでのルートを要求して、パケットを送信することができます。

RIP の取り扱い

RIP を使用するルートの場合、省略時ルートは、ネットワーク番号 FFFFFFFE で指定します。

RIP ルートを公示すると、省略時ルートは (他のすべての静的ルートと同様に)、RIP フィルターおよび水平分割の有無を調べられた後で、公示されます。

未知のあて先ネットワークについての RIP 要求に応答するときは、ルーターは、ルーティング・テーブルに省略時ルートが入っている場合に限りその要求に応答します。

パケットの転送時に、あて先ネットワークまでのルートが不明である場合には、転送側は、省略時ルートを公示しているネクスト・ホップ・ルーター (あるいは、静的

ルーティングの場合にはローカルな静的省略時ルート定義によって指示されたネクスト・ホップ・ルーター) にパケットを転送します。

次の例は、RIP 省略時ルートの構成方法を示しています。

```
IPX Config> enable route-static

IPX Config> add route-static
IPX net address: (1-fffffffe) [1]? ffffffe
IPX circuit number [1]? 2
Next-hop address, in hex: []? 400000003030
Ticks: (0-30000) [0§? 4
Hops: (0-14) [0]? 4
```

SAP との対話

一般的に、SAP 公示は、サーバーのネットワークまでのルートが認識されている場合に限り受け入れられます。サーバーのネットワークまでのルートが不明であるが、省略時ルートが認識されている場合には、公示は受け入れられます (SAP フィルターの有無が調べられた後)。

省略時ルートの存在によって受け入れられる SAP 公示は、 SAP 公示が受け入れられた (水平分割) 以外のすべての IPX サーキット上に公示されます。もちろん、この公示は、公示前に SAP フィルターの存在が条件とされます。 SAP 要求への応答についても、同じ規則が適用されます。

グローバル IPX フィルターを構成する (IPX アクセス制御)

グローバル IPX フィルターは、すべての IPX サーキットに適用されます。それらは、ルーターが IPX アドレス (ネットワーク/ホスト/ソケット) に基づいてパケットを転送しないように使用することができます。 グローバル IPX フィルターを使用して、セキュリティーを提供すること、すなわち、問題外の “やかましい” アプリケーションからのパケット転送を停止することができます。

グローバル IPX フィルターは、発信側の IPX 発信元アドレスおよび最終的なあて先の IPX アドレスに基づいています。中間のホップ・アドレスは重要ではありません。

グローバル・フィルターの IPX アドレス (発信元およびあて先) は、IPX ネットワーク番号、IPX ホスト番号、および 16 進数で指定される一定の範囲の IPX ソケット番号で構成されます。 ネットワーク番号およびホスト番号は 0 (ワイルドカードで、それぞれすべてのネットワーク番号およびすべてのホスト番号に一致する) に指定することができます。0 ～ FFFF の範囲がソケットのワイルドカードです。

グローバル・フィルター・リストは、項目の配列されたリストです。各グローバル・フィルター項目は inclusive (組み込み) または exclusive (排除) として構成することができます。ルーターは、受信したパケットをグローバル・フィルター・リストと比較します。

- パケットが組み込み項目に一致した場合は、ルーターはそのパケットを転送します。
- パケットが排除項目に一致した場合は、ルーターはそのパケットを除去します。
- パケットが一致する項目がないまま、ルーターがリストの終わりに達した場合は、ルーターはそのパケットを除去します。(この場合は、リストの終わりにワイルドカードによる排除項目があったことになります。)

IPX の使用

グローバル・フィルター・リストを作成する際、IPX について次のことを考慮してください。

- 第一に、RIP ソケットおよび SAP ソケット (X'0453' および X'0452') は、決してブロックしてはなりません。RIP および SAP は IPX パケットを正しく転送するよう要求されます。
- グローバル・フィルター・リストは、すべてのサーキットに適用されます。グローバル・フィルターで発信元またはあて先、あるいはその両方のネットワーク番号を使用して、方向制御を有効にする必要があります。
- 自分が保護を試みているサービスがある場所を理解します。IPX> プロンプトで、**slist** コマンドを入力して、サービスのアドレスを判別してください。

  注: Novell ファイル・サーバー (バージョン 3.0 以上) 上のサービスは、すべてサーバーの内部ネットワーク上にあり、通常は、ホスト 000000000001 にあります。この内部ネットワーク番号は 1 つの IPX ネットワーク全体を通じて固有であるため、内部ネットワークのソケット範囲 0 ～ FFFF へのパケットをすべてブロックすることによって、それを保護することができます。そのファイル・サーバーだけをブロックする場合は、ソケット範囲 0451 ～ 0451 を使用します。
- ソケット番号を **slist** から抽出してグローバル・フィルター・リストを作成する場合は、サービスによって固定ソケット番号をもつものもあれば、動的 (一時) ソケット番号をもつものもあることを忘れないでください。4000 ～ 7FFF の範囲のソケットは動的であるため、次にファイル・サーバーがリブートされたとき、サービスが同じソケット番号をもっているという保証はありません。これに対して、8000 ～ FFFF の範囲のソケット番号は Novell によって割り当てられ、一般的には固定されています。

注: グローバル・フィルターとサーキット・フィルターは、両方を同時に使用することはできません。グローバル SAP フィルターが使用可能にされていれば、SAP フィルターは使用可能にできません (逆も同じです)。グローバル IPX フィルターが使用可能にされていれば (*アクセス制御*)、サーキット IPX フィルターは使用可能にできません (逆も同じです)。

ルーターは各 IPX フレームごとに、グローバル・フィルター・リスト内の項目に一致するかどうかを調べます。最初の一致が適用されるため、グローバル・フィルターの配列が非常に重要です。 ルーターが IPX パケットを検査する場合の基準には、次のものがあります。

1. グローバル・フィルターのタイプ (2 つのタイプ):
   a. Inclusive (組み込み)。パケットが以下の基準に適合した場合は、そのパケットを転送することを示します。
   b. Exclusive (排除)。パケットが以下の基準に適合した場合は、そのパケットを廃棄することを示します。
2. あて先ネットワーク - パケットの「IPX あて先ネットワーク」フィールドから直接取ります。
3. あて先ホスト - パケットの「IPX あて先ホスト」フィールドから直接取ります。
4. 開始/終了あて先ソケット - パケットの「IPX あて先ソケット」フィールド (ホスト・フィールドではない) から直接取ります。(ソケット番号は、パケットをアプリケーション・サービスにバインドするプロトコル内の場所です。)

5. 発信元ネットワーク - パケットの「IPX 発信元ネットワーク」フィールドから直接取ります。
6. 発信元ホスト - パケットの「IPX 送信元ホスト」フィールドから直接取ります。
7. 開始/終了発信元ソケット - パケットの「IPX 発信元ソケット」フィールドから直接取ります。

次の例の結果は、IPX ネット 1871 上のクライアントからネットワーク 18730 上の Novell ファイル・サーバー 0000 C93A 0912 の NCP アプリケーションをあて先とした IPX パケットだけが転送されることになります。 その他のトラフィックはすべて除去されます。

```
IPX config>add access control
Enter type [E]? I
Destination network number (in hex) [ ]? 18730
Destination host number (in hex) [ ]? 0000C93A0912
Starting destination socket number (in hex) [ ]? 0451
Ending destination socket number (in hex) [ ]? 0451
Source network number (in hex) [ ]? 1871
Source host number (in hex) [ ]? 0
Starting source socket number (in hex) [ ]? 4000
Ending source socket number (in hex) [ ]? 7FFF
```

グローバル SAP フィルター

グローバル SAP フィルターは、すべてのサーキットに適用されます。それらは、サービス公示情報がルーターを通じて伝送されないようにするために使用することができます。 グローバル SAP フィルターを使用する 4 つの主な理由があります。

- 使用しているサーバー機能のバインダリー・サイズが小さく (例えば、 NetWare バージョン 2.15 以下)、SAP データベース内の情報の量を制限する必要がある。
- 特定のサービスへのリモート・アクセスは不適当なため、そのようなサービスのローカル・エリア外の公示を望まない。
- SAP テーブルからクラッターを除去したい。
- SAP 公示はかなりの量の WAN 帯域幅を消費する場合があるので、 WAN リンクでの不必要な SAP 公示を減らしたい。

注: 上記の理由のいずれも明示的にセキュリティーに言及するものではありません。グローバル SAP フィルターはサービスを保護することができません。SAP が行うのは、サービスの名前－アドレス変換を提供することだけです。侵入者がサービスのアドレスを知った場合は、グローバル SAP フィルターでその公示をブロックしても、そのサービスを保護することにはなりません。セキュリティーはアクセス制御でしか得られません。

グローバル SAP フィルターは、特定のサービス、またはサービスのグループに最大のホップ・カウントを設定することに基づいています。 一致するサービス公示が指定したホップ・カウント (以下) で受信された場合だけ、SAP テーブル内に受け入れられます。それ以外は無視されます。SAP データベース内のそのようなサービスだけが再公示または使用されて照会に応答します。

注: ルーターではサービス名は 7 ビットの ASCII でのみ入力することができます。サービス名には 2 進データを使用するものがあり、Novell SAP 仕様に違反しています。そのようなサービスは名前でフィルターすることはできません。

グローバル SAP フィルターは、あるタイプのすべてのサービスに適用することができます。Novell では各タイプのサービスごとに 4 桁の 16 進数タイプ番号を割り当てます。あるいは、グローバル SAP フィルターは、あるタイプの 1 つの特定のサービスに適用することができます。この場合は、そのサービスの名前を指定することによって行います。

同じサービス・タイプのいくつかのサーバーがあり、それぞれが固有のサービス名をもつことがありえます。この場合、固有のサービス名をフィルターするために、同じサービス・タイプをもつ複数のグローバル SAP フィルターを構成することができます。あるいは、すべてのサービス名についてサービス・タイプをフィルターする単一の SAP フィルターを構成することができます (ワイルドカード・フィルター)。

グローバル SAP フィルターを作成する

グローバル SAP フィルターを構成するには、次のように行います。

1. IPX Config> プロンプトで **add filter** を入力します。複数の重要項目 (通常は SAP 同報通信の中にある) を指定する必要があります。
   a. Number of hops (ホップの数)。この項目は SAP 項目に関して許容されるホップ・カウント (これを超える場合は、廃棄) を示します。
   b. Service type (サービス・タイプ)
   c. Service name (サービス名)
2. IPX Config> プロンプトで **set filter on** を入力して、フィルターを使用可能にします。

次の例では、特定のプリント・サーバーに対するグローバル SAP フィルターの作成を示しています。

```
IPX config>add filter
Maximum number of hops allowed [1]? 2
Service type [4]? 0047
Optional service name [ ]? rem-ptr1
IPX config> set filter on
```

このグローバル SAP フィルターにより、ルーターは、3 ホップ以上離れた **rem-ptr1** という名前のどの印刷サーバーからの SAP 公示も無視します (サービス・タイプ 0047)。このフィルターでは、ルーターが上記の基準に適合する公示を伝送しないようにします。

グローバル SAP フィルターに関するサービス・タイプを判別する

確立したいフィルターに関するサービス・タイプを判別するには、次のようにします。

1. * プロンプトで、**talk 5** と入力し、次に、+ プロンプトで、**protocol ipx** と入力します。

   IPX> プロンプトで **slist** と入力します。フィルターしたいサービスに関する項目に注意してください。
2. * プロンプトで、**talk 6** と入力し、次に、Config> プロンプトで、**protocol ipx** と入力します。フィルターしたいサービスの場合に該当するグローバル SAP フィルター、および該当するホップ・カウントを追加します。
3. フィルターの作成後、ルーターを再始動してください。

4. サービスが正常にフィルターされた場合は、そのサービスはリストから外されているはずです。 IPX> プロンプトに **slist** を入力して、そのサービスがリストから外されていることを確認します。

IPX サーキット・フィルター - 概説

IPX ルーティング・フィーチャーでは、ROUTER、RIP、SAP、IPX の 4 つのタイプのサーキット・ベースのフィルターをサポートします。サーキットごとに、*入力フィルター* が 1 つと、*出力フィルター* が 1 つ定義できます。*項目* と呼ばれるフィルター基準を集めて*フィルター・リスト* としてから、入力または出力フィルターあるいはその両方に付加されます。 フィルター・リストは、2 つ以上のフィルターに付加することができます。したがって、複数のサーキットに対して同じフィルター基準を構成する必要がなくなりました。

注: グローバル・フィルターとサーキット・フィルターは、両方を同時に使用することはできません。グローバル SAP フィルターが使用可能にされていれば、SAP フィルターは使用可能にできません (逆も同じです)。グローバル IPX フィルターが使用可能にされていれば (*アクセス制御*)、サーキット IPX フィルターは使用可能にできません (逆も同じです)。

IPX サーキット・フィルターを構成する

IPX サーキット・フィルターは、次のようにして構成します。

1. **create list** コマンドを使用してフィルター・リストを作成し、それに名前を付けます。
2. **update** コマンドとそのサブコマンドを使用して、フィルター・リストを修正し、フィルター基準、およびこのフィルター・リストが組み込みまたは排除のどちらであるか指定します。
3. **create filter** コマンドを使用し、入力フィルターか出力フィルターかを指定して、必要なサーキット上にフィルターを作成します。
4. **enable** コマンドを使用してフィルターを使用可能にします。
5. **attach** コマンドを使用してフィルター・リストをフィルターに付加します。
6. **default** コマンドを使用してフィルターに省略時アクションを設定します。付加されたフィルター・リストのどれでも突き合わせが行われない場合は、省略時アクションが取られます。

その他にも、IPX サーキット上のフィルターを削除したり、 1 つの IPX サーキット (またはすべての IPX サーキット) 上のフィルターを使用不可にしたり、フィルターからフィルター・リストを切り離したり、フィルター内でフィルター・リストを移動したり (フィルター・リストは配列されているため)、フィルターを表示したり、フィルター・キャッシュのサイズを設定したり (IPX フィルターの場合だけ) するためのコマンドもあります。

ROUTER フィルター

ROUTER フィルターは、受信されたすべての RIP 応答パケットの IPX ヘッダーで機能します。出力 ROUTER フィルターはサポートされていません。どのルーターがルーティング情報を交換することが認められるかを制御することにより、個別の IPX

ネットワークをいくつかの別個の IPX インターネットにグループ化するために ROUTER フィルターを使用することができます。

RIP ROUTER フィルターは、サーキット別に、項目が順番に配列されたリストに保持されています。項目は、受信された各 RIP 応答パケットに順に適用されます。 一致が見つかる場合は、一致したフィルター・リストで指定されたアクションが実行されます (Exclude = パケットを廃棄する、Include = パケットを受信して処理する)。排除されたパケットは廃棄されているので、それらのネットワーク項目に含まれている情報は RIP ルーティング・テーブルに入力されません。 一致が見つからない場合、指定された省略時のフィルター・アクションが実行されます。

RIP フィルター

RIP フィルターは、RIP 応答パケットのネットワーク項目で機能します。これは、選択されたネットワークについてのルーティング情報が伝送されるエクステントを制御するために使用することができます。入力 フィルターとして、このフィルターは選択されたネットワークについてのルーティング情報を保管 できないようにします。これは、他の**すべての** ネットワークが (少なくともこのルーターを通じて) 選択されたネットワークについて学習できないようにします。

RIP フィルター (入力) は、サーキット別に、項目が順番に配列されたリストに保持されています。項目は、受信された各 RIP 応答パケット内の各ネットワーク項目に順に適用されます。一致が見つかった場合は、一致するフィルター・リストで指定されたアクションが実行されます (Exclude = ネットワーク項目を無視する、Include = ネットワーク項目を処理する)。除外されたネットワーク項目は無視されるので、それらは RIP ルーティング・テーブルに入力されません。一致が見つからない場合、指定された省略時のフィルター・アクションが実行されます。

出力 フィルターとして、このフィルターは選択されたネットワークについてのルーティング情報の公示 (保管に対するものとして) をしないようにします。これは*一部* (全部に対するものとして) のネットワークが (少なくともこのルーターを通じて) 選択されたネットワークについて学習しないようにします。

RIP フィルター (出力) は、サーキット別に、項目が順番に配列されたリストに保持されています。項目は、RIP 応答パケットに入れて伝送される各ネットワーク項目に順に適用されます。一致が見つかった場合は、一致したフィルター・リストで指定されたアクションが実行されます (Exclude = パケットからのネットワーク項目を除外する、Include = パケットにネットワーク項目を組み込む)。 このフィルターは RIP ルーティング・テーブルの内容に何の影響ももちません。 一致が見つからない場合、指定された省略時のフィルター・アクションが実行されます。

SAP フィルター

SAP フィルターはすべての SAP 応答パケットのサーバー項目で機能します。これは、サービスについての情報が伝送されるエクステントを制御するのに使用することができ、低速 WAN での SAP トラフィックの量を減らすことができます。

入力 フィルターとして、このフィルターは、選択されたサーバーについてのサービス情報を保管 しないようにすることができます。 これにより、他の**すべての** ネットワークが (少なくともこのルーターを通じて) 選択されたサーバーについて学習しないようにします。

SAP フィルター (入力) は、サーキット別に、項目が順番に配列されたリストに保持されています。項目は、受信された各 SAP 応答パケット内の各サーバー項目に順に適用されます。一致が見つかった場合は、一致するフィルター・リストで指定されたアクションが実行されます (Exclude = サーバー項目を無視する、Include = サーバー項目を処理する)。除外されたサーバー項目は無視されるので、それらは SAP サービス・テーブルに入力されません。 一致が見つからない場合、指定された省略時のフィルター・アクションが実行されます。

出力 フィルターとして、このフィルターは選択されたサーバーについてのサービス情報を公示 (保管に対するものとして) しないようにします。 これは、一部 (全部に対するものとして) のネットワークが (少なくともこのルーターを通じて) 選択されたサーバーについて学習しないようにします。

SAP フィルター (出力) は、サーキット別に、項目が順番に配列されたリストに保持されています。項目は、伝送される各 SAP 応答パケット内の各サーバー項目に順に適用されます。一致が見つかった場合は、一致するフィルター・リストで指定されたアクションが実行されます (Exclude = サーバー項目を除外する、Include = パケット内のサーバー項目を組み込む)。このフィルターは SAP サービス・テーブルの内容に何の影響ももちません。一致が見つからない場合、指定された省略時のフィルター・アクションが実行されます。

IPX フィルター

IPX フィルターは IPX パケットの IPX ヘッダーで機能します。これは、選択されたサーバーおよびワークステーションが他の選択されたサーバーおよびワークステーションと通信できるエクステントを、発信元およびあて先のネットワーク、ノード、ソケット・フィールド、ならびにプロトコル・タイプおよびホップ・カウントに基づいて制御するのに使用することかできます。

入力 フィルターとして、パケットが廃棄される必要があることを示す一致では、パケットが **すべての** サーキット上に送信されないようにします。

IPX フィルター (入力) は、サーキット別に、項目が順番に配列されたリストに保持されています。項目は受信された各 IPX パケットに順に適用されます。一致が見つかった場合、一致したフィルター・リストで指定されたアクションが実行されます (Exclude = パケットを廃棄する、Include = パケットを受信して、処理または転送する)。一致が見つからない場合、指定された省略時のフィルター・アクションが実行されます。

出力 フィルターとして、パケットを転送するかどうかの決定は、出力サーキットに応じて行われ、したがって、受信したパケットが、 1 つのサーキットには転送されても、他の一部のサーキットには転送されないようにする場合もあります。

IPX フィルター (出力) は、サーキット別に、項目が順番に配列されたリストに保持されています。項目は、伝送される各 IPX パケットに順に適用されます。一致が見つ

かった場合は、一致するフィルター・リストで指定されたアクションが実行されます (Exclude = パケットを廃棄する、Include = パケットを伝送する)。一致が見つからない場合、指定された省略時のフィルター・アクションが実行されます。

IPX フィルターは、パケットが受信されるごとに起動されるため、使用するのは、高度の固有性が要求される場合 (つまり、ROUTER、RIP、SAP の各フィルターが使用できない場合) だけに限ることをお勧めします。一般に、RIP フィルターは特定のセットのネットワーク上の***すべての*** ステーション間のインターネットワーキングを扱い、SAP フィルターはどのサーバーがインターネットワーク中のワークステーションによって到達可能であるかを制御し、IPX フィルターは***個別の*** ワークステーション (または個別のワークステーション上の個別のアプリケーション) 間のインターネットワーキングを扱います。

708ページの『IPX サーキット・フィルター構成コマンド』 で、IPX サーキット・フィルターの構成に使用するコマンドについて詳しく説明します。

IPX の効率調整

IPX ルーターは、トラフィックをより効率的にルーティングするために、パケット転送について高速パスおよび低速パスの二重のパスを実施します。

高速パスではデータ・パケットだけを転送するのに対して、低速パスでは RIP パケットおよび SAP パケットなどの管理パケットを扱います。高速パスでは、ルーターがパケットを即時に転送できるようにするアドレス・キャッシュを使用します。

低速ルーティング・テーブルの表引きが行われるのは、キャッシュ項目の作成中だけです。キャッシュには、オーバーフローを知的に処理することができるようにする経時機構があります。IPX 構成メニューを用いてキャッシュ・サイズを構成することができます。

IPX 高速パス・キャッシュには、ローカルとリモートの 2 つの項目があります。各項目はそれぞれのタイプのアドレス指定の要件に対処します。

キャッシュ内に入れることのできる項目タイプの最大数に限界を設定するには、キャッシュ・コマンドを使用します。

ローカル・キャッシュ

ローカル・キャッシュのサイズは、各ルーターのローカル・ネットワーク、つまりクライアント・ネットワークのクライアントの合計数に、除去要求が過剰になることを防ぐために 10% のバッファーを加えたものに等しいことが必要です。678ページの図54 の例を使用すると、ルーター 5 (RTR R5) では、9 つのクライアント (C) にサーバー (S) を加えて、合計 10 になります。この合計を基にして、次のようにします。

1. 10% を掛ける (例の場合は 10 に)。
2. その合計 (1) をクライアント合計に加える (安全マージンとして)。
3. この新しい合計 (11) をローカル・キャッシュ項目の数として使用する。

例えば、次のように入力します。

```
IPX config>set local-cache size
New IPX local node cache size [32]? 11
```

キャッシュ項目がすべて使用中である場合は、使用頻度が最も低い項目が除去されます。

リモート・キャッシュ

リモート・キャッシュのサイズは、ルーターによって使用されるリモート・ネットワークの合計数に、除去要求が過剰になることを防ぐために 10% のバッファーを加えたものに等しいことが必要です。 678ページの図54 では、RTR R5 が IPX ネットワーク 5 を経て読み取ることができる IPX ネットワークが 10 あります。したがって、RTR/R5 には、合計 10 のクライアントがあります。この合計を基にして、次のようにします。

1. 10% を掛ける (例の場合は 10 に)。
2. その合計 (1) を、安全マージンとしてリモート・ネットワーク合計 (10) に加える。
3. この新しい合計 (11) をリモート・キャッシュ項目の数として使用する。

例えば、次のように入力します。

```
IPX config>set remote-cache size
New IPX remote network cache size [32]? 11
```

IPX 監視 **sizes** コマンドを使用して、キャッシュ項目を表示して見ることができます。

```
IPX>sizes
Current IPX cache size:
Remote network cache size (max entries): 45
0 entries now in use
Local node cache size (max entries): 86
0 entries now in use
```

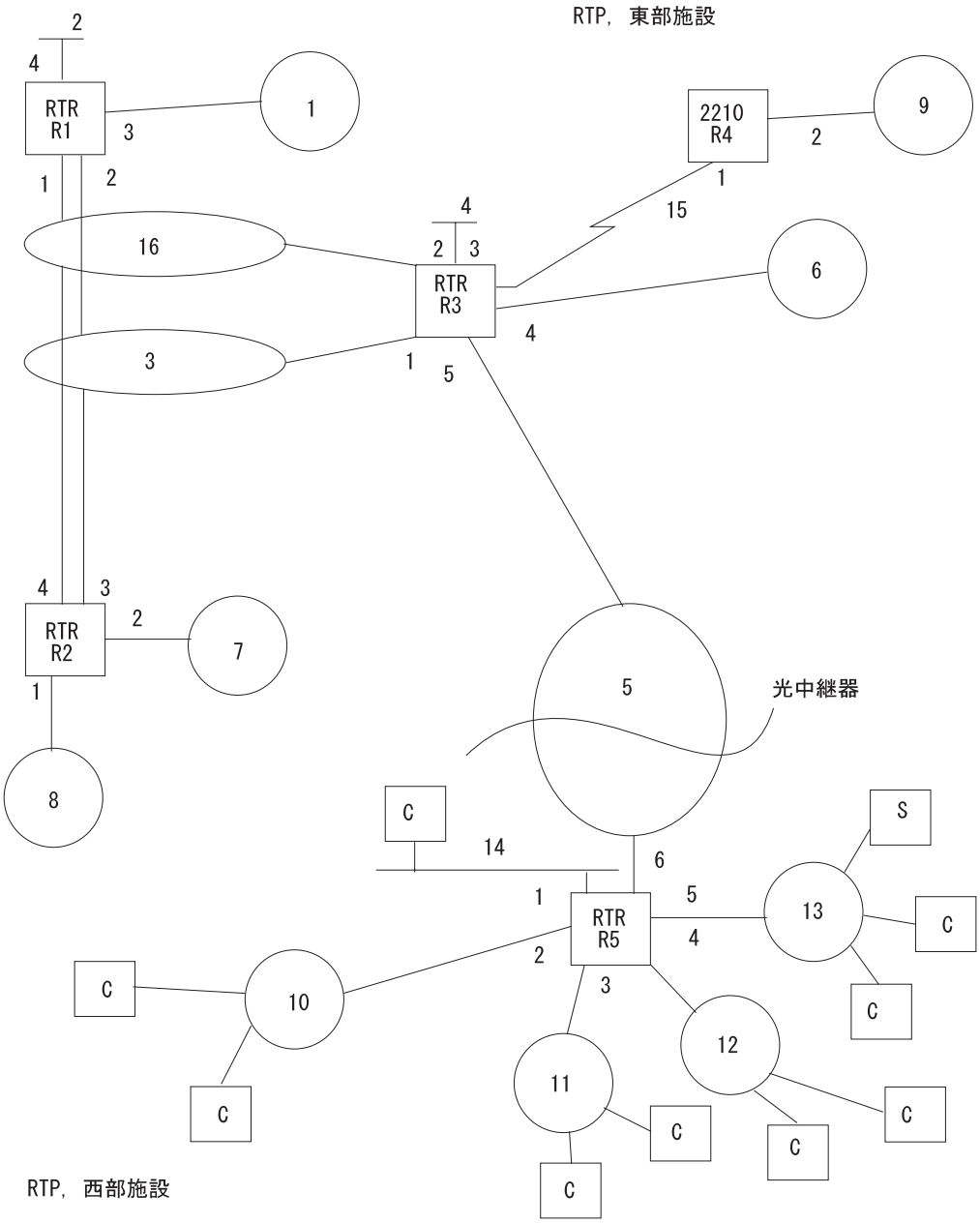


図 54. IPX ネットワーク例

水平分割ルーティング

水平分割はルーティング方式の 1 つで、RIP 更新および SAP 更新がその学習元となったルーターに同報通信されないようにするためのものです。

一般的に、すべてのサーキット上でそれぞれ水平分割を使用可能にして、パケットが無限大までカウントされることがないようにし、不必要な RIP 公示や SAP 公示を避ける必要があります。ただし、部分メッシュフレーム・リレー、ATM、X.25 の各構成のように、水平分割を使用不可にする必要がある場合もあります。

部分メッシュの RFC 1483 によってサポートされる IPX ルーティング構成は、水平分割を使用不能にする必要があるもう 1 つの場合です。

図55 に示すような部分メッシュ・フレーム・リレー・ネットワークでは、本部のルーターが他のすべてのルーターにルーティング情報をすべて同報通信しない限り、支部のルーターは相互間で通信することができません。この場合は、水平分割は、本部のフレーム・リレー・サーキットでは使用不可にし、それぞれの支部では使用可能にして、不必要なトラフィックが生成されることがないようにする必要があります。

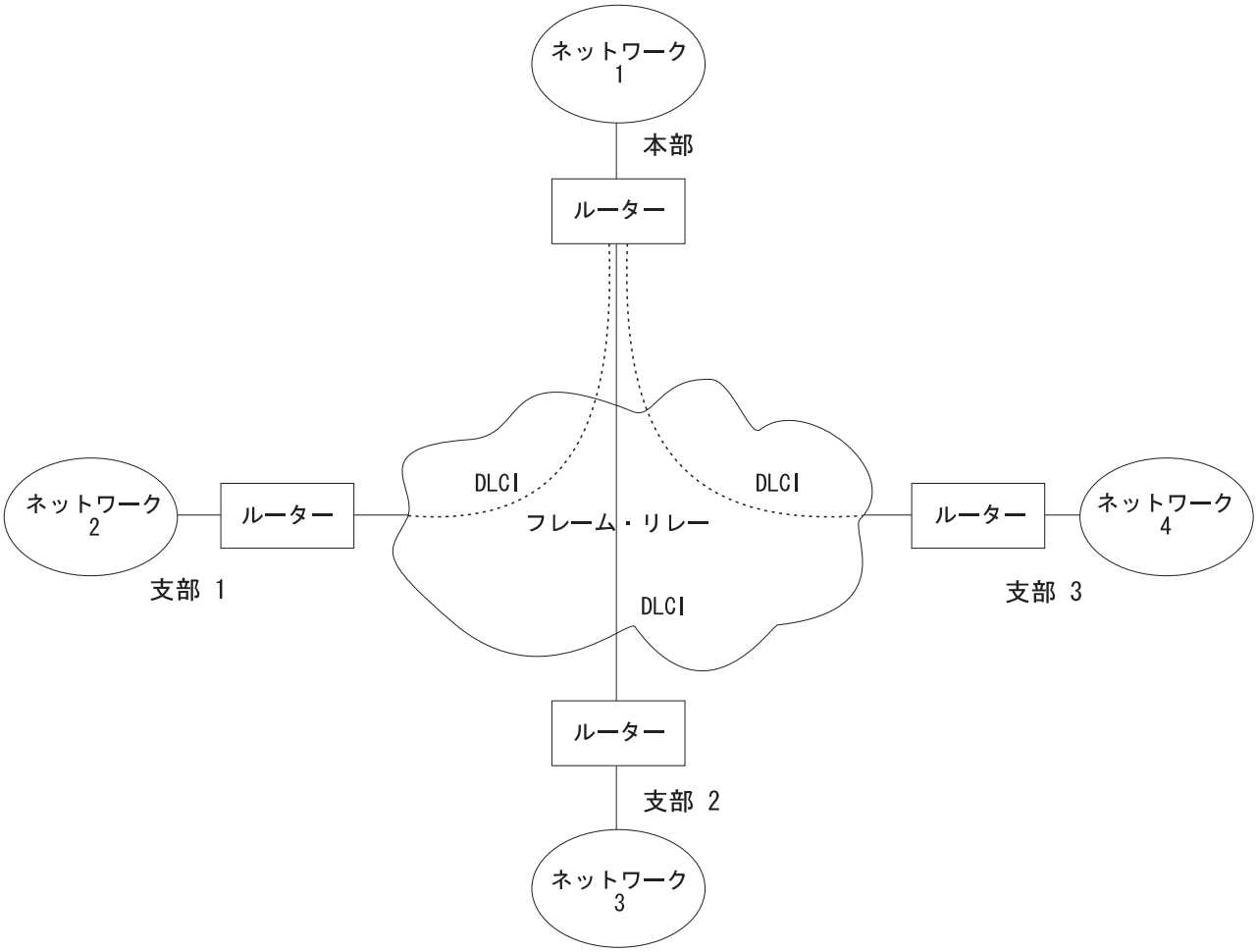


図 55. 部分メッシュ・フレーム・リレー・ネットワーク

水平分割設定値の変更を必要とする場合は、次のように **set split-horizon** コマンドを使用します。

```
IPX Config>set split-horizon enabled
Which circuit [1]? 2

IPX Config>set split-horizon disabled
Which circuit [1]? 2

IPX Config>set split-horizon heuristic
Which circuit [1]? 2
```

第31章 IPX の構成と監視

この章では、IPX プロトコルを構成する方法および IPX 構成コマンドを使用する方法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。

- 『IPX 構成環境へのアクセス』
- 『IPX 構成コマンド』
- 720ページの『IPX 監視環境にアクセスする』
- 720ページの『IPX 監視コマンド』

IPX 構成環境へのアクセス

IPX 構成環境へアクセスするには、Config> プロンプトで次のコマンドを入力します。

```
Config> protocol IPX
IPX Protocol user configuration
IPX Config>
```

IPX 構成コマンド

この節では、IPX 構成コマンドについて説明します。 表40 に IPX 構成コマンドをリストします。これらのコマンドでは、IPX パケットを伝送するルーターに関するネットワーク・パラメーターを指定します。これらのコマンドは、IPX config> プロンプトで入力します。構成変更を活動化する場合は、ルーターを再始動します。

表 40. IPX 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Add	IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを追加し、グローバル IPX フィルター (アクセス制御)、グローバル SAP フィルター、静的ルートやサービスを追加します。
Delete	IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを削除し、グローバル IPX フィルター (アクセス制御)、グローバル SAP フィルター、静的ルートやサービスを削除します。
Disable/Enable	IPX をグローバルに、または特定の IPX サーキット上で使用不可または使用可能にし、IPX 静的ルートやサービスの使用をグローバルに使用不可または使用可能にします。キープアライブ・フィルター、 RIP-SAP 同報通信歩調合わせ、最近隣サーバー獲得要求に対する SAP 応答、 NetBIOS 同報通信を使用不可または使用可能にし、特定のサーキット上で RIP や SAP を使用不可または使用可能にします。
Filter-lists	IPX サーキット・フィルター構成にアクセスします。この環境では、IPX サーキット・ベースの ROUTER、RIP、 SAP、IPX の各フィルターが構成されます。
Frame	イーサネットやトークンリングのサーキットに関するデータ・リンク形式を指定します。トークンリングやイーサネットの LAN エミュレーション・クライアントにも適用されます。

表 40. IPX 構成コマンドの要約 (続き)

コマンド	機能
List	現行の IPX 構成を表示します。
Move	グローバル IPX フィルター項目 (アクセス制御) を再配列したり、 IPX サーキットをインターフェース間で移動したりします。
Set	ホスト番号、IPXWAN ルーター名およびノード ID、IPXWAN 接続タイムアウトおよび再試行タイマー、IPX ネットワーク番号、最大 RIP および SAP テーブル・サイズ、ローカルおよびリモート・キャッシュ・サイズ、グローバル IPX フィルター (アクセス制御) およびグローバル SAP フィルター状態、キャッシュ・サイズ、RIP および SAP 更新間隔、 キープアライブ・フィルター・テーブル・サイズ、ならびに水平分割の使用法を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Add

add コマンドは、グローバル IPX フィルター (アクセス制御)、IPX 同報通信サーキット、グローバル SAP フィルター、IPX ポイント・ポイント・サーキット、静的ルートやサービスを IPX 構成に追加する場合に使用します。

構文 :

add
- access-control . . .
- broadcast-circuit . . .
- filter . . .
- ipxwan-circuit . . .
- route-static . . .
- sap-static . . .

access-control *type dest-net dest-host dest-socket-range src-net src-host src-socket-range*

IPX レベルでパケットを渡すかどうかを判別します。IPX アクセス制御は、IPX プロトコルに関して IPX パケット・レベルでグローバル・アクセス制御機能を提供します。アクセス制御リストは、パケットをフィルターする場合にルーターが使用する項目の順序付きセットです。各項目は組み込みまたは排除です。各項目には、発信元とあて先のネットワーク番号、ホスト・アドレス、およびソケット範囲が含まれます。

IPX プロトコルのパケットがネットワークから受信され、アクセス制御が使用可能になっている場合は、パケットはアクセス制御リストについてチェックされます。 一致があるまで、リストのネット/アドレス/ソケットのペアと比較されます。一致があり、項目が組み込みタイプのものである場合、パケットの受信 (および可能な転送) が行われます。一致する項目が排除タイプのものである場合は、パケットが除去されます。一致がない場合も、パケットは除去されます。

add access-control コマンドを用いてアクセス制御リストを作成した後で、**set access-control on** コマンドを用いて項目を使用可能にします。アクセス制御リストの配列を変更するには、**move** コマンドを使用します。

注: アクセス制御は受信されたすべてのパケットに適用されます。RIP (ソケット 453 16 進数)または SAP (ソケット 452 16 進数) パケットの受信を使用可能にしない場合は、IPX 転送側は機能しません。

```
add access I 0 0 453 453 0 0 0 FFFF
add access I 0 0 452 452 0 0 0 FFFF

Enter type [E] i
Destination network number (in hex) [0]? 0
Destination host (in hex) [ ]? 0
Starting destination socket number in hex [0]? 452
Ending destination socket number in hex [0]? 453
Source network number (in hex) [0]? 0
Source host number (in hex) [ ]? 0
Starting source socket number in hex [0]? 0
Ending source socket number in hex [452]? FFFF
```

Type

特定のアドレスまたはアドレスの組み合わせにパケットが送信されたか、除去されたかを識別します。 include の場合は I を入力してください。そうすると、ルーターはパケットを受信し、残りの引き数で基準に適合した場合は、パケットを転送します。 exclude の場合は E を入力してください。この場合、ルーターはパケットを廃棄します。

Dest-net

あて先のネットワーク番号。16 進数のネットワーク番号を入力してください。

有効値: X'00000000' ～ X'FFFFFFFF'

ゼロ (0) はすべてのネットワークを指定します。

省略時値: 0

Dest-host

あて先ネットワークのホスト番号。16 進数のホスト番号を入力してください。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

ゼロ (0) はネットワーク上のすべてのホストを指定します。

省略時値: なし

Dest-socket-range

あて先ソケットの範囲 (両端の数を含む) を指定する 2 つの数。あて先ソケット値は、IPX パケットをフィルターするのに使用されます。

有効値: X'0000' ～ X'FFFF'

省略時値: 0

Src-net

発信元のネットワーク番号。16 進数のネットワーク番号を入力してください。

このパラメーターは、このルーターによってフィルターされるパケットをもつ発信元 IPX ネットワークのネットワーク番号を定義します。

発信元ネットワーク値に対してのみフィルターするよう選択すると、フィルターは、すべての発信元ソケット、発信元ネットワーク、パケット・タイプ、およびホップの数に適用されます。

有効値: X'00000000' ～ X'FFFFFFFF'

ゼロ (0) はすべてのネットワークを指定します。

省略時値: 0

Src-host
発信元ネットワーク上のホスト番号。16 進数のホスト番号を入力してください。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

ゼロ (0) はネットワーク上のすべてのホストを指定します。

省略時値: なし

Src-socket-range
発信元ソケットの範囲 (両端の数を含む) を指定する 2 つの数

有効値: X'0000' ～ X'FFFF'

省略時値: 0

注: IPX が NetWare 環境で働くためには、アクセス制御および SAP フィルターを使用する必要はありません。それらは必要な場合のみ使用してください。

例: `add access-control E 201 1 451 451 329 0 0 FFFF`

このアクセス制御では、ネットワーク 329 上のすべてのノードが内部ネットワーク番号 201 のファイル・サーバーにアクセスしないようにします。

broadcast-circuit *interface# ipx-circuit# network#*
IPX 同報通信サーキットを追加します。

interface#
IPX サーキット番号が構成される対象のネットワーク・インターフェースを指定します。

有効値 : 有効なネットワーク・インターフェース番号

省略時値 : 0

ipx-circuit#
IPX サーキット番号を指定します。この番号は、ルーター内のすべての構成済み IPX サーキット間で固有である必要があり、構成コマンドの多くで IPX サーキットを参照する場合に使用します。

有効値: 1 ～ 65535

省略時値 : 次に使用可能な IPX サーキット番号

network#
IPX サーキット上で使用する IPX ネットワーク番号を指定します。IPX ネットワーク番号 0 が有効なのは、 IPXWAN 非番号制 RIP 回線か静的ルーティング回線の場合だけです。 IPX ネットワーク番号 FFFFFFFF は、IPX ネットワーク番号として有効な番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX 省略時ルート用として予約されていて、IPX ネットワーク番号として使用できない場合があります。

有効値 : 1 ～ FFFFFFFD

省略時値 : 1

例 :

```
add broadcast-circuit
Which interface [0]?
IPX circuit number [1]?
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [1]?
```

filter *hops service-type service-name*

所定のサービスのための妥当なホップ数を判別できるようにすることにより、大規模ネットワーク上のユーザーが NetWare バインダリー・オーバーフローを起こさないようにします。IPX SAP フィルターにより、プロトコルが SAP 公示内の特定の項目を無視するよう構成することができます。これは、SAP データベースのサイズを制限するために行われます。これは、古いバージョンの NetWare ファイル・サーバーでのサイズの制限のために必要になることがあります。これは、WAN リンクを介して送信される SAP データの量を制限するためにも必要な場合があります。

SAP フィルターは、フィルター項目のグローバルな番号付きリストです。各フィルター項目には、最大ホップ・カウント、サービス・タイプ、および任意選択のサービス名が含まれています。SAP 応答パケットが受信されるとき、各 SAP 項目はフィルター・リストと比較されます。SAP 項目がフィルター・リスト内の項目に一致し、指定したホップより大きい場合は、無視され、ローカル SAP データベースには入力されません。SAP 項目がフィルター・リスト内の項目に一致し、指定されたホップ数に等しいか、またはそれより小さい場合は、その SAP 項目は受け入れられ、ローカル SAP データベースに入力されます。一致がない場合は、SAP 項目は受け入れられます。このコマンド用の引き数は次のとおりです。

Hops

サービスに許容されるホップの最大数

有効値: 0 ～ 16 の範囲内の整数

省略時値: 1

Service-type

数値のサービス・クラス。

有効値: X'0000' ～ X'FFFF' の範囲内の 16 進値

すべてのサービス・タイプをフィルターするためには、X'0000' という値を使用してください。

省略時値: 4

IPX> プロンプトで **slist** コマンドを入力すると、サービス・タイプのリストを表示できます。

Service-name

サーバーの名前を識別します。一般にこのフィールドは入力しません。

有効値: 1 ～ 47 個の ASCII 文字 (X'20' ～ X'7E') のストリング

省略時値: なし

例: add filter 2 039B NOTES-CHICAGO

この例では、ホップ数が 2 を超えると、Lotus Notes サーバー『NOTES-CHICAGO』 に関する公示はすべて無視されます。

ipxwan-circuit *interface# ipx-circuit# network# [FR-circ#]*

IPXWAN ポイント・ポイント・サーキットを追加します。

interface#

IPX サーキットを構成する必要がある対象で、既存の PPP インターフェースやフレーム・リレー・インターフェースを指定します。

有効値 : 有効なネットワーク・インターフェース番号

省略時値 : 0

ipx-circuit#

IPX サーキット番号を指定します。この番号は、ルーター内のすべての構成済み IPX サーキット間で固有である必要があり、構成コマンドの多くで IPX サーキットを参照する場合に使用します。

有効値: 1 〜 65535

省略時値 : 次に使用可能な IPX サーキット番号

network#

IPX サーキット上で使用する IPX ネットワーク番号を指定します。IPX ネットワーク番号 0 が有効なのは、 IPXWAN 非番号制 RIP 回線か静的ルーティング回線の場合だけです。 IPX ネットワーク番号 FFFFFFFF は、IPX ネットワーク番号として有効な番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX 省略時ルート用として予約されていて、IPX ネットワーク番号として使用できない場合があります。

有効値 : 0 〜 FFFFFFFD

省略時値 : 1

FR-circ#

フレーム・リレー PVC サーキット番号を指定します。このパラメーターが必須なのは、IPX サーキットが、フレーム・リレー・インターフェースに追加される IPXWAN サーキットである場合だけです。

有効値 : 有効なフレーム・リレー PVC サーキット番号

省略時値 : 16

例 :

```
add ipxwan-circuit
Which interface [1]?
IPX circuit number [2]?
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [0]?
 Frame Relay PVC circuit number [16]?
```

route-static *dest-net ipx-circuit# nextHop ticks hops*

静的ルートを追加します。

dest-net

あて先 IPX ネットワーク番号を指定します。

有効値: X'1' 〜 X'FFFFFFFE'

省略時値: 1

ipx-circuit#
静的ルートが構成される必要がある対象で、既存の IPX サーキットを指定します。

有効値: 既存の IPX サーキット番号

省略時値: 1

nextHop
あて先ネットワークが到達できるネクスト・ホップ・ルーターの IPX ホスト番号を指定します。

有効値: X'1' ～ X'FFFFFFFFFFFE'

省略時値: なし

ticks
あて先ネットワークとこのルーターとの間にあるティックの数を指示します。ティックの数は、このルーターからあて先ネットワークまで 576 バイトの IPX パケットを伝送するのにかかる時間の長さを表します。各ティックは、55 ミリ秒です。

有効値: 0 ～ 30000

省略時値: 0

hops
あて先ネットワークとこのルーターとの間にあるホップの数を指示します。

有効値: 0 ～ 14

省略時値: 0

例 :

```
add route-static
IPX net address: (1-fffffffe) [1]? 30
IPX circuit number [1]? 2
IPX node address (in hex) []? 020000002030
Ticks: (0-3000) [0]? 4
Hops: (0-14) [0]? 4
```

sap-static *serviceType serviceName ipx-circuit# serverNet serverNode serverSocket hops*
静的 SAP サービスを追加します。

serviceType
サービスの 16 進サービス・クラスを指定します。

有効値: X'0' ～ X'FFFF'

省略時値: 4

serviceName
サービスの ASCII 名を指定します。

有効値: ASCII 文字 ('A' ～ 'Z'、'a'-'z'、'0' ～ '9'、'_'、'-'、'@') のうち、最高 47 文字

省略時値: なし

ipx-circuit#
SAP 静的サービスが構成される必要がある対象で、既存の IPX サーキットを指定します。

有効値: 既存の IPX サーキット番号

省略時値: 1

serverNet
サーバーの内部 IPX ネットワーク番号またはホーム IPX ネットワーク番号を指定します。

有効値: X'1' 〜 X'FFFFFFFE'

省略時値: 1

serverNode
サーバーの IPX ノードを指定します。

有効値: X'1' 〜 X'FFFFFFFFFFFE'

省略時値: なし

serverSocket
サーバーのソケット番号を指定します。

有効値: X'0' 〜 X'FFFF'

省略時値: 451

hops
サーバーとこのルーターとの間にあるホップの数を指示します。

有効値: 0 〜 14

省略時値: 0

例 :

```
add sap-static
Sap type: (0-ffff) [4]? 4
IPX circuit number [1]? 2
IPX net address: (1-fffffffe) [1]? 40
IPX node address, in hex:  []? 000000000001
IPX socket:  (0-ffff) [451]?
Hops: (0-14) [0] 4
```

Delete

delete コマンドは、IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット、グローバル IPX フィルター (アクセス制御)、グローバル SAP フィルター、静的ルーターや静的サービスを削除する場合に使用します。

構文 :

delete access-control . . .
circuit . . .
filter . . .
route-static . . .
sap-static . . .

access-control *line#*
入力する回線番号に一致するアクセス制御を削除します。 現行回線番号を表示するには、**list** コマンドを入力します。

例: delete access-control 2

circuit *ipx-circuit#*

IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを削除します。また、指定された *ipx-circuit#* に対応する静的ルート、静的サービス、サーキット・フィルターのすべても削除します。

例 : delete circuit

```
IPX circuit number [1]? 2
You are about to delete IPX broadcast circuit 2 on interface 4.
All associated static routes, static services and circuit filters
will be deleted as well.  Are you sure? [Yes]: yes
```

filter *hops service-type service-name*

指定した SAP フィルターを削除します。SAP フィルターは list コマンドを実行するときに表示されるとおりに入力する必要があります。引き数は次のとおりです。

Hops

サービスに許容されるホップの最大数

有効値: 0 〜 16

省略時値: 16

Service-type

数値のサービス・クラス。 2 バイトの 16 進数を入力します。

有効値: X'0000' 〜 X'FFFF'

省略時値: なし

Service-name

削除している項目に名前がある場合は、その名前を指定してください。

有効値: 1 〜 47 個の ASCII 文字 (X'20' 〜 X'7E') のストリング

省略時値: なし

例: delete filter 2 039B NOTES-CHICAGO

route-static *dest-net ipx-circuit# nextHop*

静的ルートを削除します。

dest-net

あて先 IPX ネットワーク番号を指定します。

有効値: X'1' 〜 X'FFFFFFFE'

省略時値: 1

ipx-circuit#

静的ルートが構成される対象の IPX サーキットを指定します。

有効値: 既存の IPX サーキット番号

省略時値: 1

nextHop

あて先ネットワークが到達できるネクスト・ホップ・ルーターの IPX ホスト番号を指定します。

有効値: X'1' 〜 X'FFFFFFFFFFFE'

省略時値: なし

例 :

```
delete route-static
IPX net address: (1-fffffffe) [1]? 30
IPX circuit number [1]? 2
IPX node address (in hex) []? 020000002030
```

sap-static *serviceType serviceName ipx-circuit#*

静的 SAP サービスを削除します。

serviceType

サービスの 16 進サービス・クラスを指定します。

有効値: X'0' ～ X'FFFF'

省略時値: 4

serviceName

サービスの ASCII 名を指定します。

有効値: ASCII 文字 ('A' ～ 'Z'、'a'-'z'、'0' ～ '9'、'_'、'-'、'@') のうち、最高 47 文字

省略時値: なし

ipx-circuit#

SAP 静的サービスが構成される対象の IPX サーキットを指定します。

有効値: 既存の ipx-circuit 番号

省略時値: 1

例 :

```
delete sap-static
Sap type: (0-ffff) [4]?
Sap name: (0-ffff) []? filesrv1
IPX circuit number [1]? 2
```

Disable

disable コマンドは、グローバルに、または特定の IPX サーキット上で使用不可にしたり、IPX 静的ルートとサービスの使用をグローバルに使用不可にする場合に使用します。また、SAP 最近隣サーバー獲得要求に対する応答、RIP-SAP 同報通信歩調合わせ、RIP、または SAP を特定のサーキット上で使用不可にする場合も、**disable** コマンドを使用します。

構文 :

disable circuit . . .
ipx
keepalive-filtering . . .
nebios-broadcast . . .
reply-to-get-nearest-server . . .
rip . . .
rip-sap-pacing . . .

route-static . . .

sap . . .

sap-static . . .

circuit *ipx-circuit#*

ipx-circuit で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを使用不可にします。

例 : disable circuit

```
IPX circuit number [1]? 2
```

ipx IPX プロトコルをグローバルに使用不可にします。

例: disable ipx

keepalive-filtering *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、キープアライブ・フィルターを使用不可にします。

例: disable keepalive-filtering

```
IPX circuit number [1]? 2
```

netbios-broadcast *ipx-circuit#*

ipx-circuit# で指定された IPX サーキット上での Novell NetBIOS 同報通信 (パケット・タイプ 20) の受信と送信を使用不可にします。省略時値は enabled (使用可能) です。Novell NetBIOS 同報通信の受信と送信は、たとえ構成で使用可能になっている場合でも、IPXWAN 静的ルーティング・サーキット上では自動的に使用不可にされます。

例 : disable netbios-broadcast

```
IPX circuit number [1]? 2
```

reply-to-get-nearest-server *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、ルーターが SAP 最近隣サーバー獲得要求に対して応答しないようにします。

注: このフィーチャーを使用不能にするには、細心の注意を払う必要があります。このコマンドを使用するのは、IPX ネットワーク上に複数のルーター (またはサーバー) があり、『最適』サーバーがこのルーターの背後にないことが分かっている場合だけにしてください。

例 : disable reply-to-get-nearest

```
IPX circuit number [1]? 2
```

rip *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、RIP を使用不可にします。省略時には、RIP がすべてのサーキット上で使用可能にされます。RIP は、たとえ使用可能に構成されている場合でも、IPXWAN 静的ルーティングを使用するサーキット上では自動的に使用不可にされます。

例:disable rip 1

rip-sap-pacing *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、RIP/SAP 同報通信歩調合わせが行われないようにします。歩調合わせが使用不可にされていると、 RIP と SAP の周期的同報通信は、サーキット上を 55 ミリ秒のパケット間ギャップ (省略時の設定値) で送信されます。歩調合わせを使用可能にするのは、 RIP と SAP 同報通信では輻輳 (ふくそう) を生じる場合があるサーキットだけにします (例えば、バーチャル・サーキットが多いフレーム・リレーや X.25 のサーキットでは、歩調合わせが使用可能にできます)。

例 : disable rip-sap-pacing

```
IPX circuit number [1]? 2
```

route-static

静的ルートの使用をグローバルに使用不能にします。

例:disable route-static

sap *ipx-circuit#*

ipx-circuit で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、SAP を使用不可にします。省略時には、SAP がすべてのサーキット上で使用可能にされます。 SAP は、たとえ使用可能に構成されている場合でも、RLAN サーキットと IPXWAN 静的ルーティングでは自動的に使用不可にされます。

例 : disable sap

```
IPX circuit number [1]? 2
```

sap-static

静的サービスの使用をグローバルに使用不能にします。

例: disable sap-static

Enable

enable コマンドは、IPX をグローバルに、または特定のサーキット上で使用可能にする場合に使用します。また、enable コマンドは、 IPX 静的ルートやサービスの使用をグローバルに使用可能にする場合にも使用でき、特定のサーキット上でキープアライブ・フィルター、RIPS-SAP 同報通信歩調合わせ、最近隣サーバー獲得に対する SAP 応答、RIP や SAP を使用可能にします。

構文 :

enable
- circuit . . .
- ipx
- keepalive-filtering . . .
- nebios-broadcast . . .
- reply-to-get-nearest-server . . .
- rip . . .
- rip-sap-pacing . . .
- route-static . . .

sap . . .

sap-static . . .

circuit *ipx-circuit# network#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを使用可能にし、IPX サーキットの IPX ネットワーク番号を指定します。IPX サーキットが使用可能にされるのは、有効な IPX ネットワーク番号が構成されている場合です。

例 : enable circuit

```
IPX circuit number [1]?
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [1]?
```

ipx-circuit#

使用可能にしたい IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを指定します。

有効値: 有効な ipx-circuit 番号

省略時値: 0

network#

サーキット上で使用したい IPX ネットワークを指定します。 IPX ネットワーク番号 0 が有効なのは、 IPXWAN 非番号制 RIP 回線か静的ルーティング回線の場合だけです。 IPX ネットワーク番号 FFFFFFFF は、IPX ネットワーク番号として有効な番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX 省略時ルート用として予約されていて、IPX ネットワーク番号として使用できない場合があります。

有効値: X'0' 〜 X'FFFFFFFD'

省略時値: 1

例 :

ipx IPX プロトコルをグローバルに使用可能にします。

例: enable ipx

keepalive-filtering *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、キープアライブ・フィルターを使用可能にします。

例 : enable keepalive-filtering

```
IPX circuit number [1]? 2
```

netbios-broadcast *ipx-circuit#*

ipx-circuit# で指定された IPX サーキット上での Novell NetBIOS 同報通信 (パケット・タイプ 20) の受信と送信を使用可能にします。省略時値は enabled (使用可能) です。Novell NetBIOS 同報通信の受信と送信は、たとえ構成で使用可能になっている場合でも、IPXWAN 静的ルーティング・サーキット上では自動的に使用不可にされます。

例 : enable netbios-broadcast

```
IPX circuit number [1]? 2
```

reply-to-get-nearest-server *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、ルーターが SAP 最近隣サーバー要求に応答できるようにします。

例 : enable reply-to-get-nearest

```
IPX circuit number [1]? 2
```

rip *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、RIP を使用可能にします。省略時には、RIP がすべての IPX サーキット上で使用可能にされます。RIP は、たとえ構成で使用可能にされている場合でも、RLAN サーキットと IPXWAN 静的ルーティングでは自動的に使用不可にされます。

例 : enable rip

```
IPX circuit number [1]? 2
```

rip-sap-pacing *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、RIP/SAP 同報通信歩調合わせを使用可能にします。

注: ルーターは、構成された RIP および SAP 更新間隔内での同報通信の完了を保証するパケット間ギャップを計算します。 ルーターが十分に大きなパケット間ギャップを計算するためには、これらの間隔をより大きな値に構成することが必要な場合があります。

歩調合わせを使用可能にするのは、RIP と SAP 同報通信では輻輳 (ふくそう) を生じる場合があるサーキット (例えば、バーチャル・サーキットが多いフレーム・リレーや X.25 のサーキット) だけにします。

例 : enable rip-sap-pacing

```
IPX circuit number [1]? 2
```

route-static

静的ルートの使用をグローバルに使用可能にします。

例 : enable route-static

sap *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキット上で、SAP を使用可能にします。

例 : enable sap

sap-static

静的サービスの使用をグローバルに使用可能にします。

例 : enable sap-static

Filter-lists

filter-lists コマンドは、IPX *filter-type*-List Config> プロンプトにアクセスするのに使用します。有効なリスト・タイプは、router、rip、sap、および ipx です。

IPX *filter-type*-List Config> プロンプトで使用可能なコマンドについては、708ページの『IPX サーキット・フィルター構成コマンド』を参照してください。

構文 :

filter-lists router-lists
rip-lists
sap-lists
ipx-lists

例: filter-lists router-lists

Frame

frame コマンドは、IPX サーキット用のパケット形式を指定する場合に使用します (CONFIG **network** コマンドを使用して、カプセル化を設定することもできます)。

注: 正しくないまたは無効な構成レコードがある場合には、省略時のフレーム値が使用されます。

構文 :

frame ethernet_II . . .
ethernet_8022 . . .
ethernet_8023 . . .
ethernet_SNAP . . .
token-ring MSB . . .
token-ring LSB . . .
token-ring_SNAP MSB. . .
token-ring_SNAP LSB. . .

ethernet_II *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキット上で、フレーム・タイプを ethernet_II に設定します。 ethernet_II カプセル化では、プロトコル・タイプ 8137 のイーサネット、バージョン 2.0 を使用します。NetWare 4.0 以上では、これが省略時値です。

例 : frame ethernet_II

```
IPX circuit number [1]?
```

ethernet_8022 *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキット上で、フレーム・タイプを ethernet_8022 に設定します。 ethernet_8022 カプセル化では、SAP E0 の LLC カプセル化を使用します。

例 : frame ethernet_8022

```
IPX circuit number [1]?
```

ethernet_8023 *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキット上で、フレーム・タイプを

ethernet_8023 に設定します。 ethernet_8023 カプセル化では、LLC ヘッダーがないイーサネット 802.3 カプセル化を使用します。4.0 より前の NetWare では、これが省略時値です。また、ルーターでもこれが省略時値です。

例 : frame ethernet_8023

```
IPX circuit number [1]?
```

ethernet_SNAP *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキット上で、フレーム・タイプを ethernet_SNAP に設定します。 ethernet_SNAP カプセル化では、 PID が 0000008137 の SNAP カプセル化を使用します。

例 : frame ethernet_SNAP

```
IPX circuit number [1]?
```

token-ring MSB *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキット上で、フレーム・タイプを token-ring MSB に設定します。 token-ring MSB カプセル化では、SAP E0 の LLC カプセル化を使用し、非正規 MAC アドレスを使用します。NetWare ではこれが省略時値です。また、ルーターでもこれが省略時値です。

例 : frame token-ring MSB

```
IPX circuit number [1]?
```

token-ring LSB *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキット上で、フレーム・タイプを token-ring LSB に設定します。 token-ring LSB カプセル化では、SAP E0 の LLC カプセル化を使用し、非正規 MAC アドレスを使用します。

例 : frame token-ring LSB

```
IPX circuit number [1]?
```

token-ring_SNAP MSB *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキット上で、フレーム・タイプを token-ring_SNAP MSB に設定します。 token-ring_SNAP MSB カプセル化では、 PID 0000008137 の SNAP カプセル化を使用し、正規 MAC アドレスを使用します。

例 : frame token-ring_SNAP MSB

```
IPX circuit number [1]?
```

token-ring_SNAP LSB *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキット上で、フレーム・タイプを token-ring LSB に設定します。 token-ring LSB カプセル化では、 PID 0000008137 の SNAP カプセル化を使用し、非正規 MAC アドレスを使用します。

List

list コマンドは、現行の IPX 構成を表示するのに使用します。

構文 :

list access-controls

all

circuit

filters

route-static

sap-static

summary

access-controls

グローバル IPX フィルター (アクセス制御) をリストします。このコマンドでは、**list all** の「アクセス制御構成」の項に示されている情報が表示されます。

all IPX 構成全体をリストします。

例 :

```
list all

IPX Globals
------------
IPX Globally                Enabled
Host Number (serial line)   020000003024
Maximum Services                 32
Maximum Networks                 32
Maximum Routes                   32
Maximum Routes per Destination   1
Maximum Local Cache entries      64
Maximum Remote Cache entries     64
Keepalive-Filtering Table Size   32

IPX Configuration:
------------------
                                 NetBIOS    Keepalive
Circ   Ifc    NetNum    IPX      Broadcast  Filtering  Encapsulation
1      0      400       Enabled  Enabled    Disabled   ETHERNET_II
2      1      411       Enabled  Enabled    Disabled   N/A
3      2      412       Enabled  Enabled    Disabled   N/A
       Frame Relay PVC circuit number: 16

RIP Configuration:
------------------
                                 Update    Split      Broadcast
Circ   Ifc    NetNum    RIP      Interval  Horizon    Pacing
1      0      400       Enabled  1         Enabled    Disabled
2      1      411       Enabled  1         Enabled    Disabled
3      2      412       Enabled  1         Enabled    Disabled

SAP Configuration:
------------------
                                 Update    Split      Broadcast  Get Nearest
Circ   Ifc    NetNum    SAP      Interval  Horizon    Pacing     Reply
1      0      400       Enabled  1         Enabled    Disabled   Enabled
2      1      411       Enabled  1         Enabled    Disabled   Enabled
3      2      412       Enabled  1         Enabled    Disabled   Enabled

IPXWAN Configuration:
---------------------
Router Name    ipxwan-413
NodeID         413
                         Routing  Connect     Retry
Circ   Ifc    NetNum    Type     Time (sec)  Time (sec)
2      1      411       RIP      60          60
3      2      412       RIP      60          60

Static Route Configuration:
---------------------------
Static Routes:  Enabled
Dest Net  Hops   Ticks  Next Hop      Circ   Ifc
ABC       3      4      020000003044  3      2

Static Services Configuration:
------------------------------
Static Services:  Enabled
Type Service Name                  Srv Net  Host         Sock Hops Circ   Ifc
4    FILESRV01                     ABC      000000000001 451  3    3      2

SAP Filter Configuration:
-------------------------
IPX SAP Filters:  Enabled
```

```
Index Max Hops  Type  Service Name
1     5         4     FILESRV02

Access Control Configuration:
-----------------------------
IPX Access Controls:  Enabled
#   T Dest Net Host         Sock Sock Src Net  Host         Sock Sock
1   E 2        000000000000 0    FFFF 3        000000000000 0    FFFF
2   I 0        000000000000 452  453  0        000000000000 0    FFFF
```

circuit *ipx-circuit#*

ipx-circuit# で指定された IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを一覧表示します。このコマンドでは、**list all** コマンドの例の 『IPX 構成』、『RIP 構成』、 『SAP 構成』、『IPXWAN 構成』 の各項に示されている情報が表示されます。

filters グローバル SAP フィルターをリストします。このコマンドでは、**list all** コマンドの例の 『SAP フィルター構成』 の項に示されている情報が表示されます。

route-static

静的ルートをリストします。このコマンドでは、**list all** コマンドの例の 『静的ルート構成』 の項に示されている情報が表示されます。

sap-static

静的サービスをリストします。このコマンドでは、**list all** コマンドの例の 『静的サービス構成』 の項に示されている情報が表示されます。

summary

IPX が使用可能にされるすべてのサーキットに関して、IPX、RIP、SAP、IPXWAN、キープアライブ・フィルターの構成の要約を一覧表示します。このコマンドでは、**list all** コマンドの例の 『IPX グローバル』、 『IPX 構成』、『RIP 構成』、『SAP 構成』、『IPXWAN 構成』 の各項に示されている情報が表示されます。

IPX Globals

以下のグローバル情報が表示されます。

- IPX がグローバルに使用可能か使用不能か
- IPX ホスト番号
- サービスの最大数
- ネットワークの最大数
- ルートの最大数
- あて先あたりの最大ルート数
- ローカル・キャッシュ項目の最大数
- リモート・キャッシュ項目の最大数
- キープアライブ・フィルター・テーブルのサイズ

IPX Configuration

IPX が使用可能にされている各サーキットごとに、それぞれ次のものが表示されます。

- IPX サーキット番号
- ネットワーク・インターフェース番号
- IPX ネットワーク番号 (Netnum)
- サーキット上で IPX が使用可能/使用不可

- NetBIOS 同報通信
- キープアライブ・フィルター
- カプセル化

RIP Configuration

IPX が使用可能にされている各サーキットごとに、それぞれ次の情報が表示されます。

- IPX サーキット番号
- ネットワーク・インターフェース番号
- IPX ネットワーク番号 (Netnum)
- RIP が使用可能か、使用不能か
- RIP 更新間隔タイマー
- split-horizon (水平分割) が使用可能か、使用不能か
- RIP 同報通信歩調合わせが使用可能か使用不可か

SAP Configuration

IPX が使用可能にされている各サーキットごとに、それぞれ次の情報が表示されます。

- IPX サーキット番号
- ネットワーク・インターフェース番号
- IPX ネットワーク番号 (Netnum)
- SAP が使用可能か、使用不能か
- SAP 更更新間隔タイマー
- split-horizon (水平分割) が使用可能か、使用不能か
- SAP 同報通信歩調合わせが使用可能かどうか
- SAP 最近隣サーバー獲得要求に対する応答が使用可能かどうか

IPXWAN Configuration

以下のグローバル情報が表示されます。

- ルーター名
- ノード ID

次の情報が各 IPXWAN サーキットごとにそれぞれ表示されます。

- IPX サーキット番号
- ネットワーク・インターフェース番号
- IPX ネットワーク番号 (Netnum)
- ルーティング・タイプ
- 接続タイマー
- 再試行タイマー

Static Routes Configuration

静的ルートがグローバルに使用可能か、使用不能かを表示します。さらに、各構成済み静的ルートについて、以下が表示されます。

- IPX あて先ネットワーク番号
- Hops (ホップ数)

- Ticks (ティック数)
- Next hop node address (ネクスト・ホップ・ノード・アドレス)
- IPX サーキット番号
- ネットワーク・インターフェース番号

Static Services Configuration

静的サービスがグローバルに使用可能か、使用不能かを表示します。さらに、各構成済み静的サービスについて、以下が表示されます。

- Service type (サービス・タイプ)
- Service name (サービス名)
- IPX network number of service (サービスの IPX ネットワーク番号)
- サービスの IPX ノード・アドレス (ホスト)
- Socket (ソケット)
- Hops (ホップ数)
- IPX サーキット番号
- ネットワーク・インターフェース番号

SAP Filter Configuration

グローバル SAP フィルターが使用可能か、使用不能かを表示します。さらに、各構成済みグローバル SAP フィルターについて、以下の情報が表示されます。

- 索引
- Max hops (最大ホップ数)
- Service type (サービス・タイプ)
- Service name (サービス名)

Access Control Configuration

グローバル IPX フィルター (アクセス制御) が使用可能か、使用不能かを表示します。さらに、各構成済みグローバル IPX フィルター (アクセス制御) について、以下の情報が表示されます。

- Access control index (#)
- Filter type (フィルター・タイプ) (include (組み込み) または exclude (排除))
- Destination IPX network number (あて先 IPX ネットワーク番号)
- 着信先 IPX ノード番号 (ホスト)
- Destination IPX socket range (あて先 IPX ソケット範囲)
- Source IPX network number (発信元 IPX ネットワーク番号)
- 送信元 IPX ノード番号 (ホスト)
- Source IPX socket range (発信元 IPX ソケット範囲)

Move

move コマンドは、グローバル IPX フィルター項目 (アクセス制御) を再配列したり、IPX サーキットをインターフェース間で移動したりする場合に使用します。

構文 :

move access-control *srcLine# dstLine#*

circuit *ipx-circuit# interface# [FR-circ#]*

access-control *srcLine# dstLine#*

srcLine#
移動したいアクセス制御の行番号を指定します。

dstLine#
指定した行番号の後が scrLine の移動対象となるアクセス制御の行番号を指定します。

該当する行のアクセス制御を移動した後は、行に番号が付け直されます。

例 :

```
move access-control
Enter index of control to move [1]? 1
Move record AFTER record number [0]? 2
About to move:
#   T Dest Net Host         Sock Sock Src Net  Host         Sock Sock
1   E 2        000000000000 0    FFFF 3        000000000000 0    FFFF
to be after:
2   I 0        000000000000 452  453  0        000000000000 0    FFFF
Are you sure this is what you want to do? [Yes]: yes
```

circuit *ipx-circuit# interface# [FR-circ#]*
インターフェース間で IPX サーキットを移動します。また、このコマンドでは、特定の *ipx-circuit#* に対応する静的ルート、静的サービス、IPX サーキット・フィルターも同じ *interface#* に移動します。IPXWAN サーキットをフレーム・リレー・インターフェースに移動する場合は、新規フレーム・サーキット番号の入力を指示するプロンプトも出ます。

ipx-circuit#
移動したい既存の IPX サーキットを指定します。

有効値 : 有効な IPX サーキット番号

省略時値 : 1

interface#
IPX サーキットの移動先となる既存のネットワーク・インターフェースを指定します。

有効値 : 有効なネットワーク・インターフェース番号

省略時値 : 0

FR-circ#
フレーム・リレー PVC サーキット番号を指定します。このパラメーターが必須なのは、IPX サーキットが、フレーム・リレー・インターフェースを移動先とする IPXWAN サーキットである場合だけです。

有効値 : 有効なフレーム・リレー PVC サーキット番号

省略時値 : 16

例 :

```
move circuit
IPX circuit number [1]?
Which interface do you want to move the IPX circuit to [0]? 5
Frame Relay PVC circuit number [16]? 18
You are about to move IPXWAN circuit 1,
from Frame Relay interface 2 (FR circuit 16) to
```

```
Frame Relay interface 5 (FR circuit 18).
All associated static routes, static service and circuit filters
will be moved as well. Are you sure? [Yes]: y
```

Set

set コマンドは、ホスト番号、IPXWAN ルーター名とノード ID、IPXWAN ルーティング・タイプ、接続タイムアウトと再試行タイマー、IPX ネットワーク番号、最大 RIP および SAP テーブル・サイズ、ローカルとリモートのキャッシュ・サイズ、グローバル IPX フィルター (アクセス制御) とグローバル SAP フィルターの状態、 RIP と SAP の更新間隔、キープアライブ・フィルター・ テーブル・サイズ、水平分割使用を構成する場合です。

構文 :

set
- access-control . . .
- filter . . .
- host-number . . .
- ipxwan . . .
- keepalive-table-size . . .
- local-cache size . . .
- maximum routes-per-destination . . .
- maximum networks . . .
- maximum services . . .
- maximum total-route-entries . . .
- name . . .
- net-number . . .
- node-id . . .
- remote-cache size . . .
- rip-update-interval . . .
- sap-update-interval . . .
- split-horizon . . .

access-control *on* **or** *off*

グローバル IPX フィルター (アクセス制御) をオンまたはオフにします。**on** または **off** を入力します。

例: `set access-control on`

filter *on* **or** *off*

グローバル SAP フィルターをオンまたはオフにします。**on** または **off** を入力します。

例: `set filter on`

host-number *host#*

IPX が稼働するシリアル・サーキットに関して使用されるホスト番号を指定します。シリアル・サーキットを通して稼働する各 IPX ルーターには、それぞ

れ固有のホスト番号が必要です。その理由は、シリアル・サーキットには、ホスト番号を構築する元になるハードウェア・ノード・アドレスがないからです。マルチキャスト・アドレスであることはできません。

注: 同じインターフェース上に IPX 同報通信と IPXWAN サーキットの混在を構成する場合は、IPXWAN ノード ID の後に X'0000' を続けて、ホスト番号を構成することをぜひともお勧めします。

有効値: X'000000000001' ～ X'FEFFFFFFFFFF' の範囲の 12 桁の 16 進数

省略時値: なし

この番号は各ルーターで固有でなければなりません。

例: `set host-number 0000000000F4`

注: IPXWAN では、ルーターのノード ID および名前を構成する必要があります。 これらのパラメーターを構成するには、**set node-ID** および **set name** コマンドを使用してください。

ipxwan *ipx-circuit# routing-type timeout retryTimer*

IPXWAN ルーティング・タイプ、接続タイムアウト、再試行タイマーを設定します。**set ipxwan** コマンドを起動する前に、IPXWAN サーキットを追加しておく必要があります。

ipx-circuit#

パラメーター指定の対象となる既存の IPXWAN ポイント・ポイント・サーキットを指定します。

有効値: 既存の IPXWAN ポイント・ポイント・サーキット番号

省略時値: 1

routingType

折衝される IPXWAN ルーティング・タイプを指定します。

- **u** は非番号制 RIP
- **r** 番号制 RIP
- **b** は非番号制と番号制の両方の RIP
- **s** は静的ルーティング

有効値: 'u'、'U'、'r'、'R'、'b'、 'B'、s、'S'

省略時値: 'u'

timeout

この値は、IPXWAN 折衝を正常に完了しなければならない時間制限を秒数で指定します。接続タイマーが満了する前に正常に完了できない場合、IPXWAN は再試行タイマーを開始します。装置は、再試行タイマーが満了するまで折衝を再試行しません。

有効値: 5 ～ 300 の範囲内の整数の秒数

省略時値: 60 秒

retryTimer

このパラメーターは、接続タイマーが満了してから接続の再確立を試みるまでに待機する時間の長さを指定します。

有効値: 5 ～ 600 の範囲内の整数の秒数

省略時値: 60 秒

例: set ipxwan

```
IPX circuit number [1]? 3
Routing type ('u'=Unnumbered, 'r'=RIP, 'b'=Both, 's'=Static) [u]
Connection Timeout (in sec) [60]?
Retry timer (in sec) [60]?
```

keepalive-table-size *value*

活動保持テーブルが保持する項目の数を設定します。これらの項目には、WAN リンクを介して接続されている現行のすべてのクライアント/サーバーおよびサーバー/サーバーのペアが含まれます。

有効値 : 1 ～ 250

省略時値 : 32

例: set keepalive-table-size

```
Number of entries [32]?
```

local-cache size *size*

ローカル・キャッシュルーティング・テーブルのサイズを指定します。

ローカル・キャッシュのサイズは、各ルーターのローカル・ネットワーク、つまりクライアント・ネットワークのクライアントの合計数に、除去要求が過剰になることを防ぐために 10% のバッファーを加えたものに等しいことが必要です。

有効値: 範囲は、1 ～ 10000 です。

省略時値: 64。 詳細については、676ページの『ローカル・キャッシュ』および 677ページの『リモート・キャッシュ』を参照してください。

例: set local-cache size

```
New IPX local node cache size [64]? 80
```

maximum routes-per-destination *routes*

IPX RIP ルート・テーブルに保管するあて先ネットワーク当りのルートの最大数を指定します。

有効値: 1 ～ 64 の範囲内の整数

省略時値: 1。複数ルートの追加情報については、666ページの『複数ルートを構成する』を参照してください。

例: set maximum routes-per-destination 8

maximum networks *size*

IPX RIP ネットワーク・テーブルのサイズを指定します。これは、IPX が稼働するインターネット内のネットワークの数を反映しています。

有効値: 1 ～ 2048

ルーターのメモリー制約により、最大テーブル・サイズを使用しないようにすることができます。

省略時値: 32。この値は、maximum total-route-entries *size* より大きいものであってはなりません。

例: set maximum networks 30

maximum services *size*

IPX SAP サービス・テーブルのサイズを指定します。これは、IPX が稼働するインターネットワーク内の SAP サービスの数が反映しています。

有効値: 1 〜 2048

ルーターのメモリー制約により、最大テーブル・サイズを使用しないようにすることができます。

省略時値: 32

例: set maximum services 30

maximum total-route-entries *size*

IPX RIP ルート・テーブルのサイズを指定します。これには、IPX が稼働するインターネットワーク内のルート (代替ルートを含む) の合計数が反映されます。

有効値: 1 〜 4096

省略時値: 32

この値は、少なくとも、*maximum networks size* 以上でなければなりません。複数ルートの詳細については、666ページの『複数ルートを構成する』を参照してください。

例: set maximum total-route-entries 40

name *router_name*

ルーターに記号名を割り当てることができます。 IPXWAN では、ルーターにノード ID とノード名が必要です。

有効値: 1 〜 47 文字からなる可変長ストリング。

router_name には、文字 A 〜 Z、0 〜 9、下線 (_)、ハイフン (-)、および「単価記号」(@) を含めることができます。

省略時値: なし

例: set name newyork_accounting

net-number *ipx-circuit# network#*

IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットの IPX ネットワーク番号を指定します。

ipx-circuit#

既存の IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを指定します。

有効値: 既存のサーキット番号

省略時値: 1

network#

IPX サーキット上で使用する IPX ネットワーク番号を指定します。 IPX ネットワーク番号 0 が有効なのは、 IPXWAN 非番号制 RIP 回線か静的ルーティング回線の場合だけです。 IPX ネットワーク番号 FFFFFFFF

は、IPX ネットワーク番号として有効な番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX 省略時ルート用として予約されていて、IPX ネットワーク番号として使用できない場合があります。 有効な IPX ネットワーク番号が構成されていないと、set コマンドは無視されます。

有効値: X'0' ～ X'FFFFFFFD'

省略時値: 1

例: set net-number

```
IPX circuit number [1]? 2
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [1]?
```

node-id *network#*

IPXWAN 内部ネットワーク番号を指定します。0、 FFFFFFFF、FFFFFFFE の各値は、内部ネットワーク番号として無効です。有効なノード ID が構成されない限り、IPXWAN は使用可能にされません。

省略時値: 1

例: set node-id 2

remote-cache size *size*

リモート・キャッシュ・ルーティング・テーブルのサイズを指定します。

リモート・キャッシュのサイズは、ルーターによって使用されるリモート・ネットワークの合計数に、除去要求が過剰になることを防ぐために 10% のバッファーを加えたものに等しいことが必要です。

有効値: 範囲は、1 ～ 10000 です。

省略時値: 64。

例: set remote-cache size

```
New IPX remote network cache size [64]? 80
```

rip-update-interval *ipx-circuit# interval*

RIP 周期的同報通信が特定の IPX サーキット上で行われる必要がある間隔を、分数で指定します。

RIP 間隔を大きくすると、WAN 回線およびダイヤル回線のトラフィックが減少します。また、ダイヤル・オンデマンド・サーキットの頻繁なダイヤルアウトも防止します。

注： 完全な RIP 公示は更新間隔による制御を受けますが、ルーターによるネットワーク・トポロジー変更の伝送は、相変わらずその確認後速やかに行われます。

ipx-circuit#

IPXWAN ポイント・ポイント・サーキットへの既存の IPX 同報通信を指定します。

有効値: 有効な IPX サーキット番号

省略時値: 1

interval

間隔を分数で指定します。

有効値: 範囲は 1 ～ 1440 分です。

省略時値: 1 分。 RIP 間隔の詳細については、664ページの『RIP 更新間隔を指定する』を参照してください。

例: set rip-update-interval

```
IPX circuit number [1]? 2
RIP Timer Value (minutes) [1]? 2
```

sap-update-interval *ipx-circuit# interval*

SAP 周期的同報通信が特定の IPX サーキット上で行われる必要がある時間の遅延を、分数で指定します。

SAP 間隔を大きくすると、WAN 回線およびダイヤル回線のトラフィックが減少します。また、ダイヤル・オンデマンド・サーキットの頻繁なダイヤルアウトも防止します。

注: 完全な SAP 公示は更新間隔による制御を受けますが、ルーターによるサービス変更の伝送は、相変わらずその確認後速やかに行われます。

ipx-circuit#

既存の IPX 同報通信サーキットや IPXWAN ポイント・ポイント・サーキットを指定します。

有効値 : 有効な IPX 番号

省略時値 : 1

interval

間隔を分数で指定します。

有効値: 範囲は 1 ～ 1440 分です。

省略時値: 1 分。

例: set sap-update-interval

```
IPX circuit number [1]? 2
SAP Timer Value (minutes) [1]? 2
```

split-horizon *heuristic enabled disabled*

IPX サーキット上で使用される水平分割のタイプを指定します。

サーキット上に単一のフレーム・リレー VC だけしかない場合は、水平分割は使用可能になり、それ以外の場合は、水平分割は使用不可になります。

一般に、水平分割は *enabled* に設定する必要があります。フレーム・リレー、ATM、X.25 の各構成での部分メッシュ同報通信サーキットでは、水平分割を使用不可にする必要がある場合があります。水平分割の詳細については、678ページの『水平分割ルーティング』を参照してください。

heuristic

フレーム・リレー IPX 同報通信サーキットを除く、IPX サーキット上で水平分割を使用可能にします。

有効値 : 有効な IPX サーキット番号

省略時値 : 1

enabled

IPX サーキット上で水平分割を使用可能にします。

有効値 : 1 ～ 1440

省略時値 : 1

disabled

IPX サーキットで水平分割を使用不可にします。

有効値 : 1 ～ 1440

省略時値 : 1

例: set split-horizon enabled 0

```
IPX circuit number [1]? 2
```

IPX サーキット・フィルター構成環境にアクセスする

IPX サーキット・フィルター構成環境にアクセスする場合は、 IPX config> プロンプトで次のようにコマンドを入力します。

```
IPX Config> filter-lists type
IPX type-List Config>
```

ここで、*type* は構成される IPX フィルターのタイプです。有効なタイプは、*router-lists*、*rip-lists*、*sap-lists*、および *ipx-lists* です。

フィルターを作成するときは、IPX サーキット番号は必須です。

IPX サーキット・フィルター構成コマンド

この節では、IPX サーキット・ベースのフィルター ; ROUTER、RIP、SAP、 IPX を構成する場合に使用するコマンドについて説明します。これらのフィルターを構成するには、IPX Config> プロンプトで filter-lists *type* コマンドを入力してから、IPX *type*-List Config> プロンプトで構成コマンドを入力します。

表 41. IPX フィルター構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Attach	指定されたフィルター・リストに指定されたフィルターを付加します。
Create	フィルターまたはフィルター・リストを作成します。
Default	フィルターの省略時アクションを、*include (組み込み)* または *exclude (除外)* に設定します。
Delete	フィルターまたはフィルター・リストを削除します。
Detach	フィルターからフィルター・リストを切り離します。
Disable	フィルターを使用不能にします。
Enable	フィルターを使用可能にします。
List	現行のフィルター構成を表示します。
Move	フィルターに付加されたフィルター・リストの順序を変えます。
Set-cache	指定されたフィルターについてキャッシュ・サイズを設定します。
Update	IPX *type*-List *filter-list* Config> プロンプトにアクセスします。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Attach

attach コマンドは、フィルター・リストをフィルターに付加するのに使用します。

構文 :

attach *list-name* *filter#*

list-name
フィルター・リストの名前を指定します。 **list** コマンドを使用して、構成済みのフィルター・リスト名のリストを表示することができます。

有効値: 最大 16 文字の、任意の英数字ストリング

省略時値: なし

filter#
フィルターの番号を指定します。構成済みのフィルターの番号付きリストは、list コマンドを使用して入手することができます。

例: attach test_list 1

Create

create コマンドは、フィルター・リストまたはフィルターを作成するのに使用します。

構文 :

create list ...

filter ...

list *list-name*
指定された名前でリストを作成します。

有効値: 最大 16 文字の、任意の英数字ストリング

省略時値: なし

リスト名を指定しないで **create list** コマンドを入力することもできます。その場合は、リスト名を入力するようプロンプト指示されます。

例: create list example_list

filter *direction ipx-circuit#*
指定したサーキット上で指定した方向に関するフィルターを作成します。指定したサーキット上で受信されたパケットをフィルターする場合は、*input* を指定します。指定したサーキットで送信されるパケットをフィルターする場合は、*output* を指定します。

フィルターが作成されると、番号が自動的に割り当てられ、その時点以降は、後続のコマンドすべてで、サーキットと方向 (入力か出力か) をキーで入力しなくても、この番号を使用してフィルターを識別します。

例: create filter input 1

Default

default コマンドは、フィルター用の省略時処置を設定するのに使用します。フィルター項目のどれについても一致が見つからない場合は、省略時処置が取られます。

構文 :

default *action filter#*

例: `default exclude 1`

action
省略時処置を指定します。**Include (組み込み)** は、フィルター項目のどれにも一致が見つからない場合、パケットが処理されることを指定します。**Exclude (排除)** は、一致が見つからない場合に、パケットが除外されることを示します。

filter#
フィルターの番号を指定します。構成されたフィルターの番号付きリストを表示するには、**list** コマンドを使用してください。

Delete

delete コマンドは、フィルター・リストまたはフィルターを削除するのに使用します。

構文 :

delete list ...
filter ...

list *list-name*
指定されたリストを削除します。list コマンドを使用して、構成済みのフィルター・リスト名を表示することができます。

例: `delete list example_list`

filter *filter#*
指定したフィルターを削除します。list コマンドを使用して、構成済みのフィルターの番号付きリストを表示することができます。

例: `delete filter 1`

Detach

detach コマンドは、フィルターからフィルター・リストを切り離すのに使用します。

構文 :

detach *list-name filter#*

list-name
フィルター・リストの名前を指定します。 list コマンドを使用して、構成済みのフィルター名のリストを表示することができます。

有効値: 最大 16 文字の、任意の英数字ストリング

省略時値: なし

filter#
フィルターの番号を指定します。 list コマンドを使用して、構成済みのフィルターの番号付きリストを表示することができます。

例: `detach test_list 1`

Disable

disable コマンドは、グローバルなフィルターを使用不能にしたり、特定のフィルターについて使用不能にするのに使用します。

構文 :

disable all
filter ...

all 現行タイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターを使用不能にします。

例: disable all

filter *filter#*
指定したフィルターを使用不能にします。構成済みのフィルターの番号付きリストを表示するには、list コマンドを使用してください。

例: disable filter 1

Enable

enable コマンドは、フィルターをグローバルに、または指定したフィルターについて使用可能にするのに使用します。

構文 :

enable all
filter ...

all 現行タイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターを使用可能にします。

例: enable all

filter *filter#*
指定したフィルターを使用可能にします。構成済みのフィルターの番号付きリストを表示するには、list コマンドを使用してください。

例: enable filter 1

List

list コマンドは、現行のフィルター・タイプをグローバルに表示したり、特定のフィルターについての情報を表示するのに使用します。

構文 :

list all

filter ...

all 現行のタイプのすべてのフィルターの状態についての情報をリストします。

例: list all

```
Filtering: ENABLED

Filter Lists:
Name                           Action
------------------------------ ----------
ipx01                          EXCLUDE
ipx02                          INCLUDE
ipx03                          EXCLUDE

Filters:
Id    Circ  Ifc   Direction  State      Default    Cache
----- ----- ----- ---------- ---------- ---------- -----
1     3     2     INPUT      ENABLED    INCLUDE       10
2     2     1     INPUT      ENABLED    INCLUDE       10
```

filter *filter#*

指定したフィルターについての情報をリストします。構成済みのフィルターの番号付きリストを表示するには、list コマンドを使用してください。

例 : list filter 2

```
Filters:
Id    Circ  Ifc   Direction  State      Default    Cache
----- ----- ----- ---------- ---------- ---------- -----
2     2     1     INPUT      ENABLED    INCLUDE       10

Filter Lists:
Name                           Action
------------------------------ ----------
ipx01                          EXCLUDE
```

Move

move コマンドは、フィルター内のフィルター・リストの配列を変更するのに使用します。パケットはリストが発生する順にフィルター・リストと突き合わせて評価されます。最初の一致でフィルター・プロセスが停止します。

構文 :

move *src-list-name dst-list-name filter#*

src-list-name
フィルター内で移動されるリストを指定します。

dst-list-name
その前で src-list-name が移動されるリストを指定します。

filter#
リストが属するフィルターを指定します。構成済みのフィルターのリストおよびそれらの付加されたフィルター・リストを表示するには、list コマンドを使用することができます。

例: move test-list-1 test-list-2 2

Set-cache

set-cache コマンドは、フィルター・キャッシュのサイズを設定するのに使用します。フィルター・キャッシュがサポートされるのは、IPX サーキット・フィルターの場合だけであり、ROUTER、RIP、SAP のサーキット・フィルターでは、キャッシュをサポートしません。

構文 :

set-cache *size filter#*

size
フィルター・キャッシュのサイズ (項目の数) を指定します。

有効値: 4 〜 64 キャッシュ項目

省略時値: 10 項目

filter#
フィルターの番号を指定します。list コマンドを使用して、構成済みのフィルターの番号付きリストを表示することができます。

例: `set-cache 10 1`

Update

update コマンドは、`IPX` *`type`*`-List` *`list-name`* `Config>` プロンプトにアクセスします。このプロンプトから、更新中のリスト内の項目を追加、削除、または移動するコマンドを出すことができます。このプロンプトから、更新中のフィルター・リスト用のアクションを設定することもできます。

構文 :

update *list-name*

list-name
フィルター・リストの名前を指定します。list コマンドを使用して、構成済みのフィルター・リスト名を表示することができます。

例: `update test-list`

Add (Update サブコマンド)

add サブコマンドは、フィルター・リストに項目を追加するのに使用します。リスト項目パラメーターは、構成中のサーキット・フィルターのタイプ (ROUTER、RIP、SAP、IPX) に応じて異なります。すべてのタイプのサーキット・フィルターに関して、**add** コマンドは、パラメーターなしで入力できます。そうすると、必要なパラメーターを入力するようプロンプト指示されます。

Add (ROUTER)

構文 :

add *node-number mask*

node-number

(マスクとの AND (論理積) を取られた後) RIP 応答パケットを送信したルーターの発信元ノード番号と比較される値を指定します。単一のノード上で突き合わせたい場合は、node-number パラメーターをアドレスに設定し、マスクを FFFFFFFFFFFF に設定します。すべてのノード上で突き合わせたい場合は、node-number パラメーターと mask パラメーターを 000000000000 に設定します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

省略時値: なし

mask

(アドレス・パラメーターと比較される前に) RIP 応答パケットを送信したルーターの発信元ノード・アドレスと AND (論理積) を取られる値を指定します。

単一のアドレスで突き合わせたい場合は、address パラメーターをそのアドレスに設定し、mask (マスク) を FFFFFFFFFFFF に設定してください。すべてのアドレスで突き合わせたい場合は、address (アドレス) パラメーターおよび mask (マスク) パラメーターを 000000000000 に設定します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

省略時値: X'FFFFFFFFFFFF'

例: add 400000001000 ffffffff0000

Add (RIP)

構文 :

add *net-range-start net-range-end*

net-range-start

フィルターされる IPX ネットワーク番号の範囲 (両端の数を含む) の始めを指定します。単一のネットワーク番号で突き合わせたい場合は、 net-range-start および net-range-end パラメーターをそのネットワーク番号に設定してください。すべてのネットワーク番号で突き合わせたい場合は、net-range-start を X'00000001' に設定し、net-range-end を X'FFFFFFFE' に設定します。

有効値: X'1' ～ X'FFFFFFFE'

省略時値: X'1'

net-range-end

フィルターされる IPX ネットワーク番号の範囲 (両端の数を含む) の終わりを指定します。

有効値: X'1' ～ X'FFFFFFFE'

省略時値: X'1'

例: add 00000001 FFFFFFFE

Add (SAP)

構文 :

add *comparitor hops sap-type name*

comparitor
このリスト項目用のホップ・カウント比較演算子のタイプを指定します。

有効値:

<
<=
=
>=
>

省略時値: <= comparitor (比較演算子) および hops (ホップ) パラメーターは出力フィルターでは無視されます。

hops
このリスト項目用のホップ・カウントを指定します。ホップ・カウントに基づいてフィルターしたくない場合は、比較演算子およびホップ・カウントについて <= 16 を入力してください。comparitor (比較演算子) および hops (ホップ) パラメーターは出力フィルターでは無視されます。

有効値: 0 〜 16

省略時値: 16

sap-type
フィルターされるサービス・タイプを指定します。サービス・タイプを入力するか、すべてのサービス・タイプに X'0000' を入力してください。

有効値: X'0' 〜 X'FFFF'

省略時値: 4

name
フィルターされるサービス名を指定します。

有効値:

1 〜 47 個の ASCII 文字 (X'20' 〜 X'7E') のストリング

疑問符 (?) およびアスタリスク (*) 文字は、ワイルドカード文字として機能します。疑問符は、サービス名の中の任意の単一文字を表すために複数回使用することができます。アスタリスクは、サービス名の任意の部分を表すために複数回使用することができます。疑問符とアスタリスクを一緒に使用することができます。

省略時値: なし

例: `add < 6 0004 *`

Add (IPX)

構文 :

add *comparitor hops ipx-type dst-net-range-start dst-net-range-end dst-node dst-mask dst-sck-range-start dst-sck-range-end src-net-range-start src-net-range-end src-node src-mask src-sck-range-start src-sck-range-end*

comparitor
このリスト項目用のホップ・カウント比較演算子のタイプを指定します。comparitor (比較演算子) および hops (ホップ) パラメーターは出力フィルターでは無視されます。

有効値:

- <
- <=
- =
- >=
- >

省略時値: <=

hops
このリスト項目用のホップ・カウントを指定します。ホップ・カウントに基づいてフィルターしたくない場合は、比較演算子およびホップ・カウントについて <= 16 を入力してください。comparitor (比較演算子) および hops (ホップ) パラメーターは出力フィルターでは無視されます。

ipx-type
フィルターされる IPX パケット・タイプを指定します。パケット・タイプを入力するか、すべてのパケット・タイプについて 00 を入力してください。

有効値: X'0' ～ X'FF'

省略時値: X'0'

dst-net-range-start
フィルターされるあて先 IPX ネットワーク番号の範囲 (両端の数を含む) の始めを指定します。単一のネットワーク番号で突き合わせたい場合は、dst-net-range-start および dst-net-range-end パラメーターをそのネットワーク番号に設定してください。すべてのネットワーク番号で突き合わせたい場合は、dst-net-range-start を X'00000001' に設定し、dst-net-range-end を X'FFFFFFFE' に設定します。

有効値: X'00000000' ～ X'FFFFFFFF'

省略時値: X'00000000'

dst-net-range-end
フィルターされるあて先 IPX ネットワーク番号の範囲 (両端の数を含む) の終わりを指定します。単一のネットワーク番号で突き合わせたい場合は、dst-net-range-start および dst-net-range-end パラメーターをそのネットワーク番号に設定してください。すべてのネットワーク番号で突き合わせたい場合は、dst-net-range-start を X'00000001' に設定し、dst-net-range-end を X'FFFFFFFE' に設定します。

有効値: X'00000000' ～ X'FFFFFFFF'

省略時値: X'00000000'

dst-node
(dst-mask との AND (論理積) を取られた後) あて先ノード・アドレスと比較される値を指定します。単一のノード上で突き合わせたい場合は、 dst-node パラメー

ターをノード番号に設定し、 dst-mask を X'FFFFFFFFFFFF' に設定します。すべてのノード上で突き合わせたい場合は、dst-node パラメーターと dst-mask パラメーターを X'000000000000' に設定します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

省略時値: X'000000000000'

dst-mask

(dst-address パラメーターと比較される前に) あて先ノード・アドレスと AND (論理積) を取られる値を指定します。単一のアドレスで突き合わせたい場合は、address パラメーターをそのアドレスに設定し、dst-mask (マスク) を X'FFFFFFFFFFFF' に設定してください。すべてのアドレスで突き合わせたい場合は、dst-address (アドレス) パラメーターおよび dst-mask (マスク) パラメーターを X'000000000000' に設定します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

省略時値: X'000000000000'

dst-sck-range-start

フィルターされるあて先 IPX ソケットの範囲 (両端の数を含む) の初めを指定します。単一のソケットで突き合わせたい場合は、dst-sck-range-start および dst-sck-range-end パラメーターをそのソケットに設定してください。すべてのソケットで突き合わせたい場合は、dst-sck-range-start を X'0000' に設定し、dst-sck-range-end を X'FFFF' に設定してください。

有効値: X'0000' ～ X'FFFF'

省略時値: 0

dst-sck-range-end

フィルターされるあて先 IPX ソケットの範囲 (両端の数を含む) の範囲の末尾を指定します。単一のソケットで突き合わせたい場合は、dst-sck-range-start および dst-sck-range-end パラメーターをそのソケットに設定してください。すべてのソケットで突き合わせたい場合は、dst-sck-range-start を X'0000' に設定し、dst-sck-range-end を X'FFFF' に設定してください。

有効値: X'0000' ～ X'FFFF'

省略時値: 0

src-net-range-start

フィルターされる発信元 IPX ネットワーク番号の範囲 (両端の数を含む) の初めを指定します。単一のネットワーク番号で突き合わせたい場合は、src-net-range-start および src-net-range-end パラメーターをそのネットワーク番号に設定してください。すべてのネットワーク番号で突き合わせたい場合は、src-net-range-start を X'00000001' に設定し、src-net-range-end を X'FFFFFFFE' に設定します。

有効値: X'00000000' ～ X'FFFFFFFE'

省略時値: X'00000000'

src-net-range-end

フィルターされる発信元 IPX ネットワーク番号の範囲 (両端の数を含む) の末尾を指定します。単一のネットワーク番号で突き合わせたい場合は、src-net-range-start および src-net-range-end パラメーターをそのネットワーク番号

に設定してください。すべてのネットワーク番号で突き合わせたい場合は、src-net-range-start を X'00000001' に設定し、src-net-range-end を X'FFFFFFFE' に設定します。

有効値: X'00000000' ～ X'FFFFFFFE'

省略時値: X'00000000'

src-node

(src-mask との AND (論理積) を取られた後) 発信元ノード番号と比較される値を指定します。単一のノード上で突き合わせたい場合は、src-node パラメーターをノード番号に設定し、src-mask を X'FFFFFFFFFFFF' に設定します。すべてのノード上で突き合わせたい場合は、src-node パラメーターと src-mask パラメーターを X'000000000000' に設定します。

有効値: X'00000000' ～ X'FFFFFFFF'

省略時値: X'00000000'

src-mask

(src-address パラメーターと比較される前に) 発信元ノード・アドレスと AND (論理積) を取られる値を指定します。単一のアドレスで突き合わせたい場合は、address パラメーターをそのアドレスに設定し、src-mask (マスク) を X'FFFFFFFFFFFF' に設定してください。すべてのアドレスで突き合わせたい場合は、src-address (アドレス) パラメーターおよび src-mask (マスク) パラメーターを X'000000000000' に設定します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

省略時値: X'000000000000'

src-sck-range-start

フィルターされる発信元 IPX ソケットの範囲 (両端の数を含む) の初めを指定します。単一のソケットで突き合わせたい場合は、src-sck-range-start および src-sck-range-end パラメーターをそのソケットに設定してください。すべてのソケットで突き合わせたい場合は、src-sck-range-start を X'0000' に設定し、src-sck-range-end を X'FFFF' に設定してください。

有効値: X'0000' ～ X'FFFF'

省略時値: X'0000'

src-sck-range-end

フィルターされる発信元 IPX ソケットの範囲 (両端の数を含む) の末尾を指定します。単一のソケットで突き合わせたい場合は、src-sck-range-start および src-sck-range-end パラメーターをそのソケットに設定してください。すべてのソケットで突き合わせたい場合は、src-sck-range-start を 0000 に設定し、src-sck-range-end を FFFFF に設定してください。

有効値: X'0000' ～ X'FFFF'

省略時値: X'0000'

例 :

```
add  <= 16  0  00000004 00000004 000000000000 000000000000
0000 FFFF 0000005A 0000006A 000000000000 000000000000 0000 FFFF
```

この例は、IPX ネットワーク 5A から 6A を経由して IPX ネットワーク 4 に至るすべてのパケットをフィルターします。

Delete (Update サブコマンド)

delete サブコマンドは、現行のフィルター・リストから項目を削除するのに使用します。

構文 :

delete *item#*

item#
リスト内の項目の数を指定します。この数は、フィルター・リスト内の項目をリストするための list コマンドを使用して入手することができます。

例: delete 4

List (Update サブコマンド)

list サブコマンドは、フィルター・リストのアクションを表示し、フィルター項目をリストするのに使用します。

構文 :

list

例 : list

```
IPX IPX-List 'ipx01' Config>list
Action: EXCLUDE
Id   Hops Type Net Range           Address      Mask         Sock Range
---- ---- ---- ------------------- ------------ ------------ -----------
1    <=16    0     4320 -     4324 4000003A0002 FFFFFFFFFFFF    0 - FFFF (Dest)
                   3A33 -    13A33 400000010000 FFFFFFFF0000    0 - FFFF (Source)
```

Move (更新サブコマンド)

move サブコマンドは、フィルター項目の配列を変更するのに使用します。フィルター項目の配列を変更した後、それらは新しい配列を反映するために番号を付け直されます。list コマンドを使用して、構成済みのフィルター項目の番号付きリストを表示することができます。

src-line# パラメーターは、移動すべき行を示します。この行は、*dest-line#* パラメーターによって指定された項目の前にくるよう移動されます。

構文 :

move *src-line# dest-line#*

例: move 5 2

Set-action (Update サブコマンド)

set-action サブコマンドは、フィルター・リストが合致したときに取られる処置を示すのに使用します。

IPX サーキット・フィルター構成コマンド (Talk 6)

構文 :

set-action include

exclude

include

現行のフィルターと一致した場合は、ROUTER および IPX フィルターについてパケットが処理される (組み込まれる) ことを指定します。RIP および SAP フィルターの場合、**include** は RIP または SAP 項目が処理されることを指定します。

例: set-action include

exclude

現行のフィルターと一致した場合は、ROUTER および IPX フィルターについてパケットが除去される (除外される) ことを指定します。RIP および SAP フィルターについて、**exclude** は、一致した場合は RIP または SAP 項目が無視されることを指定します。

例: set-action exclude

IPX 監視環境にアクセスする

IPX 監視環境にアクセスする方法についての説明は、*ソフトウェア 使用者の手引き* の「はじめに (ユーザー・サーキットの概要)」を参照してください。

IPX 監視コマンド

表42 に、IPX 監視コマンドをリストします。 IPX 監視コマンドを使用すると、IPX パケットを送信するサーキットとネットワークのパラメーターと統計を表示させて見ることができます。監視コマンドは、物理レベル、フレーム・レベル、およびパケット・レベルの構成値を表示します。 3 つのプロトコル・レベルすべてについての値を一度に見るためのオプションもあります。

IPX 監視コマンドは、IPX> プロンプトで入力してください。 表42 に、IPX 監視コマンドをリストします。

表 42. IPX 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルに使用可能なコマンドをすべて表示したり、特定のコマンド (使用可能な場合) のオプションをリストしたりします。 xxxiiiページの『ヘルプの入手』 を参照してください。
Access-controls	グローバル IPX フィルター (アクセス制御) が使用可能にされているかどうか、IPX アクセス制御ステートメント、および各アクセス制御ステートメントに一致したパケットの数を表示します。
Cache	ルーティング・キャッシュの現行の内容をリストします。
Counters	ルーティング・エラーおよびパケット・オーバーフローの数を表示します。
Delete keepalive connection	キープアライブ・フィルター・テーブル項目を削除します。
Disable	グローバルに、または特定の IPX サーキット上で、 IPX を使用不可にします。

表 42. IPX 監視コマンドの要約 (続き)

コマンド	機能
Dump routing tables	ルーティング・テーブルの内容を表示します。
Enable	グローバルに、または特定の IPX サーキット上で、 IPX を使用可能にします。
Filters	グローバル SAP フィルターが使用可能にされているかどうか、SAP フィルター・ステートメント、およびフィルターされた SAP 公示のカウントを表示します。
Filter-Lists	IPX サーキット・フィルター・コンソールにアクセスします。ここで、RIP ルーター、RIP SAP、IPX サーキット・ベースのフィルターが監視できます。
IPXWAN	IPXWAN ポイント・ポイント・サーキットに関する IPXWAN 情報を一覧表示します。
Keepalive	キープアライブ・フィルター・テーブル内の各アクティブ・クライアント/サーバー接続の状況を表示します。
List	使用可能にされているそれぞれのサーキットの現行構成や IPX アドレスを一覧表示します。
Ping	IPXPING パケットを別のホストに送信し、応答を観察します。このコマンドを使用して、インターネットワーク環境での問題を分離できます。
Recordroute	IPXPING レコード・ルート・パケットを別のホストに送信し、応答を観察します。このコマンドを使用して、この装置と別のホストとの間の往復ルートを記録して表示することができます。この情報は、インターネットワーク環境での問題を分離するのに使用できます。
Reset	特定の IPX サーキット、グローバル SAP フィルター、グローバル IPX フィルター (アクセス制御)、静的ルート、静的サービス、またはルーター、RIP、SAP、または IPX サーキット・ベースのフィルター (フィルター・リスト) をリセットします。
Sizes	ローカル・ノード・キャッシュおよびリモート・ネットワーク・キャッシュの構成済みサイズ、および現在使用中のキャッシュ項目の数を表示します。
Slist	IPX SAP サーバー・テーブルの内容を表示します。
Traceroute	IPXPING トレース・ルート・パケットを別のホストに送信し、応答を観察します。このコマンドを使用して、この装置からあて先ホストに到達するまでにパケットがとる各ホップを追跡し、表示できます。この情報は、インターネットワーク環境での問題を分離するのに使用できます。
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Access Controls

access-controls コマンドは、グローバル IPX フィルター (アクセス制御) の状況、IPX アクセス制御ステートメント、および各制御ステートメントに従った回数のカウントをリストするのに使用します。

構文 :

access-controls

例: access-controls

```
IPX Access Controls:  Enabled
#   T Dest Net Host         Sock Sock Src Net  Host         Sock  Sock Count
1   E 2        000000000000 0    FFFF 3        000000000000 0     FFFF 0
```

アクセス制御指標番号

Type 特定のアドレスまたはアドレスの組み合わせにパケットが送信されたか、除去されたかを識別します。I は include (組み込み) を意味します。この場合、パケットは送信できます。 E は exclude (排除) を意味します。この場合、ルーターはパケットを廃棄します。

Dest-net
あて先のネットワーク番号。ゼロ (0) はすべてのネットワークを意味します。

Dest-host
あて先ネットワークのホスト番号 (0) は、ネットワーク上のすべてのホストを意味します。

Dest-sck
あて先ソケットの範囲 (両端の数を含む) を指定する 2 つの数。

Src-net
発信元のネットワーク番号。ゼロ (0) はすべてのネットワークを意味します。

Src-host
発信元ネットワーク上のホスト番号。ゼロはネットワーク上のすべてのホストを意味します。

Src-sck
発信元ソケットの範囲 (両端の数を含む) を指定する 2 つの数

Count 各アクセス制御ステートメントに一致し、対応するタイプ (組み込みまたは排除) が実行されることになる着信 IPX パケットの数を指定します。

Cache

cache コマンドは、IPX ルーティング・キャッシュの内容を表示するのに使用します。

構文 :

cache

例: cache

```
Dest Net/Node          Use Count      via Net/Node          Circ  Ifc
     420               1                  412/000004200000  3     2
     412               1                  412/000000000000  3     2
     412/000004200000  1                  412/000004200000  3     2
```

最初の項目では、リモート・ネットワーク 420 は、IPX ネットワーク番号 412 のシリアル・サーキットを通して到達できることを示します。2 番目の項目は IPX ネットワーク 412 です。これはルーターに直接接続されたイーサネットです。この項目は、汎用ローカル・ネットワーク項目です。 直接接続されたネットワークが IPX パケットの転送を開始した後、それらのネットワークのそれぞれについて 1 つの汎用ローカル・ネットワーク項目ができます。 最後の項目はイーサネット上のローカル項目です。この IPX キャッシュは、ネット番号 412 上の IPX ノード番号 0000 0420 0000 にパケット 1 つを送信するのに使用されました。

Counters

counters コマンドは、発生したルーティング・エラーおよびパケット・オーバーフローの数を表示するのに使用します。例では、カウンターは記録されたエラーがないことを示しています。

構文 :

counters

例: counters

```
Routing errors
Count  Type
0      Unknown
0      Checksum error
0      Destination unreachable
0      Hop count expired
0      circuit size exceeded

Destination errors
Count  Type
0      Unknown
0      Checksum error
0      Non-existent socket
0      Congestion

IPX input packet overflows
Circ   Ifc    Name        Count
1      0       Eth/0      0
2      1       PPP/0      0
3      2       PPP/1      0
```

Routing Errors

Unknown
あて先に到達する前に、不特定エラーが発生しました。

Checksum
チェックサムが正しくないか、パケットがあて先に到達する前に他の何らかの重大な矛盾が発生しました。

Destination unreachable
あて先ホストがここから到達できません。

Hop count expired
パケットが 15 のインターネット・ルーターを通過しましたが、あて先に到達しませんでした。

circuit size exceeded
パケットが、中間ネットワークを介して転送されるには大き過ぎます。

Destination errors

Unknown
あて先で、不特定エラーが検出されました。

Checksum
チェックサムが正しくないか、あて先でパケットに他の何らかの重大な矛盾が検出されました。

Nonexistent socket
指定したソケットが指定したあて先ホストに存在していません。

Congestion
資源が不足しているためあて先はパケットを受け入れることができません。

IPX 入力パケットのオーバーフロー

Net サーキット名を指定します。

Count 資源制限のため受信できない可能性のあるパケットの数を指定します。

Delete

delete コマンドは、キープアライブ・フィルター・テーブル項目を除去するのに使用します。

構文 :

delete *entry#*

entry# 削除すべきテーブル項目を指定します。**Keepalive** コマンドを使用して、キープアライブ・フィルター・テーブルの内容をリストすることができます。

例: `delete 1`

Disable

disable コマンドは、グローバルに、または特定のサーキット上で IPX を使用不可にする場合に使用します。

構文 :

disable circuit ...

ipx

circuit *ipx-circuit#*
ipx-circuit# で指定された IPX サーキットを使用不可にします。IPX は、**enable** コマンドを使用して再使用可能にすることができます。

例 : `disable circuit 2`

ipx すべての IPX サーキット上でグローバルに使用不可にします。 IPX は、**enable** コマンドを使用すると、再度グローバルに使用可能にすることができます。

例: `disable ipx`

Dump

dump コマンドは、ルーティング・テーブルの内容を表示させる場合に使用します。

構文 :

dump

例: `dump`

```
Type Dest Net Hops Delay Age(M: S)   via Router        Circ  Ifc
Dir  412      0    6        0: 0      412/000004000000 3     2
Dir  400      0    1        0: 0      400/020000000400 1     0
Dir  411      0    1        0: 0      411/400000000400 2     1
Stat 1        3    2        0: 0      400/010101010101 1     0
RIP  420      1    7        0:30      412/000004200000 3     2
Stat 444      2    2        0: 0      400/400000000444 1     0
Stat FFFFFFFD 14   3000     0: 0      400/111111111111 1     0
```

Type

- Dir - このネットワークがルーターに直接接続されていることを指定します。
- RIP - このルートが IPX ルーティング・プロトコル、RIP によって提供されたことを指定します。
- Old - このルートがタイムアウトになり、もはや使用されないことを指定します。このルートは短時間テーブル内に留まり、他のルートにこのルートが無効になったことを通知します。この短時間間隔の経過後は、表示されなくなります。
- Stat - これが静的ルートであることを指定します。

Dest net
あて先ネットワーク番号を指定します。

Hops このあて先までのホップの数を指定します。

Delay ルーターがパケットを転送するのに要する時間、およびパケットがその着信先に到達するのに要する時間の推定値を指定します。遅延の単位は、576 バイトのパケットを送信するのに IBM PC のクロックがカチカチと刻む回数 (1 秒につき 18.21 回のクロック・ティック) です。最小限の遅延は 1 単位です。

Age ルーティング情報の経過時間を分と秒で指定します。ルーティング・テーブルの項目が更新されない場合は、ルーターは次のアクションを取ります。

- RIP 更新間隔が 3 回経過すると、ルートは Old と指定され、ルーターはそのルートが無効になったことを公示します。RIP 更新間隔は、IPX **config** コマンドを使用して表示できます。 RIP 間隔の詳細については、664ページの『RIP 更新間隔を指定する』を参照してください。
- さらに 60 秒が経過すると、そのルートは削除され、ダンプ画面に表示されなくなります。

Via router
直接接続されていないネットワークに進むパケットの次のホップを指定します。直接接続されたネットワークの場合は、パケットを送信するルーター・サーキットのアドレスです。

Circ IPX サーキット番号

Ifc ネットワーク・インターフェース番号

表示画面の最上部には、使用されるルートおよびネットワーク項目の数、および使用可能な総数が示されます。すべてのネットワーク項目が使用された場合は、ルーティング・テーブルが十分に大きくないことがありえます。サイズを拡大するには、IPX 構成の **set maximum networks** コマンドを使用してください。

ルート項目がすべて使用された場合は、IPX ネットワークへのルートのうち、新しい着信ネットワークを含めて、記録できないものもあります。使用可能なルートの数を増やしたくない場合は、ネットワーク当りのルートの最大数を減らします。

Enable

enable コマンドは、IPX をグローバルに、または特定のサーキット上で使用可能にする場合に使用します。

構文 :

enable circuit ...

ipx

circuit *ipx-circuit#*

ipx-circuit# で指定されたサーキット上で IPX を使用不可にします。IPX を使用可能にする前に、サーキットの IPX ネットワーク番号を構成しておく必要があります。

例 : enable circuit 2

ipx 使用可能にされている IPX サーキットすべてでグローバルに IPX を使用可能にします。

例: enable ipx

Filters

filters コマンドは、グローバル SAP フィルターが使用可能かどうか、SAP フィルター・ステートメント、およびフィルターされた SAP 公示のカウントを表示するのに使用します。

構文 :

filters

例: filters

```
IPX SAP Filters:  Enabled
Count  Max Hops  Type  Service Name
0      5         4     FILESRV01
```

Count フィルターされた (廃棄された) SAP 公示の数を示します。

Max Hops
サービスに許容される最大ホップ数を示します。

Type 数値サービス・クラスです。

Service name
サービスに名前が付いている場合には、サービスの名前です。

Filter-lists

filter-lists コマンドは、IPX *type*-Lists> プロンプトにアクセスするのに使用します。有効なタイプは、router-lists、rip-lists、sap-lists、および and ipx-lists です。

このプロンプトから使用可能なコマンドについては、738ページの『IPX サーキット・フィルター監視コマンド』を参照してください。

構文 :

filter-lists router-lists
rip-lists
sap-lists
ipx-lists

例: filter-lists router-lists

IPXWAN

ipxwan コマンドは、IPXWAN ポイント・ポイント・サーキットに関する IPXWAN 情報を一覧表示させる場合に使用します。

構文 :

ipxwan detailed . . .
summary

detailed *ipx-circuit#*
指定された IPX サーキットに関する IPXWAN 情報を一覧表示します。

例 : ipxwan detailed 3

```
Detailed information for IPXWAN link over circuit 3 interface 2, PPP/1
This side is the IPXWAN slave
Neighbor Name: ipxwan-420
Neighbor Node ID: 420
Negotiated Routing Type: RIP/SAP
Link Delay: 6 1/18th sec ticks
Common Net#: 412
Connection Timeouts: 0
Connection Retries: 0
Timer Requests Sent: 1
Timer Requests Received: 1
Timer Responses Sent: 1
Timer Responses Received: 0
Info Requests Sent: 0
Info Requests Received: 1
Info Responses Sent: 1
Info Responses Received: 0
```

Neighbor Name
RIP/SAP 情報要求パケットで受信された近隣のルーター名

Neighbor Node ID
近隣のノード ID (1 次ネットワーク番号としても知られている)。これは、インターネットワーク全体を通じて固有な IPX ネットワーク番号です。 これは 32 ビットの数量です。

Negotiated Routing Type
折衝されたルーティング・タイプ。現在サポートされているのは、RIP/SAP、非番号制 RIP、静的ルーティングです。非番号制 RIP と静的ルーティングが折衝されたルーティング・タイプである場合は、リンク上で共通ネットワーク番号は必要ありません。

Link Delay
マスターによって計算された 1/18 秒のティック数で示したリンク遅延。これは 16 ビットの数量です。これは常に計算されるため、省略時値はありません。

Common Net#
リンクの両端によって合意されたネットワーク番号。 この番号はインターネットワーク全体を通じて固有でなければなりません。これは 32 ビットの数量です。折衝されたルーティング・タイプが非番号制 RIP と静的ルーティングのどちらかであるときは、値 0 が **IPXWAN detailed** コマンドと **IPXWAN summary** コマンドの共通 Net# として表示されます。省略時値はありませんので、折衝される必要があります。

Connection Timeouts
接続がタイムアウトになった回数。IPXWAN パケットの交換が進行しない場合は、接続が周期的にタイムアウトになります。**set ipxwan** コマンドを使用して、タイムアウト期間を構成することができます。タイムアウト期間の省略時値は 60 秒です。

Connection Retries
タイムアウトになった後に接続が再試行される回数。待機する時間 (再試行まで) は、**set ipxwan** コマンドを使用して構成可能です。省略時値は 60 秒です。

Timer Requests Sent
送信された IPXWAN タイマー要求パケットの数

Timer Requests Received
受信された IPXWAN タイマー要求パケットの数

Timer Responses Sent
送信された IPXWAN タイマー応答パケットの数

Timer Responses Received
受信された IPXWAN タイマー応答パケットの数

Info Requests Sent
送信された IPXWAN 情報要求パケットの数

Info Requests Received
受信された IPXWAN 情報要求パケットの数

Info Responses Sent
送信された IPXWAN 情報応答パケットの数

Info Responses Received
受信された IPXWAN 情報応答パケットの数

summary
すべての IPXWAN ポイント・ポイント・サーキットに関する IPXWAN 要約情報を一覧表示します。

例: ipxwan summary

```
Circ   Ifc    Name        Common Net#  NodeID   Neighbor Name
3      2       PPP/1      412          420      ipxwan-420
```

Circ IPX サーキット番号

Ifc ネットワーク・インターフェース番号

Common Net#
リンクの両端によって合意されたネットワーク番号。 この番号はインターネットワーク全体を通じて固有でなければなりません。折衝されたルーティング・タイプが非番号制 RIP と静的ルーティングのどちらかであれば、共通 net# は 0 です。

NodeID
近隣のノード ID (内部ネットワーク番号とも呼ばれる)

Neighbor Name
RIP/SAP 情報要求パケットで受信された近隣のルーター名

Keepalive

キープアライブ・フィルター・テーブル内の各アクティブ・クライアント/サーバー接続の状況を示します。

構文 :

keepalive

例 :

```
Keepalive
Conn #     Net  /   Node     /Sock        Net  /   Node     /Sock
          ------------------------------------------------------------------
0         272727/000000000001/4001 &lt;->      302/0000C911EF1C/4004
                (server conn # 1, conn type: passive, last heard  1:00 ago)
1         272727/000000000001/4001 &lt;->      302/0000C911B0D9/4004
                (server conn # 2, conn type: passive, last heard  1:00 ago)
```

List

list コマンドは、使用可能にされている IPX サーキットの現行構成や IPX アドレスを一覧表示させる場合に使用します。

構文 :

list *addresses*

configuration

addresses
使用可能にされているそれぞれの IPX サーキットのアドレスを一覧表示します。

例 :

```
Circ   Ifc    Name        Type                          Network/Address
1      0       Eth/0      Ethernet                      400/020000000400
2      1       PPP/0      SCC Serial Line               411/400000000400
3      2       PPP/1      SCC Serial Line               412/000004000000
```

Configuration
現行 IPX 構成を一覧表示します。このコマンドで表示される情報は、**list summary** 構成コマンドで表示されるものと同じです。画面の例と出力の説明については、 696ページの『List』 を参照してください。

Ping

ping コマンドは、ルーターが与えられたあて先に 1 秒間に 1 回 IPXPING パケットを送信し (『pinging』)、応答を観察させるために使用します。このコマンドは、インターネットワーク環境での問題を分離するのに使用できます。

このプロセスは継続的に行われます。受信された一致する応答は、送信側の IPX ネットワーク番号とノード番号、ホップ数、および往復時間 (ミリ秒単位) とともに表示されます。

ping プロセスを停止するには、コンソールで任意の文字を入力してください。そうすると、パケット喪失、往復時間、および到達不能なあて先の数の要約が表示されます。

マルチキャスト・アドレスがあて先として与えられている場合、各グループ・メンバーについて 1 つずつ送信される各パケットについて複数の応答があることがあります。 戻された各応答は応答側の発信元アドレスとともに表示されます。

注:

1. 同報通信アドレス (FFFFFFFFFFFF) を指定するときは、注意を払う必要があります。というのは、これにより多数の IPXPING 応答パケットが生成されて、ネットワークおよびルーティング・ソフトウェアの効率が低下する場合があるからです。
2. パラメーターを指定せずに **ping** コマンドを入力すると、すべてのパラメーターを入力するようプロンプト指示されます。***destination network*** および ***destination node*** だけを入力すると、残りのパラメーターについては省略時値が使用されます。

構文 :

ping *dest-net dest-node src-net src-node size rate*

dest-net

あて先 IPX ネットワーク番号を指定します。このパラメーターの指定は必須です。

有効値: X'1' ～ X'FFFFFFFD'

省略時値: 1

dest-node

あて先 IPX ノード・アドレスを指定します。このパラメーターの指定は必須です。

有効値: X'1' ～ X'FFFFFFFFFFFF'

省略時値: なし

src-net

発信元 IPX ネットワーク番号を指定します。このパラメーターの指定は任意です。値は、直接接続された IPX サーキットに対応する既知のネットワーク番号である必要があります。発信元ネットワークが指定されていない場合は、 IPXPING 要求パケットが送信される IPX サーキットのネットワーク番号が発信元 IPX ノードとして使用されます。IPX サーキットが IPXWAN 非番号制 RIP や静的ルー

ティング・サーキットである場合は、発信元ネットワーク番号として使用された IPX サーキットのノード・アドレスが、発信元ノードとして使用されます。

有効値: X'1' ～ X'FFFFFFFD'

省略時値: 1

src-node

発信元 IPX ノード・アドレスを指定します。このパラメーターの指定は任意です。値は、直接接続された IPX サーキットに対応する既知のノード・アドレスである必要があります。発信元ノードが指定されていない場合は、 IPXPING 要求パケットが送信される IPX サーキットのノード・アドレスが発信元 IPX ノードとして使用されます。IPX サーキットが IPXWAN 非番号制 RIP や静的ルーティング・サーキットである場合は、発信元ネットワーク番号として使用された IPX サーキットのノード・アドレスが、発信元ノードとして使用されます。

有効値: X'1' ～ X'FFFFFFFFFFFE'

省略時値: なし

size

ping 要求に付加されるデータ・バイトの数を指定します。このパラメーターの指定は任意です。 データには要求が初めて送信された時刻が含まれるため、指定量は 4 バイトより小さくてはなりません。また、この数値は、ルーターや出力サーキットでサポートされる最大パケット・サイズより大であることはできません。この値は、構成により異なります。

有効値: 4 ～ ルーターの最大値

省略時値: 56 バイト

rate

ping 要求間の秒数を指定します。このパラメーターの指定は任意です。

有効値: 1 ～ 60

省略時値: 1

例: ping

```
Destination network number [1]? 20
Destination node number []? 00000001c200
Source network number [1]? 10
Source node number []? 000000019a00
Data size: [56]?
Rate in seconds [1]?

IPXPING 20/00000001C200: 56 data bytes
56 data bytes from 20/00000001C200: hops=3 time=0 ms
56 data bytes from 20/00000001C200: hops=3 time=40 ms
56 data bytes from 20/00000001C200: hops=3 time=0 ms

----20/00000001C200 IPXPING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/ave/max = 0/13/40
```

RecordRoute

recordroute コマンドは、あて先との間の往復パス上のすべての転送サーキットを報告する場合に使用します。 recordroute がパラメーターなしで起動されると、パラメーターをすべて入力するようプロンプト指示されます。 指定が必須なパラメーターは、

あて先 IPX ネットワーク番号 (destination IPX network number) とあて先 IPX ノード・アドレス (destination IPX node address) だけです。

recordroute を終了するイベントが 2 つあります。1 つは、ユーザーがキーを押した時です。 もう 1 つは、最大数の recordroute 要求パケットが送信された時です。

構文 :

recordroute *dest-net dest-node src-net src-node rate number*

dest-net

あて先 IPX ネットワーク番号を指定します。このパラメーターの指定は必須です。

有効値: X'1' ～ X'FFFFFFFD'

省略時値: 1

dest-node

あて先 IPX ノード・アドレスを指定します。このパラメーターの指定は必須です。

有効値: X'1' ～ X'FFFFFFFFFFFE'

省略時値: なし

src-net

発信元 IPX ネットワーク番号を指定します。このパラメーターの指定は任意です。値は、直接接続された IPX サーキットに対応する既知のネットワーク番号である必要があります。発信元ネットワークが指定されていない場合は、 recordroute パケットが送信される IPX サーキットのネットワーク番号が、発信元 IPX アドレスとして使用されます。IPX サーキットが IPXWAN 非番号制 RIP や静的ルーティング・サーキットである場合は、他の一部の番号制 IPX サーキットのネットワーク番号が、発信元アドレスとして使用されます。 IPXWAN 非番号制 RIP と静的ルーティング・サーキットには IPX ネットワーク番号が割り当てられていないからです。

有効値: X'1' ～ X'FFFFFFFD'

省略時値: 1

src-node

発信元 IPX ノード・アドレスを指定します。このパラメーターの指定は任意です。値は、直接接続された IPX サーキットに対応する既知のノード・アドレスである必要があります。発信元ノードが指定されていない場合は、 recordroute パケットが送信される IPX サーキットのノード・アドレスが、発信元 IPX ノードとして使用されます。IPX サーキットが IPXWAN 非番号制 RIP や静的ルーティング・サーキットである場合は、発信元ネットワーク番号として使用された IPX サーキットのノード・アドレスが、発信元ノードとして使用されます。

有効値: X'1' ～ X'FFFFFFFFFFFE'

省略時値: なし

rate

recordroute 要求間の秒数を指定します。このパラメーターの指定は任意です。

有効値: 1 ～ 60

省略時値: 1

number

送信される recordroute 要求の最大数を指定します。このパラメーターの指定は任意です。この値がゼロの場合、recordroute は、キーが押されるまで続行します。

有効値: 0 ～ 60

省略時値: 0

例: recordroute

```
Destination network number [1]?
20
Destination node number []? 00000001c200
Source network number [1]? 10
Source node number []? 000000019a00
Rate in seconds [1]?
Number of packets to send [0]?

RECORDROUTE 20/00000001C200: 784 data bytes
784 data bytes from 20/00000001C200: seq_no=0 time=0 ms
Recorded Routes (in hex):
                10/000000019A00
                500/0000100A0000
                500/0000100C0000
                10/000000019000
                10/000000019A00 (Final Destination)

784 data bytes from 20/00000001C200: seq_no=1 time=30 ms  (same route)
784 data bytes from 20/00000001C200: seq_no=2 time=10 ms  (same route)
...
784 data bytes from 20/00000001C200: seq_no=18 time=0 ms
Recorded Routes (in hex):
                10/000000019A00
                0/0000100A0000
                20/00000001AE00
                20/00000001C200
                0/0000100B0000
                10/000000019000
                10/000000019A00 (Final Destination)

784 data bytes from 20/00000001C200: seq_no=19 time=0 ms  (same route)
784 data bytes from 20/00000001C200: seq_no=20 time=70 ms  (same route)
784 data bytes from 20/00000001C200: seq_no=21 time=0 ms  (same route)
...
784 data bytes from 20/00000001C200: seq_no=48 time=0 ms
Recorded Routes (in hex):
                10/000000019A00
                500/0000100A0000
                500/0000100C0000
                10/000000019000
                10/000000019A00 (Final Destination)

784 data bytes from 20/00000001C200: seq_no=49 time=0 ms  (same route)
784 data bytes from 20/00000001C200: seq_no=50 time=0 ms  (same route)

----20/00000001C200 RECORDROUTE Statistics----
53 packets transmitted, 38 packets received, 28% packet loss
5 unreachables, 0 no usable source addresses, 0 buffer unavailables
round-trip (ms) min/ave/max = 0/23/100
```

パス全体が報告されるのは、最初の応答時またはパスが変更された時だけです。上の例では、パスは 2 度変更されます。

Reset

reset コマンドは、特定の IPX サーキット、グローバル SAP フィルター、グローバル IPX フィルター (アクセス制御)、静的ルート、静的サービス、またはルーター、RIP、SAP、または IPX サーキット・ベースのフィルター (フィルター・リスト) をリセットする場合に使用します。

構文 :

reset access-controls
circuit . . .
filters
filter-lists
route-static
sap-static

access-controls
構成メモリーに保管されている構成パラメーターに基づいて、グローバル IPX フィルター (アクセス制御) をリセットします。グローバル IPX フィルター構成に対して行われた変更が活動化されます。

例: reset access-controls

circuit *ipx-circuit#*
構成メモリーに保管されている構成パラメーター値を使用して、指定された IPX サーキット上に IPX をリセットします。IPX サーキット上の IPX 構成に加えられた変更が起動されます。

例: reset circuit 2

filters
構成メモリーに保管されている構成パラメーター値に基づいて、グローバル SAP フィルターをリセットします。グローバル SAP フィルターに加えられた変更が起動されます。

例: reset filters

filter-lists *filter-type*
構成メモリーに保管されている構成パラメーター値に基づいて、サーキット・ベースのフィルターをリセットします。サーキット・ベースのフィルターに加えられた変更が起動されます。有効な ***filter-type*** (フィルター・タイプ) は、router、rip、sap、および ipx です。

例: reset filter-lists rip

route-static
構成メモリーに保管されている構成パラメーター値に基づいて、静的ルートをリセットします。静的ルート構成に対して行われた変更が活動化されます。

例: reset route-static

sap-static
構成メモリーに保管されている構成パラメーター値に基づいて、静的サービスをリセットします。静的サービス構成に対して行われた変更が活動化されます。

例: reset sap static

Sizes

sizes コマンドは、ローカル・ノード・キャッシュとリモート・ネットワーク・キャッシュの構成済みサイズ、および現在使用中のキャッシュ項目の数を表示するのに使用します。(このコマンドではキャッシュの内容は表示されません。)

構文 :

sizes

例: sizes

```
Current IPX cache size:
Remote network cache size (max entries): 64
       2 entries now in use

Local node cache size (max entries): 128
       1 entries now in use
```

Slist

slist コマンドは、IPX SAP サーバー・テーブルの内容を表示するのに使用します。

構文 :

slist

例: slist

```
9 entries used out of 32

State Typ Service Name                  Hops   Age     Net  /   Host     /Sock
SAP  4    PCS12                          3     0:50        1/000000000048/0451
SAP  4    ACMPCS                         3     0:50        1/00000000004A/0451
SAP  4    DEVEL2                         1     0:50       11/0000000000B4/0451
SAP  4    PLANNING                       2     0:50       BB/0000000000B7/0451
SAP  4    DEVEL                          2     0:50       BB/0000000000EE/0451
SAP  4    SOFT2                          1     0:30      704/000000000094/0451
SAP  4    SKYSURF1                       2     0: 5 2C39ABE9/000000000001/0451
SAP  278  DIRTREE                        2     0: 5 2C29ABE9/000000000001/4005
Stat 26B  DIRTREE                        2     0: 0      444/000000000001/0045
```

State 次のパラメーターのうち 1 つを指定します。

SAP - このサービスが SAP ルーティング・プロトコルによって入手されたことを示します。

Del - このサービスがタイムアウトになり、すでに使用されていないことを示します。該当のサービスは短時間テーブル内に保持され、他のルートにそのサービスが無効になったことを通知します。 その後、そのサービスは削除され、表示されなくなります。

Stat - このサービスが静的サービスであることを示します。

Typ サーバー・タイプを 16 進数で指定します。ファイル・サーバーはタイプ 0004 です。他のタイプ番号は Novell によって割り当てられています。

Service name
このタイプのサーバーについてサーバーの固有な名前を指定します。スペースを節約するために、47 文字の名前のうち最初の 30 文字だけが表示されます。

Hops このルーターからサーバーへのルーター・ホップの数を指定します。

Age サービス情報の経過時間を指定します。SAP テーブル内の項目が更新されない場合は、ルーターが次の処置を取ります。

- SAP 更新間隔が 3 回経過すると、サービスは Del と指定され、ルーターはそのサービスが無効になったことを公示します。 SAP 更新間隔は、IPX **config** コマンドを使用して表示できます。
- さらに 60 秒が経過すると、そのサービスは削除され、**slist** 画面に表示されなくなります。

Net/Host/Sock
サービスのアドレスを指定します。アドレスには次のパラメーターが含まれます。

- ネットワーク番号
- ネットワーク・ホスト番号 (ネットワーク上の最初のサーキットのアドレス)
- サービスに到達できるソケット番号

表示画面の末尾には、使用された項目の数および使用可能な総数が表示されます。すべての項目が使用される場合は、サービス・テーブルが十分に大きくない可能性があります。サイズを大きくするには、IPX 構成の **set maximum services** コマンドを使用してください。

Traceroute

traceroute コマンドは、ping 要求が最終あて先に到達するまでに取るホップをすべて報告するのに使用します。traceroute がパラメーターなしで起動されると、パラメーターをすべて入力するようプロンプト指示されます。指定が必須なパラメーターは、着信先 IPX ネットワーク番号 (destination IPX network number) と着信先 IPX ノード・アドレス (destination IPX node address) だけです。

traceroute を終了するイベントが 3 つあります。1 つは、ユーザーがキーを押した時です。もう 1 つは、あて先アドレスから応答が受信された時です。最後の 1 つは、最大数のホップに到達した時です。

構文 :

traceroute *dest-net dest-node src-net src-node size probes rate hops*

dest-net
あて先 IPX ネットワーク番号を指定します。このパラメーターの指定は必須です。

有効値: X'1' ～ X'FFFFFFFD'

省略時値: 1

dest-node
あて先 IPX ノード・アドレスを指定します。このパラメーターの指定は必須です。

有効値: X'1' ～ X'FFFFFFFFFFFE'

省略時値: なし

src-net

発信元 IPX ネットワーク番号を指定します。このパラメーターの指定は任意です。値は、直接接続された IPX サーキットに対応する既知のネットワーク番号である必要があります。発信元ネットワークが指定されていない場合は、 traceroute パケットが送信される IPX サーキットのネットワーク番号が、発信元 IPX アドレスとして使用されます。IPX サーキットが IPXWAN 非番号制 RIP や静的ルーティング・サーキットである場合は、他の一部の番号制 IPX サーキットのネットワーク番号が、発信元アドレスとして使用されます。 IPXWAN 非番号制 RIP と静的ルーティング・サーキットには IPX ネットワーク番号が割り当てられていないからです。

有効値: X'1' 〜 X'FFFFFFFD'

省略時値: 1

src-node

発信元 IPX ノード・アドレスを指定します。このパラメーターの指定は任意です。値は、直接接続された IPX サーキットに対応する既知のノード・アドレスである必要があります。発信元ノードが指定されていない場合は、 traceroute パケットが送信される IPX サーキットのノード・アドレスが、発信元 IPX ノードとして使用されます。IPX サーキットが IPXWAN 非番号制 RIP や静的ルーティング・サーキットである場合は、発信元ネットワーク番号として使用された IPX サーキットのノード・アドレスが、発信元ノードとして使用されます。

有効値: X'1' 〜 X'FFFFFFFFFFFE'

省略時値: なし

size

traceroute 要求に付加されるデータ・バイトの数を指定します。このパラメーターの指定は任意です。 データには要求が初めて送信された時刻が含まれるため、指定される数値は 4 バイトより小さくてはなりません。また、この数値は、ルーターや出力サーキットの最大パケット・サイズより大であることはできません。この値は、構成により異なります。

有効値: 4 〜ルーターの最大値

省略時値: 56

probes

ホップ 1 つあたりの、送信する traceroute 要求の数を指定します。このパラメーターの指定は任意です。

有効値: 1 〜 10

省略時値: 3

rate

プローブ間で待機する秒数を指定します。この間、traceroute 要求への応答はありません。このパラメーターの指定は任意です。

有効値: 1 〜 60

省略時値: 1

hops

traceroute 要求を送信するホップの最大数を指定します。このパラメーターの指定は任意です。NLSP がない場合、パケットは、最大 16 個のノード (省略時値が 16

であるため) を通り抜けます。NLSP または IBM 6611 ハーフ・ルーター・ソリューションがある場合には、制限は 16 ではありません。

有効値: 1 ～ 255

省略時値: 16

例: traceroute

```
Destination network number [1]? 20
Destination node number []? 00000001c200
Source network number [1]? 10
Source node number []? 000000019a00
Data size:  [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [1]?
Maximum Hops [16]?

TRACEROUTE 20/00000001C200: 56 data bytes
1 10/000000019000: 0 ms * 500/0000100B0000 20 ms
2 * * *
3 20/00000001C200: 10 ms 60 ms 20 ms
```

traceroute 応答の発信元 IPX アドレスは、変更されない限り、一度だけ報告されます。上の例では、2 つの異なるルーターが、1 つのホップ traceroute 要求に応答しました。これは、あて先までのルートがプローブ間で変更された場合にのみ起こることです。

プローブの往復時間のほかにも、traceroute によって報告される情報があります。

- '*' - 指定された時間で受信された応答パケットはありませんでした。
- 'H!' - あて先ネットワークは到達不能です。これは、traceroute が開始された後に、あて先までのルートが無くなってしまった場合に報告されることです。
- 'BF' - 使用可能なバッファーがありません。

IPX サーキット・フィルター監視コマンド

表43 は、IPX *type*-Lists> プロンプトから使用可能なコマンドをリストしています。これらのコマンドのそれぞれについてこの節で詳しく説明します。

IPX *type*-Lists> プロンプトにアクセスするには、IPX> プロンプトで **filter-lists** *type* を入力します。有効なタイプは、router-lists、rip-lists、sap-lists、および ipx-lists です。

表 43. IPX サーキット・フィルター監視コマンドの要約

コマンド	機能
Cache	指定されたサーキットに関するフィルター・キャッシュの内容を表示します。 IPX フィルターのみがフィルター・キャッシュをサポートしています。
Clear	指定したフィルターのカウンターをクリアするか、現行のタイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターのカウンターをクリアします。
Disable	指定したフィルター、または現行のタイプのすべてのフィルターを使用不能にします。
Enable	指定したフィルター、または現行のタイプのすべてのフィルターを使用可能にします。
List	指定したフィルター、または現行のタイプのすべてのフィルターをリストします。

表 43. IPX サーキット・フィルター監視コマンドの要約 (続き)

コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 xxxivページの『下位レベル環境の終了』 を参照してください。

Cache

cache コマンドは、フィルター・キャッシュの内容を表示するのに使用します。キャッシュをサポートしているのは、IPX フィルターだけです。ROUTER、RIP、および SAP フィルターは、フィルター・キャッシュをサポートしていません。

構文 :

cache filter *filter#*

filter# フィルターの番号を指定します。list コマンドを使用して、構成済みのフィルターの番号付きリストを表示することができます。

例: cache filter 1

```
IPX IPX-Lists>cache filter 1
Hops Type Dst Net  Address      Sock Src Net  Address      Sock Action
---- ---- -------- ------------ ---- -------- ------------ ---- -------
   4   00 04000000 400003900000  802 03000040 400003004400  966 EXCLUDE
   2   00 0004A300 400000233D00  952 0763A020 4000000DD100  920 INCLUDE
```

Clear

clear コマンドは、指定したフィルターのカウンターをクリアしたり、現行のタイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターのカウンターをクリアするのに使用します。

構文 :

clear all

filter ...

all 現行のタイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターのカウンターをクリアします。

例: clear all

filter *filter#*
指定したフィルター番号のカウンターをクリアします。list コマンドを使用して、構成済みのフィルターの番号付きリストを表示することができます。

例: clear filter 1

Disable

disable コマンドは、特定のフィルターを使用不能にしたり、現行のタイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターを使用不能にするのに使用します。

構文 :

disable all

filter *filter#*

all 現行タイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターを使用不能にします。

例: disable all

filter *filter#*
指定したフィルター番号を使用不能にします。list コマンドを使用して、構成済みのフィルターの番号付きリストを表示することができます。

例: disable filter 1

Enable

enable コマンドは、特定のフィルターを使用可能にしたり、現行のタイプ (ROUTER、RIP、SAP、または IPX) のすべて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#*

all 現行タイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターを使用可能にします。

例: enable all

filter *filter#*
指定したフィルター番号を使用可能にします。list コマンドを使用して、構成済みのフィルターの番号付きリストを表示することができます。

例: enable filter 1

List

list コマンドは、特定のフィルターについて、または現行のタイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターについての情報を表示するのに使用します。

構文 :

list all

filter *filter#*

all 現行のタイプ (ROUTER、RIP、SAP、または IPX) のすべてのフィルターの構成をリストします。

例: list all

```
IPX IPX-Lists>list all
Filtering: ENABLED

Filter Lists:
Name                          Action
----------------------------- ----------
ipx01                         EXCLUDE
ipx02                         INCLUDE
ipx03                         EXCLUDE
```

```
Filters:
Id    Circ  Ifc   Direction  State      Default    Cache
----- ----- ----- ---------- ---------- ---------- -----
1     1     0     INPUT      ENABLED    INCLUDE    10
2     1     0     OUTPUT     ENABLED    INCLUDE    10
3     2     1     INPUT      DISABLED   INCLUDE    10
4     2     1     OUTPUT     DISABLED   INCLUDE    10
```

filter *filter#*

指定したフィルター番号の構成をリストします。list コマンドを使用して、構成済みのフィルターの番号付きリストを表示することができます。

例: list filter 1

```
IPX IPX-Lists>list filter 1

Filters:
Id    Circ  Ifc   Direction  State      Default    Cache
----- ----- ----- ---------- ---------- ---------- -----
1     1     0     INPUT      ENABLED    INCLUDE    10

Filter Lists:
Name                           Action     Count
------------------------------ ---------- ----------
ipx01                          EXCLUDE    43
ipx02                          INCLUDE    23453
```

第3部 付録および後付け

付録A. IBM 6611 ルーターとの相互運用

IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施と IBM 6611 ルーターのそれと相互に運用できるようにするには、いくつかの構成に関する考慮事項を処理しておく必要があります。

以下の項ではこれらの考慮事項について概説し、IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施にあたってどのフィーチャーが IBM 6611 のそれと相互に運用できるかを示します。

注: ここで引用される考慮事項は、IBM 6611 の MPNP V1.2 ソフトウェアを使って行われたテストから引き出されたものです。 これらの考慮事項は他の MPNP ソフトウェア・バージョンには適用できません。

考慮事項は次の項に類別されています。

- 『ブリッジ構成の考慮事項』
- 『DLSw に関連する考慮事項』
- 746ページの『IP に関連する構成の考慮事項』
- 746ページの『TCP に関連する考慮事項』
- 747ページの『その他の相互運用性の考慮事項』

ブリッジ構成の考慮事項

以下はブリッジ構成の考慮事項です。

- DLSw の LAN ID (セグメント番号) は IBM 2210 と IBM 6611 ルーターの両方で一致する必要があります。 ミスマッチが引き続き存在する場合は、IBM Nways マルチプロトコル・ルーティング・サービス のコンフィギュレーター (Talk 6) に入り、DLSw プロトコルを選択してください。 次に **set srb** コマンドを使用して、IBM 6611 のセグメント番号に一致するセグメント番号値を設定することができます。
- ブリッジ・フレームに使用できる最大の MTU 値は 2100 バイトです。これは IBM 6611 によって現在サポートされる最大値です。 2100 より小さい MTU 値を指定する場合は、構成した値が IBM 2210 と IBM 6611 ルーターの両方で一致することが重要です。

DLSw に関連する考慮事項

DLSw に関連する相互運用性の考慮事項は次のとおりです。

- IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施では、SSP_IAMOKAY メッセージ (SSP メッセージ・タイプ X'x1D') をサポートしませんが、IBM 6611 の DLSw の実施ではサポートされています。 この SSP メッセージは RFC 1434 では文書化されておらず、IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施では受信時に暗黙に廃棄されます。

IBM 6611 ルーターとの相互運用

- IBM 6611 の DLSw の実施では IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施から受信された SSP_ENTER_BUSY/EXIT_BUSY メッセージを処理しますが、同様のフロー制御に関連した SSP メッセージを生成しません。
- IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施では、APPN ネットワーク・ノードとして機能する IBM 6611 DLSw ルーターによって生成されるユーザー定義の SSP_TEST_CIRCUIT_REQ メッセージ (SSP メッセージ・タイプ X'x7A') をサポートしません。 このメッセージの受信時に、IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施ではユーザー定義の SSP_TEST_CIRCUIT_RSP メッセージ (SSP メッセージ・タイプ X'x7B') を戻します。 この応答は、IBM 6611 DLSw ルーターの APPN ネットワーク・ノードの実施では予期されています。

IP に関連する構成の考慮事項

以下は、IP 構成の考慮事項です。

- IBM Nways マルチプロトコル・ルーティング・サービス の DLSw 近隣が相互を動的に見つけることを可能にするクライアント/サーバーおよびピア間の DLSw グループ・フィーチャーは IBM 6611 の DLSw の実施で相互に運用できません。 その結果、隣接 IBM 6611 DLSw ピアの静的 IP アドレスを定義するためには DLSw の **add tcp neighbor** 構成コマンドを使用する必要があります。
- IBM Nways マルチプロトコル・ルーティング・サービス の DLSw グループ・フィーチャーに対する上記の相互運用性の制限は RIP/OSPF の選択に意味をもちます。
  - 2210 で DLSw グループを使用するには、OSPF/MOSPF も構成する必要があります。しかし、これらの DLSw グループは 6611 と相互に運用できないので、2210 は RIP だけを使用可能にし、OSPF 構成なしに構成することが可能です。
  - OSPF および RIP の両方を IBM 2210 サイドで使用可能にすることができるとはいえ、MOSPF (OSPF 構成を通じて選択された場合) は IBM 6611 によってサポートされていません。
- IBM Nways マルチプロトコル・ルーティング・サービス の IP 構成内で、所定のインターフェース上の同報通信アドレス用に構成された充てんパターンは IBM 6611 での同等の定義に一致します。
- DLSw 上の SNA トラフィックの移送用の帯域幅を確保するために使用できる IBM Nways マルチプロトコル・ルーティング・サービス の帯域幅予約システム (BRS) は、IBM 6611 の DLSw の実施で相互に運用できません。

  BRS のために IBM 2210 ハードウェアによって割り当てられた優先順位はアウトバウンド方向では実施できますが、中間の IP ルーターが BRS をサポートしない場合には、優先順位は保証されません。 また、6611 は回線の端点で BRS をサポートしないので、BRS は単一の方向でのみ適用できます。

TCP に関連する考慮事項

以下は、TCP の相互運用性の考慮事項です。

TCP 接続中断検出の相異

IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施で TCP 接続が中断されているのを検出するのは、Keepalive (キープアライブ) 応答が受信されない (Keepalive オプションが接続のために使用可能にされていると想定します) 場合、またはデータを送達できない場合のいずれかです。

TCP Connection Reestablishment Differences

TCP 接続が中断されると、IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施では、エンド・ステーションからの DLC TEST メッセージの受信時に新しい DLSw SSP_CANUREACH が生成される場合に、TCP 接続を再確立します。 IBM 6611 は同じ行動を示さない場合があります。

Keepalive Disable/Enable Related Differences

前述したように、IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施では、TCP 近隣の IP アドレスが追加される (構成される) ときに、活動保持オプションを使用可能および使用不能にできます。 IBM 6611 の DLSw の実施での TCP は、TCP セッションで受信された活動保持メッセージに応答しますが、常駐の 6611 TCP を構成して TCP 活動保持メッセージの生成を可能にするメカニズムはありません。

Maximum Number of TCP Connections Supported

IBM Nways マルチプロトコル・ルーティング・サービス の DLSw の実施では、サポートされる TCP 接続の最大数に対してハードウェアでコード化されているための制限はありません。 その結果、サポートされる TCP 接続の最大数は IBM 2210 の使用可能なメモリーに直接関連しています。 IBM 6611 の場合、DLSw の実施でサポートできる TCP 接続はハードウェアでコード化しているため 100 という内部制限があります。

その他の相互運用性の考慮事項

次のその他の相互運用性の考慮事項に注意してください。

- IBM 6611 によって開始された DLSw 接続を確立しようとしているときに問題が検出された場合、IBM 6611 構成を検査して、MAC アドレスのフィルター・リングが関連する発信元またはあて先の MAC アドレスを不注意に使用可能にしなかったか確認してください。
- RFC 1434 は孤立 DLSw セッション (例えば、DLSw サーキットが確立された状態にとどまり、後続の活動がない DLSw セッション) の問題を特に扱いませんが、IBM Nways マルチプロトコル・ルーティング・サービス と IBM 6611 の両方の DLSw の実施では孤立 DLSw セッション・タイムアウトを提供することにより、この問題を解決します。 DLSw サーキットが確立された状態で 30 秒を超えて非アクティブにとどまっている DLSw セッションは両方の実施によって除去されます。

付録B. IBM 6611 ブリッジとの相互運用

IBM 6611 のブリッジングと相互に運用するために IBM 2210 上のブリッジングを実施する前に、いくつかの構成問題を考慮する必要があります。

この付録では、これらの問題の概要を提供し、IBM 2210 のブリッジの実施のどのフィーチャーが IBM 6611 のブリッジの実施と相互に運用できないかを示します。

IBM 6611 と IBM 2210 を PPP およびフレーム・リレーのシリアル回線を介する 2 つのエンド・ブリッジとして使用する場合は、非互換ネットワークを構築してしまうのを避けるために、以下に述べるブリッジの構成に関する問題を考慮する必要があります。

PPP の場合、IBM 2210 ブリッジは RFC 1638 の *PPP Bridging Control Protocol* で記述されているように、異なる MAC タイプ (イーサネットおよびトークンリング) をサポートします。フレーム・リレーの場合は、IBM 2210 は、RFC 1490 の *Multiprotocol Interconnect over Frame Relay* をサポートします。

現在、IBM 6611 ブリッジは、PPP およびフレーム・リレーを介するイーサネットおよびトークンリングの MAC タイプをサポートしています。 ただし、PPP またはフレーム・リレーに関連するブリッジ・ポートが**ソート・ルーティング**・ポートとして構成されている場合は、 IBM 6611 ブリッジがサポートするのは、トークンリング MAC フレームだけです。 したがって、IBM 6611 と IBM 2210 が PPP またはフレーム・リレーを介する 2 つのエンド・ブリッジである場合は、ネットワーク・トポロジーに特定の制限が生じることになります。

RFC 1638、セクション 5.3 では、ベンダーが対等ブリッジに PPP を介してサポートされる MAC タイプをどのように告知し、ピアが PPP を介してサポートされていない MAC タイプのトラフィックを送信しないようにできるかを説明しています。 現在、IBM 2210 ブリッジは PPP ネットワークあての非イーサネット・フレームを除去しません。 またはこのブリッジは、すべてのフレームを PPP を介して送信する前にそれらをイーサネット・フレームに変換しようともしません。この結果、IBM 6611 ブリッジは PPP を介して非イーサネット・フレームを受信し、構成にミスマッチがあるときはそれらを廃棄します。

PPP に関するその他の考慮事項

ブリッジ・ネットワーク内で 2210 と 6611 を構成する際には、次の点を念頭に置いていただく必要があります。

- PPP リンクを介してトラフィックをブリッジするためには、折衝されたされた最大受信単位 (MRU) は、ブリッジされたフレームが入るだけの大きさのものでなければなりません。ブリッジされたフレームには、元の LAN からのデータおよび MAC レイヤー・ヘッダーが含まれています。

  例えば、イーサネット・フレームには、1500 バイトのデータを入れることができます。WAN リンクを介してブリッジされた場合、ブリッジされたトラフィックにさらに 14 バイトのイーサネット MAC ヘッダーが入れられ、パケット・サイズは 1514 になります。これは、折衝された PPP MRU は、フレームをブリッジするのに少なくとも 1514 でなければならないことを意味しています。

ブリッジされたフレームを保持して余りある大きさの MRU サイズを考慮してください。MRU の開始値として 2000 または 2048 を使用してみてください。

- PPP リンクの両端は、必ず同じサイズの MRU であるようにしてください。 2210 に省略時の MRU を使用したら、6611 の MRU は 2210 の MRU 値に必ず一致させる必要があります。

構成の例

以下は、働か**ない**ネットワーク・トポロジーの例です。 可能な代替構成は **Alt** とマークされています。 WAN を考慮する場合は、LAN タイプを MAC タイプに拡張することができます。

例 1: トークンリング (SR) - IBM 2210 (SR-TB) - PPP (TB) - IBM 6611 (TB) - イーサネット

Alt: トークンリング (SR) - IBM 2210 (SRB) - PPP (SR) - IBM 6611 (SR-TB) - イーサネット

例 2: Token Ring (TB) - IBM 2210 (TB) - PPP (TB) - IBM 6611 (TB) - ETH/TKR

Alt: トークンリング (SR) - IBM 2210 (SRB) - PPP (SR) - IBM 6611 (SR-TB) - ETH

Alt: トークンリング (SR) - IBM 2210 (SRB) - PPP (SR) - IBM 6611 (SRB) - TKR

Alt: トークンリング (TB) - IBM 2210 (SR-TB) - PPP (SR) - IBM 6611 (SRB) - TKR

Alt: トークンリング (TB) - IBM 2210 (SR-TB) - PPP (SR) - 6611 (SR-TB) - ETH

境界アクセス・ノード (BAN) および DLSw によって生成された LAN フレームはソート・ルーティングされたトークンリング・フレームです。 媒体タイプおよび関連する発信ブリッジ・ポートのブリッジ構成の性質に基づき、IBM 2210 ブリッジはソート・ルーティングされたトークンリング・フレームを次のように変換します。

1. イーサネットで ETH (TB)
2. トークンリング TB 形式で PPP/FR/トンネル /
3. トークンリング SR 形式で PPP/FR/トンネル /
4. トークンリング TB 形式で TKR (TB)
5. トークンリング SR 形式で TKR (SR)

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 アドレス指定 (arbitrary MAC addressing)

AMP アクティブ・モニター・プレゼント (active monitor present)

ANSI 米国規格協会 (American National Standards Institute)

AP2 AppleTalk フェーズ 2 (AppleTalk Phase 2)

APPN 拡張ピアツーピア・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 are you there (相手確認)

BAN 境界アクセス・ノード (Boundary Access Node)

BBCM ブリッジング・ブロードキャスター・プログラム (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 (bandwidth reservation)

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

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 あて先アドレス・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 あて先サービス・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 あて先タイプ (destination type)

DVMRP
距離ベクトル・マルチキャスト・ルーティング・プロトコル (Distance Vector Multicast Routing Protocol)

E1 2.048 Mbps 伝送速度 (2.048 Mbps transmission rate)

EDEL 終了区切り文字 (end delimiter)

EDI エラー検出標識 (error detected indicator)

EGP 外部ゲートウェイ・プロトコル (Exterior Gateway Protocol)

EIA 米国電子工業会 (Electronics Industries Association)

ELAN エミュレート LAN (Emulated LAN)

ELAP EtherTalk リンク・アクセス・プロトコル (EtherTalk Link Access Protocol)

ELS イベント・ログ・システム (Event Logging System)

ESI エンド・システム識別子 (End system identifier)

EST 東部標準時 (Eastern Standard Time)

Eth イーサネット (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

FRL フレーム・リレー

FTP ファイル転送プロトコル (File Transfer Protocol)

GMT グリニッジ標準時 (Greenwich Mean Time)

GOSIP
米国政府 OSI 調達仕様 (Government Open Systems Interconnection Profile)

GTE 一般電話会社 (General Telephone Company)

GWCON
ゲートウェイ・コンソール (Gateway Console)

HDLC ハイレベル・データ・リンク制御 (high-level data link control)

HEX 16 進法 (hexadecimal)

HPR 高性能ルーティング (high-performance routing)

HST TCP/IP ホスト・サービス (TCP/IP host services)

HTF ホスト・テーブル形式 (host table format)

IBD 統合ブート装置 (Integrated Boot Device)

ICMP インターネット制御メッセージ・プロトコル (Internet Control Message Protocol)

ICP インターネット制御プロトコル (Internet Control Protocol)

ID 識別 (identification)

IDP イニシアル・ドメイン・パート (Initial Domain Part)

IDP インターネット・データグラム・プロトコル (Internet Datagram Protocol)

IEEE 米国電気電子学会 (Institute of Electrical and Electronics Engineers)

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 - 同報通信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 非同報通信マルチアクセス (Non-Broadcast Multiple Access)

NBP ネーム・バインディング・プロトコル (Name Binding Protocol)

NBR 近隣、ネイバー (neighbor)

NCP ネットワーク制御プロトコル (Network Control Protocol)

NCP ネットワーク・コア・プロトコル (Network Core Protocol)

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)

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 Request for Comments (コメント要求)

RI リング標識、ルーティング情報 (ring indicator; routing information)

RIF ルーティング情報フィールド (routing information field)

RII ルーティング情報標識 (routing information indicator)

RIP ルーティング情報プロトコル (Routing Information Protocol)

RISC 縮小命令セット・コンピューター (reduced instruction-set computer)

RNR 受信不可 (receive not ready)

ROM 読み取り専用メモリー (read-only memory)

ROpcon
リモート・オペレーター・コンソール (Remote Operator Console)

RPS リング・パラメーター・サーバー (ring parameter server)

RTMP ルーティング・テーブル保守プロトコル (Routing Table Maintenance Protocol)

RTP ルーティング更新プロトコル (RouTing update Protocol)

RTS 送信要求 (request to send)

Rtype ルート・タイプ (route type)

rxmits 再送 (retransmissions)

rxmt 再送する (retransmit)

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 活動時間 (time to live)

TTY テレタイプライター (teletypewriter)

TX 送信 (transmit)

UA 非番号制確認 (unnumbered acknowledgment)

UDP ユーザー・データグラム・プロトコル (User Datagram Protocol)

UI 非番号制情報 (unnumbered information)

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)

VR バーチャル・ルート (virtual route)

WAN 広域ネットワーク (wide area network)

WRS WAN 復元 / 再ルート (WAN restoral/reroute)

X.25 パケット交換網 (packet-switched networks)

X.251 X.25 物理レイヤー (X.25 physical layer)

X.252 X.25 フレーム・レイヤー (X.25 frame layer)

X.253 X.25 パケット・レイヤー (packet layer)

XID 交換 ID (exchange identification)

XNS Xerox ネットワーク・システム (Xerox Network Systems)

XSUM チェックサム (checksum)

ZIP AppleTalk ゾーン情報プロトコル (AppleTalk Zone Information Protocol)

ZIP2 AppleTalk ゾーン情報プロトコル 2 (AppleTalk Zone Information Protocol 2)

ZIT ゾーン情報テーブル (Zone Information Table)

用語集

この用語集には、以下からの用語および定義が含まれています。

- *American National Standard Dictionary for Information Systems*、ANSI X3.172-1990 (米国規格協会 (ANSI) が 1990 年に著作権を取得)。この複写版が米国規格協会 (ANSI: 11 West 42nd Street, New York, New York 10036)から発売されています。定義の後に記号 (A) を付けて出典を示してあります。
- ANSI/EIA Standard--440-A、*Fiber Optic Terminology*。この複写版が米国電子工業会 (2001 Pennsylvania Avenue, N.W., Washington, DC 20006) から発売されています。定義の後に記号 (E) を付けて出典を示してあります。
- *Information Technology Vocabulary*。国際標準化機構および国際電気標準会議の第 1 合同技術委員会第 1 分科会 (ISO/IEC JTC1/SC1) によって編さんされたものです。この語い集の刊行部分から転載した定義については、その後に記号 (I) を付けて示してあります。また、ISO/IEC JTC1/SC1 で編さん中の国際規格草案、分科会草案、および作業文書から採用した定義については、その後に記号 (T) を付けて、SC1 の加盟各国諸団体間で最終合意がなされていないことを示してあります。
- *IBM Dictionary of Computing* , New York: McGraw-Hill, 1994
- Internet Request for Comments: 1208、*Glossary of Networking Terms*
- Internet Request for Comments: 1392、*Internet Users' Glossary*
- *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

この用語集では、以下の形で相互参照しています。

と対比:
反対の意味または実質的に異なる意味をもつ用語を示します。

の同義語:
この用語集の該当箇所に記述されている、優先的に使用してほしい、同じ意味をもつ用語を示します。

と同義:
逆方向参照として、定義の対象となっている用語から、同じ意味をもつ他の用語をすべて参照します。

を参照:
一部の語 (特に最後の語) が同じ複数語からなる用語を参照します。

も参照:
関連する意味 (同義ではない) をもつ用語を参照します。

A

AAL. ATM アダプテーション・レイヤー (ATM Adaptation Layer)。ヘッダーを追加/除去し、セルへ/からのデータを細分化/再組み立てすることにより、ATM ネットワークへ/からのユーザー・データを適応させるレイヤー。

AAL-5. ATM アダプター・レイヤー 5 (ATM Adaptation Layer 5)。複数ある標準 AAL の 1 つ。 AAL-5 はデータ通信用に設計されたもので、LAN エミュレーションおよびクラシカル IP によって使用される。

抽象構文 (abstract syntax). データ伝送に必要な特性はすべて含んでいるが、その他の明細 (たとえば、特定のコンピューター・アーキテクチャーに依存する明細など) は省略 (抽象化) されているデータ仕様。*抽象構文表記法 (ASN.1) (abstract syntax notation 1 (ASN.1))* および*基本符号化規則 (BER) (basic encoding rules (BER))* も参照。

抽象構文表記法 1 (ASN.1) (abstract syntax notation 1 (ASN.1)). 次の標準で指定されている抽象構文の開放型システム間相互接続 (OSI) 方式。

- ITU-T 勧告 X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T 勧告 X.680 (1994) | ISO/IEC 8824-1: 1994

基本符号化規則 (BER) (basic encoding rules (BER)) も参照。

ACCESS. シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理ノードがオブジェクトに対して提供する最小レベルのサポートを定義する、管理情報ベース (MIB) モジュール内の文節。

確認応答 (acknowledgment). (1) 受信側が送信側に肯定応答として確認応答文字を伝送すること。 (T) (2) 送信された項目が受信されたことを示すこと。

アクティブ (active). (1) 運用可。 (2) 別のノードまたは装置に接続された、またはそれへの接続が利用可能なノードまたは装置に関する用語。

アクティブ・モニター (active monitor). トークンリング・ネットワークにおいて、一度に 1 つのリング・ステーションによって実行される機能で、トークンの伝送を開始し、トークン誤り回復機能を提供する。現在のアクティブ・モニターに障害が起こった場合、リング上の任意のアクティブ・アダプターが、アクティブ・モニター機能を提供することができる。

アドレス (address). データ通信において、通信ネットワークに接続された各装置、ワークステーション、またはユーザーに割り当てられる固有のコード。

アドレス・マッピング・テーブル (AMT) (address mapping table (AMT)). 現在のノード・アドレスとハードウェア・アドレスのマッピングを提供する、AppleTalk ルーター内に維持されているテーブル。

アドレス・マスク (address mask). インターネット・サブネットワークにおいて、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットを識別するために使用される、32 ビットのマスク。サブネット・マスク *(subnet mask)* およびサブネットワーク・マスク *(subnetwork mask)* と同義。

アドレス解決 (address resolution). (1) ネットワーク・レイヤー・アドレスを媒体特有アドレスにマッピングする方法。 (2) *アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP))* および *AppleTalk アドレス解決プロトコル (AARP) (AppleTalk Address Resolution Protocol (AARP))* も参照。

アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP)). (1) インターネット・プロトコルにおいて、サポートされる大都市圏ネットワークやローカル・エリア・ネットワーク (イーサネットやトークンリングなど) が使用するアドレスに、IP アドレスを動的にマップするプロトコル。 (2) *逆アドレス解決プロトコル (RARP) (Reverse Address Resolution Protocol (RARP))* も参照。

アドレッシング (addressing). データ通信において、端末局がデータの送信先の端末局を選択する方法。

隣接ノード (adjacent nodes). 他のノードとは接続していない少なくとも 1 つのパスによって相互に接続されている 2 つのノード。 (T)

管理ドメイン (Administrative Domain). 1 つの管理機関によって管理される、ホストとルーターおよび相互接続ネットワークの集合。

拡張ピアツーピア・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、*同報通信アドレス (broadcast address)* の同義語。

米国規格協会 (ANSI) (American National Standards Institute (ANSI)). 認定組織が米国の自主業界標準を作成して維持するための手順を決める、生産者、消費者、および一般の関係団体から構成される組織。 (A)

アナログ (analog). (1) 連続的に変化する物理量から構成されるデータに関する用語。 (A) (2) *ディジタル (digital)* と対比。

AppleTalk. Apple Computer, Inc. によって開発されたネットワーク・プロトコル。このプロトコルは、ネットワーク上の装置を相互接続するために使用される。装置は、Apple 製品と非 Apple 製品を混合して使用できる。

AppleTalk アドレス解決プロトコル (AARP) (AppleTalk Address Resolution Protocol (AARP)). AppleTalk ネットワークにおいて、(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). *拡張対等間通信ネットワーキング機能 (APPN) ネットワーク (Advanced Peer-to-Peer Networking (APPN) network)* を参照。

APPN ネットワーク・ノード (APPN network node). *拡張ピア間通信ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node)* を参照。

任意 MAC アドレッシング (AMA) (arbitrary MAC addressing (AMA)). DECnet 体系において、一元管理アドレスとローカル管理アドレスをサポートする、 DECnet フェーズ IV-Prime によって使用されるアドレッシング機構。

エリア、区域 (area). インターネットおよび DECnet ルーティング・プロトコルにおいて、ネットワーク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)

属性値対 (Attribute Value Pair) (AVP). メッセージのタイプと本体を符号化する汎用方式。この方式によって、L2TP は相互運用性が許容されると同時に、拡張性が最大化される。

属性値ペア (AVP) (Attribute Value Pair (AVP)). メッセージ・タイプおよび本文をコード化する一律的な方法。この方式は、 L2TP の相互運用性を可能にすると同時に、拡張性を最大化する。

認証障害 (authentication failure). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、要求側クライアントが SNMP コミュニティーのメンバーでない場合に、認証エンティティーが生成するトラップ。

自律システム (autonomous system). TCP/IP において、1 つの管理機関の下にあるネットワーク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)。同報通信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。

同報通信 (broadcast). (1) すべてのあて先に同じデータを伝送すること。 (T) (2) 複数のあて先に同時にデータを伝送すること。 (3) マルチキャスト *(multicast)* と対比。

同報通信アドレス (broadcast address). 通信において、リンク上のすべてのステーションに共通のアドレスとして確保されているステーション・アドレス (8 桁の 1 で構成)。全ステーション・アドレス *(all-stations address)* と同義。

BUS. 同報通信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) *物理サーキット (physical circuit)* およびバーチャル・サーキット *(virtual circuit)* も参照。

注:

1. データ交換装置相互間では、データ回線は、データ交換装置で使用するインターフェースのタイプによって、データ回線終端装置 (DCE) を含むことがある。
2. データ端末とデータ交換装置またはデータ集線装置との間では、データ回線は、データ装置側のデータ回線終端装置を含み、またデータ交換装置またはデータ集線装置側の DCE と類似の装置を含むことがある。

データ回線終端装置 (DCE) (data circuit-terminating equipment (DCE)). データ端末において、データ端末装置 (DTE) と回線の間で信号変換および符号化を行う装置。 (I)

注:

1. DCE は、独立した機器であるか、DTE または中間装置に組み込まれている。
2. DCE は、伝送路のネットワーク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着信先アドレスが入っている。インターネット・プロトコル (IP) データグラムは、IP ヘッダーと後続のトランスポート・レイヤー・データによって構成される。 (3) *パケット (packet)* および *セグメント (segment)* も参照。

データグラム送達プロトコル (DDP) (Datagram Delivery Protocol (DDP)). AppleTalk ネットワーク・ノードおいて、インターネット・レイヤーのコネクションレス・ソケット間送達サービスによってネットワークの接続性を提供するプロトコル。

DCE レディー (DCE ready). EIA 232 標準において、ローカル・データ回線終端装置 (DCE) が通信チャネルに接続され、データ送信が可能になっていることを、データ端末装置 (DTE) に知らせる信号。データ・セット・レディー *(DSR) (data set ready (DSR))* と同義。

DECnet. 通常は資源の共用、分散計算、またはリモート・システム構成の目的で、Digital Equipment Corporation のシステムを相互連結するのに使用される、一連のソフトウェア・モジュール、データベース、およびハードウェア・コンポーネント動作を定義するネットワーク体系。 DECnet ネットワークの実現方式は、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。

あて先ノード (destination node). 要求またはデータの送信先のノード。

あて先ポート (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。

あて先サービス・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) *管理領域 (Administrative Domain)* およびドメイン名 *(domain name)* を参照。

ドメイン名 (domain name). インターネット・プロトコルにおける、ホスト・システムの名前。ドメイン名は、区切り文字によって区切られた一連のサブネームから構成される。たとえば、ホスト・システムの完全修飾ドメイン名 (FQDN) が `ralvm7.vnet.ibm.com` である場合、以下がそれぞれドメイン名である。

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

ドメイン名サーバー (domain name server). インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップすることにより名前からアドレスへの変換を行うサーバー・プログラム。ネーム・サーバー *(name server)* と同義。

ドメイン名システム (DNS) (Domain Name System (DNS)). インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップするために使用される分散データベース・システム。

ドット 10 進表記 (dotted decimal notation). 基底を 10 とし、ピリオド (ドット) で相互を分離して書かれた、4 つの 8 ビット数字からなる 32 ビット整数の構文表記。 IP アドレスを表すのに使用される。

ダンプ (dump). (1) ダンプしたデータ。 (T) (2) 誤り情報を収集するために、バーチャル記憶装置のコンテンツの全部または一部をコピーすること。

動的再構成 (DR) (dynamic reconfiguration (DR)). 完全な構成テーブルを再生成したり、影響を受けるメジャー・ノードを停止せずに、ネットワーク構成 (周辺 PU および LU) を変更するプロセス。

動的ルーティング (Dynamic Routing). 初期化時に静的に構成されたルートではなく、動的に確認されたルートを使用するルーティング。

E

エコー (echo). データ通信において、通信チャネル上の反射信号。たとえば、通信端末装置では各信号は 2 度表示される。ローカル端末に入ったときに一度表示され、通信リンクを経由して戻ってきたときに再度表示される。これにより、信号が正確であるかどうかを検査することができる。

EIA 232. データ通信において、順次 2 進データ交換を使用して、データ端末装置 (DTE) とデータ回線終端装置 (DTE) 間のインターフェースを定義する米国電子工業会 (EIA) の仕様。

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) *拡張対等間通信ネットワーキング (APPN) エンド・ノード (Advanced Peer-to-Peer Networking (APPN) end node)* およびローエントリー・ネットワーキング *(LEN) エンド・ノード (low-entry networking (LEN) end node)* を参照。 (2) 通信において、頻繁に 1 つのデータ・リンクに接続されるノードで、中間ルーティング機能を実行できないもの。

入り口点 (EP) (entry point (EP)). SNA において、分散ネットワーク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、着側サブエリア・アドレス、明示ルート番号、および逆明示ルート番号によって識別される。バーチャル・ルート *(VR) (virtual route (VR))* と対比。

探索フレーム (explorer frame). *探索パケット (explorer packet)* を参照。

探索パケット (explorer packet). LAN において、発信元ホストによって生成され、LAN のソース・ルーティング全体を探索して、ホストが利用可能なパスに関する情報を収集するパケット。

外部ゲートウェイ (exterior gateway). インターネット通信において、ある自律システム上の、別の自律システムと通信するゲートウェイ。*内部ゲートウェイ (interior gateway)* と対比。

外部ゲートウェイ・プロトコル (EGP) (Exterior Gateway Protocol (EGP)). インターネット・プロトコルにおいて、ドメインと自律システム間で使用され、ネットワーク到達可能性情報を公示および交換することができるプロトコル。ある自律システム内の IP ネットワーク・アドレスが、EGP に参加しているルーターによって、別の自律システムに公示される。 EGP の例としては、ボーダー・ゲートウェイ・プロトコル (BGP) がある。内部ゲートウェイ・プロトコル (IGP) (Interior Gateway Protocol (IGP)) と対比。

F

ファックス (fax). ファクシミリ機から受け取ったハードコピー。***テレコピー (telecopy)*** と同義。

ファイル転送プロトコル (FTP) (File Transfer Protocol (FTP)). インターネット・プロトコルにおいて、TCP および Telnet サービスを使用して、計算機間またはホスト間で大量データ・ファイルを転送する、アプリケーション・レイヤー・プロトコル。

フラッシュ・メモリー (flash memory). プログラム式で、消去可能で、連続的な電力を必要としない、データ記憶装置。他のプログラム式、消去可能データ記憶装置と比べたフラッシュ・メモリーの主な長所は、回路ボードから取り外さずに再プログラムできることである。

フロー制御 (flow control). (1) SNA において、データ・トラフィックがネットワークのコンポーネント間を通過する速度を管理するプロセス。フロー制御の目的は、メッセージの流れを最適化してネットワーク輻輳 (ふくそう) を最小にすることである。つまり、受信側または中間ルーティング・ノードのバッファーがオーバーフローせず、また受信側が追加メッセージ単位の到着を待つこともないようにする。 (2) ペーシング *(pacing)* も参照。

フラグメント (fragment). *分割 (fragmentation)* を参照。

断片化 (fragmentation). (1) 伝送する物理媒体の容量に合わせるために、データグラムをより小さい部分つまり断片に分割する処理。 (2) *分割 (segmenting)* も参照。

フレーム (frame). (1) ある特別な情報で構成されるデータ構造。特別な情報とは、いくつかのスロットで成り立ち、各スロット内の属性値を読むことにより適切な接続手順が決められる。 (T) (2) IBM トークンリング・ネットワークなどのローカル・エリア・ネットワークにおける伝送単位。区切り文字、制御文字、情報、および検査文字が含まれる。 (3) SDLC において、SDLC 手順を使用して伝送される、コマンド、レスポンス、およびすべての情報を運ぶ手段。

フレーム・レベル (frame level). *データ・リンク・レベル (data link level)* と同義。*リンク・レベル (link level)* を参照。

フレーム・リレー (frame relay). (1) ユーザーの装置と高速パケット・ネットワークの境界を記述したインターフェース標準。フレーム・リレー・システムでは、無効なフレームは廃棄される。回復はホップごとではなく、エンド・エンドで行われる。 (2) サービス総合ディジタル網 (ISDN) D チャネル標準から導出された技法。接続は高信頼性で、ネットワークの誤り検出と制御のオーバーヘッドはないものと想定している。

フロントエンド・プロセッサー (front-end processor). メインフレームの通信制御タスクを軽減する、IBM 3745 または 3174 のようなプロセッサー。

G

ゲートウェイ (gateway). (1) ネットワーク体系が異なる 2 つのコンピューター・ネットワークを相互に接続する機能単位。ゲートウェイは、異なる体系をもつネットワークまたはシステムを接続する。ブリッジは、同一または類似の体系をもつネットワークまたはシステムを接続する。 (T) (2) IBM トークンリング・ネットワークにおいて、ローカル・エリア・ネットワークを、異なる論理リンク・プロトコルを使用する別のローカル・エリア・ネットワークまたはホストに接続する、装置と関連ソフトウェア。 (3) TCP/IP においては、*ルーター (router)* の同義語。

汎用データ・ストリーム (GDS) (general data stream (GDS)). LU 6.2 セッション内の会話に使用されるデータ・ストリーム。

汎用データ・ストリーム (GDS) 変数 (general data stream (GDS) variable). 識別子と長さフィールドで始まり、アプリケーション・データ、ユーザー制御データ、または SNA 定義制御データのいずれかを持つ RU 副構造の 1 タイプ。

H

ヘッダー (header). (1) ユーザー・データの前に置かれるシステムが定めた制御情報。 (2) 1 つまたは複数の着信先フィールド、発信元ステーションの名前、入力シーケンス番号、メッセージのタイプを示す文字列、メッセージの優先順位レベルなどの制御情報が入っているメッセージの部分。

ヒープ・メモリー (heap memory). データ構造を動的に割り振るために使用される RAM の量。

ハロー (Hello). 協働する承認ルーターが最小遅延ルートを見付けるために使用するプロトコル。

ハロー・メッセージ (hello message). (1) ルーター相互間またはルーターとホスト間の到達可能性を設定し、テストするために定期的に送られるメッセージ。 (2) インターネット・プロトコルにおいて、ハロー・プロトコルによって内部ゲートウェイ・プロトコル (IGP) として定義されるメッセージ。

ヒューリスティック (heuristic). 最終結果に向けての進展状況を評価することによって解答を見付けるという、問題解決の探索的方法を表わす用語。

ハイレベル・データ・リンク制御 (HDLC) (high-level data link control (HDLC)). データ通信において、HDLC 国際規格 ISO 3309 フレーム構造および ISO 4335 手順要素に準拠して、指定された一連のビットを使用してデータ・リンクを制御すること。

高性能ルーティング (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、ピア間通信ネットワーキング機能 (APPN) 体系の追加機能。

ホップ (hop). (1) APPN において、中間ノードを含まないルート部分。隣接ノード間を接続する 1 つの伝送グループだけで構成される。 (2) ルーティング・レイヤーにおいては、ネットワークの 2 つのノード間の論理距離。

ホップ・カウント (hop count). (1) 2 点間の距離の尺度。 (2) インターネット通信において、着信先までの線路でデータグラムが通過するルーターの数。 (3) SNA において、着信先までのパスで通過するリンク数の尺度。

ホスト (host). インターネット・プロトコルにおいて、エンド・システムのこと。エンド・システムはどのワークステーションでも構わず、必ずしもメインフレームである必要はない。

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) および最短パス優先オープン (OSPF) がある。

中間ノード (intermediate node). 複数の分岐の終端にあるノード。 (T)

中間セッション・ルーティング (ISR) (intermediate session routing (ISR)). そのノードを通過するが、エンドポイントは別の場所にあるすべてのセッションに対して、セッション・レベルのフロー制御と障害報告を提供する、APPN ネットワーク・ノード内のルーティング機能の 1 タイプ。

国際標準化機構 (ISO) (International Organization for Standardization (ISO)). 製品やサービスの国際的な交流を容易にするため、また知的、科学的、技術的、経済的活動の分野における相互協力を進めるための標準化を推進するために設立された国際的な組織。

国際電気通信連合 (ITU) (International Telecommunication Union (ITU)). 世界の周波数割り振りおよび無線規制を含めて、標準化された通信手順および実施要領を提供するために設立された米国の特殊通信機関。

インターネット (internet). 一組のルーターによって相互接続され、1 つの大規模ネットワーク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着信先が、データグラムの発信元に戻される。 ICMP は、インターネット・プロトコルの一部である。

インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP)). 例外通知、メトリック通知、および PING サポートを提供するバーチャル・ネットワーキング・システム (VIrtual NEtworking System (VINES))。*ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP))* も参照。

インターネット技術特別調査委員会 (IETF) (Internet Engineering Task Force (IETF)). インターネットの短期的な技術問題の解決を担当する、インターネット体系委員会 (IAB) の特別調査委員会。

インターネットワーク・パケット交換機能 (IPX) (Internetwork Packet Exchange (IPX)). (1) Novell のサーバー、または IPX を実装したワークステーションまたはルーターと、他のワークステーションを接続するために使用される、ネットワーク・プロトコル。 IPX は、インターネット・プロトコル (IP) に類似しているが、異なるパケット・フォーマットおよび用語を採用している。 (2) *Xerox ネットワーク・システム (XNS) (Xerox Network Systems (XNS))*も参照。

インターネット・プロトコル (IP) (Internet Protocol (IP)). 1 つのネットワークまたは相互接続ネットワークを通してデータをルーティングするコネクションレス・プロトコル。 IP は、上位のプロトコル・レイヤーと物理ネットワーク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。

相互運用性 (interoperability). ユーザーが装置固有の特性をほとんど (または、まったく) 知らなくても、種々の機能単位間で通信したり、プログラムを実行したり、あるいはデータを転送できること。 (T)

エリア内ルーティング (intra-area routing). インターネット通信において、エリア内部でデータをルーティングすること。

逆アドレス解決プロトコル (InARP) (Inverse Address Resolution Protocol (InARP)). インターネット・プロトコルにおいて、事前設定されたハードウェア・アドレスを使用してプロトコル・アドレスを見付けるために使用されるプロトコル。フレーム・リレー文脈において、データ・リンク・コネクション識別子 (DLCI) は、事前設定ハードウェア・アドレスと同義。

IPPN. 他のプロトコルが IP を通してデータをトランスポートする場合に使用するインターフェース。

IP アドレス (IP address). インターネット・プロトコル、標準 5、Request For Comments (RFC) 791 によって定義された 32 ビット・アドレス。通常は、ドット付き 10 進表記で示される。

IP データグラム (IP datagram). インターネット・プロトコルにおいて、インターネットを通して伝送される情報の基本単位。発信元と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 あて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 (L2TP Access Concentrator) (LAC). PPP プロトコルと L2TP プロトコルの両方の取り扱いが可能な 1 本または複数本の公衆交換電話網 (PSTN) または ISDN 伝送路に接続された集線装置。装置 には、L2TP が稼働する媒体をインプリメントする必要がある。 L2TP は 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) にトラフィックを渡す。L2TP は、PPP ネットワークが伝えるプロトコルであれば、いずれもトンネル伝送することができる。

L2TP ネットワーク・サーバー (L2TP Network Server) (LNS). LNS は、PPP エンド・ステーションとなりうるプラットフォームであればどこでも動作する。 LNS は L2TP プロトコルのサーバー側を処理する。 L2TP では到着する L2TP トンネル経路が通る媒体は 1 つだけなので、 LNS には単一の LAN または WAN インターフェースしかないが、LAC でサポートされる全範囲の PPP インターフェースのどれから到着する呼でも終了することができる。これには非同期 ISDN、同期 ISDN、 V.120、およびその他のタイプの接続が含まれる。

L2TP アクセス集線装置 (LAC) (L2TP Access Concentrator (LAC)). PPP プロトコルと L2TP プロトコルの両方を扱うことができる 1 つまたは複数の公衆サービス電話網 (PSTN) 回線または ISDN 回線に接続される集線装置。装置には、L2TP が稼働するためのメディアをサポートする必要がある。L2TP はトラフィックを 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) に渡す。L2TP は、PPP ネットワークによって搬送されたプロトコルをトンネルすることができる。

L2TP ネットワーク・サーバー (LNS) (L2TP Network Server (LNS)). LNS は PPP エンド・ステーションなど任意のプラットフォーム上で稼働する。 LNS は L2TP プロトコルのサーバー側を扱う。L2TP は、L2TP トンネルを通じて到着する単一の媒体にだけ依存しているので、LNS は単一の LAN または WAN インターフェースだけをもつが、LAC によってサポートされる全範囲の PPP インターフェースのうちどのインターフェースから到着する呼び出しも着信する。これらには、非同期 ISDN、同期 ISDN、V.120、およびその他のタイプの接続が含まれる。

LAN ブリッジ・サーバー (LBS) (LAN bridge server (LBS)). IBM トークンリング・ネットワーク・ブリッジ・プログラムにおいて、2 つ以上のリング間で (ブリッジを介して) 転送されたフレームに関する統計情報を保持しているサーバー。 LBS は、LAN 報告機構 (LRM) を通して、これらの統計を該当の LAN マネージャーに送信する。

LAN エミュレーション (LE) (LAN Emulation (LE)). ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

LAN エミュレーション・クライアント (LEC) (LAN Emulation Client (LEC)). エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

LAN エミュレーション構成サーバー (LECS) (LAN Emulation Configuration Server (LECS)). 構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

LAN エミュレーション・サーバー (LES) (LAN Emulation Server (LES)). LAN 着信先を ATM アドレスにする、LAN エミュレーション・サービス・コンポーネント。

LAN ネットワーク管理プログラム (LNM) (LAN Network Manager (LNM)). ユーザーが中央のワークステーションから LAN 資源を管理および監視できるようにする、IBM ライセンス・プログラム。

LAN セグメント (LAN segment). (1) 独立して動作することができるが、ブリッジによってネットワークの他の部分に接続されている LAN の部分 (たとえば、バスまたはリング)。 (2) ブリッジのない環状ネットワークまたはバス・ネットワーク。

レイヤー (layer). (1) ネットワーク体系において、階層式に配列された一組のグループのうちの 1 つで、ネットワーク体系に一致するすべてのシステム間にまたがっている、概念的に完全なサービス・グループ。 (T) (2) 開放型システム間相互接続参照モデルにおいて、7 つの概念的に完全な、階層式に配列されたサービス、機能、およびプロトコルのグループのうちの 1 つで、すべての開放型システム間にまたがっている。 (T) (3) SNA において、他のグループの機能からは論理的に分離されている、関連する機能の集まり。あるレイヤーの機能の実現方式を変更しても、他のレイヤーの機能には影響を与えない。

LE. LAN エミュレーション (LAN Emulation)。 ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

LEC. LAN エミュレーション・クライアント (LAN Emulation Client)。エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

LECS. LAN エミュレーション構成サーバー (LAN Emulation Configuration Server)。構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

LES. LAN エミュレーション・サーバー (LAN Emulation Server)。 LAN 着信先を ATM アドレスにする、LAN エミュレーション・サービス・コンポーネント。

回線交換 (line switching). *サーキット交換 (circuit switching)* の同義語。

リンク (link). リンク接続機構 (伝送媒体) と、2 つのリンク局 (リンク接続機構の両側に 1 つずつ) の組み合わせ。多地点構成またはトークンリング構成では、1 つのリンク接続を複数のリンクで共用できる。

平衡型リンク・アクセス・プロトコル (LAPB) (link access protocol balanced (LAPB)). リンク・レベルで X.25 ネットワークにアクセスするのに使用されるプロトコル。 LAPB は、ポイント・ポイント通信に使用される全二重、非同期、対称プロトコルである。

リンク・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、送信先サービス・アクセス・ポイント (DSAP)、送信元サービス・アクセス・ポイント (SSAP)、制御フィールド、およびユーザー・データが入っている。

論理区画 (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) 選択された着信先グループに同じデータを伝送すること。 (T) (2) パケットのコピーが可能なすべてのあて先のサブセットだけに伝達される、特殊な形式の同報通信。

マルチパス・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、あて先の方向にある『NBMA ネクスト・ホップ』の非同報通信マルチアクセス (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、着信先自体である場合もあれば、 NBMA ネットワーク内にあって、あて先に『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、あて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保守担当者が使用する。

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。*着信先 (destination)* も参照。

孤立回線 (orphan circuit). その利用可能性が動的に学習される未構成の回線。

P

ペーシング (pacing). (1) オーバーランまたは輻輳 (ふくそう) を防止するために、受信側コンポーネントが送信側コンポーネントの伝送速度を制御する方法。 (2) *フロー制御 (flow control)*、*受信ペーシング (receive pacing)*、*送信ペーシング (send pacing)*、*セッション・レベル・ペーシング (session-level pacing)*、およびバーチャル・ルート (VR) ペーシング *(virtual route (VR) pacing)* も参照。

パケット (packet). データ通信において、1 つのまとまりとして送信および交換される、データと制御信号を含

む 2 進数の列。データ、制御信号、および誤り制御情報が、特定の形式に配列されている。 (I)

パケット・インターネット・グローパー (PING) (packet internet groper (PING)). (1) インターネット通信において、インターネット制御メッセージ・プロトコル (ICMP) エコー要求をあて先に送って応答を待つことにより、あて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). パケットが指定のあて先に到達しない、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。

NBBS ネットワークでは、PCM は音声および FAX データを運ぶための回線エミュレーション・サービス (CES) の代替である。

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。

- モデムを使用して交換回線を介して
- NBBS ネットワークを介して (リモート・コンソールが、イーサネット LAN を通してそのアクセス Nways スイッチに接続されている場合)

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、NBBS 中継線、NBBS ポート、およびコネクションは論理資源である。

NBBS ネットワークでは、資源を活用する前に、それを構成しておくことが必要である。

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着信先に達するために使用するパス。

ルート (経路) ブリッジ (route bridge). 2 つのブリッジ・コンピューターが通信リンクを使用して 2 つの LAN を接続することができる、IBM ブリッジ・プログラムの機能。各ブリッジ・コンピューターは LAN の 1 つに直接接続されており、通信リンクが 2 つのブリッジ・コンピューターを接続する。

ルート拡張機能 (REX) (route extension (REX)). SNA において、サブエリア・ノードと隣接周辺ノード内のネットワーク・アドレス可能単位 (NAU) 間のパス部分を形成する、周辺リンクを含めたパス制御ネットワーク・コンポーネント。*明示ルート (ER) (explicit route (ER))*、*パス (path)*、および*バーチャル・ルート (VR) (virtual route (VR))* も参照。

ルート選択制御ベクトル (RSCV) (Route Selection control vector (RSCV)). APPN ネットワーク内のルートを記述する制御ベクトル。 RSCV は、発信元ノードからあて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あて先アドレスなど) から得られた情報に基づいて、複数のパスから選ばれる。 (2) 参照モデル・ネットワーク・レイヤーにおいて、類似または異なる体系を使用する 2 つの LAN セグメントを接続する装置。 (3) OSI 用語では、エンティティーに到達できるパスを判別する機能。 (4) TCP/IP では、*ゲートウェイ (gateway)* と同義。 (5) *ブリッジ (bridge)* と対比。

ルーティング (routing). (1) メッセージを着側に到達させるためのパスを割り当てること。 (2) SNA において、メッセージ単位で運ばれるパラメーター (伝送ヘッダー内の着信先ネットワーク・アドレスなど) によって決められた、ネットワークの特定パスを通ってメッセージ単位を転送すること。

ルーティング・ドメイン (routing domain). インターネット通信において、ルーティング・プロトコルを使用してネットワーク全体の表示が各中間システム内で同一になるようにしている、中間システムのグループ。ルーティング・ドメインは、外部リンクによって相互に接続されている。

ルーティング情報プロトコル (RIP) (Routing Information Protocol (RIP)). インターネット・プロトコルにおいて、領域間のルーティング情報を交換し、インターネット・ホスト間の最適ルートを決めるために使用される、内部ゲートウェイ・プロトコル。 RIP は、リンク伝送速度ではなく、ルート・メトリックに基づいて最適ルートを決める。

ルーティング・ループ (routing loop). コンバージェンスが起こるまで、あるいは関係のネットワークが到達不能とみなされるまで、ルーターが相互間で情報を循環するときに発生する状態。

ルーティング・プロトコル (routing protocol). ルーターが他のルーターを見付け、到達可能なネットワークに達する最善ルートに関する情報を最新に保つために使用される技法。

ルーティング・テーブル (routing table). データグラムを転送したり、接続を確立するために使用されるルート

の集まり。この情報は、ネットワーク・トポロジーと着側への到達可能性を識別するために、ルーター間で受け渡される。

ルーティング・テーブル保守プロトコル (RTMP) (Routing Table Maintenance Protocol (RTMP)). AppleTalk ネットワークにおいて、AppleTalk ルーティング・テーブルを用いて、トランスポート・レイヤーでルーティング情報を生成し、保守する機能を提供するプロトコル。 AppleTalk ルーティング・テーブルは、インターネットを通して、発信元ソケットから着信先ソケットにパケットを伝送する。

ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP)). ルーティング・データベースを維持しているバーチャル・ネットワーキング・システム (VIrtual NEtworking System (VINES)) プロトコルで、VINES ノード間でのルーティング情報の交換を可能にする。*インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP))* も参照。

rsh. ログイン・ステップを完全に飛ばして、リモート UNIX 機械上のコマンド解釈プログラムを呼び出し、そのコマンド解釈プログラムにコマンド行引き数を渡す、rlogin コマンドの変数。

S

SAP. サービス・アクセス・ポイント (service access point) を参照。

シード・ルーター (seed router). AppleTalk ネットワークにおいて、ネットワーク構成データ (たとえば、ネットワーク範囲の数やゾーン・リスト) を維持するルーター。各ネットワークには、少なくとも 1 つのシード・ルーターがある。シード・ルーターは、構成ツールを使用して、最初に設定する必要がある。*非シード・ルーター (nonseed router)* と対比。

セグメント (segment). (1) コンポーネント間または装置の相互間のケーブル区間。セグメントは、1 本のパッチ・ケーブル、相互接続された複数のパッチ・ケーブル、または相互接続された建物ケーブルとパッチ・ケーブルの組み合わせから成る。 (2) インターネット通信において、異なる機械にある TCP 機能の間の転送単位。各セグメントには、制御フィールドとデータ・フィールドが入っており、現在のバイト・ストリーム位置、実際のデータ・バイト、および受信データを妥当性検査するためのチェックサムが付加されている。

分割 (segmenting). OSI において、サポートするレイヤーからの 1 つのプロトコル・データ単位 (PDU) を複数の PDU にマップするためにレイヤーが実行する機能。

シーケンス番号 (sequence number). 通信において、伝送の流れやデータの受信を制御するために、フレームまたはパケットに割り当てられる番号。

シリアル・ライン・インターネット・プロトコル (Serial Line Internet Protocol) (SLIP). シリアル・ライン (たとえば、シリアル・ケーブルまたは電話回線を介したモデムへの RS232 接続) を介した 2 つの IP ホスト間のポイント・ポイント接続上で使用されるプロトコル。

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、照会を同報通信できる機構。
- ワークステーションが、特定タイプのすべてのサーバーの名前とアドレスを見付けるために、NetWare を稼働するすべてのファイル・サーバーを照会することができる機構。

セッション (session). (1) ネットワーク体系において、装置間のデータ通信を目的として、接続の確立、維持、および解放の過程で生じるすべての活動。 (T) (2) 要求に応じて、活動化し、さまざまのプロトコルを提供するように調整し、非活動化することができる、ネットワーク・アクセス可能単位 (NAU) 間の論理結合。 各セッションは、セッション中に交換されるすべての伝送を伴う伝送ヘッダー (TH) の中で固有に識別される。 (3) L2TP

において、ダイヤル・ユーザーと LNS 間でエンドツーエンド PPP 接続が試行されるとき、ユーザーがセッションを開始したか、 LNS がアウトバウンド・コールを開始したかどうかにかかわらず、L2TP はセッションを生成する。そのセッション用のデータグラムは、LAC と LNS 間のトンネルを通じて送信される。 LNS および LAC は、LAC に接続された各ユーザーについての状態情報を保持する。

シンプル・ネットワーク管理プロトコル (SNMP) (Simple Network Management Protocol (SNMP)). インターネット・プロトコルにおいて、ルーターと接続ネットワークを監視するのに使用されるネットワーク管理プロトコル。 SNMP は、アダプテーション・レイヤー・プロトコルである。管理される装置に関する情報が定義され、そのアプリケーションの管理情報ベース (MIB) に保管される。

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、最終着側の代わりに中間ノードによって確認応答されて処理される技法。たとえば、IBM 6611 データ・リンク交換では、SNA フレームはカプセル化して TCP/IP パケットに入れられ、非 SNA 広域ネットワーク・ノードを通って伝送され、別の IBM 6611 によってアンパックされて、最終着側に渡される。スプーフィングの利点は、エンド・エンド・セッションのタイムアウトを防止できることである。

標準 MIB (standard MIB). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理情報構造 (SMI) の管理の下に置かれ、インターネット技術作業部会 (IETF) によって標準とみなされている MIB モジュール。

静的ルート (static route). ルーティング・テーブルに手入力される、ホスト間、ネットワーク・ノード間、またはその両方のルート。

ステーション (station). 通信機能を使用するシステムの入力または出力ポイント。たとえば、通信回線を通してデータを送信または受信することができる、ある特定の場所にある 1 台または複数のシステム、コンピューター、端末、装置、および関連のプログラム。

StreetTalk. バーチャル・ネットワーキング・システム (VINES) において、利用者がネットワークのトポロジーを知らなくても、ネットワーク上の任意のリソースを見付けてアクセスすることができる、ネットワーク全体の固有のネーミング/アドレッシング・システム。*インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP))* および *ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP))* も参照。

管理情報構造 (SMI) (Structure of Management Information (SMI)). (1) シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、ネットワーク管理プロトコルを用いてアクセスできるオブジェクトを定義するのに使用される規則。 (2) OSI において、情報の管理に関連する標準の集合。この集合には、*管理情報モデル (Management Information Model)*および*管理オブジェクト定義の指針 (Guidelines for the Definition of Managed Objects)*が含まれる。

サブエリア (subarea). サブエリア・ノード、接続された周辺ノード、および関連の資源から構成される SNA ネットワークの部分。サブエリア・ノード内では、すべてのネットワーク・アクセス可能単位 (NAU)、リンク、およびサブエリア内のアドレス可能な隣接リンク端末 (接続された周辺ノードまたはサブエリア・ノード内の) は、共通のサブエリア・アドレスを共用し、異なる要素アドレスを持っている。

サブネット (subnet). (1) TCP/IP において、IP アドレスの一部によって識別されるネットワークの部分。 (2) *サブネットワーク (subnetwork)* の同義語。

サブネット・アドレス (subnet address). インターネット通信において、ホスト・アドレスの一部がローカル・ネットワーク・アドレスとして解釈される、基本 IP アドレッシング機構の拡張。

サブネット・マスク (subnet mask). *アドレス・マスク (address mask)* の同義語。

サブネットワーク (subnetwork). (1) 1 組の共通特性 (同一ネットワーク ID など) を持つノードの集まり。 (2) *サブネット (subnet)* の同義語。

サブネットワーク・アクセス・プロトコル (SNAP) (Subnetwork Access Protocol (SNAP)). LAN において、パケットが属している非 IEEE 標準プロトコル・ファミリーを識別する、5 バイトのプロトコル識別子。 SNAP 値を使用して、`$AA` をサービス・アクセス・ポイント (SAP) 値として使用する各プロトコルを区別する。

サブネットワーク接続点 (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ための、サブエリア・ネットワーク内のコンポーネント。相互に対等の立場で協働する複数の SSCP は、ネットワークを複数の制御領域に分割し、各 SSCP が自身の領域内の物理装置および論理装置に対して階層的な制御関係を持つようにすることができる。

システム・ネットワーク体系 (SNA) (Systems Network Architecture (SNA)). ネットワークを通して情報単位を伝送し、ネットワークの構成と運用を制御するための、論理構造、フォーマット、プロトコル、および動作手順の記述。 SNA の階層化された構造により、情報の最終的な発信元と着信先 (つまり、利用者) が、情報交換に使用される SNA ネットワークの特定のサービスや機能から独立し、その影響を受けなくすることができる。

T

TCP/IP. (1) 伝送制御プロトコル/インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)。(2) 本来は米国国防総省によって開発された UNIX に似ている、イーサネットを基礎にしたシステム相互接続プロトコル。 TCP/IP により、レイヤー 4 が TCP でレイヤー 3 が IP のパケット交換方式リサーチ・ネットワークである ARPANET (拡張研究プログラム機関ネットワーク (Advanced Research Projects Agency Network)) の便利性が向上した。

Telnet. インターネット・プロトコルにおいて、リモート端末接続サービスを提供するプロトコル。このプロトコルによって、あるホストのユーザーがリモート・ホストにログオンし、そのホストに直接接続されている端末ユーザーとして対話することができる。

しきい値 (threshold). (1) IBM ブリッジ・プログラムにおいて、『しきい値超過』 オカレンスがカウントされてネットワーク管理プログラムに通知される前に、誤りのためにブリッジを通過して転送されないフレームの最大数として設定される値。 (2) そこからカウンターが 0 まで減分される初期値、または初期値からカウンターが増分または減分されて到達する値。

スループット・クラス (throughput class). パケット交換において、データ端末装置 (DTE) パケットがパケット交換ネットワークを通過する速度。

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・ノード間に同報通信され、各ネットワーク・ノードに完全

に複写される、新規または変更されたリンクまたはノードに関するメッセージ。 TDU には、以下のものを識別する情報が入っている。

- 送信元ノード
- ネットワークの各種資源のノード特性およびリンク特性
- 記述されている各資源の最新の更新のシーケンス番号

トレース (trace). (1) コンピューター・プログラムの実行の記録。命令が実行された順序を表す。 (A) (2) データ・リンクの場合は、送信または受信されたフレームとバイトの記録。

トランシーバー (送受信装置) (transceiver (transmitter-receiver)). LAN において、ホスト・インターフェースをイーサネットのようなローカル・エリア・ネットワークに接続する物理装置。イーサネット・トランシーバーには、ケーブルに信号を送って衝突を検出する電子機器が内蔵されている。

伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP)). インターネット、およびインターネットワーク・プロトコルに関する米国国防総省の規格に準拠するその他のすべての通信ネットワークで使用されている通信プロトコル。 TCP は、パケット交換通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発呼装置を定義する 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, 英字, 数字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

［タ行］

［ナ行］

［ハ行］

［マ行］

［ラ行］

［数字］

A

B

C

D

E

F

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Printed in Japan

SC88-6371-06

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 V3.2 プロトコルの構成 解説書 第 1 巻