アクセス・インテグレーター・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

SD88-6064-00
英文原典：SC30-3990-00

アクセス・インテグレーター・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

英文原典：SC30-3990-00
SD88-6064-00

お願い

本書をご使用になる前に、xviiページの『特記事項』をお読みください。

第 1 版 (1998 年 11 月)

本書は、新版またはテクニカル・ニュースレターで特に断りのない限り、IBM アクセス・インテグレーター・サービスの バージョン 3.2 とそれ以降のすべてのリリースおよび変更に適用されます。

原　典： SC30–3990–00
Access Integration 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 1999.2

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

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

目次

図

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

本書において解説されているライセンス・プログラムおよびそのライセンス・プログラム資料は、「IBMプログラム使用契約書」の契約条件にもとづいて弊社が提供するものです。

本書は、プロダクション使用を目的としたものでなく、いかなる種類の保証も含まれていません。このため、商用および特定の目的への適合性の保証を含め、すべての保証に対し本書は関与しません。

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

以下の用語は米国またはその他の国における IBM 社の商標です。

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 がライセンスしている米国ならびに他の国における登録商標です。

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

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

まえがき

本書には、 IBM 2212 のブリッジング機能およびルーティング機能を構成するのに必要な情報が収められています。本書では、ソフトウェアで提供されるフィーチャーおよび機能のすべてを説明しています。説明されているすべてのフィーチャーおよび機能が、どの IBM 2212 でも提供されるわけではありません。装置に特有のフィーチャーまたは機能については、該当する章または節で、その制約を指摘してあります。

本書は IBM 2212 をサポートし、この製品を “ルーター” または “装置” と呼んでいます。本書の例は IBM 2212 の構成を表していますが、実際の出力は本書のものとは異なる場合があります。示されている例は、ユーザーの装置を構成する際に表示される内容のガイドラインとして使用してください。

本書の対象読者: 本書は、コンピューター・ネットワークの導入と運用を担当する方々を対象にしています。コンピューター・ネットワーキングのハードウェアおよびソフトウェアの使用経験は、プロトコル・ソフトウェアを使用する上で役立ちますが、プログラミングの経験は必要ありません。

追加情報の入手: 本書の印刷後に内容が変更されている場合があります。本書の印刷後に追加情報が得られた場合、または変更が必要になった場合には、構成プログラム・ディスケットのディスケット 1 の中のファイル (README という名前) に入っています。このファイルは ASCII テキスト・エディターで見ることができます。

ソフトウェアについて

IBM アクセス・インテグレーター・サービスは、IBM 2212 (ライセンス・プログラム番号 5639-F73) 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、装置に導入されたアクセス・インテグレーター・サービスの基本コードを構成、監視、および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通してローカルでアクセスすることも、Telnet セッションまたはモデムに接続された装置を介してリモートからアクセスすることもできます。

  基本コードは工場で 2212 にインストールされています。
- IBM アクセス・インテグレーター・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、スタンド・アローン型ワークステーションから装置を構成できるようにするグラフィカル・ユーザー・インターフェースです。構成プログラムには、エラー検査とオンライン・ヘルプ情報が含まれています。

  構成プログラムは、工場でプリロードされていません。装置とは別に、ソフトウェアの発注の一部として納入されます。

IBM アクセス・インテグレーター・サービス用の構成プログラムは、IBM ネットワーキング・テクニカル・サポートのホーム・ページからも入手できます。サーバーのアドレスおよびディレクトリーについては、*マルチプロトコル / アクセス・サービス製品、構成プログラム 使用者の手引き*、GC88-6657 を参照してください。

本書の表記上の規則

本書では、コマンドの構文およびプログラムの応答を表示するのに、以下の規則を使用しています。

1. コマンドの省略形は、次の例にあるように、下線を付けて表されています。

   ```
   reload
   ```

   この例では、コマンド全体 (reload) を入力することも、その省略形 (rel) を入力することもできます。

2. パラメーターについてのキーワード選択項目は、大括弧で囲まれ、「または」の語で区切られています。たとえば、

   ```
   command [keyword1 または keyword2]
   ```

   キーワードの 1 つをパラメーターの値として選択してください。

3. オプションの後に 3 つのピリオドが続いている場合は、そのオプションの後に追加データ (たとえば、変数) を入力することを示しています。たとえば、

   ```
   time host ...
   ```

   この例では、ピリオドの代わりにホストの IP アドレスを入力します (このコマンドの説明の箇所に説明してあります)。

4. コマンドに応答して表示される情報では、オプションの省略時値を、オプションの直後に大括弧に入れて示してあります。たとえば、

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

   この例では、ユーザーが STP を指定しなかった場合、デフォルトの媒体は UTP になります。

5. キーボードのキーの組み合わせは、本文の中で次のように表示しています。

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

   キーの組み合わせ **Ctrl -** は、Ctrl キーとハイフンを同時に押す必要があることを示しています。一定の状況下では、このキーの組み合わせは、コマンド行プロンプトを変更します。

6. キーボード・キーの名前は次のように示されています。**Enter**
7. 変数 (つまり、定義するデータを表すために使用される) はイタリックで示されます。たとえば、次のようになります。

   ファイル名: *filename.ext*

ライブラリーの概説

以下のリストは、IBM 2212 ライブラリーの資料をタスク別に並べています。

情報の更新および訂正: 資料が印刷された後に組み込まれた技術変更、説明、および修正の最新の情報を入手するには、次のアドレスで、IBM 2212 のホーム・ページを参照してください。

`http://www.networking.ibm.com/2212/2212prod.html`

計画

GA88-6571

IBM 2212 入門と計画の手引き

この資料は IBM 2212 と一緒に出荷されます。導入の準備の仕方と初期構成の方法について説明しています。

導入

GA88-6572

IBM 2212 アクセス・ユーティリティー導入および初期構成の手引き

この小冊子は IBM 2212 と一緒に出荷されます。IBM 2212 の導入方法とその導入の検査方法について説明しています。

GX27-4048

2212 Hardware Configuration Quick Reference

この参照カードは、IBM 2212 が正しい状態にあるかどうかを調べるのに使用するハードウェア構成情報を記入し、保管しておくために使用します。

診断および保守

GY27-0362

IBM 2212 Access Utility Service and Maintenance Manual

この資料は IBM 2212 と一緒に出荷されます。IBM 2212 に関する問題を診断し、修理する方法を示しています。

運用およびネットワーク管理

以下のリストは、アクセス・インテグレーター・サービス プログラムをサポートする資料を示しています。

SD88-6062

ソフトウェア使用者の手引き

この資料では、以下について説明しています。

- アクセス・インテグレーター・サービス ソフトウェアの構成、監視、および使用方法。
- アクセス・インテグレーター・サービス Nways マルチプロトコル・アクセス・サービスのコマンド行ユーザー・インターフェースを使用して、IBM 2212 と一緒に出荷されるネットワーク・インターフェースおよびリンク・レイヤー・プロトコルを構成および監視する方法。

SD88-6063

AIS 機構の使用と構成

SD88-6064

プロトコルの構成と監視 解説書 第 1 巻

SD88-6065

プロトコルの構成と監視 解説書 第 2 巻

この 2 つの資料は、アクセス・インテグレーター・サービスのコマンド行ユーザー・インターフェースにアクセスし、これを使用して、製品と一緒に出荷されるルーティング・プロトコル・ソフトウェアの構成および監視を行う方法について説明しています。

装置がサポートする各プロトコルに関する情報も含まれています。

SC88-6373

イベント・システム・メッセージの手引き

この資料には、出される可能性があるエラー・コードのリストとエラーの説明、およびエラーを訂正するための推奨処置が記載されています。

構成

GC88-6657

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

この資料は、構成プログラムの使用法について解説しています。

安全性

SD21-0030

Caution: Safety Information--Read This First

この資料は IBM 2212 と一緒に出荷され、IBM 2212 の導入および保守作業に適用される注意と危険に関するただし書きが掲記されています。

製品情報

URL: **http://www.networking.ibm.com/2212/2212prod.html**

この IBM Web ページは、World Wide Web を通して製品情報を提供しています。

IBM 2212 ソフトウェア・ライブラリーの変更の要約

IBM 2212 は新製品ですが、共通コードを使用します。以下のリストは、バージョン 3.2 で行われた、共通コードの変更に適用されます。

- **新規機能:**
  - IP バージョン 6
    - TCP6、UDP6、Telnet、PING-6 および traceroute-6、ICMPv6、ならびに IPsec
    - ホスト自動構成用の近隣ディスカバリー・プロトコル (NDP)
    - 静的ルート、RIPng、プロトコル独立マルチキャスト密度モード (PIM-DM)、およびマルチキャスト・リスナー・ディスカバリー (MLD)
    - IPv4 ネットワークを介した IPv6 パケットの構成済みまたは自動トンネル伝送
  - 資源予約プロトコル (RSVP)

- IPv4 ネットワーク上のアプリケーションがパケット送達に必要なサービス品質を達成するためにネットワーク資源を予約できるようにする信号送信メカニズム

– シン・サーバー・サポート
  - ネットワーク・ステーションのブート・サーバーとして行動する
  - サポートされるサーバーには、OS/400 上でのネットワーク・ステーション・マネージャー (NSM) R2.5 および 3.0 ならびに Windows NT、OS/390、AIX、および VM といった NFS サーバー用 NSM R3.0 が含まれる

– BSC インターフェース用のバイナリー同期リレー (BRLY)サポート

  IPv4 ネットワークを介したパートナー 2210 または 2212 ルーターへの BISYNC 同期 (BSC) 伝送をトンネル伝送するための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
  - 大量の ELS メッセージの取り込み、形式設定、およびオフロードを行うためのイベント・ログ・システム (ELS) 拡張
  - 複数の圧縮ダンプ・ファイルを保守するためのサポート
  - 再ロードと再始動の間持続する構成ツールからの時間指定構成変更サポート
  - PPP、フレーム・リレー、および V.34 インターフェースのためのパケット・トレース・サポート

– フレーム・リレーを介したソース・ルート・ブリッジングのためのマルチアクセス・ブリッジ・ポートのブリッジング・サポート。マルチアクセス・ポートは、拡張を容易にするために、単一のブリッジ・ポートで多数の DLCI を受け入れます。

– DIAL
  - Microsoft ダイヤルアップ・ネットワーク・クライアントによってサポートされている機能の DIAL サポート
    • コールバック・コントロール・プロトコル (CBCP) のサポート
    • Microsoft ポイント・ポイント暗号化 (MPPE) および Microsoft PPP CHAP (MS-CHAP) のサポート
  - Shiva パスワード認証プロトコル (SPAP) が使用される場合にダイヤルアップ接続を中断および再開するためのバーチャル・コネクション

– IP 項目
  - IP 優先順位/TOS フィルター拡張
  - ポリシー・ベース・ルーティング
  - インターフェース別の IP MTU の構成
  - IBM 6611 ルーター・ネットワークの移行を容易にするための OSPF 拡張
  - 近隣ごとのポリシーの BGP-4 サポートおよびパス選択のための追加属性
  - DVMRPv3 サポート
  - IGMP プルーニングおよびグラフティング・サポート

– コーラー ID に基づくコールバックおよびコール・ブロック化のための ISDN サポート

- 2212 が自身と別のルーターとの間に L2TP トンネルを作成できるようにする L2TP クライアント・モデルのための L2TP サポート。このトンネルは、2212 に入るどのトラフィックにも使用できます。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するよう、L2TP ネットワーク・サーバー (LNS) 機能も拡張されました。
- ネットワーク・ディスパッチャー項目
  - 無国籍 UDP アプリケーションのサポート
  - ネットワーク・ニュース転送プロトコル (NNTP)、ポスト・オフィス・プロトコル (POP3)、シンプル・メール転送プロトコル (SMTP)、および Telnet のための新規プロトコル・アドバイザー
  - TN3270 サーバーを平衡化していると、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 2212 に入ります。
- ACE/サーバーを使用した PPP 認証のサポート
- セキュリティー機能強化
  - 最大 2 つのネスト・レベルのセキュリティー・アソシエーションを作成するための IPsec トンネル内トンネル・サポート
  - IPsec ESP NULL アルゴリズム・サポート
  - パス MTU の *don't fragment* ビットおよび伝達を設定するための IPsec サポート
  - IPsec の高度な動的再構成
- PPP 専用回線、ISDN、V.25bis、および V.34 接続を束ねるための混合媒体マルチリンク PPP サポート
- APPN 拡張
  - APPN SDLC 2 次マルチポイント・サポート
  - あらゆるリンク・ステーション・タイプについての APPN 伝送グループ (TG) 番号の構成
  - Talk 5 内での APPN Ping (APING) コマンドのサポート
  - 新規トレース・オプション
- TN3270 拡張

  注: これらの TN3270 拡張は、V3.2 の初期リリースでは使用できませんでしたが、1998 年 12 月 31 日までには、2212 Web サーバー上で使用できるようになります。
  - SNA LU を名前付きのプールにグループ分けできるようにする TN3270 LU プール・サポート
  - LU 名への TN3270 IP アドレスのマッピング
  - 自己定義従属 LU (SDDLU) および動的定義従属 LU (DDDLU) サポート
  - 複数 TCP ポート・サポート
- DLSw 拡張
  - 重複 MAC アドレスのサポート
  - リモート SDLC 装置が連絡するまで SDLC 投資のポーリングを遅らせるためのサポート
- X.25 拡張

- ある範囲の PVC を定義するための構成サポート
- 最大 2500 の PVC のサポート

– スイッチド・バーチャル・サーキットのためのフレーム・リレー・サポート

– 番号制の RIP、無番号 RIP、および静的ルーティングのためのサポートを含む、フレーム・リレー・パーマネント・バーチャル・サーキット (PVC) 上の IPXWAN サポート

- **変更の説明と訂正箇所の表示**

  技術的な変更および追加は、変更箇所の左側に縦線 (|) を付けて表示してあります。

ヘルプの入手

コマンド・プロンプトでは、そのレベルで利用可能なコマンドのリストの形でヘルプを入手することができます。これを行うには、 **?** (**help** コマンド) を入力してから、 **Enter** を押します。**?** は、現行のレベルから利用可能なコマンドをリストするのに使用します。通常は、特定のコマンド名の後に **?** を入力して、そのオプションをリストすることができます。たとえば、* プロンプトで **?** を入力すると、以下の情報が表示されます。

```
*?

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

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

下位レベル操作環境の終了

ソフトウェアの複数レベルの性質から、2212 を構成または操作するときに、2 次、 3 次、またはさらに低いレベルの環境に入ります。次に高いレベルに戻るには、 **exit** コマンドを入力します。2 次レベルに戻るには、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。

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

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

1 次レベル (OPCON) を表示する必要がある場合は、インターセプト文字 (デフォルトでは **Ctrl P**) を入力します。

変更の要約

第1部 ブリッジ機能の構成および監視

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動作に関する基本的な情報について説明します。本章には、以下の節が含まれています。

ブリッジングの概説

ブリッジというのは、2 つまたはそれ以上のローカル・エリア・ネットワークを結合する装置です。ブリッジは、各接続ネットワークからのデータ・フレームを受け入れ、フレームに入ってい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めます。本来、ブリッジは 2 つまたはそれ以上の同種のネットワークを結合するものでした。*同種 (homogeneous)* という用語は、接続されるネットワークが同一のブリッジング方式および媒体タイプを使用していることを意味しています。その例としては、ソース・ルーティング・ブリッジング方式**のみ** をサポートするネットワーク、あるい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などがあります (これらの方式については、後で説明します)。

現在のブリッジは、異種のネットワーク間の通信も可能です。*異種 (non-homogeneous)* というのは、異なるブリッジング方式が混在することが可能であり、より多くの構成オプションを提供することもできるネットワークのことを言います。4ページの図 1 は、シンプル・ブリッジング構成とコンプレックス・ブリッジング構成の例を示しています。

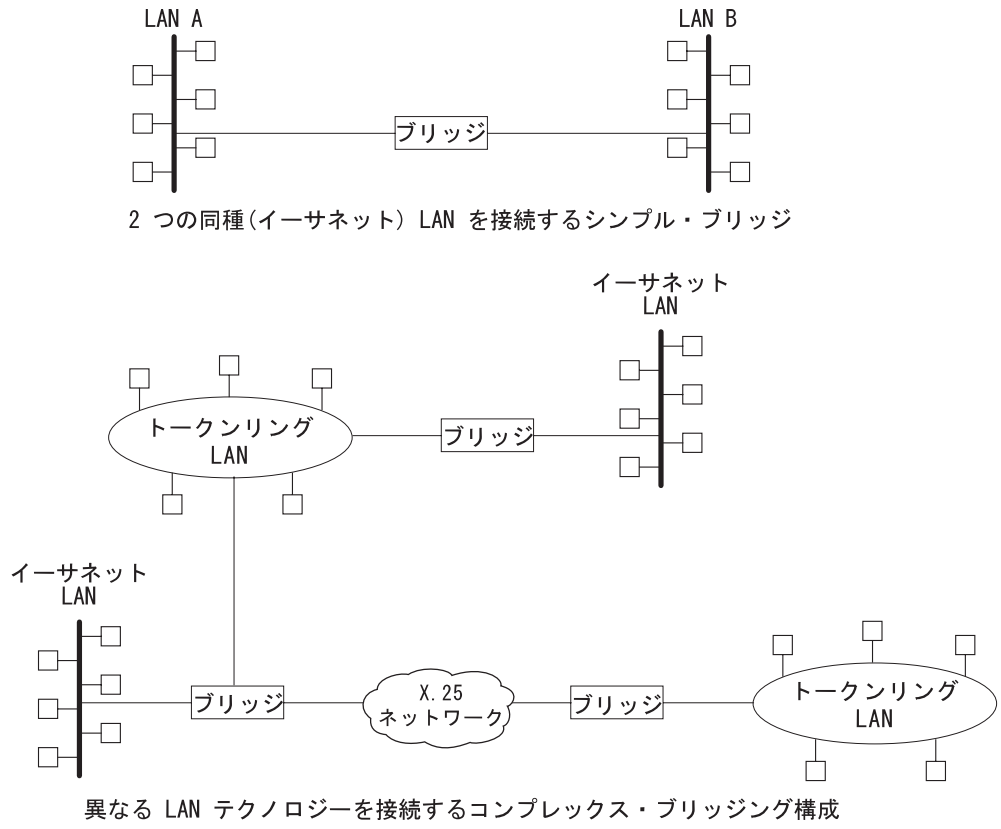


図 1. シンプル・ブリッジング構成とコンプレックス・ブリッジング構成

ブリッジングおよびルーティング

2212 はブリッジングとルーティングの両方の機能を実行することが可能です。プロトコル・フィルターというのは、着信したデータをルートするのか、ブリッジするのかを決めるプロセスを言います。

プロトコル・フィルター

着信データ・パケットを処理するときに、次の処置が取られます。

- 特定のプロトコル転送機能がグローバルに使用可能にされている場合、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、パケットはフィルターに掛けられます。
- ルーティングまたはフィルターの対象にならないパケットは、ブリッジングの候補となり、あて先の媒体アクセス制御 (MAC) アドレスに基づいて判断されます。

5ページの表1 は、『ブリッジかルートか?』 という質問に対して、あて先アドレスの内容に基づいて答を出す方法を示しています。

表 1. ルート/ブリッジ決定表

受信したフレームのあて先 MAC アドレスの内容	ブリッジが取る処置
ブリッジ・アドレス	ブリッジは、フレームをルートするように構成されたプロトコルに、フレームを渡します。
マルチキャストまたは同報通信アドレス	フレーム内に構成されたプロトコルがある場合、フレームはルートされます。そうでない場合、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。

インターフェースごとでのルーティングおよびブリッジング

IP、IPX、、および AppleTalk の場合、特定のインターフェースを介してのルーティングまたはブリッジングには以下の規則が適用されます。

- 特定のプロトコルが受信インターフェース用に構成されている場合、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、パケットは受信インターフェース上でフィルターに掛けられます。
- ルーティングまたはフィルターの対象にならないパケットは、ブリッジングの候補となり、あて先の媒体アクセス制御 (MAC) アドレスに基づいて判断されます。

ルーターの接続

レイヤー 3 でルーターに接続すると、地理的に遠い場所にあるエンド・ステーション間の接続可能性およびパス選択が提供されます。ルーティング・プロトコルを用いて、遠方にあるさまざまな LAN と接続するための最善のパスを選択することができます。大規模ネットワークでは、多様なネットワークおよびサブネットワーク構成オプションが利用可能なので、通常はネットワーク・レイヤーを通して LAN を接続するのが望ましい方法です。また、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でも非常に効率的に情報を移動できることが実証されています。

ブリッジの接続

レイヤー 2 でブリッジに接続すると、物理リンクを介した接続可能性が提供されます。この接続は、基本的には、ネットワークに接続されたホストに対して 『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』 とは考えられていません。ソース・ルーティングおよび透過型ブリッジの詳細については、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、物理的 (レイヤー 3 は論理的であるのに対して) アドレッシング機構、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・フレームの順次配信を維持します。上位レイヤー・プロトコルから分離されていることは、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、上位レイヤーのプロトコル情報を気にする必要がありません。これにより、処理のオーバーヘッドが軽減され、ネットワーク・レイヤーのプロトコル・ト

ラフィックの通信が速くなります。ブリッジはレイヤー 3 の情報には無関係なので、2 つまたはそれ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 (たとえば、IP または IPX) を転送することも可能です (ルーターと同様に)。

さらにブリッジは、レイヤー 2 フィールドに基づいてフレームをフィルターに掛けることもできます。このことは、特定タイプのフレームのみ、あるいは特定のネットワークから発信されたフレームのみを受け入れて転送するようにブリッジを構成できることを意味しています。このようにフィルターを構成できることは、効率的なトラフィック・フローを維持するために非常に役立ちます。

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便利です。大規模ネットワークにおけるブリッジングの利点をまとめると、以下のようになります。

- ブリッジングにより、ネットワークの特定区域を分離し、大きなネットワーク問題にさらされる危険を減らします。
- フィルターに掛けることにより、特定セグメントに転送されるトラフィックの量を調整することができます。
- ブリッジは、ブリッジに接続されている 1 つの LAN 上でサポートされる数より多くの相互接続装置間の通信を可能にします。
- ブリッジングは、ノード制限 (1 つのセグメントの総ノード数) を排除します。ローカル・ネットワーク・トラフィックは、他の接続ネットワークのすべてには渡されません。
- ブリッジは、遠距離の LAN セグメントを接続できるので、接続された LAN の『長さ』 を延長します。ブリッジは、レイヤー 2 で 2 つの LAN セグメントを接続するので、より大規模なネットワークを形成できます。これにより、イーサネットにおけるステーション数の過剰やトークンリング体系における 256 というステーション数制限にともなう輻輳 (ふくそう) 問題を解決できます。

ブリッジ対ルーター

ブリッジやルーターのような相互接続装置は、ネットワーク・セグメントを接続するという点では似たような機能を持っています。しかし、それぞれの装置は異なる方法で LAN 間の接続を確立し、維持します。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て、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

以下の節では、ブリッジの特定のタイプを識別し、それらをハードウェアおよびソフトウェア機能によって分類する方法を説明します。

シンプル・ブリッジ

シンプル・ブリッジは、ローカル・エリア・ネットワークを接続する 2 つまたはそれ以上のリンク・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 の個々の 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、分離されたローカル・エリア・ネットワーク (LAN) を相互接続します。

シンプル・ブリッジの主な機能を要約すると、次のようになります。

- 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 をアドレスとして指定しているフレームを受信します。シンプル・ブリッジは、受信したデータ・フレームのコンテンツやフォーマットを変更しません。また、追加ヘッダーを入れてフレームをカプセル化することも行いません。

  最も単純なブリッジには、ルーティング・アドレス情報とルーティング情報が入っています。最小限として、ブリッジは、渡すべきフレームを判別できるようにするために、各接続ネットワーク上のアドレスを知っていることが必要です。
- ブリッジは、LAN B をアドレス指定しているデータ・フレームを、その LAN の MAC プロトコルを使用して LAN B に再送します。ブリッジが転送するより速くデータ・フレームが到着することがあるので、ブリッジには、ピーク時のデータ通信量に見合う十分なバッファー・スペースが必要です。
- ブリッジは、LAN B から LAN A へのデータ・フレーム・トラフィックも、同様の方法で行います。

コンプレックス・ブリッジ

コンプレックス・ブリッジは、シンプル・ブリッジより複雑な機能を実行します。その一例として、ブリッジは他のブリッジの状態に関する情報を維持します。この情報には、通信パス・コストや各接続ネットワークに到達するために必要なホップ数が含まれます。ブリッジ間で定期的に情報を交換し、すべてのブリッジ情報を更新します。この交換により、ブリッジ間の動的ルーティングが可能になります。

コンプレックス・ブリッジは、フレームを変更し、異なる LAN テクノロジー (たとえば、トークンリング、およびイーサネット) からのパケットを認識し、転送することも可能です。このようなブリッジは *変換 (translational)* ブリッジと呼ばれます。

適応ソース・ルーティング透過型 (ASRT) ブリッジは、2212 に実現されたブリッジ・テクノロジーです。ASRT ブリッジは、上述のいくつかのブリッジング・オプションに追加機能を加えた、ソフトウェア・コンポーネントの集合です。これらの機能のすべてについて、本章の後半で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複数の LAN セグメント間を接続します。この例としては、企業の本社内の各種の LAN を接続す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、異なる地理的区域にある複数の LAN セグメントを接続します。この例としては、企業の本社の LAN と全国の支社の LAN を接続するブリッジがあります。この構成は、地理的区域が異なっているので、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・ブリッジとローカル・ブリッジには、相違点がいくつかあります。大きな相違点の 1 つは、データの転送速度です。WAN 接続は LAN 接続より遅いことがあります。この速度の違いが、時間に敏感なアプリケーションを実行する際には、非常に大きな相違になる可能性があります。もう 1 つの相違点は、リモート・ブリッジとローカル・ブリッジを LAN に接続する物理的な方法です。ローカル・ブリッジは、ローカル・ケーブル媒体 (たとえば、イーサネット、Thinet) を介して接続します。リモート・ブリッジは、シリアル・ラインを介して接続します。

基本的なブリッジ動作

IEEE 802 LAN 標準により、ステーション・アドレスはすべて MAC レベルで指定されます。論理リンク制御 (LLC) レベルで指定できるのは、SAP (サービス・アクセス・ポイント) アドレスだけです。したがって、MAC レベルが、ブリッジが機能するレベルということになります。このレベルでブリッジング機能がどのように実行されるのかを、以下の例で説明します。

動作例 1: 2 つの LAN を接続するローカル・ブリッジ

図2 は、2 つの別々の LAN 上にあるエンド・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 および MAC レイヤーを持つ 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間でフレームを転送することにより、両者間にデータ・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・プロセスを要約すると、このブリッジは、あて先アドレスがローカル LAN (つまり、転送フレームを受信するインターフェースに接続された LAN) 上にない MAC フレームを受け取ります。次に、それらを該当するあて先 LAN に転送します。このプロセスの全体を通して、2 つのエンド・ステーション内のピア LLC エンティティー間で対話が行われます。体系上は、ブリッジに LLC レイヤーが組み込まれている必要はありません。LLC レイヤーの機能は、OSI モデルの上位レベルから来た MAC フレームを中継するに過ぎないからです。

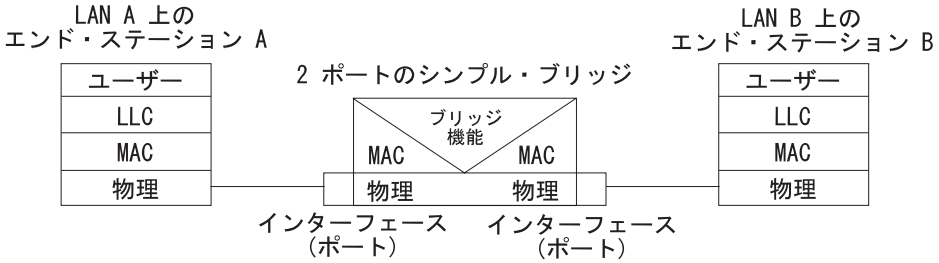


図2. 2 つの LAN を接続する 2 ポート・ブリッジ

動作例 2: シリアル・リンクを介したリモート・ブリッジング

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 および MAC レイヤーを持つ LAN (つまり、2 つのトークンリング LAN) を接続しています。

こ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 フレームを受け取り、その LAN のブリッジを介して該当するあて先 LAN に転送します。このプロセスの全体を通して、2 つのエンド・ステーション内のピア LLC エンティティー間で対話が行われます。体系上は、ブリッジに LLC レイヤーが組み込まれている必要はありません。LLC レイヤーの機能は、OSI モデルの上位レベルから来た MAC フレームを中継するに過ぎないからです。

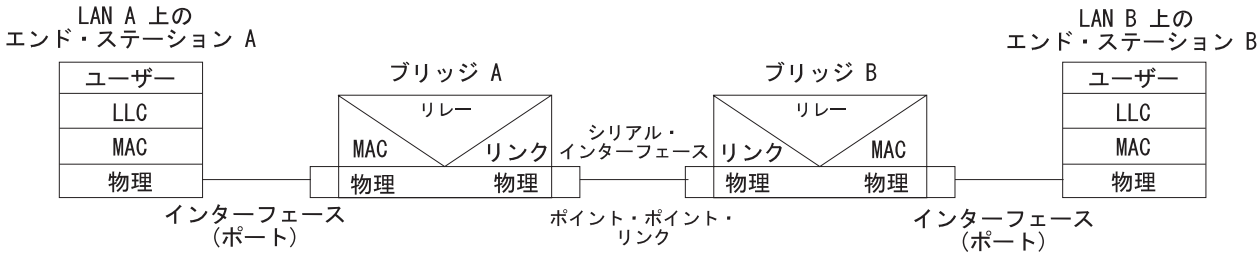


図3. ポイント・ポイント・リンクを介したブリッジング

このブリッジはシリアル・リンクを介してデータ通信を行うので、データはカプセル化されます。図4 は、カプセル化のプロセスを示しています。

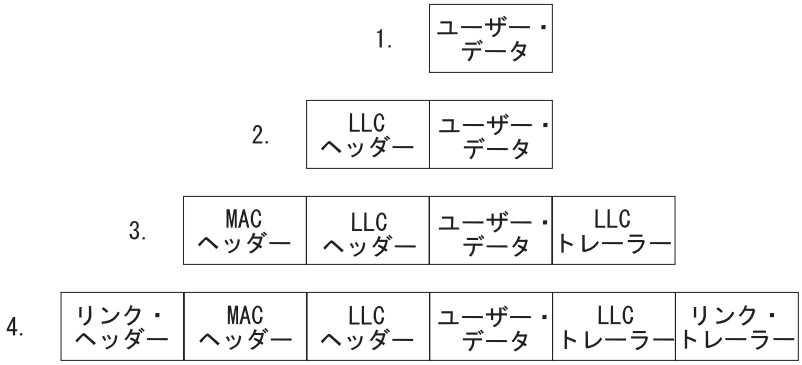


図4. ポイント・ポイント・リンクを介したデータのカプセル化

カプセル化は、次の手順で行われます。

1. エンド・ステーション A が、その LLC にデータを提供します。
2. LLC はヘッダーを付加し、得られたデータ単位を MAC レベルに渡します。
3. 次に、MAC はヘッダー (3) とトレーラーを付加して MAC フレームを作成します。ブリッジ A はこのフレームを受け取ります。
4. ブリッジ A は MAC フレームをそのままあて先 LAN に中継することが役目なので、MAC フィールドを除去しません。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 (たとえば、HDLC) ヘッダーとトレーラーを付加し、その MAC フレームをリンクを介して転送します。

データ・フレームがブリッジ B (ターゲット・ブリッジ) に到達すると、リンク・フィールドが除去され、ブリッジ B は元の、未変更の MAC フレームをあて先 (エンド・ステーション B) に転送します。

MAC ブリッジ・フレームのフォーマット

前に述べたように、ブリッジは、ブリッジされた LAN の個々の MAC エンティティー間でデータ・フレーム (特に、MAC フレーム) を中継することによって、LAN を相互接続します。MAC フレームは、フレーム転送に必要な 『どこ?』 の情報を、発信元アドレスとあて先アドレスの形で提供します。この情報は、データを正常に送受信するために欠かせないものです。

IEEE 802 は 3 つのタイプの MAC フレームをサポートします。つまり、CSMA/CD (802.3)、トークン・バス (802.4)、およびトークンリング (802.5) です。図5 は、ブリッジによってサポートされる MAC フレーム・フォーマットを示しています。特定のフレームについて、以下の節で詳しく説明します。

注: LLC レベルでは、別のフレーム・フォーマットが使用されます。このフレームが該当する MAC フレームに組み込まれます。

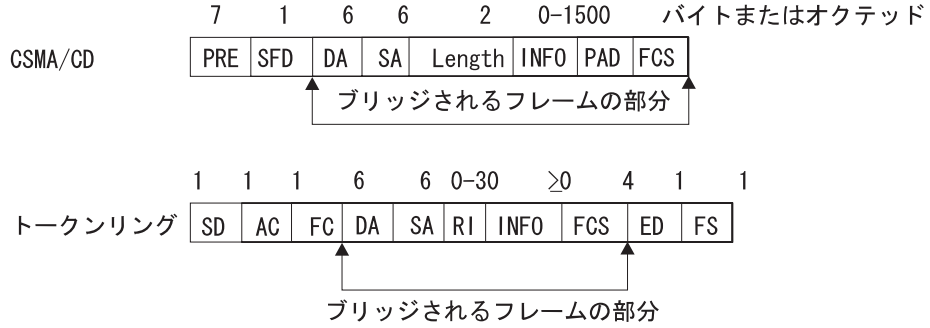


図5. MAC フレーム・フォーマットの例

CSMA/CD (イーサネット) MAC フレーム

CSMA/CD (イーサネット) MAC フレームに含まれる各フィールドについて、以下に説明します。

- *プリアンブル (Preamble (PRE))*。受信側エンド・ステーションがビット同期を確立した後、フレームの最初のビットを見つけるのに使用する 7 ビット・パターン。
- *開始フレーム区切り文字 (Start Frame Delimiter (SFD))*。フレームの開始を示します。

実際にブリッジされるフレームの部分は、以下のフィールドから構成されます。

- *あて先アドレス (Destination Address (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)、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をあて先とする)、またはグ

ローバル・アドレス (全ステーションをあて先とする) です。フォーマットは 48 ビット (6 オクテット) で、特定の LAN 上のすべてのステーションで同一であることが必要です。

- *発信元アドレス (Source Address (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。フォーマットはあて先アドレスのフォーマットと同じであることが必要です。
- *長さ*。後に続く LLC バイトの数を指定します。
- *情報 (Info (INFO))*。サービス・アクセス・ポイント情報、制御情報、およびユーザー・データが入っている、LLC レベルで作成された組み込みフィールド
- *埋め込み (Pad)*。フレームの長さを、正しい衝突検出 (CD) 動作が行われる十分な長さにするバイト・シーケンス
- *フレーム検査シーケンス (Frame Check Sequence (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全フィールドに基づきます。

トークンリング MAC フレーム

トークンリング MAC フレームの各フィールドについて、以下に説明します。

- *開始区切り文字 (Starting Delimiter (SD))*。フレームの開始を示す固有な 8 ビット・パターン
- *アクセス制御 (Access Control (AC))*。PPPTMRRR フォーマットのフィールド。ただし、PPP と RRR は、3 ビットの優先順位と予約変数、M は監視ビット、そして 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、この他にあるのは、終了区切り文字 (ED) フィールドだけです。
- *フレーム制御 (Frame Control (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、このフィールドのビットは、トークンリング MAC プロトコルの動作を制御します。

実際にブリッジされるフレームの部分は、以下のフィールドから構成されます。

- *あて先アドレス (Destination Address (DA))*。CSMA/CD およびトークン・バスと同じです。
- *発信元アドレス (Source Address (SA))*。フレームを発信した特定のステーションを識別します。このフィールドは、2 オクテットまたは 6 オクテットのアドレスです。両方のアドレス長とも、フレーム内の発信元アドレスの後に、ルーティング情報フィールド (RIF) が存在するかどうかを示すルーティング情報表示 (RII) が入っています。これは、次のとおりです。

  RII=1　ルーティング情報フィールドが存在します。

  RII=0　ルーティング情報フィールドは存在しません。

  このフィールドについては、24ページの『ソース・ルート・ブリッジング (SRB)』で詳しく説明します。

- *ルーティング情報フィールド (Routing Information Field (RIF))*。RIF はソース・ルーティング・プロトコルのために必要です。これは、2 オクテットのルーティング

制御フィールドと、一連の 2 オクテットのルート指定フィールドから構成されています。このフィールドについては、24ページの『ソース・ルート・ブリッジング (SRB)』で詳しく説明します。

- *情報 (Info (INFO))*。サービス・アクセス・ポイント情報、制御情報、およびユーザー・データが入っている、LLC レベルで作成された組み込みフィールド。
- *フレーム検査シーケンス (Frame Check Sequence (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全フィールドに基づきます。

最後に、*終了区切り文字 (End Delimiter (ED))* には、エラー検出 (E) ビットおよび中間フレーム (I) ビットが入っています。I ビットは、これが複数フレーム伝送の最終フレームではないことを示します。*フレーム状態 (Frame Status (FS))* には、アドレス認知 (A) ビットとフレーム複写 (C) ビットが入っています。

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 (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、特定の技術について概説した後、その技術によってサポートされるデータ・フレームについて説明します。本章には、以下の節が含まれています。

- 『透過ブリッジング』
- 24ページの『ソース・ルート・ブリッジング (SRB)』
- 31ページの『ソース・ルーティング透過型 (SRT) ブリッジ』
- 34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、通常、スパンニング・ツリー・ブリッジ (STB) とも呼ばれます。*透過* という用語は、ユーザーに*透明* の状態あるいは見えない状態で、ブリッジが接続された LAN に非ローカル・トラフィックを静かに転送することを表しています。エンド・ステーションのアプリケーションは、ブリッジの存在を知りません。ブリッジは、通過するトラフィックを listen することによって、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、同じ LAN に接続されているエンド・ステーションのアドレスのデータベースを作成します。

ブリッジは、フレームを受信するたびに、そのフレームのあて先アドレスをデータベースのアドレスと照合してチェックします。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、フレームは転送されません。あて先が別の LAN 上にある場合、フレームは転送されます。あて先アドレスがデータベースに存在しない場合、フレームは、発信元の LAN を除いて、ブリッジに接続されているすべての LAN 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・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、物理設計ではループが含まれる可能性のあるブリッジ・ネットワークであっても、ループのないトポロジーを形成して維持します。2 つの LAN 間に 2 つ以上のブリッジが接続されているメッシュ・トポロジーでは、*ループ* が起こります。そのような場合、並行するブリッジを通ってデータ・パケットが 2 つの LAN 間で行き来 (バウンス) します。これによりデータ・トラフィックに冗長性が生じ、いわゆるループと呼ばれる現象が起こります。

ループが起こった場合、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、物理的なループを除去することが必要になります。スパンニング・ツリーを使用すれば、自動構成アルゴリズムにより、ループを形成することなく LAN 内のどこにでもブリッジを追加することができます。新しいブリッジが追加されると、スパンニング・ツリー・プロトコルは自動的に LAN 上のすべてのブリッジを再構成し、単一のループのないスパンニング・ツリー を形成します。

ブリッジング方式

スパンニング・ツリーは、2 つのエンド・ステーション間に決して 2 つ以上のアクティブ・データ・ルートを持つことはなく、これによりデータのループを排除します。このアルゴリズムは、データを転送できるブリッジ・ポートと、データをブロックしなければならないブリッジ・ポートを決めて、ループのないトポロジーを形成します。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 構成内の物理的データ・リンク・ループを検出し、排除します。
- *データ・パスの自動バックアップ*。冗長パスに接続されるブリッジは、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。
- *ユーザーによる構成可能性*。ユーザーがネットワーク・トポロジーを調整できるようにします。ときには、デフォルトの設定では希望通りのネットワーク・トポロジーが得られないことがあります。ユーザーがブリッジ優先順位、ポート優先順位、およびパス・コスト・パラメーターを調整し、ユーザーのネットワーク・トポロジーに適したスパンニング・ツリーを形成することができます。
- *シームレスな相互接続性*。多様な通信環境に起因する構成上の制約なしに LAN の相互接続を可能にします。
- *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・プロトコルをコスト効率よくブリッジングします。

ルーターと透過型ブリッジ

スパンニング・ツリー・オプションを備えたルーターの稼働時には、ブリッジとルーターのソフトウェアが同時に実行されます。このモードでは、ルーターはブリッジでもあり、ルーターでもあります。

この稼働時には、次の処置が取られます。

- 特定のプロトコル転送機能がグローバルに使用可能にされている場合、パケットはルーティングされます。
- 特定のプロトコル・フィルターが構成されている場合、パケットはフィルターに掛けられます。
- ルーティングまたはフィルターの対象にならないパケットは、ブリッジングの候補となり、あて先の媒体アクセス制御 (MAC) アドレスに基づいて判断されます。

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・ブリッジを実現します。ネットワーク上のすべての透過型ブリッジ (イーサネットおよびトークンリング) が 802.1D スパンニング・ツリー・ブリッジでなければなりません。このスパンニング・ツリー・プロトコルは、一部の旧ブリッジで使用されていた Digital Equipment Corporation 専有のスパンニング・ツリー・プロトコルを実装しているブリッジとは整合性がありません。

透過型ブリッジの動作

2 つの LAN 間に 2 つ以上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 が並列ブリッジを介してパケットを行き来 (バウンス) させるループ現象が起こる可能性があります。ループというのは、2 つの LAN 間に 複数のデータ・パスが存在する状態を言います。スパンニング・ツリー・プロトコルが動作している場合は、冗長パスをブロックして、自動的にループを排除します。

スタート時に、ハロー・ブリッジ・プロトコル・データ単位 (BPDU) を交換して、ネットワーク内のすべての関係ブリッジが、各ブリッジの構成情報を提供します。BPDU には、ブリッジ ID、ルート ID、およびルート・パス・コストなどの情報が入っています。この情報は、どのブリッジがルート (根) ブリッジであり、どのブリッジが接続された LAN の指定ブリッジであるかを、すべてのブリッジが一斉に判別するのに役立ちます。

HELLO メッセージで交換される情報のうち、スパンニング・ツリーを計算する上で最も重要なのは、以下のパラメーターです。

- *ルート・ブリッジ ID*。 ルート・ ブリッジ ID というのは、そのブリッジのブリッジ識別子です。ルート (根) ブリッジは、それが接続されているすべての LAN の指定ブリッジです。
- *ルート・パス・コスト*。このブリッジのルート (根) ポートを介してルート・ブリッジに到達するまでの指定パス・コストの合計です。トポロジーが変更されると、この情報はルート・ブリッジと指定ブリッジの両方から転送され、すべてのブリッジのパス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・ツリーを決めるために使用するユニーク ID。ネットワーク内の各ブリッジに、固有な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 メッセージを転送したポートの ID。

この情報が得られると、スパンニング・ツリーはその形状と方向を判別し、論理パス構成を作成します。このプロセスを要約すると、次のようになります。

1. ネットワーク内の各ブリッジのブリッジ ID を比較して、そのネットワークのルート・ブリッジを選択する。最低の ID (つまり、最高の値) を持つブリッジが選択されます。
2. スパンニング・ツリー・アルゴリズムが 各 LAN の指定ブリッジを選択する。同じ LAN に 2 つ以上のブリッジが接続されている場合は、ルートまでのパス・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。パス・コストが同一のときは、最低のブリッジ ID を持つブリッジが、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が、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) 状態に入れる。BLOCKED 状態にあっても、ブリッジはハロー BPDU を listen しているので、ネットワークに生じた変更 (たとえば、指定ブリッジに障害が起きるなど) に応じて状態を BLOCKED から FORWARDING (つまり、データを転送する) に変更することができます。

このプロセスを通して、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 LAN ネットワークを、単一のスパンニング・ツリーに絞り込みます。スパンニング・ツリーを使用すると、2 つのエンド・ステーション間に 2 つ以上のア

クティブ・データ・パスが存在することは決してなく、これによりデータのループはなくなります。ネットワーク上の各ブリッジに対して、スパンニング・ツリーは、ループの形成を防止するためにブロックすべきブリッジ・ポートを決めます。

この新規構成は、タイム・ファクターと結び付けられています。指定ブリッジに障害が起こったり、物理的に除去された場合、LAN 上の他のブリッジは、ブリッジ最大エージ時間に設定された時間内にハロー BPDU を受け取らなかった時点で、この状況を検出します。この事象により、別のブリッジを指定ブリッジとして選択するための新規構成プロセスが起動されます。ルート・ブリッジに障害が起きた場合も、新規構成が作成されます。

スパンニング・ツリーの形成

スパンニング・ツリーがデフォルト設定を使用すれば、通常は、スパンニング・ツリー・アルゴリズムは受け入れられる結果を生成します。しかし、ときにはアルゴリズムが低性能のスパンニング・ツリーを形成することもあります。その場合は、ユーザーがブリッジ優先順位、ポート優先順位、およびパス・コストを調整することにより、ユーザーの期待するネットワーク性能を満たすスパンニング・ツリーを形成することができます。次の例で、その方法を説明します。

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を形成している 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・ツリー構成で、デフォルトのブリッジ優先順位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順位が同一なので、最低の物理アドレスを持つブリッジがルート・ブリッジとして選択されます。この例の場合、これはブリッジ 2 です。

ルート・ブリッジからのハロー BPDU が、事前設定された間隔 (ブリッジ・ハロー・タイム) で繰り返し転送されるので、新規に構成されたスパンニング・ツリーはそのままです。このプロセスを通して、指定ブリッジはすべての構成情報を用いて更新されます。その後、指定ブリッジはハロー BPDU からの情報を再生成し、それぞれが指定ブリッジになっている LAN にその情報を配布します。

表 2. スパンニング・ツリーのデフォルト値

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

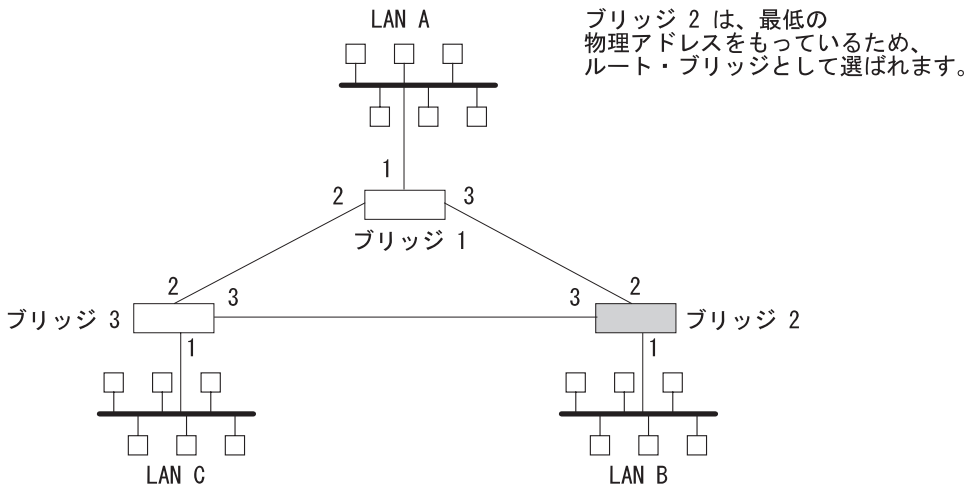


図 6. スパンニング・ツリーの前の LAN ネットワーク

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 (ポート 2) に接続するポートをバックアップ・ポートとして指定し、ループ状態の原因になるので、そのポートがフレーム転送を行うのをブロックします。16ページの表2 のデフォルト値を使用するアルゴリズムによって作成されたスパンニング・ツリーが、図7 に、ブリッジ 1 をブリッジ 2 を接続し、次にブリッジ 2 をブリッジ 3 に接続する太線として示されています。ルート・ブリッジは、ブリッジ 2 です。

このスパンニング・ツリーは、結果的に低性能のネットワークを形成することになります。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のに、ブリッジ 1 とブリッジ 3 の間の直接接続を使用するのではなく、ブリッジ 2 を経由して間接的にしか行けないからです。

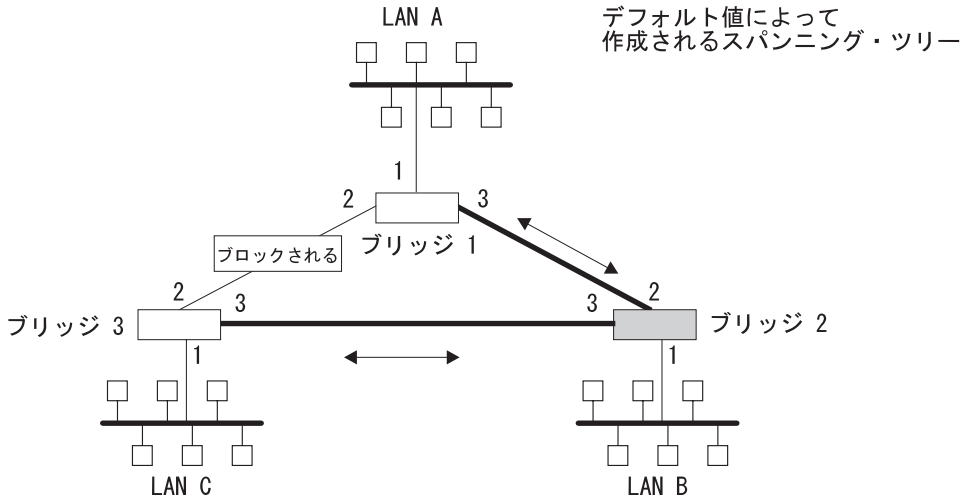


図 7. デフォルト値を用いて作成されたスパンニング・ツリー

通常、このネットワークはブリッジ 2 とブリッジ 3 の間のポートはまれにしか使用しません。そこで、ブリッジ 1 をスパンニング・ツリーのルート・ブリッジにすることによって、ネットワークの性能を改善することができます。これは、ブリッジ 1 に最高の優先順位である 1000 を割り当てることによって実現できます。この修正の結

果としてのスパンニング・ツリーが、図8 に、ブリッジ 1 とブリッジ 3 およびブリッジ 1 とブリッジ 2 を結ぶ太線として示して示されています。この場合のルート・ブリッジは、ブリッジ 1 です。ブリッジ 2 とブリッジ 3 の間の接続はブロックされ、バックアップ・データ・パスの役目を果たします。

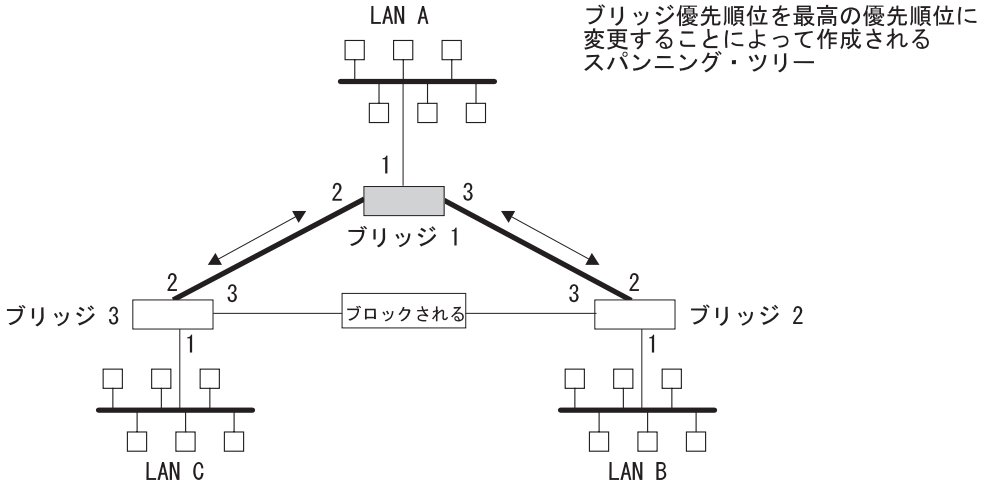


図 8. ユーザーが調整したスパンニング・ツリー

スパンニング・ツリー・ブリッジとイーサネット・パケット・フォーマットの変換

2212 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) ブリッジに従って、ブリッジング・ルーターのパケット転送機能を提供します。このプロトコルは、イーサネット・パケットのパケット変換機能も提供します。

イーサネット/IEEE 802.3 ネットワークは、MAC ヘッダー内の長さ/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・レイヤーと 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、イーサネット・フォーマットへの (からの) 変換を行って、混在する LAN タイプ間に透過性を提供する必要があります。使用されるアルゴリズムは、最新の IEEE 標準に基づいています。

基本的なアプローチは、IEEE 802 SNAP SAP を使用して、イーサネット・パケットを IEEE 802.2 非番号制情報 (UI) パケットに変換することから成っています。SNAP プロトコル識別子は、組織ユニーク識別子 (OUI) 00-00-00 を持っています。最後の 2 バイトは、イーサネット・タイプ 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 を稼働する IBM RT PC、または OS/2 EE を稼働する 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 パケット内に SNA をカプセル化します。この場合は、MAC ユーザー・データ長が入っている特殊な Ethertype ヘッダーと、その後に IEEE 802.2 (LLC) ヘッダーが必要です。

これらのフレームの処理は、ポート単位で使用可能／使用不可にすることができます。使用可能モードのときは、ブリッジはソース・ステーションの動作を確認 (learn) します。フレームのターゲットがそれらのステーションになっている場合、ブリッジは正しいフレーム・フォーマットを生成します。ステーションの動作に関する情報がない場合 (マルチキャスト、または不定ステーションの場合など)、ブリッジは重複するフレームを作成します。1 つは IEEE 802.3 および IEEE 802.2 フォーマットのもので、もう 1 つは IBM-RT ヘッダーを含むものです。

XNS フレームの UB カプセル化

XNS イーサネット・フレームは Ethertype 0x0600 を使用します。トークンリング・フォーマットに変換されるときに、これらのフレームは IEEE 802.1H の指定通りに SNAP を取り込みます。一部のトークンリング・エンド・ステーションでは、このようなフレームのために SNAP 内の Ungermann-Bass OUI を使用するので、このカプセル化を起動するための構成スイッチが用意されています。このカプセル化を起動するスイッチは、**frame token_ring_SNAP** コマンドを使用して設定します。

透過ブリッジングとフレーム・リレー

サーキットでブリッジングが使用可能になっている場合、フレーム・リレー・インターフェースがイーサネットおよびトークンリングから透過フレームの転送を行います。IP トンネル伝送を使用する必要はありません。

ハロー BPDU が生成され、透過ブリッジング用に構成されている各サーキットに転送されます。スパンニング・ツリー・プロトコルは、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・サーキットをブロック (BLOCKED) にさせ、それによってループを排除します。

10/100 イーサネット・アダプターでの透過ブリッジング

10/100 イーサネット・アダプター・ハードウェアは、ブリッジング・ソフトウェアをオフロードするためにローカル LAN パケットの透過型ブリッジ・フィルターを提供します。アダプターが起動すると、フィルターは初期化されて使用可能にされ、次のように機能します。

- アダプターが発信元 MAC アドレスを確認し、それをハードウェア・キャッシュ内に保管します。
- アダプターが各フレーム内のあて先 MAC アドレスを監視します。アダプターは、LAN に対してローカルのアドレスにあてられたフレームをフィルターします。
- アダプターは、エージング・アルゴリズムを使用してハードウェア・キャッシュからアドレス・エントリーを除去します。

透過型ブリッジの用語と概念

この節では、透過ブリッジングで一般的に使用される用語および概念を復習します。

エージング・タイム

エントリーをもつポートが転送状態にあるとき、フィルター・データベースから動的エントリーが除去される前の時間 (エージ) の長さ。動的エントリーがエージング・タイムまでの間に参照されない場合、そのエントリーは削除されます。

ブリッジ

ローカル・エリア・ネットワーク (LAN) を接続する、プロトコルから独立した装置。これらの装置は、データ・リンク・レイヤーで動作し、LAN 間でデータ・パケットを保管および転送します。

ブリッジ・アドレス

スパンニング・ツリー・アルゴリズムによって、ネットワーク上のブリッジを識別するために使用される、ブリッジ識別子の最下位 6 オクテット部分。ブリッジ・アドレスは、デフォルトでは最低番号ポートの MAC アドレスに設定されます。デフォルト・アドレスは **set bridge** 構成コマンドを使用してオーバーライドできます。

ブリッジ・ハロー・タイム

ブリッジ・ハロー・タイムは、スパンニング・ツリーのルート・ブリッジになったときに、ブリッジがハロー BPDU (ブリッジ構成情報が入っている) を送信する頻度を指定します。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・タイムを制御するので、この値はルート・ブリッジに対してのみ有効です。ブリッジ・ハロー・タイムは **set protocol bridge** コマンドを使用して設定します。

ブリッジ転送遅延

ブリッジ・ポートが listening (待機) 状態および learning (確認) 状態に費やす時間の長さ。転送遅延は、スパンニング・ツリー・トポロジーを調整するためにブリッジ・ポートが listen する時間の長さです。これは、スパンニング・ツリーの構成中に、ブリッジが受信する各パケットの発信元アドレスを確認 (learn) するのに費やす時間の長さでもあります。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転送遅延を制御するので、この値はルート・ブリッジに対してのみ有効です。

ルート・ブリッジは、この値をすべてのブリッジに伝えます。この時間は **set protocol bridge** コマンドを使用して設定します。このパラメーターの設定手順については、次章で説明します。

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・ツリーを決めるために使用する固有な識別子。ネットワーク内の各ブリッジには固有なブリッジ識別子が必要です。

ブリッジ識別子は、2 つの部分から構成されています。最下位 6 オクテットのブリッジ・アドレスと、最上位 2 オクテットのブリッジ優先順位です。デフォルトのブリッジ・アドレスは、最低番号のポートの MAC アドレスに設定されます。デフォルト・アドレスは **set bridge** 構成コマンドを使用してオーバーライドできます。

ブリッジ最大エージ

プロトコルが情報を廃棄し、トポロジーが変更される前の、スパンニング・ツリー・プロトコル情報が有効とみなされている時間の長さ。スパンニング・ツリー内のすべてのブリッジは、このエージを使用して、データベース内の受信した構成情報をタイムアウトにします。これにより、スパンニング・ツリー内のすべてのブリッジのタイムアウトが統一されます。ブリッジ最大エージは **set protocol bridge** コマンドを使用して設定します。

ブリッジ優先順位

set protocol bridge コマンドによって設定された、ブリッジ識別子の最上位 2 オクテット部分。この値は、各ブリッジがネットワークのルート・ブリッジになる確率を示します。ブリッジ優先順位を設定することにより、スパンニング・ツリー・アルゴリズムは、最高優先順位をもつブリッジをスパンニング・ツリーのルート・ブリッジとして選択します。最も低い数値をもつブリッジが、最高の優先順位値です。

指定ブリッジ

特定の LAN 上で、ルート・ブリッジに最も近いとされたブリッジ。この近さは、ルート・ブリッジへのパス・コストを累算して測定されます。

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・データベースと固定データベース

LAN に接続された特定のポート番号のポートに属するステーション・アドレスに関する情報が入っているデータベース

フィルター・データベースは、固定データベースからのエントリーによって初期設定されます。これらのエントリーは固定的であり、電源オン/オフやシステム・リセットの後も残ります。スパンニング・ツリー構成コマンドを使用して、これらのエントリーを追加したり、削除したりすることができます。固定データベースのエントリーは、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、エントリー数は SRAM のサイズによって制限されます。

注: エントリー (静的) は、監視コマンドを使用して追加することもできますが、これらのエントリーは、電源オン/オフおよびシステム・リセットの後は***残りません***。

フィルター・データベースは、エージング・タイムが関連付けられている、ブリッジによって確認されたエントリー (動的エントリー) も累積します。エントリーが一定時間 (エージ・タイム) 参照されない場合、それらのエントリーは削除されます。静的エントリーはエージを持たないので、動的エントリーは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固定データベースには、以下の情報が入っています。

- *アドレス*。そのエントリーの 6 バイトの MAC アドレス
- *ポート・マップ*。そのエントリーに関連するすべてのポート番号を指定します。
- *エントリー・タイプ*。次のタイプの 1 つを指定します。
  - 予約エントリー。IEEE 802.1d 委員会によって将来の利用のために確保されています。
  - 登録エントリー。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機能によって使用可能にされたマルチキャスト・アドレスから構成されます。
  - 固定エントリー。構成プロセスで、ユーザーによって入力されます。電源オン/オフおよびシステム・リセットの後も残ります。
  - 静的エントリー。監視プロセスで、ユーザーによって入力されます。電源オン/オフおよびシステム・リセットの後は残らず、エージを持っていません。
  - 動的エントリー。ブリッジによって動的に確認されます。電源オン/オフおよびシステム・リセットの後は残らず、エージが関連付けられています。
  - 空き。自由にアドレス・エントリーを記入できるデータベース内の場所。
- *アドレス・エージ (動的エントリーのみ)*。アドレス・エントリーが廃棄される前にカウントダウンされる時間のレゾリューション。この値はユーザーが設定できます。

固定データベースの変更はスパンニング・ツリー構成コマンドを使用して行い、フィルター・データベースの変更は GWCON 監視プロセスで行います。

並列ブリッジ

同じ LAN を接続する複数のブリッジ

パス・コスト

各ポート・インターフェースにパス・コストが関連付けられています。これは、このポートを使用してブリッジ・ネットワーク内のルート・ブリッジに到達するための相対的な値を示します。スパンニング・ツリー・アルゴリズムは、パス・コストを使用して、ルート・ブリッジからネットワーク・トポロジー内の他のすべてのブリッジへのコストが最小になるパスを計算します。すべての指定コストとルート・ポートのパス・コストの合計を、ルート・パス・コストと呼びます。

ポート

接続された各 LAN または WAN へのブリッジの接続。ブリッジとして機能するためには、ブリッジには少なくとも 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。最上位オクテットはポート優先順位を表し、最下位オクテットはポート番号を表します。ポート番号とポート優先順位は両方ともユーザーが指定可能です。ポート ID はブリッジ内でユニークでなければなりません。

ポート番号

ユーザーが指定するポート ID の 1 オクテット部分で、その値は物理媒体への接続を表します。ゼロのポート番号は使用できません。

ポート優先順位

ポート ID の 2 番目の 1 オクテット部分。この値はポートの優先順位を表し、スパンニング・ツリー・アルゴリズムがポート選択のために比較したり、決定をブロックするのに使用します。

レゾリューション

動的データベースがデータベース内で時間が経過する際にカウントダウンされるタイム・ファクター。範囲は 1 ～ 60 秒です。

ルート・ブリッジ

最高優先順位のブリッジ ID を持っているので、スパンニング・ツリーの *ルート (根)* として選択されたブリッジ。このブリッジは、定期的にハロー BPDU (ブリッジ構成情報が入っている) を 発信することにより、スパンニング・ツリーを完全な状態に保つ責任があります。ルート・ブリッジは、それが接続されているすべての LAN の指定ブリッジです。

ルート・ポート

ルート・ブリッジに最低コストのパスを提供するブリッジ・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 1 つだけデータ・ルートが存在するブリッジの接続形態 (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は、エンド・ステーションのアプリケーションに *透過的* なメカニズムを含んでいます。透過ブリッジングは、スパンニング・ツリー・アルゴリズムによりデータ・フレーム転送を指示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。

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・ネットワークを通してフレームを転送する 1 つの方法で、ソース・ステーションがフレームの通るルートを識別します。分散ルーティング方式では、各ブリッジのルーティング・テーブルが、データがネットワークを通るパスを決めます。これに対して、ソース・ルーティング方式では、ソース・ステーションが、転送されるフレームの中にルート全体を定義します。

ソース・ルーティング・ブリッジ (SRB) は、図9 に示すように、4 Mbps および 6 Mbps のトークンリングを介したローカル・ブリッジングを提供します。また、最高 E1 の速度で動作する通信リンクを介してリモート LAN に接続することも可能です。

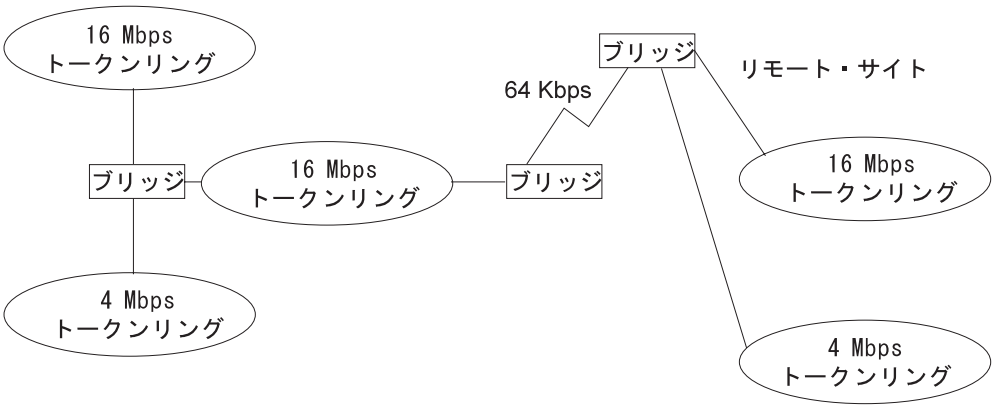


図 9. ソース・ルーティング・ブリッジ接続性の例

ソース・ルーティング・ブリッジが提供するフィーチャーには、次のものが含まれます。

- *ブリッジの通信可能性*。ブリッジを使用して、OS/2、PC LAN マネージャー、および NetBIOS などのシステムを稼働する IBM PC LAN 間を接続することができます。また、ブリッジは PC LAN とメインフレーム間で IBM SNA トラフィックを伝送するともできます。
- *性能と速度*。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・レイヤーで実行されるので、パケット変換やアドレス・テーブルの保守の必要はありません。これによりオーバーヘッドが削減され、ルーティングの決定を迅速に下すことができます。
- *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、性能低下やネットワーク・サイズの制約なしに、相互接続ネットワークを通して希望するあて先エンド・ステーションに、これらのパケットを動的にルーティングすることができます。

  ネットワークの複雑さに関係なく、ソース・ルーティングのエンド・ステーションは、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・ルーティング構成に一般的に見られる 7 ホップという距離制限を解決することができます。この機能により、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 (たとえば、イーサネット・ネットワーク) を介して接続することも可能になります。

ソース・ルーティング・ブリッジの動作

前に述べたように、ソース・ルーティング構成では、ソース・ステーションが転送するフレームの中に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・ディスカバリーおよび転送プロセスに参加します。以下のステップで、このプロセスを説明します。

1. あるソース・ステーションがフレームを送信し、フレームのあて先がそれ自身の (ローカル) セグメントまたはリング上にないことを見つける。
2. ソース・ステーションは *ルート・ディスカバリー* 同報通信フレームを作成し、それをローカル・セグメントに送信する。
3. ローカル・セグメント上のすべてのブリッジがルート・ディスカバリー・フレームを受け取り、それぞれの接続ネットワークを介してそのフレームを転送する。

   ルート・ディスカバリー・フレームがあて先エンド・ステーションの探索を続ける間、それを着信転送する各ブリッジは、自分のブリッジ番号とセグメント番号をフレームの情報フィールド (RIF) に追加します。フレームがブリッジ・ネットワークを通過し続ける間に、RIF はあて先までのパスを説明する、ブリッジ番号とセグメント番号の組みからなるリストを編成します。

   同報通信フレームが最後にそのあて先に到着したときには、フレームには発信元からあて先までの正確な順序のアドレスが入っています。
4. あて先エンド・ステーションは、フレームを受信すると、通信のルート・パスが入っているレスポンス・フレームを生成する。ブリッジ・ネットワークの他の部分をさまよっているフレームは (その間に無関係のルーティング情報が蓄積されます)、決してあて先エンド・ステーションに到達せず、どのステーションも永久にそれらを受信しません。
5. ソース・ステーションが、確認されたルート・パスを受け取る。これにより、この確立されたパスを介して情報を転送することができます。

ソース・ルーティング・フレーム

前に述べたように、ブリッジは、ブリッジ LAN の個々の MAC エンティティー間のデータ・フレーム (特に、MAC フレーム) を中継することによって、LAN を相互に接続します。MAC フレームは、フレーム転送に必要な 『どこ?』 の情報を、発信元アドレスとあて先アドレスの形で提供します。この情報は、データを正常に送受信するために欠かせないものです。

ソース・ルーティングでは、データ・フレームの転送の決定は、フレーム内のルーティング情報に基づいて行われます。フレームを転送する前に、エンド・ステーションは*ルート・ディスカバリー・プロセス*により、あて先ステーションへのルートを入手します。フレームを生成するソース・ステーションは、転送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んで、フレームが通るルートを指定します。各種タイプのソース・ルーティング・ブリッジ・フレームを詳しく見ていくうちに、ブリッジがこのルーティング情報を入手し、転送する様子を理解できるようになると思います。

ソース・ルーティング MAC フレームには、マルチリング環境を介したデータ通信に必要なルーティング情報が入っているので、そのフォーマットは典型的なトークンリング MAC フレームとはいくぶん異なっています。発信元アドレス・フィールド内

の RII が 『1』 のときは、ルーティング情報が入っている RIF が、発信元アドレスの後に続いていることを示しています。図10 は、ソース・ルーティング・フレームの発信元アドレス・フィールドの詳細なフォーマットを示しています。

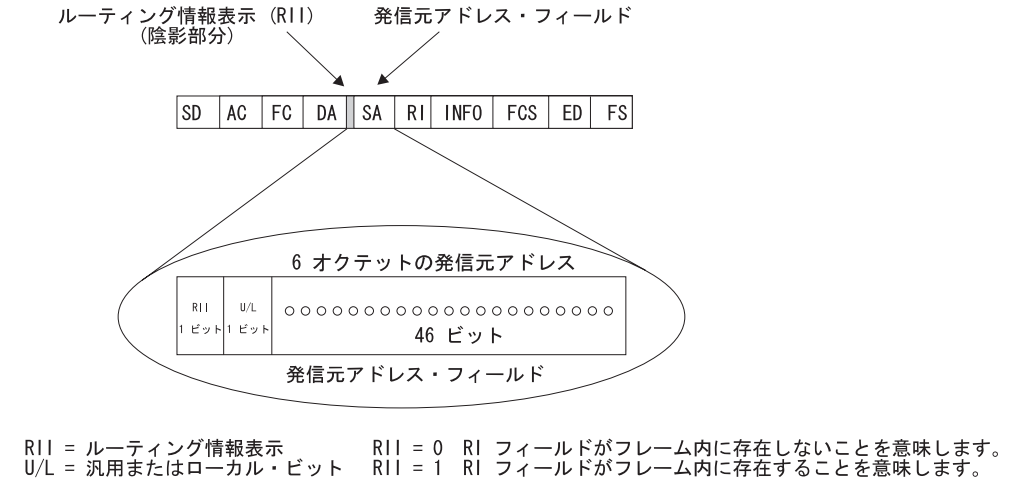


図 10. 802.5 発信元アドレス・フォーマット

発信元アドレス・フィールドの RII が 1 にセットされているときは、発信元アドレスの後に RIF があります。RIF は、ソース・ルーティングでルート情報を提供するものなので必ず必要です。これは、2 オクテットのルーティング制御 (RC) フィールドと、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ています。図 11 は、ルーティング情報フィールドの詳細なフォーマットを示しています。

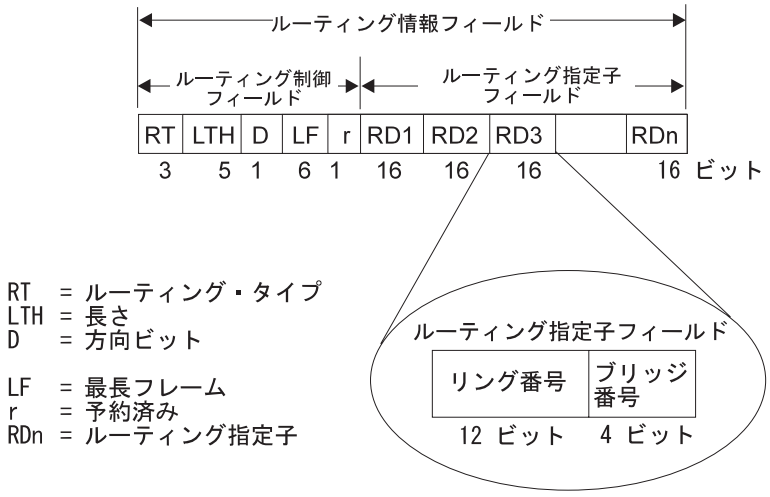


図 11. 802.5 ルーティング情報フィールド

RIF の各フィールドについて、以下に説明します。

- **ルーティング・タイプ (RT)**

  ネットワーク上の特定ルートを通ってフレームを転送するのか、あるいはすべての相互接続された LAN に到達するルートを通って転送するのかを、ビットの設定値によって指示します。このフィールドのビット設定値に基づいて、ソース・ルーティング・フレームを次のタイプの 1 つとして識別することができます。

- 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)
- 特別ルート・フレーム (ルーティング・フレーム)
- スパンニング・ツリー・ルート・フレーム (ルーティング・フレーム)

全パス探索フレーム は、RT ビットが 100 にセットされているときに存在します。これらのフレームは、ネットワーク上の反復しないすべてのルート (発信元からあて先まで) で生成され、ルーティングされます。このプロセスの結果、ソース・エンド・ステーションからあて先エンド・ステーションまでの間に存在するルートの種類と同じ数のフレームが、あて先に到着することになります。このルーティング・タイプは、スパンニング・ツリーに沿って利用可能なすべてのルートを使用して現行のソース・ステーションに送られた、ルート・ディスカバリー・フレームを受信したことに対するレスポンスです。転送するブリッジは、ルーティング指定子をフレームに追加します。

スパンニング・ツリー探索フレーム は、 RT ビットが 110 にセットされているときに存在します。 スパンニング・ツリー・ブリッジのみが、このフレームをあるネットワークから別のネットワークにリレーします。このことは、フレームはネットワーク上の各リングに 1 回しか現れず、したがってあて先エンド・ステーションにも 1 回しか現れないことを意味しています。ルート・ディスカバリー・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、ルーティング指定子フィールドをフレームに追加します。また、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あてに送信するフレームにも使用できます。これについては、次節で詳しく説明します。

特別ルート・フレーム は、最初の RT ビットが 0 にセットされているときに存在します。この場合、特定のルーティング情報が入っているルート指定子 (RD) フィールドが、フレームがネットワークを経由してあて先アドレスまで案内します。フレームがあて先に到着し、ルート・パスが見つかると、あて先ステーションは特別ルート・フレーム (SRF) をソース・ステーションに戻します。ソース・ステーションは、データを特別ルート・フレームに入れて転送します。

- **長さビット (LTH)**。RI フィールドの長さ (オクテット) を示します。
- **方向ビット(D)**。フレームが接続ネットワークを移動する方向を示します。このビットが 0 にセットされている場合、フレームはルーティング情報フィールドに指定されている順序 (たとえば、RD1 から RD2 ... RDn) で接続ネットワークを移動します。方向ビットが 1 にセットされている場合には、フレームは逆の順序でネットワークを移動します。
- **最大フレーム・ビット (LF)**。2 つの通信エンド・ステーション間で特定のルートを通して送信できる INFO フィールドの最大フレーム・サイズを示します。LF ビットは、STE および ARE フレームに対してのみ有効です。特別ルート・フレーム (SRF) の場合、ブリッジは LF ビットを無視し、それを変更することはできません。探索フレームを発信するステーションは、LF ビットを、そのステーションが扱える最大フレーム・サイズにセットします。着信転送するブリッジは LF ビットを、少なくとも以下を超えない最大値にセットします。
  - 受信した LF ビットに指定されている値
  - ブリッジによって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
  - フレームを受信したポートによってサポートされる最大 MSDU サイズ

– フレームを転送する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、あて先ステーションはさらに LF 値を減じて、その最大フレーム容量を示します。

LF ビット符号化は、3 ビットの基本符号化と 3 ビットの拡張符号化 (合計 6 ビット) によって構成されます。SRT ブリッジ (後節で説明) には LF モード表示が含まれているので、このブリッジは基本または拡張 LF ビットのいずれかを選択できます。LF モード表示が *基本モード* に設定されている場合、ブリッジは探索フレームの LF ビットを最大フレーム基本値にセットします。LF モード表示が *拡張モード* に設定されている場合、ブリッジは探索フレームの LF ビットを最大フレーム拡張値にセットします。

- **ルート指定子フィールド (RDn)** RD フィールドのシーケンスによってネットワークを通る特定のルートを示します。各 RD フィールドには、同一の 2 つのリングを接続する場合 (並列ブリッジ) に、複数のブリッジを区別するためのネットワーク固有の 12 ビット・リング番号と 4 ビット・ブリッジ番号が入っています。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 (オール 0) です。

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は、ネットワーク内の同一の LAN を接続するブリッジが複数ある場合に、あて先への単一のルートを選択することを可能にします。このフィーチャーを使用可能にすると、ユーザーが選択したブリッジだけがスパンニング・ツリー探索 (STE) フレームを受け取ります。スパンニング・ツリー・プロトコルと混同しないことが必要ですが、このオプションは次の機能を提供するものです。

- スパンニング・ツリー・ネットワークをシミュレートする
- トラフィックの負荷の平衡を取る

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・ステーション間に単一のデータ・ルートが存在します。ユーザーのネットワークで 2 つまたはそれ以上の並列ブリッジが使用されている場合 (29ページの図12 のように)、手動で重複するディスカバリー・フレームがネットワーク上に送られるのを防止することにより、ネットワーク上にスパンニング・ツリーを構成することができます。スパンニング・ツリー探索が使用可能でない場合、ステーション Q がステーション R にディスカバリー・フレームを送信すると、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。その結果、セグメント 2 は、同じフレームの 2 つのコピーを受け取ることになります。

スパンニング・ツリー探索が使用可能になっていると、ネットワーク上の各 LAN セグメントは、転送されたフレームのコピーを 1 つだけ受け取ります。ユーザーが選択したブリッジのみが STE フレームを受信できるので、冗長フレームが作成されることが少なくなり、ネットワークのオーバーヘッドを削減できます。

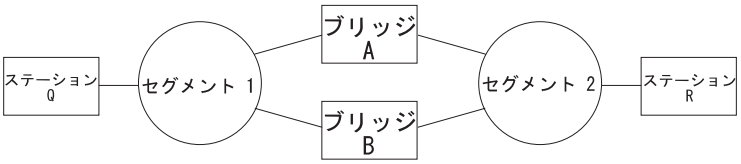


図 12. 並列ブリッジの例

トラフィックの負荷の平衡化

スパンニング・ツリー探索オプションは、負荷のバランスを取るために利用することもできます。たとえば、図13 では、ブリッジ A はセグメント 2 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に構成されています。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に構成されています。トラフィックは矢印の方向に流れます。この構成では、並列ブリッジがトラフィックの負荷を共有することができます。

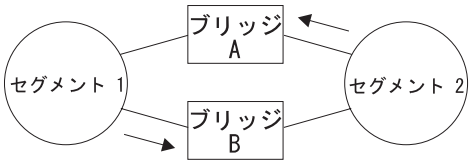


図 13. 負荷のバランスを取るためのスパンニング・ツリー探索の使用

注: ソース・ルーティングを機能させるためには、一部のエンド・ノード・アプリケーション (IBM PC LAN プログラムなど) では、接続されたインターフェース上でスパンニング・ツリー探索が使用可能になっていることが必要です。並列ブリッジ構成の場合、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 つでのみ使用可能にします。ただし、スパンニング・ツリーが使用可能になっているインターフェースが多過ぎても、重大な障害 (いくらか余分なトラフィックが生じる以外に) は起こりません。

スパンニング・ツリー探索オプションを使用している場合、単一ルート・パス上のいずれかのブリッジがダウンすると、ソース・ルーティング・トラフィックはあて先に到達することができません。ユーザーが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・ブリッジングとフレーム・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れば、ソース・ルート・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機能との間で転送されます。各フレーム・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・ポートとして扱うようブリッジを構成することができます。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・サーキットを、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化することができます。詳細については、58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。ループのないトポ

ロジーを維持するために、アクティブ・データ・パスに含まれていない一部のバーチャル・サーキットはブロック (BLOCKED) されます。

ソース・ルーティング・ブリッジの用語と概念

この節では、ソース・ルーティング・ブリッジングで一般的に使用される用語および概念を復習します。

ブリッジ・インスタンス

ブリッジ・インスタンスは、ソフトウェアで定義されたブリッジのシーケンスを識別します。たとえば、2 つの構成されたブリッジを持つブリッジでは、ブリッジ・インスタンスは 1 と 2 になります。

単一ブリッジ内のブリッジ・インスタンスは、それぞれ独立しており、通信しません。たとえば、図14 では、ステーション A はブリッジ・インスタンス 2 上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 にのみフレームを渡すことができます。つまり、このブリッジ・インスタンスは 2 つの別々のネットワークを作成することを可能にします。これらのネットワークは、どこか別の地点で物理的に相互接続されていない限り、通信しません。

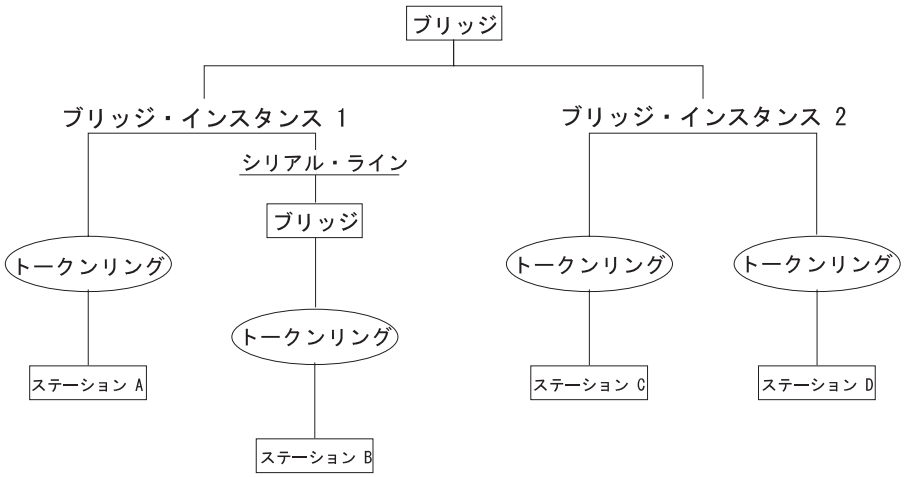


図 14. ブリッジ内のブリッジ・インスタンス

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ているブリッジは同一のブリッジ番号を持つことができますが、並列ブリッジ (同一の 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が必要です。

探索フレーム

ソース・ルーティング・ブリッジは、ネットワークを通して探索フレームをあて先エンド・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 2

種類あります。つまり、全ルート探索 (ARE) フレームとスパンニング・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、一方の STE フレームは、スパンニング・ツリー・プロトコルによる転送が指定さ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/製品内の 『物理』 インターフェースを識別するものであり、ブリッジ (つまり、ポート) が理解できる 『論理』 インターフェースに結び付けておくことが必要です。ルーター・ソフトウェアを構成する際に、ルーター/ブリッジのポートに順次に番号を付けます。ソース・ルーティング・ブリッジを使用するためには、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ことが必要です。

ルート

ルートとは、一連の LAN とブリッジ (たとえば、SRB ブリッジ) を通るパスのことです。

ルート・ディスカバリー

ルート・ディスカバリーとは、あて先エンド・ステーションまでのルートを確認するプロセスを言います。

セグメント番号

セグメント番号は、個々の LAN (1 つのトークンリングやシリアル・ラインなど) を識別します。セグメントはブリッジに接続しますが、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、移動するルートをフレームの中で指定することによって、複数 LAN ネットワーク上でフレームをルーティングするブリッジング方式のことです。

ソース・ルーティング透過型 (SRT) ブリッジ

標準技術 (イーサネットとトークンリングは両方とも IEEE で定義) を採用しようと努力をしたが、実際に接続しようする段階になって、専用ネットワークに後戻りせざるを得ないというようなことがあります。これは、トークンリング・ネットワークとイーサネット・ネットワークでは、ブリッジの機能に相違があるためです。

ビット順序、パケット・サイズ、および確認応答ビットなどの相違の他に、ブリッジング方式の相違も障害の原因の 1 つになっています。イーサネット・ブリッジは、ブリッジがネットワーク上のトラフィックのルートを決める透過ブリッジング方式を使用しています。トークンリング・ネットワークでは、透過ブリッジングは一部でしか使用されず、一般的には、基本的なブリッジング方式はソース・ルーティングに依存しています。

ブリッジング方式

透過パケットにはルーティング情報が入っていないので、ソース・ルーティングは透過環境では運用できません。この場合、ブリッジはパケットを転送するかどうかを判断する方法がありません。一方、透過ブリッジングはソース・ルーティング環境で運用できますが、ルーティング情報をエンド・ステーションに渡しません。重要な情報 (たとえば、パケット・サイズ) が欠落していて、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 (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整合性をほとんど解決しようとするブリッジング技術です。透過ブリッジングの標準に並列ブリッジング体系を追加する (代替ではなく) ことにより、2 種類のトラフィックをサポートするために複数のブリッジと別々のリンクを設置するコストを節約できます。

概説

ソース・ルーティング透過型ブリッジは、ルーティング情報を持つソース・ルーティング・フレームを受信した場合はソース・ルーティングを行い、ルーティング情報のないフレームを受信した場合は透過ブリッジングを行う MAC ブリッジです。SRT 内では、イーサネットとトークンリング間のすべてのブリッジが透過的です。ブリッジはデータ・リンク・レイヤーの MAC サブレイヤーで動作し、エンド・ステーションからはまったく見えません。

SRT ブリッジは、フレームの RII フィールド内の値を検査して、2 つのタイプのフレームを見分けます (詳しい説明は、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 値が 1 のときは、そのフレームにルーティング情報が入っていることを示し、RII の値が 0 のときは、ルーティング情報が存在しないことを示しています。この方法により、SRT ブリッジは、発信媒体 (トークンリングを含む) に合わせて変換せずに、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・ドメインだけに限定されます。

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 ブリッジによって接続された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・ネットワークは、ソース・ルーティングのサブドメインを持つ、より大きな透過ブリッジング・ドメインを提供します。このように、透過フレームは SRT および TB ブリッジ LAN の最遠端まで到達できるのに対して、ソース・ルーティング・フレームは SRT および SRB ブリッジ LAN だけに限定されます。SRT ブリッジング・モデルでは、ソース・ルーティング部分と透過ブリッジング部分は、同じスパンニング・ツリーを使用します。SRT ブリッジ・ドメインでは、エンド・ステーションは『ソース・ルーティングか、透過ブリッジングか』 の質問に答える責任があります。

ソース・ルーティング透過型ブリッジの動作とアーキテクチャー

SRT ブリッジでは、各ブリッジ・ポートは、そのポートに関連する個々の MAC エンティティーが提供する MAC サービスを使用して、接続されたローカル・エリア・ネットワークとの間でフレームを送受信します。MAC リレー・エンティティーは、ブリッジ・ポート間のフレームを中継するするという、MAC から独立したタスクを受け持ちます。受信したフレームがソース・ルーティングでない場合 (RII = 0)、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。受信したフレームがソース・ルーティングの場合 (RII = 1)、フレームは、ソース・ルーティング論理に従って処理されます。このプロセスが、図15 に示されています。矢印はデータ・パスを示しています。

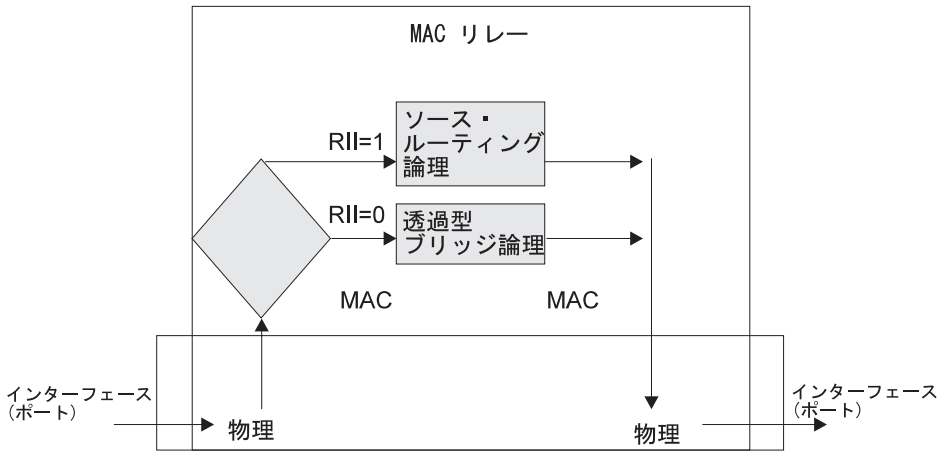


図 15. SRT ブリッジの動作

SRT は、フレームごとに、ソース・ルーティング・トラフィックと非ソース・ルーティング・トラフィックを区別します。パケットがソース・ルーティングの場合、ブリッジはそれとして転送します。パケットが透過型ブリッジ・パケットの場合、ブリッジはあて先アドレスを調べ、パケットを転送します。

ソース・ルーティング透過ブリッジングとフレーム・リレー

SRT ブリッジングがサーキット上で使用可能になっていると、ソース・ルート・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機能と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

この節では、SRT ブリッジングで一般的に使用される用語および概念を復習します。

探索フレーム

ソース・ルーティング・ブリッジは、ネットワークを通して探索フレームをあて先エンド・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見つけます。探索フレームには 2 種類あります。

- 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、一方の STE フレームは、スパンニング・ツリー・プロトコルによる転送が指定さ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・フレームの転送の決定は、フレーム内のルーティング情報に基づいて行われます。フレームを転送する前に、エンド・ステーションは *ルート・ディスカバリー* ・プロセスにより、あて先ステーションへのルートを入手します。フレームを発信するステーション (つまり、ソース・ 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) にルートの記述を埋め込むことによって、フレームが通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 フレームには、マルチリング環境を介したデータ通信に必要なルーティング情報が入っているので、そのフォーマットは典型的なトークンリング MAC フレームとはいくぶん異なっています。ルーティング情報標識と呼ばれる発信元アドレス・フィールドが 1 のときは、ルーティング情報が入っているルーティング情報フィールドが、発信元アドレスの後に続いていることを示しています。SRT ブリッジは、RII フィールドの値が 1 であるか 0 であるかを検査することにより、それがソース・ルート・フレームであるか、非ソース・ルート・フレームであるかを見分けます。

ソース・ルーティング

通過するルートをフレーム内に指定することによって複数の LAN ネットワーク上でフレームをルーティングする、ブリッジング方式

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 1 つだけデータ・ルートが存在するブリッジの接続形態 (トポロジー)

透過ブリッジング

エンド・ステーションに対して透過的なメカニズムが含まれているブリッジングのタイプ。透過ブリッジングは、スパンニング・ツリー・アルゴリズムによりデータ・フレームの転送を指示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。

ASRT ブリッジの概要

適応ソース・ルーティング透過 (ASRT) ブリッジは、いくつかのブリッジング・オプションを集合したソフトウェアです。ASRT ブリッジ・ソフトウェアは、透過ブリッジングとソース・ルーティングを組み合わせ、別々に機能することも、結合して単一の ASRT ブリッジとすることも可能にしています。この拡張機能は、ASRT ブリッジを介して、ソース・ルーティングだけに限定されたエンド・ステーションと透過エンド・ステーション間の通信を可能にします。使用される構成コマンド・セットに応じて、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/Draft 6 (1991) に記述されているソース・ルーティング透過型ブリッジをモデルにしています。ASRT ブリッジには、SRT 標準に準拠するのみならず拡張機能もユーザーに提供できるように変更が加えられています。ASRT ブリッジは、導入されたソース・ルーティング・ブリッジの基本機能と整合性を保ちながら、イーサネット、およびトークンリング LAN にリンクすることができます。また ASRT は、後述するように、いくつかの追加された重要な方法で基本 SRT 機能を拡張しています。

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 モデルでまだ利用可能ですが、隣接したソース・ルーティング・トークンリング相互間でしか使用できません。ソース・ルーティングのみのブリッジは、イーサネット およびトークンリング LAN をリンクする SRT ブリッジと共存することはできません。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ので、RIF を省略するように構成することが必要になります。また、エンド・ノードを RIF を省略するように構成した場合、その RIF を必要とする通常のソース・ルーティング・ブリッジとは通信できなくなります。

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) を使用するネットワークを相互に接続します。両方のドメインを透過的に結合します。動作時には、両方のドメインのステーションは、互いの存在や SR-TB ブリッジの存在に気付きません。ステーションの立場からは、結合されたネットワーク上にあるステーションは、すべて自分と同じドメイン内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ことによって (あるいは、その逆を行って) この機能を達成します。これを達成するために、ブリッジは、ソース・ルーティング・ドメイン内のエンド・ステーション・アドレスのデータベース (それぞれ、そのルーティング情報フィールドを含んでいる) を維持しています。また、ブリッジは、透過ブリッジング・ドメインに存在するエンド・ステーションのためのルート・ディスカバリーも行います。ルート・ディスカバリー・プロセスを使用して、ソース・ルーティング・ドメインにあるあて先ステーションへのルートを見つけます。確認不能のあて先に送られるフレームは、スパンニング・ツリー探索 (STE) フォーマットで送信されます。

SR-TB ブリッジは、3 つのタイプのスパンニング・ツリーを予想します。

- 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 ブリッジの特殊スパンニング・ツリー

以下の節では、SR-TB ブリッジの動作について、さらに詳しく説明します。

ソース・ルーティング - 透過型ブリッジの動作

SR-TB 動作時には、ネットワークは一連の 2 つ以上の分離された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 セグメントの集合から構成され、ブリッジはすべて共通のブリッジング方式の下で動作します。これにより、2 つのタイプのドメイン (ブリッジング方式に基づく) からネットワークを構成することが可能になります。

- 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

図16 は、このようなドメインの例を示しています。分離されたドメインでは、各ソース・ルーティング・ドメインが、そのブリッジ用に設定された単一ルート同報通信トポロジーを持っています。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、単一ルート同報通信標識が入っているフレームは、ソース・ルーティング・ドメインのすべてのセグメントに送られます。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に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コピーが 1 つだけ到着します。

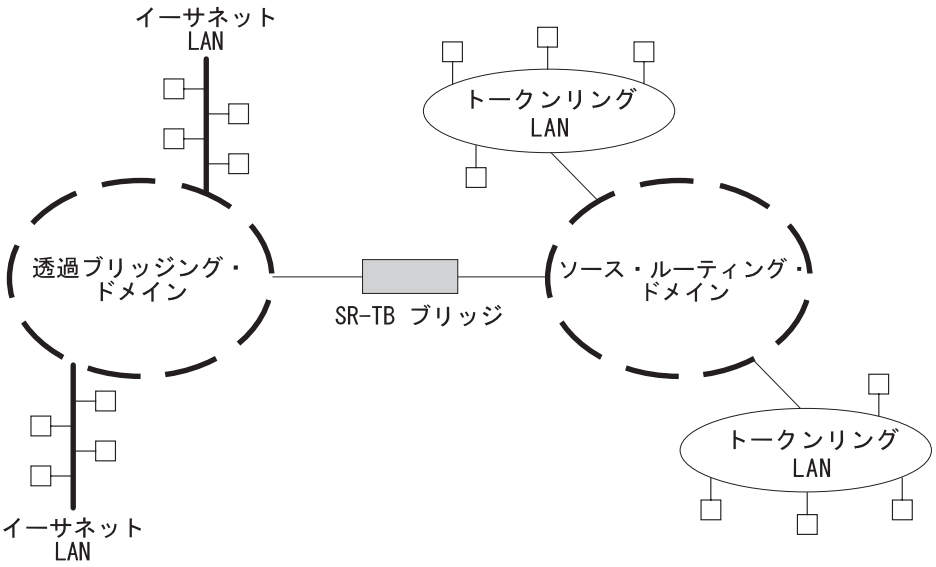


図 16. 2 つのドメインを接続する SR-TB ブリッジ

特殊ソース・ルーティングと透過ブリッジングの動作

SR-TB ブリッジは、ソース・ルーティング側の LAN セグメントに割り当てられた MAC インターフェースと、透過ブリッジング側の LAN セグメントに割り当てられた MAC インターフェースとを持つ *2 ポート装置* です。各エンド・ステーションは、それぞれの LAN セグメント用の MAC レイヤーを読み取ります。このことは、ブリッジング機能を 2 つのタイプの動作に分割できることを意味しています。

- 透過ブリッジング動作

- ソース・ルーティング・ブリッジング動作

透過ブリッジング側では、SR-TB ブリッジは他の透過型ブリッジと同様に動作します。ブリッジは、透過ブリッジング・ステーションであることが分かっているステーションのアドレス・テーブルを維持しています。複数の SR-TB ブリッジが異なるドメインを結んでいるので、SR-TB ブリッジはスパンニング・ツリーを作成して維持するために必要なブリッジ間 プロトコルを順守します。

SR-TB ブリッジは、フレームで運ばれたあて先アドレスがブリッジの透過ブリッジング側アドレス・テーブルに見つからない場合にのみ、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します。

ソース・ルーティング・ブリッジング側では、SR-TB ブリッジが特殊な方法を用いて、ソース・ルーティング・ブリッジの機能とソース・ルーティング・エンド・ステーションの機能を結合します。ソース・ルーティング側では、ブリッジはソース・ルーティング・エンド・ステーションとして、あて先アドレスとルーティング情報の関連を維持します。ブリッジは、ブリッジ自体に搭載されたアプリケーション (たとえば、ネットワーク管理) のためのエンド・ステーションとして、あるいは透過ブリッジング側のステーションのための中間ステーションとして通信します。

SR-TB ブリッジは、フレームで運ばれたあて先アドレスがブリッジの透過ブリッジング側アドレス・テーブルに見つからない場合にのみ、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します。ブリッジのソース・ルーティング・ステーションによって転送されたフレームには、ブリッジに関連したルーティング情報が入っています (ブリッジがそのような情報を知っており、保持している場合)。

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・ディスカバリー・プロセスおよびすでにルーティング情報が入って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、ソース・ルーティング側の個々の LAN の LAN 番号とブリッジの個々のブリッジ番号から構成されます。

またブリッジは、透過ブリッジング側のすべての LAN を代表する単一の LAN 番号も維持しています。SR-TB は、表3 に説明されているように、転送するフレームの個々のケースに応じて異なった処理をします。

表 3. SR-TB ブリッジの決定方法の一覧表

受信したフレームのタイプ	SR-TB ブリッジが取る処置
ソース・ルーティング・ステーションが非ルーティング・フレームを受信	ルーティング情報が入っているフレームをコピーまたは転送しません。
ソース・ルーティング・ステーションが全ルート同報通信フレームを受信	フレームをコピーし、コピーしたフレームに同報通信標識の A および C ビットをセットします。あて先アドレスが透過ブリッジング・テーブルに存在する場合、ブリッジはルーティング情報を付けずに、フレームを透過ブリッジング・ネットワークに転送します。そうでない場合、フレームは転送されません。

表 3. SR-TB ブリッジの決定方法の一覧表 (続き)

受信したフレームのタイプ	SR-TB ブリッジが取る処置
ソース・ルーティング・ステーションが単一ルート同報通信フレームを受信。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。	フレームをコピーまたは転送しません。
ソース・ルーティング・ステーションが単一ルート同報通信フレームを受信。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。	フレームをコピーし、同報通信標識の A および C ビットをセットし、フレームからルーティング情報を除去し、変更されたフレームを透過ブリッジング側に転送します。保存し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 番号を追加します。同報通信標識を非同報通信に変更し、D ビットを補い、このルーティング情報をフレームの発信元アドレス用として保管します。
ソース・ルーティング・ステーションが非同報通信フレームを受信	フレームに特定のルートが指定されている場合、ブリッジはルーティング情報を調べます。SR-TB ブリッジがルートの一部に含まれており、それがソース・ルーティング側の LAN 番号と透過型ブリッジ側の LAN 番号の間に表示されている場合、ブリッジはフレームをコピーし、コピーしたフレームに A および C ビットをセットします。そして、ルーティング情報を付けずに、フレームを透過ブリッジング側に転送します。ブリッジがまだ発信元アドレスの固定ルートを持っていない場合は、ルーティング情報のコピーを保存し、D ビットを補い、保存したルーティング情報をフレームの発信元アドレスとして保管します。
透過ブリッジング側からフレームを受信	フレームをソース・ルーティング側に転送するために、ブリッジは最初に、フレームに入っているあて先アドレスに関連したルーティング情報を持っているかどうかを調べます。持っている場合、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 にセットし、フレームをソース・ルーティング側に転送するための待ち行列に入れます。持っていない場合、ブリッジは単一ルート同報通信標識と 2 つのルート指定子 (最初の 2 つの LAN 番号と自身の固有のブリッジ番号が入っている) が含まれているルーティング制御フィールドをフレームに追加します。

SR-TB ブリッジング: 4 つの例

SR-TB は、ドメインを透過的に結合することによって、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。動作時には、両方のドメインのステーションは、互いの存在や SR-TB ブリッジの存在に気付きません。エンド・ステーションの立場からは、結合されたネットワーク上にあるステーションは、すべて自分と同じドメイン内にあるように見えます。

以下の節では、SR-TB ブリッジングにおけるフレーム転送の具体的な例を示します。例では、SR-TB 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ものと想定しています。図17 は、各節で説明される状況に付随する以下の情報を提供しています。

- 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ます。

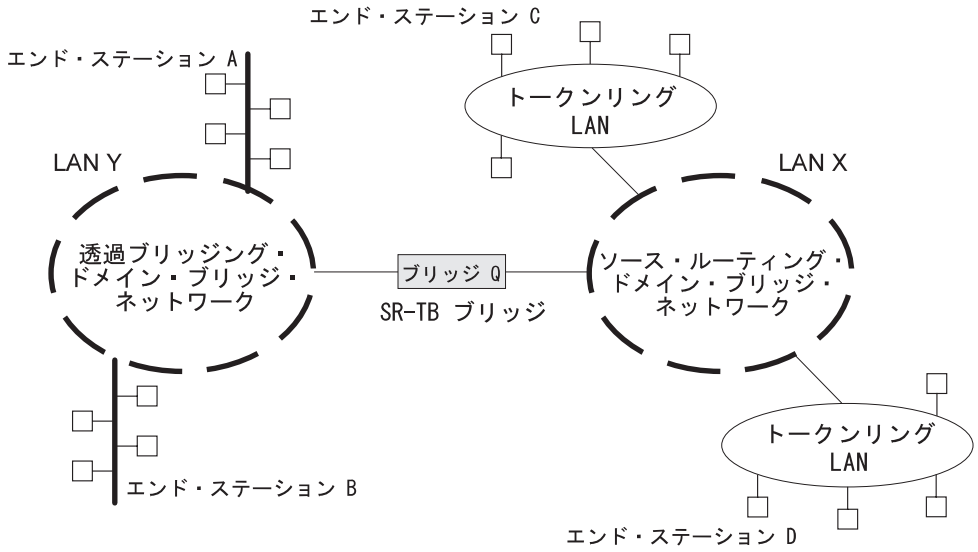


図 17. SR-TB ブリッジングの例

例 1 エンド・ステーション A からエンド・ステーション B にフレームを送信

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 のフレームを受信した場合、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・テーブルに入れます。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分かっているステーションのアドレスが入っています。これは通常の透過ブリッジングのプロセスです。

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・テーブルに存在する場合、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・テーブルに存在せず、またソース・ルーティング側のアドレス・テーブルにも存在しない場合、その場所は SR-TB ブリッジには確認不能 (不定) です。この場合、フレームは単一ルート同報通信として、ルート探索の戻りを要求せずに、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はすべて (そのあて先に関係なく)、そのアドレスが透過ブリッジング・アドレス・テーブルに追加されます。これにより、今後エンド・ステーション B をアドレス指定したフレームが、ソース・ルーティング側に転送されるのを防止することができます。

例 2 エンド・ステーション A からエンド・ステーション C にフレームを送信

この例では、エンド・ステーション A のアドレスは、前の例と同様に処理されます。エンド・ステーション C のアドレスは、透過型ブリッジ・アドレス・テーブルには存在しないことが明らかなので、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。

次に、ブリッジはソース・ルーティング・アドレス・テーブルで、エンド・ステーション C のアドレスを探します。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分かっているステーションのすべての既知のアドレスが、関連のルーティング情報と共に入っています。C のアドレスがソース・ルーティング・テーブルに存在する場合、ブリッジはアドレス・テーブルのルーティング情報を使用して、フレームを転送します。C アドレスがソース・ルーティング・テーブルに存在しない場合 (あるいは、テーブルに表示されているが、ルーティング情報が空の場合)、ブリッジはフレームを単一ルート同報通信として、ルート探索の戻りを要求せずに、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 は、このフレームを受信すると、エンド・ステーション A のアドレスを、SR-TB ブリッジから形成されたルートとは逆方向のルートと共にソース・ルーティング・テーブルに入力し、それに一時的エントリーとしてのマークを付けます。後にエンド・ステーション C がエンド・ステーション A へのフレーム送信を試みるときに、この特定ルートを使用します。そして、このルートは一時的というマークが付いているので、フレームはルート探索の戻りを要求する 非同報通信ルートとして送信されます。

戻りのフレームが SR-TB ブリッジに到着すると、フレームはルーティング情報を付けずに透過ブリッジング側に転送されますが、エンド・ステーション C へのルートは、一時ルートとしてソース・ルーティング・テーブルに記入されます。その結果、ネットワーク管理エンティティーは、全ルート同報通信のルート探索フレームをエンド・ステーション C に戻します。これにより、エンド・ステーション C は、エンド・ステーション A あての最適ルートを選択し、それを SR-TB ブリッジのソース・ルーティング・テーブルに固定ルートとして記入することができます。

例 3 エンド・ステーション C からエンド・ステーション D にフレームを送信

フレームが非同報通信として送信され、SR-TB ブリッジが接続されているセグメントを通過する場合、ブリッジは RII フィールドをスキャンしてルーティング・シーケンス (LAN X - ブリッジ Q - LAN Y) を探します。このシーケンスは見つからないので、フレームを転送しません。

フレームが単一ルート同報通信として送信された場合、エンド・ステーション D がソース・ルーティング側に存在することがすでに分かっている場合、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・ルーティング側に存在することが分かっていない場合、ブリッジはフレームを透過ブリッジング側に転送し (ルーティング情報を付けずに)、『Q から Y』 をルーティング情報に追加します。最後に、エンド・ステーション C のルーティング情報を、非同報通信標識と方向ビットを補って、一時ルートとしてソース・ルーティング・テーブルに保存します。

フレームが全ルート同報通信として送信された場合、SR-TB ブリッジはフレームを廃棄し (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・テーブルに存在しないため)、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・テーブルに存在することを確認します。

例 4 エンド・ステーション C からエンド・ステーション A にフレームを送信

フレームが非同報通信として送信された場合、ブリッジは RII フィールドをスキャンしてルーティング・シーケンス (X から Q から Y) を探します。それを見つけると、フレームを透過ブリッジング側に転送します。さらに、エンド・ステーション C 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た場合、ブリッジはフレームを (ルーティング情報を付けずに) 透過ブリッジング側に転送し、『Q から Y』 をルーティング情報に追加します。さらに、非同報通信標識をセットし、方向ビットを補い、 C のルーティング情報をソース・ルーティング・テーブルに記入します。

エンド・ステーション C の一時的エントリーが、すでにソース・ルーティング・テーブルに存在する場合、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た場合、ブリッジは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・テーブルに存在することを確認します。

SR-TB とフレーム・リレー

フレーム・リレー・インターフェースは、ブリッジングがサーキット上で使用可能になっている限り、ブリッジされたすべてのフレームを該当のブリッジング転送機能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。

ソース・ルーティング - 透過型ブリッジ (SR-TB) の用語と概念

この節では、SR-TB ブリッジングで一般的に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 内の反復しないすべてのルートを通っ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

リング上のフレームが通過するすべてのステーションがフレームをコピーする、フレームのアドレッシング・プロセス (あて先アドレスにオール 1 を入れる)

ブリッジ

ローカル・エリア・ネットワーク (LAN) を接続する、プロトコルから独立した装置。ブリッジはデータ・リンク・レイヤーで動作し、LAN 間のデータ・パケットを保管および転送する。

ブリッジ番号

ブリッジを識別する固有な番号。これは、同一の 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、ネットワークを通して探索フレームをあて先エンド・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見つけます。探索フレームには 2 種類あります。つまり、全ルート探索 (ARE) フレームとスパンニング・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、一方の STE フレームは、スパンニング・ツリー・プロトコルによる転送が指定さ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上のリングを識別する固有な番号

ルート

一連の LAN とブリッジ (たとえば、ソース・ルーティング・ブリッジ) を通るパス

ルート指定子

ネットワークを通るルートを形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とブリッジ番号

ルート・ディスカバリー

あて先エンド・ステーションまでのルートを確認する (learn) プロセス

セグメント番号

個々の LAN (たとえば、1 つのトークンリング回線、またはシリアル・ライン) を識別する番号。セグメントはブリッジに接続しますが、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を正確に 1 つだけのフレーム・コピーが通過するようして、ネットワーク上で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

通過するルートをフレーム内に指定することによって複数の LAN ネットワーク上でフレームをルーティングする、ブリッジング方式

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 1 つだけデータ・ルートが存在するブリッジの接続形態 (トポロジー)

透過ブリッジング

エンド・ステーションのアプリケーションに対して*透過的* なメカニズムが含まれているブリッジングのタイプ。透過ブリッジングは、スパンニング・ツリー・アルゴリズムによりデータ・フレームの転送を指示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・ルーティングの整合性 - 問題と解決

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) を通して、透過型ブリッジと通常のソース・ルーティングとの整合性を提供します。SR-TB は本来、802.5 仕様の一部として提案されたものです。この実現方式は IBM の 8209 変換ブリッジに似ており、相互運用が可能です。

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 (または、その逆に) 変換します。言い換えると、単にパケット内に RIF が存在するかどうかをチェックして、あて先と思われる場所にそれを転送するのではなく、ASRT ブリッジはパケットをどちらかのフォーマットに変換することができます。つまり、必要に応じて RIF を挿入したり除去したりして、透過型ブリッジまたはソース・ルーティング・ブリッジのいずれかとして機能することができます。この機能により、パケットはイーサネット と SRT トークンリング LAN 間を移動することが可能になり、しかも導入済みのソース・ルーティング・トークンリング LAN の基本機能との整合性も保たれます。

パケット・サイズの問題の解消

SR-TB は、一緒にブリッジされてイーサネット・ドメインを通過するトークンリングのパケット・サイズ問題も解消します。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・ステーション相互間に 1518 バイトの最大フレーム・サイズを使用するネットワークが存在することを動的に判別できます。手動で構成しなくても、エンド・ステーションは自動的にこの限界を守ります。この逆の状況で、ブリッジングによってイーサネットがトークンリング・ドメインを通過する場合は、トークンリングのパケット・サイズの許容値がはるかに大きいので、パケット・サイズの問題は生じません。

ハードウェア・アドレス・フィルター

ASRT ブリッジが提供するもう 1 つの重要な機能に、ハードウェア・アドレス・フィルターがあります。ハードウェア・アドレス・フィルターは、イーサネット技術とトークンリング LAN 技術間に存在するパケット確認方式の対立を解決します。このフィルターは MAC レイヤーで適用され、あて先 MAC アドレスに基づいて正確に確認応答ビットをセットできる唯一の技法です。ASRT ブリッジは、コンテンツ・アドレス可能メモリー (CAM) を使用して、ハードウェア・アドレス・フィルターを実現します。この技術は、性能を低下させることなく、瞬時に MAC アドレスを検索する機能を提供し、ブリッジにハイレベルの知能を与えます。

STB および SRB ブリッジのビット順序

ブリッジは、異なる MAC アドレス・タイプを持つ LAN を接続するために継続的に構築されているので、データ伝送時のビット順序は、これらの技術間の相互運用性に影響を与えます。

MAC アドレスを管理するために、IEEE は 48 ビットのアドレスを割り当てており、これは IEEE グローバル指定ユニーク MAC アドレスと呼ばれています。これらのアドレスは、 802.3、802.4、および 802.5 LAN によってサポートされています。このアドレッシング方式が開発された当時は標準が確立されていなかったので、2 つの異なる状況が生じました。

- 802.3 (イーサネット) および 802.4 LAN では、発信元およびあて先アドレスは、グループ・ビットが最初に送信され、LLC データ・フィールドは最下位ビット (LSB) が最初に送信されます。
- 802.5 (トークンリング) LAN では、発信元およびあて先アドレスは、グループ・ビットが最初に送信され、LLC データ・フィールドは最上位ビット (MSB) が最初に送信されます。

注: 説明を分かりやすくするために、802.3 および 802.4 ブリッジと LAN を、LSB ブリッジと LAN と呼び、 802.5 ブリッジと LAN を、MSB ブリッジと LAN と呼ぶことにします。

このビット伝送標準の相違は、LSB から MSB LAN へのブリッジは、MAC フレームの開始点であて先と発信元 MAC アドレスのビット順序を逆にしなければならないことを意味しています。これは、この各種の LAN タイプは、MAC アドレスについては同じビット順序 (つまり、グループ・ビットが最初) を使用していますが、ユーザー・データについては異なるビット順序 (LSB が最初、または MSB が最初) を使用しているためです。

ビット順序が逆であるためにアドレスが誤って解釈されることに加えて、一部の高位レベル通信プロトコルでは MAC アドレス全体が誤って解釈されるという事実があり、これらが合わさって発生します。IP および Novell IPX は、初期の開発当時には MAC アドレスの標準解釈が得られていなかったので、ブリッジング・アドレスが間違って解釈されています。

ビット順序の相違は、ブリッジング技術 (データ・リンク・レイヤー技術) とルーティング技術 (ネットワーク・レイヤー技術) とを組み合わせることによって、最も上手に解決できます。ユーザーに今日の通信プロトコルを 『リバース・エンジニアリング』 することを要求し、各ブリッジごとに個別のアドレスを 『反転』 または逆に構成するよりも、これらのプロトコルをルーティングすることによって、より容易に問題を解決できます。

ルーティングは、高位レイヤーで動作する詳細なパケット・アドレスにアクセスすることによって、ビット順序およびプロトコル・アドレッシングの問題を解消します。ただし、ルーティングだけでは完全な解決策にはなりません。IBM フレームや NetBIOS のようなプロトコルはルーティングできず、SNA のルーティングには限界があるからです。そこで、ブリッジングとルーティングが協働する装置には SRT を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 ブリッジ標準に記述されているスパンニング・ツリー・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上で使用します。異なるタイプのブリッジが存在する環境では、複数のスパンニング・ツリーが形成される可能性があります。たとえば、IEEE 802.1d プロトコル (たとえば、STB および SRT) に参加している全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しているというようなことが考えられます。構成でループが形成される場合は、状態を訂正する必要があります。

TCP/IP ホスト・サービスは、SDLC リレーをサポートします。純粋なブリッジとして動作している場合 (IP ルーターとして動作しない場合) は、IP ルーターに関連している機能は利用不能になります。たとえば、BootP 転送機能や ARP サブネット・ルーティング機能は得られません。

ASRT 構成マトリックス

ASRT ブリッジを使用する場合、ブリッジとすべての接続インターフェースの構成パラメーターの集合が、そのブリッジのブリッジ・パーソナリティー を形成します。下記のマトリックスは、ユーザーのネットワークに適合するブリッジ・パーソナリティーを形成するのに必要な各インターフェース・タイプの構成設定のガイドを示しています。

		インターフェース・タイプ & ブリッジング方式の設定			
ブリッジ・パーソナリティー	SR <-> TB 変換使用可能?	トークンリング	イーサネット	シリアル・ラインまたはトンネル	
STB	不可	TB	TB	TB	TB
SRB	不可	SR	--	SR	SR
STB & SRB	不可	SR	TB	TB または SR	TB または SR
SR-TB	可	SR	TB	TB	TB
SR-TB	可	SR	TB	SR	SR
SRT	不可	SR & TB	TB	SR & TB	SR & TB
ASRT	可	SR & TB	TB	SR & TB	SR & TB
ASRT	可	SR	TB	SR & TB	SR & TB
ASRT	可	SR または TB	TB	SR & TB	SR & TB

ブリッジ・パーソナリティー・キー :
STB = 透過型 (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・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) ブリッジで利用可能なブリッジング・フィーチャーについて説明します。本章には、以下の節が含まれています。

- 『ブリッジ・トンネル』
- 49ページの『TCP/IP ホスト・サービス (ブリッジ専用管理)』
- 49ページの『ブリッジ MIB サポート』
- 50ページの『NetBIOS ネーム・キャッシュ』
- 50ページの『NetBIOS 重複フレーム・フィルター』
- 50ページの『NetBIOS ネームおよびバイト・フィルター』
- 53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』
- 55ページの『スレッド (ルーター・ディスカバリー)』
- 58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 パケットにカプセル化することにより、ブリッジング・ルーターは、大規模な IP 相互接続ネットワークを経由して、あて先エンド・ステーションまで動的にパケットをルートすることができます。

エンド・ステーションは、ネットワークの複雑さに関係なく、IP パス (トンネル) を単一のホップと見なします。これにより、ソース・ルーティング構成に通常見られる 7 ホップという距離制限を克服することができます。また、ソース・ルーティング・エンド・ステーションを、イーサネット・ネットワークのような非ソース・ルーティング媒体を介して接続することも可能になります。

さらに、ブリッジ・トンネルは、以下のようなソース・ルーティングに一般的に伴ういくつかの制限を克服することができます。

- 7 ホップという距離制限
- 広域ネットワーク (WAN) でソース・ルーティングがもたらす大量のオーバーヘッド
- WAN の障害や故障に対するソース・ルーティングの敏感さ (パスに障害が起きた場合、すべてのシステムが転送をやり直す必要があります)

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場合、ソフトウェアはパケットを TCP/IP パケットにカプセル化します。このパケットは、ルーターには TCP/IP パケットのように見えます。フレームを IP エンベロープにカプセル化した後は、IP 転送機能があて先 IP アドレスに基づいて、適切なネットワーク・インターフェースを選択します。このパケットは、性能低下やネットワーク・サイズの制約なしに、大規模な相互接続ネットワークを経由して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、ネットワークの複雑さに関係なく、このパス (トンネ

ル) を単一ホップと見なします。 図18 は、構成内にトンネル・フィーチャーを使用している IP 相互接続ネットワークの例を示しています。

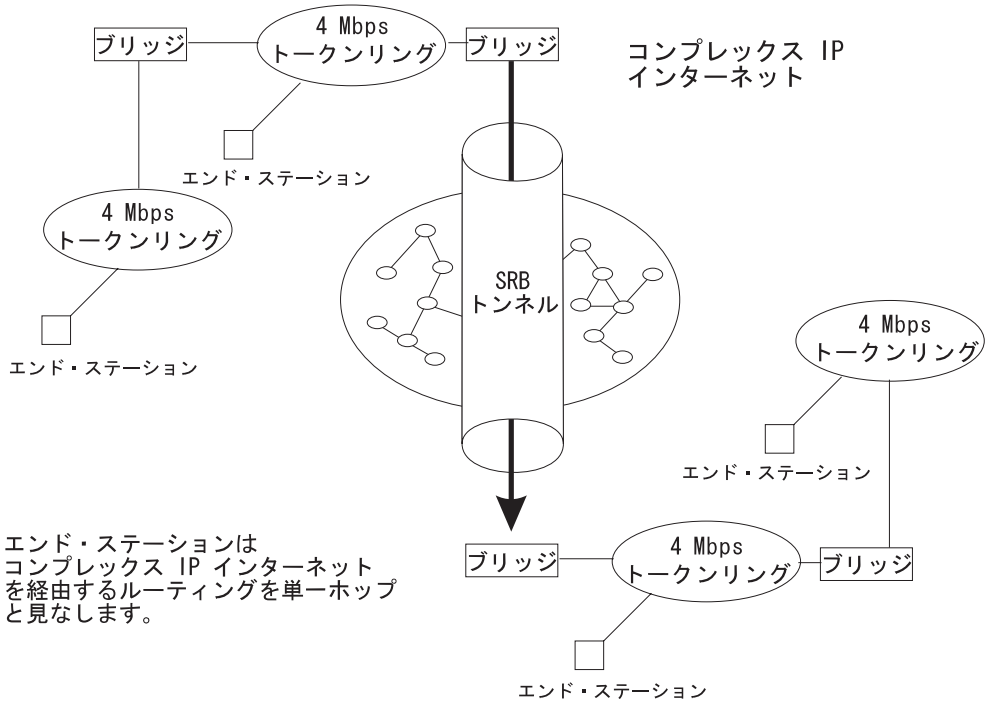


図 18. ブリッジ・トンネル・フィーチャーの例

トンネルはエンド・ステーションには透過的です。トンネル伝送に参加しているブリッジング・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着すると、TCP/IP ヘッダーが自動的に 取り除かれ、内部のパケットは標準ソース・ルーティング・パケットとして処理が進められます。

カプセル化と OSPF

カプセル化・フィーチャーの大きな利点の 1 つは、OSPF 動的ルーティング・プロトコルがルーティング・プロセスに追加されることです。OSPF は、カプセル化と共に使用した場合、次のような利点を提供します。

- *最小コスト・ルーティング*。OSPF は最小の遅延で最速のパス (トンネル) にアクセスするので、ネットワーク管理者は最も安価なルートを通ってトラフィックを送達することができます。
- *動的ルーティング*。OSPF は最小コストのパスを見つけ、さらに低いオーバーヘッドで障害を検出したり、トラフィックをう回させることができます。
- *マルチパス・ルーティング*。ロード・シェアリングにより、利用可能な帯域幅をより効率的に利用できます。

OSPF を用いて、トンネルは相互通信ネットワークの内部のパスを自動的に管理します。パス上の伝送路やブリッジに障害が起きると、トンネルは自動的に新しいパスにトラフィックをう回させます。パスがう回されると、トンネルは自動的にその最良パスに更新します。このう回は、エンド・ステーションに対しては完全に透過的

です。OSPF の詳細については、323ページの『第15章 OSPF の使用』から始まる構成と監視に関する各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。これは、ルーティング機能が使用不可能になったときに、ブリッジの構成と監視を行えるようにします。このオプションは、次の機能を提供します。

- SNMP を通した管理
- Telnet サーバー機能
- TFTP プロトコルによる構成のダウンロードとアップロード
- TFTP 近隣ブート機能
- PING およびルート・トレースの IP 診断ツール
- SNMP 集合および telnet クライアントを介した装置の制御

ブリッジの監視インターフェースから見た場合、TCP/IP ホスト・サービスは、独自の構成プロンプトと監視プロンプトをもつ新規プロトコルとして扱われます。これらのプロンプトへのアクセスは、`talk 6` および `talk 5` で **protocol** コマンドを使用して行います。

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ことにより起動されます (215ページの『第12章 TCP/IP ホスト・サービスの構成および監視』を参照してください)。この IP アドレスは、単一のインターフェースに関連するのではなく、ブリッジ全体に関連付けられます。ネットワーク上でブートすると、ブリッジの IP アドレスとデフォルトのゲートウェイを、ブート PROM を持つ ROMCOMM インターフェースを介して自動的に確認する (learn) ことができます。デフォルトのゲートウェイ割り当ては、ユーザーが構成することも可能です。

ブリッジングがルーター・ソフトウェア・ロードのオプションの 1 つになっている場合は、必ず TCP/IP ホスト・サービスが利用可能です。

ブリッジ MIB サポート

SNMP を介してブリッジを管理する場合、IBM アクセス・インテグレーター・サービス は RFC 1493 および RFC 1525 で指定された管理情報ベース (MIB) をサポートします。ただし、次の MIB は***除きます***。

- dot1dStaticTable
- dot1dTpFdbTable
- dot1dPortPairTable

NetBIOS ネーム・キャッシュ

NetBIOS ネーム・キャッシュ・フィーチャーは、ブリッジング・ルーターが発信リングからブリッジ経由で転送する Name-Query (ネーム照会) フレームの数を、大きく削減できます。NetBIOS ネーム・キャッシュの構成は、NetBIOS 構成の一部として行います。詳細については、155ページの『NetBIOS ネーム・キャッシュとルート・キャッシュ』を参照してください。

NetBIOS 重複フレーム・フィルター

通常は、3 つのタイプのフレームが、6 つのグループで送信されます。

- 名前照会
- 名前追加
- グループ名追加

重複フレーム・フィルター機能は、タイマーを使用して、ユーザーが指定した時間内は各タイプのフレームの 1 つのインスタンスだけがブリッジを通過して転送されるようにします。

このプロセスは、ネーム・キャッシュで使用されるのとは別のデータベースを使用します。重複フレーム・データベースのエントリーには、クライアントの MAC アドレスと 3 つのタイム・スタンプ (前述の各フレーム・タイプにつき 1 つ) が入っています。重複フレーム・フィルターは、ネーム・キャッシュの前に行われます。詳細については、147ページの『重複フレームのフィルター』を参照してください。

NetBIOS ネームおよびバイト・フィルター

NetBIOS フィルターは、ASRT ブリッジングの性能の向上を達成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、パケットをブリッジ (転送) するのか、フィルター (廃棄) するのかを決めるするために NetBIOS パケットに適用する規則の集合です。

NetBIOS フィルターのタイプ

NetBIOS フィルターには 2 つのタイプがあります。ホスト・ネーム とバイト です。

ホスト・ネーム

ホスト・ネーム・フィルターは、NetBIOS パケット内のフィールドを使用して、ブリッジまたはフィルターする特定の NetBIOS ホスト・ネームを持つパケットを選択する方法で実現します。ホスト・ネーム・フィルターは、ブリッジングにのみ適用されます。フレーム・タイプに応じて NetBIOS 発信元またはあて先のネームを使用できます。

ネーム・フィルターは、ブリッジまたはデータ・リンク交換される NetBIOS トラフィックに適用されます。

バイト　バイト・フィルターは、NetBIOS パケット内のバイト (任意のフィールド) を使用して、ブリッジまたはフィルターする特定の NetBIOS パケットを指定する方法で実現します。

これらのフィルターに関連付けられた限界値やタイマーはなく、ユーザーが使用不可にするか除去するまでアクティブのままです。NetBIOS フィルターは 3 つの部分から構成されています。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です (詳細については、52ページの『フィルターの作成』で説明しています)。

NetBIOS の構成および監視については、165ページの『第8章 NetBIOS の構成および監視』で説明します。本節の残りの部分では、NetBIOS ホスト・ネーム・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・ネーム・フィルター

ホスト・ネームを使用する NetBIOS フィルターは、ブリッジまたはフィルターする特定の NetBIOS ホスト・ネームを持つパケットを選択することができます。ブリッジまたはフィルターする特定の NetBIOS ホスト・ネーム (または、 NetBIOS ホスト・ネームの集合) を持つパケットを指定すると、以下の NetBIOS パケット・タイプの発信元ネームまたはあて先ネーム・フィールドが調べられます。

- 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・ネーム・フィルター・リストは、4 つのタイプの NetBIOS パケットの発信元またはあて先ネーム・フィールドと比較する NetBIOS ネームを指定します。ホスト・ネーム・フィルター・リストを適用した結果、NetBIOS パケット が 4 つのタイプのうちの 1 つに該当していない場合、結果は *Inclusive (包含)* になります。

ホスト・ネームを使用する NetBIOS フィルターを構成するときには、フィルターを適用するポートと、そのポートの入力または出力パケットのいずれに適用するのかを指定します。NetBIOS 非番号制情報 (UI) パケットのみがフィルターの適用対象になります。フィルターは、ソース・ルーティング・ブリッジング (全 RIF タイプ) または透過ブリッジングのためにルーターに到着した NetBIOS パケットに適用されます。

フィルターで NetBIOS ホスト・ネームを指定するときは、16 進形式の名前の 16 番目 (最後) の文字を、分離された引き数として示すことができます。このようにした場合、名前の最初の 15 バイトは指定されたものと見なされ、16 番目のバイト (何かが指定されている場合) は、最後の引き数によって判別されます。16 文字より少ない字数を指定した場合 (そして、16 番目のバイトがない場合)、15 番目の文字までは 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扱われます。

特定の NetBIOS ホスト・ネームを評価する場合、その名前は特定 NetBIOS パケットの特定フィールドとのみ比較されます。フィルター項目の NetBIOS ホスト・ネームには、ワイルドカード文字 (?) を NetBIOS ホスト・ネームのどの位置にでも含めることができ、またアスタリスク (*) を NetBIOS ホスト・ネームの最終文字として含

めることができます。? は、ホスト・ネームの任意の 1 文字と照合されます。* は、ホスト・ネームの最後の 1 字または複数の文字と照合されます。

NetBIOS バイト・フィルター

もう 1 つのフィルター方式であるバイト・フィルターは、NetBIOS パケット内の MAC アドレスに関連するフィールドを使用して、ブリッジまたはフィルターする NetBIOS パケットを指定することができます。この場合は、すべての NetBIOS パケットが、構成されたフィルター基準に一致するかどうかを調べられます。

バイト・フィルターを作成するには、次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
- 照合するバイト・パターン
- NetBIOS ヘッダーの選択されたフィールドに適用する任意選択のマスク

マスク (もしあれば) の長さは、バイト・パターンと同じ長さにする必要があります。マスクは、ルーターがヘッダー・バイトと 16 進パターンを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と論理 AND するバイトを指定します。マスクが指定されていない場合は、オール 1 と見なされます。16 進パターン (つまり、マスク) の最大長は 16 バイト (32 桁の 16 進数字) です。

特定バイトを使用する NetBIOS フィルターを構成するときには、フィルターを適用するポートと、それらのポートの入力または出力パケットのいずれに適用するのかも指定します。

フィルターの作成

各フィルターは、1 つまたは複数のフィルター・リストから構成されます。各フィルター・リストは、1 つまたは複数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ている順序でパケットと照合され、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、ルーターは、次のように処理します。

- フィルター・リストが*包含 (Inclusive)* として指定されている場合は、パケットをブリッジします。
- フィルター・リストが*排他 (Exclusive)* として指定されている場合は、パケットを廃棄します。

フィルター・リスト内のフィルター項目が 1 つも一致しなかった場合、ルーターは、次のように処理します。

- フィルター全体が*包含* として指定されている場合は、パケットを転送します。
- フィルター全体が*排他* として指定されている場合は、パケットを廃棄します。

フィルター項目は、NetBIOS パケットの特定フィールドに適用される 1 つの規則です。この規則を適用した結果は、包含 (ブリッジ) または排他 (フィルター) のいずれかの表示です。NetBIOS フィルターでは、次のフィルター項目を構成することができます (最初の 2 つの項目はホスト・ネーム・フィルター、最後の 2 つの項目はバイト・フィルターです)。

- NetBIOS ホスト・ネームの任意選択の 16 番目の文字 (16 進数) を含める。
- NetBIOS ホスト・ネームの任意選択の 16 番目の文字 (16 進数) を除外する。
- オフセット 16 進マスクから始まる NetBIOS ヘッダー 16 進パターンへの 10 進バイト・オフセットを含める。
- オフセット 16 進マスクから始まる NetBIOS ヘッダー 16 進パターンへの 10 進バイト・オフセットを除外する。

フィルターの指定部分では、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は、ブリッジするのか (包含)、フィルターするのか (排他) を指示します。これは、フィルター・リストのデフォルト・アクションです。フィルター・リストのデフォルト・アクションは、初期には「包含」に設定されていますが、この設定はユーザーが変更できます。

シンプル・フィルターとコンプレックス・フィルター

シンプル・フィルターは、1 つのフィルター・リストと、ルーターのポート番号および入力/出力の指定の組み合わせで構成されています。これは、そのフィルター・リストを、指定された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・リストの評価が「包含」の場合、対象となったパケットはブリッジされます。そうでない場合、パケットはフィルターされます。

コンプレックス・フィルターは、ポート番号、入力/出力の指定、および論理演算子 AND または OR のうちの 1 つによって分離された複数のフィルター・リストを指定することによって構成できます。コンプレックス・フィルターのフィルター・リストは、厳密に左から右に評価され、コンプレックス・フィルター内の各フィルター・リストが評価されます。各「包含」フィルター・リスト結果は、真として扱われ、各「排他」フィルター・リスト結果は、偽として扱われます。全フィルター・リストとそ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、そのパケットがブリッジされるか、フィルターされるかを示します。入力/ポートまたは出力/ポートの各組み合わせに対して、最高で 1 つのフィルターしか適用できません。

複数スパンニング・ツリー・プロトコル・オプション

ASRT ブリッジでは、可能な構成オプションの数と同数まで、スパンニング・ツリー・プロトコル・オプションを拡張することができます。以下の節では、これらのフィーチャーについて説明します。

背景: 複数のスパンニング・ツリー・プロトコルに伴う問題

ブリッジング技術は、各種のブリッジング方式をサポートするために、種々のバージョンのスパンニング・ツリー・アルゴリズムを採用しています。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形成することです。

透過ブリッジ (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、ハロー BPDU とトポロジー変更通知 (TCN) BPDU が透過フレームに入れられて、関

係のすべての媒体 (トークンリング、イーサネット、 など) の既知のグループ・アドレスに送信されます。この交換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 に転送して、ループのないトポロジーを決めます。このアルゴリズムは、ハロー BPDU を透過フレームに入れて、既知の機能アドレスに送信します。SRB は、TCN BDPU を使用しないので、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たポート状態の設定は、全ルート探索 (ARE) フレームおよび特別ルート・フレーム (SRF) トラフィックには影響を与えません。

IBM 8209 ブリッジを使用するブリッジング構成では、異なるスパンニング・ツリー方式を使用して並列 8209 ブリッジを検出します。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 を使用します。この方式では、8209 は透過ブリッジとその他の IBM 8209 ブリッジを持つスパンニング・ツリーを構築することができます。ただし、SRB スパンニング・ツリー・プロトコルには参加せず、SRB によって送信されたハロー BPDU はフィルターされてしまいます。したがって、8209 がルート・ブリッジになるのを防止する手段がありません。8209 ブリッジがルートとして選択された 場合、2 つの透過ブリッジ・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くなる可能性があります。

このように、複数のスパンニング・ツリー・プロトコルを実行している場合、アルゴリズムが独自のループのないトポロジーを作成する方法が整合性の問題の原因なることがあります。

STP/8209

STP/8209 ブリッジング・フィーチャーを使用すると、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、トークンリング上のループのないツリーは手動でしか構成できませんでした。これが、並列 SR-TB ブリッジの場合、ループを防止する唯一の方法でした。 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になります。

- 純粋な透過ブリッジ (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とソース・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・プロトコルなし) が使用されます。
- SR-TB ブリッジ - TB ポートには IEEE 802.1d スパンニング・ツリー・プロトコルが使用され、SRB ポートでは IBM 8209 BPDU が使用されて、TB と SR-TB の単一ツリーが形成されます。SRB ハロー BPDU は、SR ドメインの通過は許されますが、処理はされません。IBM 8209 ブリッジはこのようなフレームをフィルターしますが、これは他方のポートが TB ポートである 2 ポート・ブリッジであるために可能なことです。

- 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、通過は許されますが、処理はされません。
- ASRT ブリッジ - IEEE 802.1d スパンニング・ツリー・プロトコルを使用して、TB および SRT ブリッジを持つツリーが作成されます。また、すべての SR インターフェースで 『8209 と同様の』 BPDU も生成されます。これらの BPDU は、受信されるとただちに処理されます。その結果、2 つの BPDU が生成され、すべての SR インターフェースで受信されることになります。両方の BPDU には同じ情報が入っているので、ポート情報の矛盾は生じません。このようにして、ASRT ブリッジは、IBM 8209 と SR-TB ブリッジだけでなく、他の TB および SRT ブリッジも含むスパンニング・ツリーを作成します。

スレッド (ルーター・ディスカバリー)

スレッドは、トークンリング・エンド・ステーション・プロトコル (たとえば、IP、IPX、または AppleTalk) が、ソース・ルーティング・ブリッジ・ネットワークを通って別のエンド・ステーションに到達するルートを見つけるために使用するプロセスです。

スレッド・プロセスの詳細は、エンド・ステーション・プロトコルによって異なります。以下の節では、IP、IPX、および AppleTalk のスレッド・プロセスについて説明します。

ARP による IP スレッド

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 を見つけます。IP エンド・ステーションとブリッジの両方が、ルート・ディスカバリーおよび転送プロセスに参加します。以下のステップで、IP スレッド・プロセスを説明します。

1. IP エンド・ステーションは、ARP テーブルと RIF テーブルを維持しています。ARP テーブルの MAC アドレスが、RIF テーブルのあて先 RIF の相互参照として使用されます。特定 MAC アドレスの 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) を入れた ARP REQUEST パケットをローカル・セグメントに転送します。
2. ローカル・セグメント上のすべてのブリッジが ARP REQUEST パケットを受け取り、それぞれの接続ネットワークを介して送信します。

   ARP REQUEST パケットがあて先エンド・ステーションの探索を続ける間、それを転送する各ブリッジは、自身のブリッジ番号と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・ネットワークを通過し続ける間に、RIF はあて先までのパスを説明する、ブリッジ番号とセグメント番号の組みからなるリストを編成します。

   ARP REQUEST パケットが最後にそのあて先に到着したときには、フレームには発信元からあて先までの正確な順序のブリッジ番号とセグメント番号が入っています。

3. あて先エンド・ステーションは、フレームを受信すると、MAC アドレスとその RIF を、自身の ARP テーブルと 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 パケットを受信した場合、そのパケットは廃棄されます。
4. 次に、あて先エンド・ステーションは、RIF が入っている ARP REPLY パケットを生成し、それを発信元エンド・ステーションに返送します。
5. 発信元エンド・ステーションは、確認されたルート・パスを受け取ります。そして、MAC アドレスとその RIF を、ARP および RIF テーブルに入れます。次に、その RIF をデータ・パケットに付加して、あて先に転送します。
6. RIF エントリーのエージングは、IP ARP リフレッシュ・タイマーによって処理されます。

IPX スレッド

IPX エンド・ステーションは、受信した各パケットの RIF をチェックします。RIF がテーブル内に存在しない場合は、RIF をテーブルに追加し、そのルートを *HAVE_ROUTE* として指定します。RIF に、その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が示されている場合、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信する必要があるが、MAC アドレスの RIF テーブル内にエントリーが存在しない場合、エンド・ステーションはデータを STE として送信します。

RIF タイマーが満了すると、テーブル内のエントリーは消去され、そのエントリーの RIF が入っている別のパケットが到着するまで、再記入されません。

AppleTalk 2 スレッド

AppleTalk エンド・ステーションは、ARP および XID パケットを使用して、ルートを見つけます。AppleTalk エンド・ステーションとブリッジの両方が、ルート・ディスカバリー・プロセスおよび転送に参加します。以下のステップで、AppleTalk スレッド・プロセスを説明します。

1. 特定 MAC アドレス用の 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) を入れた ARP REQUEST パケットをローカル・セグメントに転送します。
2. ローカル・セグメント上のすべてのブリッジが ARP REQUEST パケットを受け取り、それぞれの接続ネットワークを介して送信します。ARP REQUEST パケットがあて先エンド・ステーションの探索を続ける間、それを転送する各ブリッジは、自身のブリッジ番号と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・ネットワークを通過し続ける間に、RIF はあて先までのパスを説明する、ブリッジ番号とセグメント番号の組みからなるリストを編成します。
3. あて先エンド・ステーションは、フレームを受信すると、MAC アドレスとその RIF を、自身の ARP テーブルと RIF テーブルに入れ、エントリーの状態を *HAVE_ROUTE* として指定します。あて先エンド・ステーションが、同じ発信元から他の ARP REQUEST パケットを受信した場合、そのパケットは廃棄されます。

4. 次に、あて先エンド・ステーションは、RIF が入っている ARP REPLY パケットを生成し、RIF の方向ビットを逆にして、発信元エンド・ステーションに返送します。
5. 発信元エンド・ステーションは、確認されたルート・パスを受け取ります。そして、MAC アドレスとその RIF を、ARP および RIF テーブルに入れ、状態を *HAVE_ROUTE* として指定します。RIF に、その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が示されている場合、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 を入れた XID が送信され、状態は *DISCOVERING* に変更されます。XID の応答を受信しない場合、そのエントリーは廃棄されます。

SR-TB 重複 MAC アドレス・フィーチャー

重複 MAC アドレス (DMAC) フィーチャーは、重複する MAC アドレスが構成されている SR ブリッジ・ネットワークに、SR-TB ブリッジを接続することを可能にします。重複 MAC アドレス・フィーチャーは、2 つのオプションを用いて使用可能にすることができます。

- **ロード・バランシングなしの重複 MAC フィーチャー**

  このオプションでは、ロード・バランシングなしで重複 MAC アドレスを使用可能にすることができます。この場合は、重複 MAC アドレスに対して 1 つだけ RIF が確認され、この確認された RIF に基づいてエージングが行われます。TB ドメインからのすべてのステーションが、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 のエントリーのエージが満了すると、TB ドメインからの次のフレームが、スパンニング・ツリー探索 (STE) フレームとして送信されます。

- **ロード・バランシングありの重複 MAC フィーチャー**

  このオプションは、ロード・バランシングを行う重複 MAC アドレスを使用可能にすることができますが、あらかじめ「ロード・バランシングなし DMAC」を使用可能にしておかないと使用可能することができません。この場合は、重複する MAC アドレスのそれぞれに対して 2 つの RIF が確認され、維持されます。この 2 つの RIF は、それぞれ独自のエージング・タイマーを持っています。ブリッジが特定の RIF を含むフレームを受信するたびに、その RIF に対応するエージング値がリフレッシュされます。TB ドメインからのステーションが初めて重複 MAC アドレスあてにフレームを送信するときに、そのフレームの送信にどちらの RIF を使用するかは、ブリッジ・ソフトウェアが決めます。その送信元ステーションからのその後のフレームはすべて、同じ RIF を使用して送信されます。ブリッジは、最高 7 つまでの重複 MAC アドレスに対して、1 次および 2 次 RIF を維持します。重複 MAC アドレスに対して別々のエージ値を指定した場合、該当する値を使用してその重複 MAC アドレスに対応するエントリーのエージング処理が行われるので、重複 MAC アドレスのエージング値を調整することが可能になります。

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、1 つ 1 つはブリッジ・ポートとして構成されていないフレーム・リレー・バーチャル・サーキットをすべて含むブリッジ・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ており、この番号はソース・ルーティング・ブリッジングに使用されます。

マルチアクセス・ブリッジ・ポートには、以下の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。
- 完全メッシュ構成は、あらゆる接続をサポートするため、ブリッジング・ループを避けるためにスパンニング・ツリー・プロトコルを使用することがあります。
- 同一のマルチアクセス・セグメント上のバーチャル・サーキット間のブリッジングはサポートされないため、部分メッシュ構成は、支局とデータセンター間の接続しかサポートしません。この構成は、スパンニング・ツリー・プロトコルを使用できないので、STE フレームの転送を使用可能にする必要があります。特に指定のない限り、スパンニング・ツリー・プロトコルは使用不可で、STE フレームの転送は使用可能です。

  注: これは優先構成です。なぜなら、スパンニング・ツリー・プロトコルは大量の WAN 帯域幅を消費する可能性があり、ほとんどの構成は部分メッシュだからです。

- 1 対 N のブリッジ・バーチャル・セグメントが必要です。
- 類似のエンド・ステーション間でのプロトコルに依存しない接続と、異なる媒体上のエンド・ステーション間での限定された接続を可能にします。
- 複数の IBM 2218 装置について効率のよいデータ・キャッチャーを提供できます。(59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・ポートは、ネクスト・ホップ・セグメントを、フレームを受け取ったフレーム・リレー・バーチャル・サーキットにマップするマルチアクセス・ブリッジを保持します。データベース・エントリーは、セグメントが ARE、STE、または特定ルート・フレームをサーキットから受け取ったときに作成されたり、更新されます。マルチアクセス・セグメントに転送される STE フレームと ARE フレームは、マルチアクセス・セグメント内のすべてのバーチャル・サーキットにあふれます。マルチアクセス・セグメントにあふれる特定ルート・フレームは、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・エントリーがある場合に限り、転送されます。

ソフトウェアは、**multiaccess-age** コマンドで指定した速度でマルチアクセス・データベース内のエントリーを “エージングにより除去” します。

マルチアクセス・ブリッジ・ポートの構成

以下の例 は、フレーム・リレー・インターフェース 1 および 4 でのマルチアクセス・ブリッジ・ポートの構成方法を示しています。ポート 5 は、次に使用可能なブリッジ・ポートであり、ソース・ルーティングは、今回初めて使用可能にされます。

```
* 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は、ブリッジ番号とバーチャル・セグメント番号の入力を求めるプロンプトは出されません。

IBM 2218 装置との相互運用

データ・キャッチャーとして多重アクセス・ポートを 2210/2212/2216 装置と使用すると、ネットワーク内の 2218 について高密度高可用性トポロジーが得られます。

- 高密度になるのは、単一のマルチアクセス・ブリッジ・ポートを介して多くの 2218 装置が 1 つのデータセンター・ブリッジに接続できるためです。
- 高可用性となるのは、マルチアクセス・ブリッジ・ポートを介して基本およびバックアップ・データセンター・ブリッジのに接続するよう 1 つの 2218 を構成するためです。このようにすると、2218 は、フレーム・リレー・ネットワーク内で問題を検出したときに基本とバックアップ・サーキット との間で切り替えることができます。

2218 が自身と中央ブリッジとの間の LLC 接続を切断せずに基本ブリッジと中央ブリッジとの間で切り替わるようにするには、次のことを行う必要があります。

- 基本およびバックアップ・データセンター・ブリッジを同じブリッジ 1 対 N バーチャル・セグメント番号で構成する。
- 基本およびバックアップ・データセンター・ブリッジを同じソース・ルート・ブリッジ番号で構成する。
- 基本およびバックアップ・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: この構成は、支局とデータセンター間の接続しかサポートしません。

60ページの図19 に、2212 と 2218 との間の一般的なネットワーク接続を示します。

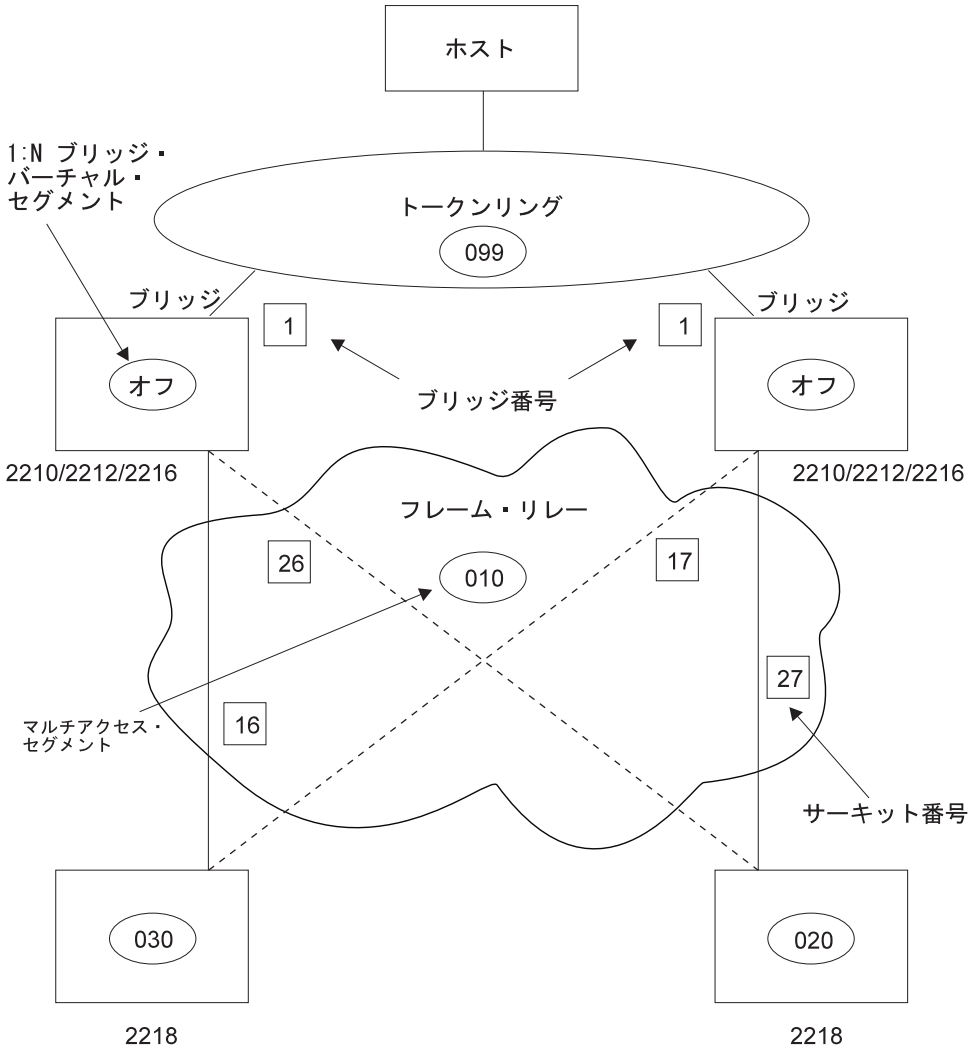


図 19. 2218 およびマルチアクセス・ブリッジ・ポートのある構成例

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、2212 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 エンド・ステーションが広域リンクを介して SNA 環境と通信するための、高信頼性で低コストの方法を提供します。本章には、以下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 は、以下の SNA ノード・タイプに接続するのに使用できます。

- 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・ノードの例であり、VTAM と共に、複合 APPN ネットワーク・ノードを形成します。

BAN フィーチャーは、2212 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。このフィーチャーは、2212 に接続された IBM タイプ 2.0 および 2.1 エンド・ステーションが、フレーム・リレーを介して、RFC 1490 ブリッジ 802.5 (トークンリング) フレーム・フォーマットをサポートする SNA ノードに直接接続することを可能にします。BAN フィーチャーは、IBM SNA 環境と通信するための、より良好な、より低コストの方法を提供します。IBM では、IBM 3745 の IBM ネットワーク制御ソフトウェア (NCP) を、この環境をサポートするように変更しました。

BAN を使用している場合、62ページの図20 に示すように、エンド・ステーションは、トークンリング、イーサネット、または SDLC 回線を介して SNA ノードに直接接続されているかのように機能します。データは実際には 2212 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・ステーションには透過的です。

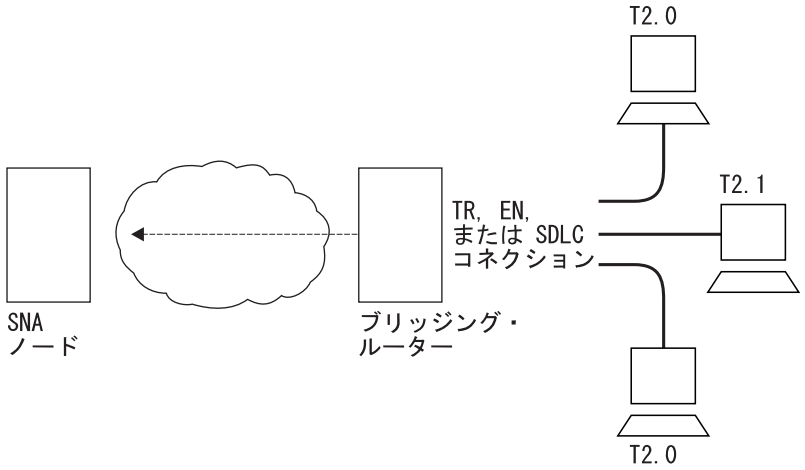


図 20. BAN を使用したエンド・ステーションと SNA ノードの直接接続

BAN の利点

BAN は、完全な DLSw を実現する必要はないユーザーのニーズを満たすために設計されたもので、IBM 環境に接続する経済的な方法です。BAN は、完全な DLSw 機能へのパスを提供し、IBM 環境との相互接続ネットワークを必要とするユーザーに 3 つの大きな利点を提供します。

1. 別の DLSw ルーターによるフレーム変換を必要とせずに、イーサネットまたはトークンリング・トラフィックを直接 SNA ノードにブリッジできる。これにより、中央サイトに別のルーターやホストを置く必要がなくなるので、機器の資本コストを節約できます。
2. 単一のフレーム・リレー・データ・リンク・コネクション識別子 (DLCI) を介する多重化 LLC タイプ 2 (*LLC2*) コネクションの数に、アーキテクチャー上の制限がない。これに対して、従来の NCP フレーム・リレー境界ノード (BN) サポートでは、DLCI 当たりの LLC2 コネクションの数が 127 に制限されています。これにより、フレーム DLCI 提供者のコストを大きく節約できます。
3. エンド・ステーションにローカルの 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い。これにより、BAN 設定の構成および管理が容易になります。

   注: IP トラフィックに対しては BAN DLCI を使用できます。これにより、SNA 用に使用している (BAN を介して) のと同じ DLCI 上で、ルーターを管理する (SNMP を介して) ことが可能になります。

BAN の機能

ルーターの BAN フィーチャーは、タイプ 2.0 または 2.1 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という方法で動作します。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・フォーマットに適合するように、ルーターによって変更されます。ルーターは各フレームを調べ、BAN DLCI MAC アドレスを持つものだけを、DLCI 経由でメインフレームに渡すことを許しま

す。ブリッジされた 802.5 フレームのあて先 MAC アドレスが、SNA ノードあてのフレームの境界ノード識別子で置き換えられます。

BAN を使う場合、通常は 1 つだけ DLCI が必要です。ただし、BAN はルーターと IBM 環境の間に多数の DLCI コネクションを使用することも可能です。場合によっては、BAN トラフィックを処理するために、複数の DLCI を設定したいことがあります。詳細については、70ページの『複数の DLCI の設定』を参照してください。

BAN フィーチャーを使用するには 2 通りの方式があります。

- 2212 のブリッジング機能を使用したストレート・ブリッジング
- DLSw 終端。BAN は DLSw を実行するルーター上で LLC2 コネクションを終端します。

以下の節では、それぞれの方式の構成方法について説明します。

ブリッジ BAN 対 DLSw BAN

BAN は 2 通りの方式で実現することができます。すなわち、ストレート・ブリッジングと DLSw 終端です。ストレート・ブリッジングでは、タイプ 2.0 またはタイプ 2.1 エンド・ステーションからのフレームを直接 SNA ノードにブリッジするように BAN を構成します。DLSw 終端では、BAN は LLC2 コネクションを、DLSw を実行するルーター上で終端します。以下の説明では、ストレート・ブリッジングを *BAN タイプ 1* と呼び、DLSw 終端を *BAN タイプ 2* と呼びます。

64ページの図21 は、BAN タイプ 1 (ブリッジ) コネクションを示しています。この図では、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ません。代わりに、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・フォーマット (RFC 1490) フレームに変換し、直接 SNA ノードにブリッジします。

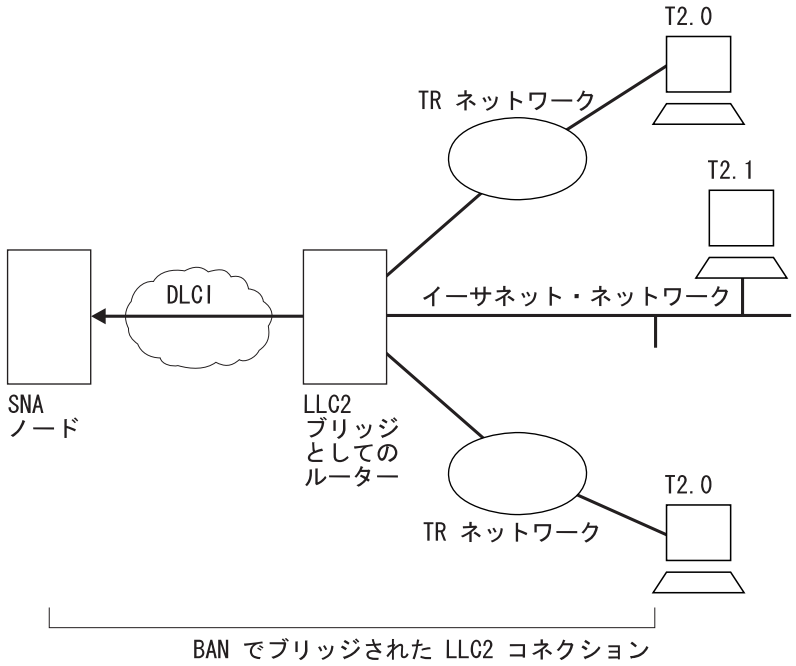


図 21. BAN タイプ 1: LLC2 ブリッジとしてのルーター

この場合、ルーターは SNA ノードとエンド・ステーション間のブリッジとして機能します。DLSw は、ルーターで LLC2 セッションを終了しません (BAN タイプ 2 のように)。エンド・ステーション・フレームはトークンリング、あるいはイーサネット (このタイプのフレームをサポートするようにブリッジが構成されている場合) が可能です。

65ページの図22 は、BAN タイプ 2 (バーチャル BAN DLSw) コネクションを示しています。この図では、DLSw ルーターはブリッジとして機能し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ます。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 ノードへの新規 LLC2 コネクションを確立します。このように、このトランザクションの中には 2 つの LLC2 コネクションが存在していますが、両者間の中断は SNA ノードにもエンド・ステーションにも透過的です。結果的に SNA ノードとエンド・ステーション間にバーチャル LLC2 コネクションが確立されることになります。

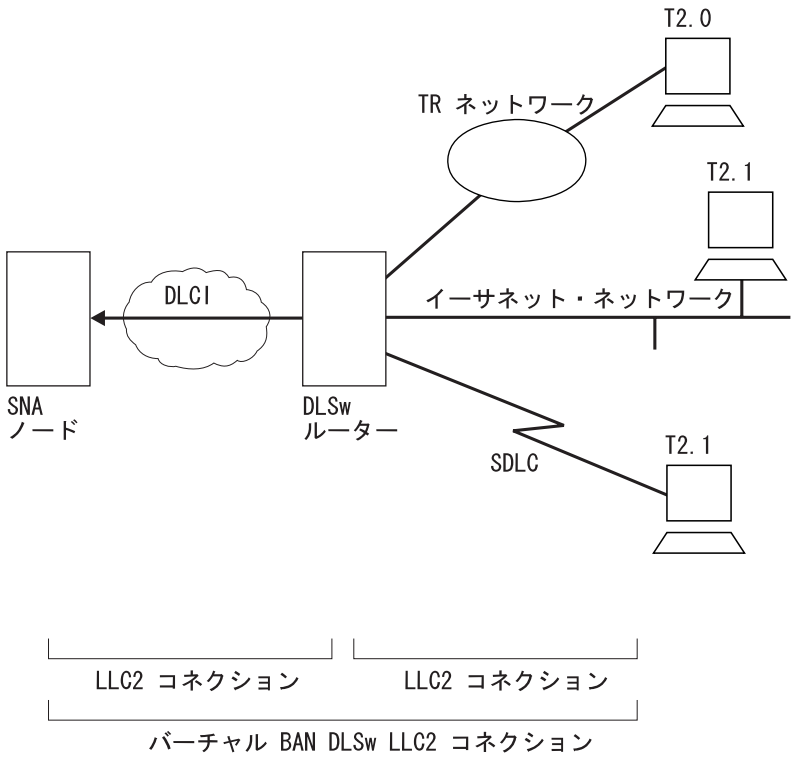


図 22. BAN タイプ 2: ローカル DLSw コネクション

SDLC セッションはルーターで終了され、別の LLC2 セッションが、ルーターと SNA ノード間に存在します。SNA ノードからは、SDLC ステーションはフレーム・リレー接続されたステーションのように見えます。

どちらのタイプの BAN も、リモート DLSw をサポートします。DLSw パートナーとして機能するルーターは、BAN タイプ 1 またはタイプ 2 コネクションのいずれかを使用して、タイプ 2.0 または 2.1 エンド・ステーションを SNA ノードに接続することができます。

どちらの方式を使用するか

一般的には、フレームのストレート・ブリッジング (BAN タイプ 1) が望ましい方法です。ネットワークのオーバーヘッドを最小限にし、データを高速で送達できるからです。ただし、例外があります。DLCI の使用率が非常に高い場合には、ブリッジされた構成ではセッション・タイムアウトが発生する可能性があります。逆に、DLSw 構成 (BAN タイプ 2) では、セッション・タイムアウトはめったに起こりません。このタイプの構成は、ローカル (DLSw) ルーターで LLC2 セッションをいったん終了し、その後で LLC2 セッションを再作成するからです。

BAN フィーチャーの使用

BAN の構成時には、システムがユーザーに情報の入力を指示します。しばしば、システムがデフォルト値を提供するので、ユーザーは **Return** キーを押してこれを受け入れることができます。

BAN フィーチャーを使用するためには、以下のことが必要です。

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)

これらのステップについて、以下の例で説明します。例では、BAN トラフィックを伝送する単一の DLCI を設定するものと想定しています。ユーザーの環境とニーズに応じて、冗長度のために、あるいは IBM 環境の総帯域幅を増やすために、複数の DLCI を設定することも可能です。この場合、2212 の BAN DLCI MAC アドレスは、ISDN バックアップ 2212 の BAN DLCI MAC と同一であることが必要です。また、2212 の内部ブリッジ・セグメントの値は、バックアップ 2212 の内部ブリッジ・セグメントの値と異なっていることが必要です。詳細については、70ページの『複数の DLCI の設定』を参照してください。

ステップ 1: 2212 をフレーム・リレー用に構成

フレーム・リレー構成プロンプトにアクセスするには、下の例に示すように、Config> プロンプトで **network** *interface#* を入力します。(*Interface#* 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、下の例に示すように、パーマネント・サーキットを追加します。ルーターは、以下を入力するように指示します。

- サーキット番号。これは DLCI 番号です。
- 認定情報速度

```
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>
```

作成された DLCI は、 BAN の使用時に 2212 と SNA ノードを接続する PVC になります。次のステップでは、この PVC をブリッジ・ポートとして構成します。

注: 同一のまたは異なる SNA ノードに接続されている複数の BAN DLCI を設定したい場合は、各 DLCI ごとに個別にフレーム・リレーを構成する必要があります。詳細については、70ページの『複数の DLCI の設定』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

次に、PVC をブリッジ・ポートとして構成することが必要です。これを行うには、下に示すように、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、下の例の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の入力を求めるプロンプトを出します。指定するインターフェース番号は、そのブリッジの FR インターフェース番号です。また、ポート番号とサーキット番号の入力も求められます。指定するサーキット番号は、ステップ 1 でフレーム・リレーを介するブリッジング用の装置を構成するときに使用した番号と同一であることが必要です。

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

次に、ソース・ルーティングを使用可能にし、フレーム・リレー・ポートのソース・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、次のように、ブリッジ・ポートの透過ブリッジングを使用不可にします。

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

BAN タイプ 2 コネクションを使用する場合は、ブリッジング用に DLSw を使用可能にします。

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

次のステップでは、ルーターを BAN 用に構成します。

ステップ 3: ルーターを BAN 用に構成

ASRT config> プロンプトから、ルーターを BAN 用に構成することが必要です。ルーターの BAN ポートの追加は、ルーターをリスタートするまで検証されません。ステップ 1 および 2 と同様に、ブリッジ・ポート 5 がこのステップ全体を通して使用されます。

```
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するポート番号 (5) を追加します。次のように BAN DLCI MAC アドレスおよび境界ノード識別子を入力するように指示されます。

```
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。(64ページの図21 および 65ページの図22 を参照してください。) もう 1 つのアドレス 4FFF00000000 は、デフォルトの境界ノード識別子アドレスです。これを受け入れるために **Enter** を押します。

注: 境界ノード識別子は、2212 から SNA ノードに送信されたブリッジされた 802.5 フレームに入っているあて先 MAC アドレスに一致します。デフォルトの 4FFF00000000 は、IBM ネットワーク制御プログラム (NCP) によって使用されるデフォルト値に一致しています。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 キーワードで指定されます。フレーム・リレーを介するブリッジされた 802.5 フレームをサポートする SNA ノードが他にもある場合、境界ノード識別子は、その SNA ノードをこのバーチャル・サーキットに構成するときに使用された MAC アドレスに設定することが必要です。

BAN コネクション・タイプの指定: 次のプロンプトは、追加する BAN コネクションのタイプ (ブリッジされた、または DLSw 終端) を指定するように求めています。この 2 つの方式については、前節で BAN タイプ 1 および BAN タイプ 2 として説明しました。タイプ 1 (ストレート・ブリッジング) がデフォルトです。インバウンド・トラフィックをルーターで終端させたいのでなければ、デフォルトを受け入れます。

b または **t** を入力すると、ルーターは BAN ポートが追加されたことをユーザーに知らせます。

```
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 (BAN タイプ 2 のみ)

BAN タイプ 2 コネクションを使用する場合は、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、ならびに FR インターフェースおよび LAN インターフェースに関連したサービス・アクセス・ポイント (SAP) のオープンが含まれます。この DLSw 構成を行わないと、BAN タイプ 2 (DLS 終端) コネクションは使用できません。

DLSw の使用可能化は `DLSw config>` プロンプトから **enable dls** コマンドを使用して行います。

DLSw セグメント番号の設定は `DLSw config>` プロンプトから **set srb** コマンドを使用して行います。

ローカル DLSw TCP パートナーの追加は `DLSw config>` プロンプトから、次のように入力して行います。

```
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>
```

SAP のオープンは `DLSw config>` プロンプトから、次の例のように入力して行います。

```
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 に対して **open** コマンドを発行すると、LAN インターフェース上の SAP がオープンします。FR インターフェース上の SAP をオープンするときも、同じコマンドを発行します。どちらの場合も、SAP をオープンするために番号 **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 トラフィックのための複数の DLCI の使用

IBM 環境との間を往来する BAN トラフィックを扱うのに、通常は 1 つの DLCI で十分ですが、場合によっては 2 つまたはそれ以上の DLCI を設定すると便利なことがあります。

シナリオ 1: 耐障害 BAN コネクションの設定

複数の SNA ノードへの冗長コネクションは、単一の SNA ノード障害から保護します。また、BAN トラフィックを複数の DLCI 間で共有することにより、1 つの SNA ノードが過負荷になる可能性を減らすことができます。冗長 DLCI 構成では、PU タイプ 2.0 および 2.1 エンド・ステーションは、図23 に示すように、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 を同一の DLCI MAC アドレスを使用して、別々の FR ASRT ブリッジ・ポート上に構成します。ただし、SR-TB 変換が使用可能になっている場合は、このオプションは使用できません。

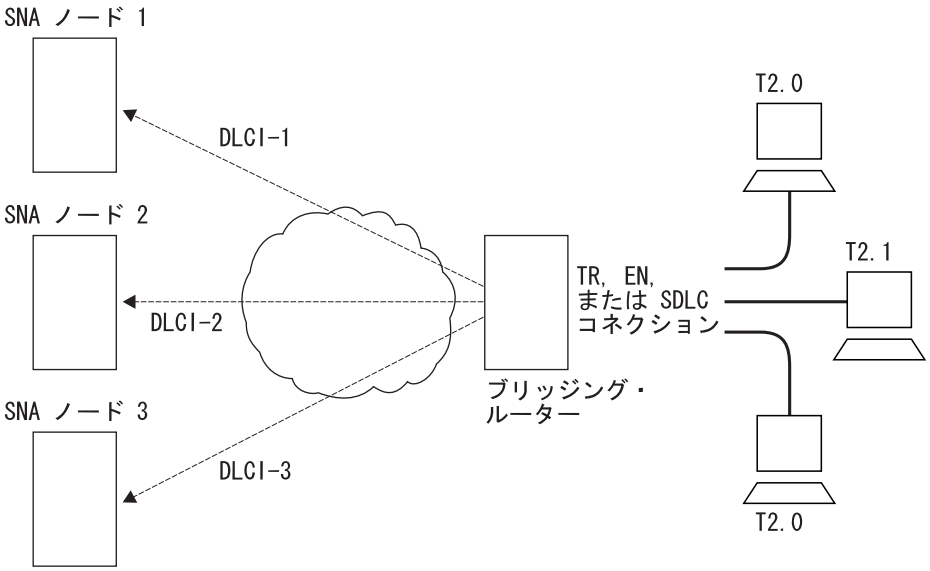


図 23. 異なる SNA ノードへの複数の DLCI をもつ BAN 構成

シナリオ 2: IBM 環境への帯域幅の増加

同じ SNA ノードへの複数のコネクションは、IBM 環境との通信に利用可能な総帯域幅を増やします。これにより、単一 DLCI 上の輻輳 (ふくそう) の可能性が減ります。

大量の BAN トラフィックとユーザーが自由に使える別の FR コネクションがある場合、2 つまたはそれ以上の DLCI を設定することが可能です。2 つ目の DLCI は SNA ノードへの総帯域幅を拡大し、予期しない障害の発生を防止することができます。

複数の DLCI の設定

複数の DLCI の設定は、特に BAN の初期構成時に行う場合は、非常に簡単です。複数のコネクションを設定するときは、各フレーム・リレー DLCI が IBM 環境の特定の SNA ノードに対応することに注意してください。BAN フレームをその SNA ノードに渡すためには、フレーム・リレー・コネクションを設定するときに、正しいサーキット番号を指定することが必要です。各コネクションのサーキット番号は、フレーム・リレー提供者に尋ねると分かります。

異なる SNA ノードへの DLCI コネクションを設定するには (69ページの『シナリオ 1: 耐障害 BAN コネクションの設定』)、以下のことが必要です。

1. 次の処置の 1 つを行う。
   - **ASRT 構成の場合**、その DLCI にブリッジ・ポートを追加します。
   - **フレーム・リレー構成の場合**、第 2 のブリッジ・ポート上に別のフレーム・リレー DLCI を定義します。
2. 67ページの『ステップ 3: ルーターを BAN 用に構成』 で説明したように、そのブリッジ・ポートを BAN 用に構成する。

同じ SNA ノードへの第 2 の DLCI コネクションを設定する場合も (『シナリオ 2: IBM 環境への帯域幅の増加』を参照)、同じ手順に従います。『シナリオ 2: IBM 環境への帯域幅の増加』では、第 2 のフレーム・リレー・ポートに指定されるサーキット番号は、最初のポートのものとは異なります。ただし、各サーキット番号は、異なる DLCI と IBM 環境への異なるパスを識別します。

BAN 構成のチェック

ルーターをリスタートすると、ルーターは、BAN ブリッジ・ポートがソース・ルーティングをするフレーム・リレー・ブリッジ・ポートであるかどうかを検査します。BAN 構成の検査は、下に示すように、list コマンドを用いて行います。

```
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** コマンドは BAN 構成の各局面を表示し、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識別子、およびそのポートがブリッジであるか DLSw 終端であるかを示します。

スタート時に BAN が正しく初期化されたかどうかを検証するには、GWCON を用いて、次のように指定します。

```
+ 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 3 つの状態メッセージを提供します。

- Init Fail 状態は、構成問題が存在することを示します。
- Down 状態は、DLCI が動作していないことを示します。
- Up 状態は、指定通りにフレーム・リレー DLCI が起動されて、動作していることを示します。

Up 以外の状態を受け取った場合は、ルーターの ELS メッセージをチェックして問題を診断します。ELS メッセージを使用可能にする方法については、『BAN のイベント・ログ・システム (ELS) メッセージの使用可能化』で説明します。

BAN のイベント・ログ・システム (ELS) メッセージの使用可能化

BAN を初期構成しリスタートした後、ELS メッセージを使用可能にして、構成が予定どおりに動作するかどうかを見るのは良い考えです。次のように Config> プロンプトから BAN 特定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。ELS はユーザーにすべての BAN 関連の動作を知らせます。しばらく BAN を動作した後で、一部のメッセージをオフにすることもできます。特定の ELS BAN メッセージをオフにするには、**nodisplay** コマンドを使用して、特定のメッセージ番号を指定します。次の例は ban.9 メッセージをオフにする方法を示しています。

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

BAN 関連メッセージの全リストおよび説明は、イベント・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) ブリッジの基本構成を作成する方法について説明します。本章には『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詳しい情報が必要な場合は、77ページの『第6章 ブリッジングの構成および監視』を参照してください。

ASRT ブリッジングの変更についての概要は、50ページの『NetBIOS ネームおよびバイト・フィルター』を参照してください。

NetBIOS フィルターの設定例については、159ページの『NetBIOS ホスト・ネーム・フィルターとバイト・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 『はじめに』 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、最小限のコマンドを用いて基本ブリッジング構成を行うことができます。たとえば **enable bridge** コマンドを使用すると、正しく構成されたすべての装置を透過ブリッジングに参加させて、このプロセスを開始します。さらに、スパンニング・ツリー・アルゴリズムのすべてのデフォルト値が使用可能になります。

次に、透過ブリッジング以外のブリッジング機能が 『ポート単位』 で使用可能にされます。ソース・ルーティングが使用可能のときは、セグメント番号やブリッジ番号などのユーザー入力が必要であり、説明されている基本コマンドの他にこれらを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 ブリッジは、次のインターフェースの 1 つまたは複数の組み合わせを介したブリッジングをサポートします。

- イーサネット
- トークンリング
- シリアル回線

イーサネット・インターフェースは、透過ブリッジングをサポートし、一方、トークンリング・インターフェースは、ソース・ルーティングおよび透過ブリッジングをサポートすることができます。

シリアル・ライン・インターフェースは、透過トラフィックおよびソース・ルーティング・トラフィックのために、ポイント・ポイント接続を提供します。シリアル・ラインを介するブリッジ構成は、両方のエンドポイントに矛盾がないように構成することが重要です。つまり、両方のエンドポイントを次のように構成します。

- 透過 - 透過
- ソース・ルーティング - ソース・ルーティング
- ソース・ルーティング/透過 - ソース・ルーティング/透過

混合ブリッジングを希望する場合は、シリアル・ラインを両方のブリッジング方式用に構成するのが最良の方法です。また、ブリッジング・ルーターがブリッジング方式または特定プロトコルのルーティングに矛盾していないことを確認することも重要です。

以下では、ASRT ブリッジが提供するブリッジング・オプションを使用可能にするのに必要な初期ステップについて概説します。その後で構成を変更する方法については、本章のコマンドの項で詳しく説明しています。これらのタスクを完了した後で、新規構成を有効にするためにルーターをリスタートすることが必要です。

透過型ブリッジの使用可能化

透過ブリッジングを使用可能にするには、 以下のコマンドを使用します。

- **Enable bridge** は、すべてのローカル・エリア・ネットワーク (LAN) インターフェースの透過ブリッジングを使用可能にします。**add port** コマンドを使用して、広域ネットワーク (WAN) インターフェース (シリアル・ラインなど) を組み込むことができます。
- **Disable transparent** *port#* は、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から除外します。透過ブリッジング構成から除外するすべてのインターフェースに対して、このコマンドを繰り返します。

ソース・ルーティング・ブリッジの使用可能化

ソース・ルート・ブリッジングを使用可能にするには、以下のコマンドを使用します。

- **Enable bridge** は、すべてのローカル・エリア・ネットワーク・インターフェースのブリッジングを使用可能にします。**add port** コマンドを使用して WAN インターフェース (たとえば、シリアル・ライン) を組み込むことができます。
- **Disable transparent** *port#* は、すべてのポートの透過ブリッジングを使用不可にします。
- **Enable source-routing** *port# segment# [bridge#]* は、指定されたポートのソース・ルーティングを使用可能にします。3 つ以上のポートでソース・ルーティングを使用可能にする場合は、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・フィーチャーしか必要ない場合は、インターフェース上の透過ブリッジングを使用不可にします。

注: 従来からソース・ルーティングをサポートしていないインターフェースは**含めない**ように注意する必要があります。たとえば、イーサネット・ポートで、透過ブリッジングが使用不可にされ、ソース・ルーティングが使用可能にされている場合、このポートのブリッジング機能は使用不可にされます。

SR-TB ブリッジの使用可能化

SR-TB ブリッジングを使用可能にするには、以下のコマンドを使用します。

- **Enable bridge** は、すべてのローカル・エリア・ネットワーク・インターフェースのブリッジングを使用可能にします。**add port** コマンドを使用して WAN インターフェース (たとえば、シリアル・ライン) を組み込むことができます。
- **Disable transparent** *port#* は、下位のすべてのソース・ルーティング・インターフェースの透過ブリッジングを使用不可にします。
- **Enable source routing bridge** *port# segment# [bridge#]* は、指定されたポートのソース・ルーティングを使用可能にします。3 つ以上のポートでソース・ルーティングを使用可能にする場合は、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。
- **Enable sr-tb-conversion** *segment#* は、ソース・ルート・フレームの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します。透過ブリッジング・ドメイン全体を表すために、ドメイン・セグメント番号とドメイン MTU サイズも指定する必要があります。

上述の手順をすべて完了した後で、**list bridge** コマンドを使用して、現行のブリッジ構成を表示して見るようにしてください。これにより、構成を検証し、チェックすることができます。

上記のすべてのコマンドの詳細については、77ページの『第6章 ブリッジングの構成および監視』を参照してください。

第6章 ブリッジングの構成および監視

この章では、適応ソース・ルーティング透過型 (ASRT) ブリッジ・プロトコルの構成方法、および ASRT 構成コマンドの使用法について説明します。本章には、以下の節が含まれています。

- 『ASRT 構成環境へのアクセス』
- 『ASRT 構成コマンド』
- 119ページの『トンネル構成コマンド』
- 89ページの『BAN』
- 123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 ブリッジとそのネットワーク・インターフェースのネットワーク・パラメーターを指定することができます。また、これらのコマンドを用いて、 ブリッジ IP トンネル、NetBIOS、および ATM インターフェース・フィーチャーを使用可能にしたり、構成したりすることもできます。

新規構成を有効にするためには、ルーターをリスタートする必要があります。

ASRT 構成コマンドは ASRT config> プロンプトで入力します。コマンドにアクセスするには、次のようにします。

- IP トンネルの構成コマンドは TNL config> プロンプトで入力します。TNL config> プロンプトは、メジャー ASRT コマンドのサブセットであり、本章で後述する ASRT config> **tunnel** コマンドを入力することによりアクセスします。
- NetBIOS の構成コマンドは NetBIOS config> プロンプトで入力します。NetBIOS config> プロンプトは、メジャー ASRT コマンドのサブセットであり、本章で後述する ASRT config> **netbios** コマンドを入力することによりアクセスします。
- NetBIOS フィルターの構成コマンドは NetBIOS Filter config> プロンプトで入力します。このプロンプトは NetBIOS コマンドのサブセットです。

ASRT 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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix ページの『ヘルプの入手』 を参照してください。
Add	固定データベースのステーション・アドレス・エントリー、特定アドレス・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経由するエンド・ステーション間のトンネルを追加します。
Ban	境界アクセス・ノード (BAN) 構成プロンプトにアクセスし、BAN 構成コマンドを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・エントリー、特定アドレス・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経由するエンド・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可にします。 • 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ピング • スパンニング・ツリー探索フレームの伝送 • 指定されたポートのソース・ルーティング • トンネルを介したスパンニング・ツリー探索フレームの受信 • SR-TB 変換 • 指定されたポートの透過 (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 ロード・バランシング
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・アドレスと機能アドレス間のマッピング • スパンニング・ツリー探索フレームの伝送 • 指定されたポートのソース・ルーティング • トンネルを介したスパンニング・ツリー探索フレームの受信 • SR-TB 変換 • 指定されたポートの透過 (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 ロード・バランシング
List	ブリッジ構成全体、または選択された構成パラメーターに関する情報を表示します。
NetBIOS	NetBIOS 構成プロンプトを表示します。

表 4. ASRT 構成コマンドの要約 (続き)

コマンド	機能
Set	以下のパラメーターを設定します。 • 動的アドレス・エントリーのエージング・タイム • ブリッジ・アドレス • トンネル伝送の最大フレーム・サイズ • 最大フレーム (LF) ビット符号化 • 最大フレーム・サイズ • スパンニング・ツリー・プロトコルのブリッジおよびポート・パラメーター • ルート記述子 (RD) 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) のエージング値 • マルチアクセス・データベース・エントリーのエージング値
Tunnel	トンネル構成プロンプトにアクセスし、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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、以下の情報をブリッジング構成に追加するのに使用します。

- 固定データベースのステーション・アドレス・エントリー
- 指定されたプロトコルの特定アドレス・マッピング
- マルチアクセス・ポート
- LAN/WAN ポート
- プロトコル・タイプに基づいてパケットを選択的にフィルターするプロトコル・フィルター
- エンド・ステーション間を結び、IP ネットワーク・セグメントを経由する IP トンネル
- 最大 7 つの重複 MAC アドレス

ブリッジの IP トンネル機能の場合、**add** コマンドは、IP インターネットワークを経由するエンド・ステーション間に IP トンネルを作成することができます。このトンネルは、IP インターネットを通るパスがどんなに複雑であっても、エンド・ステーション間のただ 1 つ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*

固有なステーション・アドレス・エントリーを固定データベースに追加します。これらのエントリーは、ブリッジをリスタートしたときに、フィルター・データベースに固定エントリーとしてコピーされます。*addr-value* は、追加するエントリーの MAC アドレスです。これには、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を使用することができます。また、各着信ポートに対して発信転送ポート・マップを指定するオプションもあります。固定データベースのエントリーは、電源オン/オフ・プロセスによって破棄されることはなく、エージングの設定も適用されません。固定エントリーは、動的エントリーによって置き換えることはできません。

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

デフォルト値: なし

以下の節では、**add address** コマンドを用いてアドレス・エントリーを管理する方法について具体的な例を示します。

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: プロンプトにおける 『Yes または No』 の質問では、『No』 がデフォルト値です。デフォルト値を受け入れるときは **Return** を押します。

Exclude destination address ...

このプロンプトでは、そのエントリーのあて先アドレス・フィルターを設定することができます。このプロンプトに 『Yes』 と応答すると、どのポートから来たかに関係なく、このアドレスをあて先アドレスとするすべてのフレームがフィルターに掛けられます。

Use same output mapping...

このプロンプトに 『Yes』 と応答すると、特定のポートにのみマッピングするのではなく、すべての着信ポートを対象にして 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、各着信ポートを選択するための別のプロンプ

ト (Input Port Number [1]?) が出ます。この特定着信ポート・プロンプトから、その着信ポート用の固有なポート・マップを作成することができます。

Input Port 1, Port 2

前のプロンプトに 『No』 と応答すると、各着信ポートと関連の発信ブリッジ・ポートを選択するための、着信ポートごとのプロンプト (Input Port Number [1]?) が出ます。

Bridge to all ports?

このプロンプトに 『Yes』 と応答すると、すべてのポートが含まれている発信ポート・マップが作成されます。したがって、このアドレスをあて先アドレスとするフレームを受信すると、そのフレームは、着信したポートを除くすべての発信転送ポートに転送されます。ポート・マップに従ってこれを実行する方法を、以下の例で示します。

フレームをポート *1* で受信し、ポート・マップが 1 (ポート 1) を示している場合、フレームはフィルターに掛けられます。

同じフレームをポート *2* で受信し、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 に転送されます。フレームをポート 1 で受信し、照合アドレス・エントリーのポート・マップが 1、2、または 3 を示している場合、フレームはポート 2 と 3 に転送されます。

ポート・マップにノー・ポート (NONE/DAF) が指示されている場合、フレームはフィルターに掛けられます。これは、あて先アドレス・フィルター (DAF) と呼ばれます。

受信したフレームに一致するアドレス・エントリーが見つからなかった場合、フレームは、発信元ポートを除くすべての転送ポートに転送されます。

Bridge to Port 1, Port 2, etc.

このプロンプトでは、アドレス・エントリーをその特定ブリッジ・ポートに関連付けることができます。『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・エントリーのポート・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・マッピングを飛ばします。

continue to another bridge port?

このプロンプトでは、構成する次の着信ポートを選択します。

Source address filtering

これは、ポート特定発信元アドレス・フィルター (SAF) を可能にします。SAF が適用されると (このプロンプトで 『yes』 と応答)、受信したフレーム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・フィルターが使用可能にされているアドレス・エントリーに一致した場合、フレームは廃棄されます。このメカニズムにより、ネットワーク管理者は、あるエンド・ステーションへのトラフィックがブリッジされるのを禁止することによって、そのエンド・ステーションを分離することができます。

エントリーのあて先アドレス・フィルターを使用可能にする

この例は、あるエントリーのあて先アドレス・フィルターを選択する場合のコマンド・プロンプトへの応答の仕方を示しています。

```
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・エントリーを追加した後で **list range** コマンドを使用して、その状態を検証することができます。次の例は、そのエントリー (太字) にはポート・マップが存在せず、あて先アドレス・フィルター (DAF) がオンになっている場合を示しています。

```
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
```

複数の着信ポートをもつアドレス・エントリーの発信ポート・マップを作成する

この例は、複数の着信ポートをもつアドレス・エントリーに対して別々の発信ポート・マップを作成する場合のコマンド・プロンプトへの応答の仕方を示しています。

```
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・エントリーを追加した後で **list range** コマンドを使用して、その状態を検証することができます。次の例は、ポート 1 と 2 を着信ポートとし、両方の着信ポートに対して別々のポート・マップを持っているエントリー (太字) の例を示しています。発信元アドレス・フィルター (SAF) も使用可能になっています。

```
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・エントリーに関連する全着信ポートに対して単一の発信ポート・マップを作成する

この例は、あるアドレス・エントリーに関連するすべての着信ポートに対して単一の発信ポート・マップを作成する場合のコマンド・プロンプトへの応答の仕方を示しています。

```
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・エントリーを追加した後で **list range** コマンドを使用して、その状態を検証することができます。下の例は、すべての着信ポート用として単一のポート・マップを持っているエントリー (太字) を示しています。発信元アドレス・フィルター (SAF) も使用可能になっています。

```
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*

Adds up to 7 duplicate MAC address entries to the database. *addr-value* は、追加するエントリーの MAC アドレスです。重複 MAC アドレス機能についての追加情報は、57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'

デフォルト値: なし

例:

アドレスを追加した後で **list dmac** コマンドを使用して、DMAC 情報を検証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*

指定されたプロトコル識別子のグループ・アドレス・マッピングに、特定の

機能アドレスを追加します。アドレス・マッピングは、トークンリング経由でイーサネットへ行く (または、その逆の) あて先アドレス上でのみ変換されます。

注: 個々の Ether-type マップ値に対して、対応する SNAP-type 値を追加する必要があります。これは双方向マッピングのために必要です。

dlh-type

(data-link-header type) は、 DSAP、Ether-type、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) プロトコル・タイプは 1 ～ FE (16 進値) の範囲で入力します。

DSAP 有効値: X'1' ～ X'FE'

一般的な値は、次のとおりです。

プロトコル - SAP (16 進値)

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

DSAP デフォルト値: 1

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

イーサネット有効値: X'5DD' ～ X'FFFF'

プロトコル - イーサネット・タイプ (16 進値)

– IP - 0800
– ARP - 0806
– CHAOS - 0804
– メインテナンス・パケット・タイプ - 7030
– DECnet MOP ダンプ/ロード - 6000
– DECnet MOP リモート・コンソール - 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 フェーズ 1 - 809B
– Apple ARP フェーズ 1 - 80F3
– ループバック・アシスタンス - 9000

イーサネット・デフォルト値: 1

サブネットワーク・アクセス・プロトコル (SNAP) プロトコル・タイプは 10 桁の 16 進フォーマットで入力します。

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

一般的な値は、次のとおりです。

– AppleTalk フェーズ 2 08-00-07-80-9B

– Apple ARP フェーズ 2 00-00-00-80-F3

SNAP デフォルト値: 00 0000 0800

ga-address

6 バイト (12 桁の 16 進値) 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'

デフォルト値: なし

fa-address

非標準フォーマットの機能アドレス。機能アドレスは、ローカル管理グループ・アドレスです。これらは、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'

デフォルト値: 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#]*

マルチアクセス・ポートをブリッジング構成に追加します。このコマンドは、ポート番号をフレーム・リレー・インターフェースと関連付け、そのポートがソース・ルート・ブリッジングに参加できるようにします。

interface#

マルチアクセス・ポートを構成しようとするフレーム・リレー・インターフェースを指定します。

有効値: 任意の既存フレーム・リレー・インターフェース番号

デフォルト値: 0

port# ブリッジ・ポート番号を指定します。この番号は、ルーター内のすべての構成済みブリッジ・ポートで固有なものでなければなりません。

有効値: 1 ～ 254

デフォルト値: 次に使用可能なポート番号

segment#

マルチアクセス・セグメントを表す、12 ビットの、16 進ソース・ルーティング・セグメント番号を指定します。このマルチアクセス・セグメントに接続されるブリッジはすべて、同じセグメント番号をもっている必要があります。

有効値: X'001' ～ X'FFF'

デフォルト値: X'001'

bridge#

マルチアクセス・セグメント上のこのブリッジを表す、4 ビットの、16 進ソース・ルーティング・ブリッジ番号を指定します。このパラメーターは、初めてソース・ルーティングを使用可能にする場合にのみ必要です。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で固有なものでなければなりません。

有効値: X'0' ～ X'F'

デフォルト値: X'0'

virtual-segment#

オプションの 12 ビットの、16 進ソース・ルーティング・セグメント番号を指定します。このパラメーターは、3 つ以上のポートについて初めてソース・ルーティングを使用可能にする場合または複数のブリッジ・ポートを初めて構成する場合にのみ必要です。

有効値: X'001' ～ X'FFF'

デフォルト値: 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#*

LAN/WAN ポートをブリッジング構成に追加します。このコマンドは、ポート番号をインターフェース番号に関連付け、そのポートが透過ブリッジングに参加できるようにします。

ポート番号の有効値: 1 ～ 254

ポート番号のデフォルト値: なし

例: ポートを追加

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

prot-filter snap ether dsap

プロトコル・タイプに基づいてパケットを選択的にフィルターに掛けられるようにブリッジを構成できます。フィルターは、すべてのポートに適用するか、または選択されたポートのみに適用することができます。

このパラメーターはプロトコル識別子を指定し、その特定プロトコルの受信フレームは、ブリッジ論理を適用せずに排他的に廃棄されます。このプロトコル・タイプの ARP パケットも廃棄されます。プロトコル・フィルターは受信パケットにのみ適用されます。利用可能なプロトコル・フィルターには、以下のものがあります。

SNAP パケット
プロトコル・タイプを 10 桁の 16 進フォーマットで入力する、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 進値) 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 進値) の範囲で入力されるあて先サービス・アクセス・ポイント・プロトコル

注:

1. タイプ X'AA' 用の DSAP フィルターを追加することにより、すべての SNAP フォーマットのパケットをフィルターに掛けることはできません。カプセル化された SNAP プロトコルは、個別にフィルターに掛ける必要があります。スライディング・ウィンドウ・フィルターの使用を検討してください。 *AIS 機構の使用と構成*の『MAC フィルターの使用』 という表題の章を参照してください。

一般的なプロトコル・フィルターとそれぞれの値は、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 でのみ使用)
Novell IPX SAP	E0 (802.5 でのみ使用)
NetBIOS SAP	F0
ISO コネクションレス型インターネット	FE

SNAP プロトコル識別子

プロトコル	SNAP OUI/IP (10 桁)
AppleTalk フェーズ 2	08-00-07-80-9B
Apple ARP フェーズ 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 進値)
IP	0800
ARP	0806
CHAOS	0804
メインテナンス・パケット・タイプ	7030
DECnet MOP ダンプ/ロード	6000
DECnet MOP リモート・コンソール	6002
DECnet	6003
DEC LAT	6004
DEC LAVC	6007

プロトコル	イーサネット・タイプ (16 進値)
XNS	0600
Apollo Domain	8019 (イーサネット)
Novell NetWare IPX	8137 (イーサネット)
Apple ARP フェーズ 1	80F3
ループバック・アシスタンス	9000

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

```
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・パケットで使用)

```
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 パケットで使用)

```
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・ポートへのユーザー定義の 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できるようになります。

IBM LAN および端末トラフィックと非 IBM トラフィック (つまり、Novell) を単一のバックボーンを介して組み合わせることができるように、ブリッジング・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・フィーチャーおよび SDLC (同期データ・リンク制御) リレー・フィーチャーは、IBM トラフィックを業界標準の TCP/IP パケット内にカプセル化します。次に、ブリッジング・ルーターはこれらのパケットを IP パス、つまり *トンネル* を使用して、大規模な IP インターネットワーク上に伝送します。トンネルの利点は、機能性とネットワークの使用効率が拡大し、さらにネットワークの利用可能性が向上し、使いやすさも改善されることです。

ネットワークの複雑さに関係なく、エンド・ステーションは IP パス (トンネル) を単一のホップと見なします。これにより、ソース・ルーティング構成に一般的に見られる 7 ホップという距離制限の解決することができます。また、ソース・ルーティング・エンド・ステーションを、イーサネット・ネットワークのような非ソース・ルーティング媒体を介して接続することも可能になります。

さらに、ブリッジ・トンネルは、以下のようなソース・ルーティングに一般的に伴ういくつかの制限を克服することができます。

- 7 ホップという距離制限

- 広域ネットワーク (WAN) でソース・ルーティングがもたらす大量のオーバーヘッド
- WAN の障害や故障に対するソース・ルーティングの敏感さ (パスに障害が発生した場合、すべてのシステムが伝送をやり直す必要があります)

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場合、ソフトウェアはパケットを TCP/IP パケットにカプセル化します。このパケットは、ルーターには TCP/IP パケットのように見えます。フレームを IP エンベロープにカプセル化した後は、IP 転送機能があて先 IP アドレスに基づいて、適切なネットワーク・インターフェースを選択します。このパケットは、性能低下やネットワーク・サイズの制約なしに、大規模なインターネットワークを経由して動的にルーティングすることができます。エンド・ステーションは、インターネットワークの複雑さに関係なく、このパス (トンネル) を単一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的です。トンネル伝送に参加しているブリッジング・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着すると、TCP/IP ヘッダーが自動的に 取り除かれ、内部のパケットは標準ソース・ルーティング・パケットとして処理が進められます。

Add Tunnel ブリッジ・ポートへのユーザー定義の 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るパスがどんなに複雑であっても、エンド・ステーション間のただ 1 つのホップとして数えられます。トンネル・フィーチャーを使用するためには、IP 転送機能が使用可能になっていることが必要です。

トンネルは 1 つだけ追加できます。他の LAN ポートに使われていない *Port Number* を指定することが必要です。ブリッジング・トンネルにポート番号を割り当てた後は、ポート番号をパラメーターとして必要とする他のすべてのブリッジング・コマンドを、トンネル特性の構成のために使用できるようになります。エンドポイントの IP アドレスなど、トンネル特定の構成には **tunnel** コマンドを使用します (117ページの『Tunnel』を参照してください)。

デフォルトでは、このポートでは透過ブリッジングが使用可能になりますが、 **Enable Source-Routing** オプションを使用すれば、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
そのブリッジで使用されていない固有なポート番号

BAN

ban コマンドは、境界アクセス・ノード (BAN) 構成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 BAN 構成プロンプト (BAN config>) で入力します。個々のコマンドについては、117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、ブリッジング構成のソース・ルーティング・ブリッジとセグメント番号を変更します。

構文:

change bridge . . .

segment . . .

bridge *new-bridge#*
ブリッジング構成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以下の情報を削除するのに使用します。

- 固定データベースのステーション・アドレス・エントリー
- 指定されたプロトコルの特定アドレス・マッピング
- LAN/WAN ポート
- プロトコル・タイプに基づいてパケットを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・フィーチャーの場合、**delete port** コマンドでそのトンネルに対応するポート番号を指定すると、IP インターネットワークを経由するブリッジ間のトンネルが削除されます。

構文:

delete address

dmac-addr

mapping . . .

port . . .

prot-filter . . .

address *addr-value*
固定データベースからアドレス・エントリーを削除します。このアドレスは、指定するエントリーの MAC アドレスです。削除するエントリーの addr-value (12 桁の 16 進フォーマット) を入力して **Return** を押します。予

約済みのマルチキャスト・アドレスは削除できません。存在しないアドレス・エントリーを削除しようとすると、次のような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'

デフォルト値: なし

例: delete address

dmac-addr *addr-value*

重複 MAC アドレス・エントリーをデータベースから削除します。*addr-value* は、削除するエントリーの MAC アドレスです。

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

デフォルト値: 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*

指定のプロトコルの特定アドレス・マッピングを削除します。

dlh-type

(data-link-header type) は、DSAP、Ether-type、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) プロトコル・タイプは 1 ～ FE (16 進値) の範囲で入力します。

有効値: X'1' ～ X'FE'

一般的な値は、次のとおりです。

プロトコル - SAP (16 進値)

デフォルト値: 1

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

有効値: X'5DD' ～ X'FFFF'

デフォルト値: 1

サブネットワーク・アクセス・プロトコル (SNAP) プロトコル・タイプは 10 桁の 16 進フォーマットで入力します。

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

一般的な値は、次のとおりです。

デフォルト値: 00 0000 0800

ga-address

6 バイト (12 桁の 16 進値) 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'

デフォルト値: 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。**enable bridge** コマンドは、デフォルトではすべての LAN 装置がブリッジングに参加するように構成するので、ユーザーはこのコマンドを用いて、ブリッジングに参加する装置としない装置をカスタマイズすることができます。ポート番号の値は、通常はインターフェース番号より 1 だけ大きい値です。

このコマンドの後に IP tunnel port# を付けると、IP トンネルがブリッジング構成から除去されます。

例: delete port 2

prot-filter snap ether dsap

以前に指定した、フィルターに使用されるプロトコル識別子を削除します。フィルターの削除は、全ポートまたは選択されたポートを対象にして行うことができます。これらのフィルターには、以下のものが含まれます。

SNAP パケット

プロトコル・タイプを 10 桁の 16 進フォーマットで入力する、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・タイプを 5DD ～ FFFF (16 進値) の範囲で入力する、イーサネット・タイプ

DSAP パケット

プロトコル・タイプを 0 ～ FE (16 進値) の範囲で入力する、あて先サービス・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可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ピング
- スパンニング・ツリー探索フレームの伝送
- 指定されたポートのソース・ルーティング
- SR-TB 変換
- 指定されたポートの透過 (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 ロード・バランシング
- DLSw

トンネル・フィーチャーの場合、disable コマンドは IP インターネットワークを介したエンド・ステーション間のトンネルを使用不可にします。

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完全に使用不可にします。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は削除しません。

例: disable bridge

dls ブリッジ上の DLSw の動作を使用不可にします。(DLSw を稼働するルーターは、エンド・ステーションからは 1 つのブリッジとして見えます。) 詳細については、479ページの『第24章 DLSw の使用』を参照してください。

例: disable dls

duplicate *frame-type*

混合ブリッジング環境に存在する重複フレームの作成を使用不可にします。802.5 インターフェース (ソース・ルーティングおよび透過ブリッジングが使用可能) で SR-TB ブリッジング機能が使用可能にされている場合、フレームを不定の (または、マルチキャスト) あて先にブリッジングするときに矛盾が発生します。ブリッジには、あて先がソース・ルーティング (専用) ドメインに存在するのか、透過ブリッジング・ドメインに存在するのかが分かりません。

この状態に対処するために、ブリッジはこれらのフレームを重複して送信します (デフォルトで)。一方のフレームにはソース・ルーティング・フィールド (スパンニング・ツリー探索 RIF) が存在し、他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 が存在しません)。**disable duplicate** コマンドは、これらのフレーム・タイプの一方の作成を禁止することにより、この重複をなくします。**disable duplicate** コマンドは、両方のタイプのフレームを同時に使用不可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、ブリッジがソース・ルーティング環境用に作成したスパンニング・ツリー探索フレームを送信するのを禁止します。コマンドの後に **TSF** を入力すると、ブリッジが透過ブリッジング環境用の透過スパン・フレームを送信するのを禁止します。いずれの場合も、通常は両方のタイプのフレームが送信される状況です。インターフェースの透過ブリッジングを使用不可にすると、透過フレームの作成も使用不可にされます。

例: disable duplicate TSF

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

dmac-addr

重複 MAC アドレス機能を使用不可にします。

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・フィーチャーの重複 MAC ロード・バランシングを使用不可にします。

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 フレームをイーサネット・タイプ 2 フォーマット (OS/2 EE を稼働する IBM RT によって使用される) に変換するのを使用不可にします。

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 (および、その逆へ) のマッピングを使用不可にします。ある種の状況下では、グループ・アドレスと機能アドレス間のマッピングをグローバルに使用不可にしたい場合があります。

例: disable fa-ga-mapping

ibm8209_spanning_tree

ブリッジが IBM 8209 ブリッジを使用するスパンニング・ツリー・プロトコルに参加しないようにします。

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、ポートがスパンニン

グ・ツリー探索フレームを伝送するのを禁止します。このコマンドは、その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のみ使用されます。この状況は透過スパンニング・ツリーによって自動的に分かります。

例: disable spanning-tree-explorer 2

source-routing *port#*
指定されたポートのソース・ルーティングを使用不可にします。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るのに使用します。

例: disable source-routing 2

sr-tb-conversion
ソース・ルート・フレームを透過フレームに (および、その逆に) 変換することを使用不可にします。

例: disable sr-tb-conversion

stp ブリッジのスパンニング・ツリー・プロトコルを使用不可にします。デフォルトは使用可能です。

例: disable stp

transparent *port#*
指定されたポートの透過ブリッジング機能を使用不可にします。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より望ましい場合に便利です。

注: このコマンドは、正しく使用しないと不合理な構成が生じてしまう可能性があります。たとえば、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のブリッジング機能を使用不可にしてしまいます。このコマンドは SRB および SR-TB ブリッジ機能を実行するために使用します。

例: disable transparent 2

tree *port#*
ブリッジの STP への参加をポート単位で使用不可にします。

例: disable tree 1

注: 並列ブリッジが存在するので、ポート単位で STP を使用不可にすると、ネットワーク・ループが生じる可能性があります。

ub-encapsulation
XNS フレームの Ungermann-Bass OUI カプセル化を使用不可にします。XNS フレームは、 OUI をオール 0 にした 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

enable コマンドは、以下のブリッジング機能を使用可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ピング
- スパンニング・ツリー探索フレームの伝送
- 指定されたポートのソース・ルーティング
- SR-TB 変換
- 指定されたポートの透過 (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 ロード・バランシング
- DLSw

IP トンネル機能の場合、**enable** コマンドは IP 相互接続ネットワークを介したエンド・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

bridge

ブリッジング・ルーターに構成されているすべての 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。各インターフェースにポート番号が、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。たとえば、インターフェース 0 が LAN 装置の場合、そのポート番号は 1 になります。

例: `enable bridge`

dls ブリッジ上の DLSw の動作を使用可能にします。DLSw を稼働する装置は、エンド・ステーションからは 1 つのブリッジとして見えます。詳細については、479ページの『第24章 DLSw の使用』を参照してください。

例: `enable dls`

duplicate *frame-type*

重複 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・ツリー) の生成を使用可能にします。このコマンドは、**disable duplicate** コマンドをオフセットするのに使用できます。デフォルトでは、重複フレームが生成されます。**enable duplicate** コマンドの後にフレーム・タイプ **TSF** または **STE** を指定すると、フレーム・タイプの 1 つを特定して使用可能にすることができます。あるいは、フレーム・タイプ **BOTH** を指定すると、このパラメーターでフレーム・タイプを指定しなかった場合と同じ結果になります。

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可能にします。重複 MAC アドレス・フィーチャーについての追加情報 は、57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。

例 (ロード・バランシングあり):

```
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 (ロード・バランシングなし):

```
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・フィーチャーの重複 MAC ロード・バランシングを使

用可能にします。重複 MAC ロード・バランシングについての説明 は、57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。

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

SNA フレームをイーサネット・タイプ 2 (OS/2 EE を稼働する IBM PC RT で使用) に変換するのを使用可能にします。この結果、SNA フレームはイーサネット上の不定ホストへの 802.3/802.2 および IBM-RT フォーマット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 (および、その逆へ) のマッピングを使用可能にします。このマッピングは、トークンリングと他の媒体 (シリアル・ラインを除く) の間でフレームを転送するときに行われます。機能アドレスはローカルに割り当てられるグループ・アドレスですが、トークンリング・ドメインでは、ハードウェアに制約があるために、機能アドレスが使用されるのが一般的です。他の媒体では、グループ・アドレスが広く使用されます。通常の状況下では、グループ・アドレスと機能アドレス間のマッピングは不可避です。

マッピング・アドレスが追加されている場合、デフォルトではマッピングは使用可能です。マッピングの使用可能/使用不可は、追加されたマップ・レコードを削除するときの選択肢になります。

例: enable fa-ga-mapping

ibm8209_spanning_tree

ブリッジが IBM 8209 ブリッジを使用するスパンニング・ツリー・プロトコルに参加できるようにします。

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、ポートがスパンニング・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、トークンリングおよび WAN ポートに対してのみ有効です。ポートにソース・ルーティングが構成されている場合、デフォルトではこのフィーチャーは使用可能になります。

例: `enable spanning-tree-explorer 2`

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

指定されたポートのソース・ルーティングを使用可能にします。このコマンドは通常、ブリッジ側でソース・ルーティングが必要な場合に使用されます。ソース・ルーティング機能のみを必要とする場合は、そのインターフェースの透過ブリッジングを使用不可にすることが必要です。このコマンドを最初に使用するときは、必ずブリッジ番号を入力することが必要です。それ以降は、入力する必要はありません。

port# ブリッジ構成に参加している有効なポート

有効値: X'0' ～ X'FFF'

デフォルト値: 1

segment#

媒体が接続されている LAN/WAN を表す 12 ビットの数値。この LAN/WAN に接続されている他のブリッジ上のすべての媒体の構成で、これと同じ値を使用する必要があります。ソース・ルーティング機能が正しく動作するためには、この LAN/WAN に接続されているすべてのブリッジが同一の LAN/WAN 識別値を使用することが非常に重要です。

bridge#

同じ LAN/WAN に接続されているすべてのブリッジ間で固有な 4 ビット値。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場合、この値は必須です。それ以降のインターフェースでは、この入力は任意選択です。bridge# はそのセグメントで固有な値を使用するようにしてください。

有効値: X'0' ～ X'F'

デフォルト値: 1

注: 構成時に、すでに 2 つのセグメントが構成済み (つまり、1:N SRB 構成) の状況のときは、追加の *virtual-segment#* パラメーターを入力するように求められます。

例: `enable source-routing 2 1 1`

sr-tb-conversion

このオプションは、ソース・ルーティングから透過ブリッジングへ (および、その逆へ) のフレーム・フォーマットの変換を使用可能にします。これにより、ソース・ルーティング・ドメインと透過ブリッジング・ドメイン間の整合性を保つことができます。このフィーチャーが使用可能のとき、ブリッジはソース・ルート・フレームの RIF フィールドを除去し、透過フレームに変換することによって、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、受け渡すソース・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 から入手します。この RIF 情報を使用して、透過フレームをソース・ルート・フレームに変換します。ステーションの RIF を入手できない場合、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。

変換機能が正しく動作するためには、透過ブリッジング・ドメインにセグメント番号を割り当てる必要があります。このドメインに接続されたすべての SR-TB ブリッジも、これと同じセグメント番号を用いて構成することが必要です。

TB ドメインのセグメント番号の有効値: X'1' ～ X'FFF'

TB ドメインのセグメント番号のデフォルト値: 1

最大伝送単位 (MTU) は、指定の物理ネットワークを通って転送することができる、データ・フレーム当たりのオクテット数です。IP データグラムが、あるホストから別のホストに移動するときには、異なる物理ネットワークを通る可能性があります。一部の物理ネットワークにこの MTU が設定されており、長い IP データグラムは物理フレームに入らないことがあります。物理ネットワークが扱える長さより長いフレームを転送しようとすると、フレームは分割されます。

TB ドメイン MTU の有効値: 576 ～ 18000 バイト

TB ドメイン MTU のデフォルト値: 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 ブリッジのスパンニング・ツリー・プロトコルを使用可能にします。これがデフォルトです。

例: enable stp

transparent *port#*

指定されたポートの透過ブリッジング機能を使用可能にします。通常の状況下では、このコマンドは必要ありません。

例: enable transparent

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

tree *port#*

ブリッジの STP への参加をポート単位で使用可能にします。

例: enable tree 1

ub-encapsulation

SNAP ヘッダー内の Ungermann-Bass OUI を使用して、イーサネット・タイプ 2 フレームをトークンリング・フレームに変換します。UB OUI ヘッダーを入れたトークンリング・フレームは、802.3/802.2 フレームとしてではなく、タイプ 0x0600 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

list コマンドは、ブリッジ構成全体に関する情報を表示するか、あるいは選択された構成パラメーターに関する情報を表示するのに使用します。

構文:

list address
bridge
dmac
filtering . . .
mapping . . .
multiaccess
permanent . . .
port . . .
prot-filter . . .
protocol
range . . .

address *addr value*

固定データベースからアドレス・エントリーを読み取ります。addr 値は、読み取るエントリーの MAC アドレスです。これには、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を使用することができます。固定データベースは、電源オン/オフ・プロセスによって破棄されることはなく、エージング設定も適用されません。固定エントリーは、動的エントリーによって置き換えることはできません。

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

デフォルト値: 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 進フォーマットのアドレス・エントリー

Entry Type

Permanent

このエントリーは固定的であり、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

このエントリーは、IEEE 802.1d 委員会によって将来の利用のために確保されていることを示します。予約済みアドレスあてのフレームは廃棄されます。

Registered
このエントリーはそのブリッジ自体のもの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ている場合に、エントリー・タイプの後に表示されます。

Input Port
そのアドレス・エントリーに関連付けられている着信ポートの数を表示します。

Output Port
そのアドレス・エントリーに関連付けられている発信ポートの数を表示します。『NONE/DAF』 という表示は、そのアドレス・エントリーに関連付け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
ブリッジの現在の状態を示します。値は ENABLED または DISABLED です。

Bridge Behavior
そのブリッジで使用されているブリッジ方式を示します。値は、透過の STB、ソース・ルーティングの SRB、およびソース・ルーティング透過変換ブリッジングの ADAPTIVE SRT です。

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

Bridge priority
ブリッジ識別子の高位 2 オクテットのブリッジ・アドレスで、最低番号のポートから入手した MAC アドレスか、Set Bridge コマンドによって設定されたアドレスのいずれかです。

Source Routing Bridge Number
ブリッジを識別する固有な番号。同一の 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
ソース・ルーティング・ブリッジングに関連した指定インターフェースのブリッジから転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であるか使用不可であるかを示します。

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
透過ブリッジが送受信できる最大フレーム・サイズ (最大転送単位) を指定します。

1:N Source Routing
1:N ソース・ルーティングの現在の状態が ACTIVE であるか NOT ACTIVE 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
このブリッジのソース・ルーティングが使用可能の場合、最大フレーム (LF) ビット符号化の解釈法を示します。これは BASIC または EXTENDED として表示されます。

FA-GA conversion
FA-GA 変換が使用可能であるか使用不可であるかを示します。

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

DLS for the bridge
このブリッジでデータ・リンク交換プロトコルが使用可能であるか使用不可であるかを示します。

Number of ports added
ブリッジング構成に追加されたブリッジ・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
ブリッジを通してネットワーク・セグメントに接続されている装置を示します。ブリッジングに参加するためには、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。インターフェース番号 255 は、ブリッジング用に使用されます。

Port Behavior
そのポートで使用されているブリッジング方式を示します。透過ブリッジングの場合は STB で、ソース・ルート・ブリッジングの場合は SRB です。

VPI ATM ポートに関連する VPI を指定します。

VCI ATM ポートに関連する VCI を指定します。

dmac 重複 MAC アドレス機能の構成済み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 コマンドでは、以下の一般的なデータ・グループを表示することができます。

All すべてのフィルター・データベース・エントリーを表示します。

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・エントリーを表示します。

SAP SAP プロトコルのフィルター・データベース・エントリーを表示します。

SNAP SNAP プロトコル識別子のフィルター・データベース・エントリーを表示します。

list filtering 表示オプションのそれぞれの例を、以下に示します。

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
```

パケットの伝達方法を説明するのに使用される記述子は、次のとおりです。

Routed
転送のためにルーティング転送機能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プロトコル・フィルターによって管理的にフィルターに掛けら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機能ではないプロトコル・エンティティーが存在するプロトコル識別子を記述します。その一例は、リンク・レベル・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、登録されたアドレスに送信された場合、ブリッジされるか、ローカルに処理されます。登録されたマルチキャスト・アドレス宛てのマルチキャスト・パケットは、転送されて、ローカルに処理されます。

これらの記述子はすべて、この Ethertype をもつ 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*
指定されたプロトコルの特定アドレス・マッピングをリストします。

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 を選択します。

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) プロトコル・タイプは 1 ～ FE (16 進値) の範囲で入力します。
- イーサネット (Ether) プロトコル・タイプは 5DD ～ FFFF (16 進値) 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) プロトコル・タイプは 10 桁の 16 進フォーマットで入力します。

multiaccess
マルチアクセス・データベース内のエントリーのエージング・タイムを表示

し、マルチアクセス・ブリッジ・ポートを表示します。ブリッジ・ポート・パラメーターの説明については、**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

ブリッジの固定データベース内のエントリーの数を表示します。

例: `list permanent`

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

port *port#*

すでに構成された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。番号を指定しないと、すべてのポートが選択されます。

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:  Ox116     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:  Ox117     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 ID は、ポート優先順位とポート番号の 2 つの部分から構成されます。この例では、128 が優先順位で、1、2、および 3 がポート番号です。16 進フォーマットで表示され、低位バイトはポート番号を示し、高位バイトは優先順位を示します。

Port state 指定されたポートの現在の状態を表示します。これは ENABLED または DISABLED 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 (たとえば、透過ブリッジング、ソース・ルート・ブリッジング) を表示します。

SRB SRB が使用可能のときにのみ表示され、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 進値)、最大転送単位のサイズ、およびスパンニング・ツリー探索フレームの転送が使用可能であるか使用不可であるかが含まれます。

Duplicate Frames Allowed
許容される重複フレームのタイプの明細と数を表示します。

Assoc interface
表示されたポートに関連付けられているインターフェース番号を表示します。また、VPI/VCI またはあて先 ATM アドレス (ポートが ATM インターフェース上に存在する場合) も表示します。

Path Cost 可能なルート・パス・コストの計算に使用される、ポートに関連したコスト。範囲は 1 ～ 65535 です。

prot-filter *port#*

フィルター・プロトコル・タイプの現行リストを読み取ります。フィルターは、ポート別にリストすることも、全ポートを一度に表示することもできます。Port# 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 全ポートを表示することを選択した場合、各ポートのポート番号が表示されます。

Protocol Class プロトコル・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 進フォーマットで表示します。

Protocol State 選択されたポートのプロトコルはフィルターに掛けられることを示します。

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

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: これらのブリッジ関連の各パラメーターについては、前章でも詳しく説明しています。

Bridge Identifier

ASCII フォーマットの 8 バイト値。この情報を表示する前にブリッジ・アドレスを設定しなかった場合、低位 6 バイトは 0 として表示され、ポートのデフォルト 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 (根) ブリッジとして選択されている場合、このブリッジによってブリッジ最大エージおよびブリッジ・ハロー・タイムが HELLO BPDU を介してネットワーク上の全ブリッジに転送されます。

Bridge-Max-Age

スパンニング・ツリー・プロトコル関連の情報をタイムアウトにするのに使用する最大エージ (期間)。

Bridge-Hello-Timer

HELLO BPDU の相互間の時間間隔

Bridge-Forward-Delay

別の状態に変わる前に使用される時間間隔 (このブリッジがルートになる場合)。

range *start-index stop-index*

固定データベースからアドレス・エントリーの範囲を読み取ります。これを指定するためには、最初に **list permanent** コマンドを使用して、データベースのサイズを調べます。この値から、エントリー範囲の 『スタート・インデックス』 値を決めることができます。スタート・インデックスは、1 からデータベースのサイズまでの範囲です。次に、限定された数のエントリーを表示するために 『ストップ・インデックス』 を選択することができます。この入力は任意選択です。ストップ・インデックスを指定しない場合、デフォルト値はデータベースのサイズです。

アドレス・エントリーには、以下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

そのエントリーの 6 バイト MAC アドレス

Type of Entry

次のタイプの 1 つを指定します。

- Reserved (予約済み) - エントリーは IEEE 802.1d 委員会によって将来の利用のために確保されています。
- Registered (登録済み) - エントリーは、ボックスに接続された専有の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機能によって使用可能にされたマルチキャスト・アドレスから構成されます。
- Permanent (固定) - 構成プロセスでユーザーによって入力されたエントリーで、電源オン/オフまたはシステム・リセットの後も存続します。
- Static (静的) - 監視プロセスでユーザーによって入力されたエントリーで、電源オン/オフまたはシステム・リセットの後は存続せず、エージを持っていません。
- Dynamic (動的) - ブリッジによって 『動的』 に 『確認』 された (learned) エントリーで、電源オン/オフまたはシステム・リセットの後は存続せず、エントリーに関連付けられた 『エージ』 を持っています。
- Free (空き) - 自由にアドレス・エントリーを記入できるデータベース内の場所。

Port Map

すべての着信ポート用の発信ポート・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** と入力すると、NetBIOS 構成プロンプトが表示されます。個々の NetBIOS 構成コマンドについては、168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・フィーチャーを購入していない場合、 このコマンドを使用すると、次のようなメッセージを受け取ります。

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

Set

set コマンドは、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のに使用します。これには、以下のものが含まれます。

- フィルター・データベースの動的アドレス・エントリーのエージング・タイム
- 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) ビット符号化の解釈
- MAC サービス・データ単位 (MSDU) サイズ
- スパンニング・ツリー・プロトコルのブリッジおよびポート・パラメーター
- ルート記述子 (RD) 限界
- ブリッジ・フィルター・データベースのサイズ
- 重複 MAC アドレスに関連した RIF のエージング・タイム
- マルチアクセス・データベース内のエントリーのエージング・タイム

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*

そのエントリーをもつポートが転送状態にあるとき、フィルター・データベースから動的エントリーをエージングによって除去するための時間を設定します。SR-TB ブリッジ・パーソナリティー (ネットワーク構成情報) の場合、このエージは RIF テーブル内の RIF エントリーのエージングにも使用されます。

各プロンプトの後に必要な値を入力して **Return** を押します。

エージング・タイムの有効値: 10 ～ 1000000

エージング・タイムのデフォルト値: 30

レゾリューション値は、エージング・タイマーによって設定されたエージ限界を超えたかどうかを調べるために、フィルター・データベース内の動的エントリーをスキャンする頻度を指定します。

レゾリューションの有効値: 1 ～ 60 秒

レゾリューションのデフォルト値: 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、ブリッジ識別子の低位 6 オクテットのブリッジ・アドレスです。デフォルトでは、bridge-addr-value は、初期化時の最低番号の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、デフォルトのアドレスをオーバーライドし、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: スパンニング・ツリー・プロトコルが正しく動作するためには、ネットワーク内の各ブリッジが固有のアドレスを持っていることが必要です。

重要: シリアル・ライン・インターフェース (または、トンネル) が最低番号のポートである場合は、必ずこのコマンドを使用して、ブリッジがリスタート時に固有のアドレスを持つようにすることが必要です。シリアル・ラインは独自の MAC アドレスを持っていないので、このプロセスが必要になります。

プロンプトで、ブリッジ・アドレスを 12 桁の 16 進フォーマットで入力して **Return** を押します。

間違ったフォーマットでアドレスを入力すると、メッセージ `Illegal Address` を受け取ります。プロンプトでアドレスを入力しないと、メッセージ `Zero length address supplied` を受け取り、ブリッジは前の値を維持します。ブリッジ・アドレスをデフォルト値に戻すには、オール 0 のアドレスを入力します。

有効値: 12 桁の 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を使用しないでください。スパンニング・ツリー・プロトコルが正しく動作するためには、ネットワーク内の各ブリッジが固有のアドレスを持っていることが必要です。

デフォルト値: 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 エントリーをエージングにより除去する時間を設定します。この値は、確認された重複 MAC アドレスに対してのみ適用されます。その他のすべてのアドレスの場合、エージングには **set age** コマンドで指定した値が使用されます。

各プロンプトの後に必要な値を入力して **Return** を押します。

DMAC エージング・タイムの有効値: 10 ～ 1000000

DMAC エージング・タイムのデフォルト値: 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・データベースに保持できるエントリーの数を設定します。

デフォルト値: 1024 にブリッジ・ポート数を掛けた値

list filtering コマンドの詳細については、105 ページを参照してください。

例: set filtering

```
database-size [2048]?
```

lf-bit-interpretation *encode-mode*

このブリッジのソース・ルーティングが使用可能の場合、最大フレーム (LF) ビット符号化の解釈を設定します。

例: set lf-bit-interpretation basic

Encode-mode

basic または **extended** のいずれかを入力します。基本 (basic) モードでは、ルーティング制御フィールドの 3 ビットしか使用できません。これが既存のソース・ルーティング・ブリッジの一般的な方法です。拡張 (extended) モードでは、ルーティング制御フィールドの 6 ビットを使用して、ブリッジがサポートする最大データ単位を表すことができます。デフォルト値は **extended** です。拡張ノードと基本ノードには整合性があります。

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、ポートの最大 MAC サービス・データ単位 (MSDU) のサイズを設定します。MSDU 値の設定は、従来の透過媒体に対しては意味を持ちません。ルーターに構成されているパケット・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ていない場合、使用されるデフォルト値は、そのインターフェースのパケット・サイズとして構成されているサイズです。

有効値: 16 ～ 65535 の範囲の整数を指定します。

デフォルト値: ポートに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・データベース内のエントリーをエージングにより除去する時間を設定します。データベースは、**set age** コマンドの *resolution* パラメーターによって設定される速度でスキャンされます。

有効値: 1 ～ 1 000 000

デフォルト値: 300

例: set multiaccess-age

```
seconds [300]? 500
```

port *block* **or** *disable*

ポートのスパンニング・ツリー・プロトコルへの参加を開始します。これは、状態表示値 『block』 を入力することによって行います。これにより、スタート時にポートは 『blocked』 状態に入ります。ポートの実際の状態は、後にトポロジーを決めるスパンニング・ツリー・プロトコルによって決められます。状態表示値 『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外されます。

例: set port block

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

protocol *bridge* **or** *port*

新規構成のためにスパンニング・ツリー・プロトコルのブリッジまたはポートを変更するか、または特定のトポロジーに適合するように構成パラメーターを調整します。

ブリッジ・パラメーターを変更する場合は、オプションとして 『bridge』 を入力します。このコマンドで変更できるブリッジ関連のパラメーターについては、以下で説明します。

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場合は、**srb** または **tb** を指定します。

これらの値を設定する際には、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。そうでないと、入力はリジェクトされます。

2 X (ブリッジ転送遅延 - 1 秒) ≥ ブリッジ最大エージ
ブリッジ最大エージ ≥ 2 X (ブリッジ・ハロー・タイム + 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・プロトコル関連の情報をタイムアウトにするのに使用する最大エージ (期間)。

このブリッジング・ルーターがスパンニング・ツリーのルート (根) ブリッジとして選択された場合、このパラメーター値は、他のアクティブ・ブリッジがそれぞれ受信した構成ブリッジ・プロトコル・データ単位 (BPDU) を保管する期間を指定します。BPDU が、置き換えられずにその最大エージ限界に達した場合、ネットワーク上のアクティブ・ブリッジはそれを廃棄し、ルート・ブリッジに障害が起こったものと想定します。その場合は、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、ブリッジ・ハロー・タイム・パラメーターの設定によって影響を受けることがあります。また、このパラメーターの設定は、ブリッジ転送遅延パラメーターの設定に影響を与えることがあります。

有効値: 6 ～ 40 秒

デフォルト値: 20 秒

Bridge Hello Timer
HELLO BPDU の相互間の時間間隔

このブリッジング・ルーターがスパンニング・ツリーのルート・ブリッジとして選択された場合、このパラメーターは、このブリッジが構成ブリッジ・プロトコル・データ単位 (BPDU) を転送する頻度を指定します。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入っており、トポロジーの変更を反映します。

依存関係

このパラメーターの設定は、最大エージ・パラメーターの設定に影響を与えることがあります。

有効値: 1 ～ 10 秒

デフォルト値: 2 秒

Bridge Forward Delay
別の状態に変わる前に使用される時間間隔 (このブリッジがルートになる場合)。

このブリッジング・ルーターがスパンニング・ツリーのルート・ブリッジとして選択された場合、このパラメーターは、すべてのブリッジのアクティブ・ポートが*待機状態 (listening state)* のままでいる時間の長さを指定します。転送遅延時間が満了すると、待機状態のポートは *転送状態 (forwarding state)* に移行します。状態の変更は、スパンニング・ツリーのトポロジーの変更 (たとえば、アクティブ・ブリッジに障害が起こったり、遮断されるなど) の結果として起こります。

ルート・ブリッジは、この値をすべてのブリッジに伝えます。この処理により、すべてのブリッジの変更に一貫性が保たれます。

依存関係

このパラメーターの設定は、SRB ブリッジ最大エージ・パラメーターの設定によって影響を受けることがあります。

有効値: 4 ～ 30 秒

デフォルト値: 15

Bridge Priority
ブリッジ識別子の高位 2 オクテットのブリッジ・アドレス - 最低番号のポートから入手した 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です。

ブリッジ優先順位は、このブリッジがスパンニング・ツリーのルート・ブリッジになる確率を示します。ブリッジ優先順位パラメータ

ーの数値が低いほど、ブリッジの優先順位は高くなり、そのブリッジが選択される確率が高くなります。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最低の数値を持つブリッジを、ルート・ブリッジとして選択します。

有効値: 0 ～ 65535

デフォルト値: 32768

スパンニング・ツリー・プロトコルのポート・パラメーターを変更する場合は、オプションとして **port** を入力します。各プロンプトで必要な値を入力し **Return** を押します。

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・ポート番号。パス・コストおよびポート優先順位を変更するポートを選択します。

Path Cost

そのポートに関連付けられているコスト。可能なルート・パス・コストを計算するのに使用されます。

各ポート・インターフェースには、パス・コストが関連付けられています。これは、そのポートを使用してブリッジ・ネットワーク内のルート・ブリッジに到達するための相対的な値を示します。スパンニング・ツリー・アルゴリズムは、パス・コストを使用して、ルート・ブリッジからネットワーク・トポロジー内の他のすべてのブリッジへのコストが最小になるパスを計算します。

このパラメーターは、このブリッジング・ルーターがルート・ブリッジになった場合、このポート・インターフェースを介してフレームを渡すことに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・ルートを決める際に、この値をファクターとして適用します。値 0 は、ブリッジング・ルーターが独自の公式を使用して自動的にこのポートのパス・コストを計算することを示します。

有効値: 1 ～ 65535

デフォルト値: 0 (コストは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順位を識別します。これは、スパンニング・ツリー・アルゴリズムによって、ポートの選択 (どのポートがルート・ブリッジへの最低コストのパスを提供するか) およびブロッキングを決めるための比較に使用されます。

有効値: 0 ～ 255

デフォルト値: 128

route-descriptor-limit *limit-type*

ソース・ルーティングが使用可能の場合、ブリッジによって転送される全ルート探索 (ARE) またはスパンニング・ツリー探索 (STE) フレームの最大ルート記述子 (RD) 長さを関連付けることができます。

例: `set route-descriptor-limit ARE`

Limit-type

RD-limit-value が適用されるのが全ルート探索 (ARE) フレームであるか、スパンニング・ツリー探索 (STE) フレームであるかに応じて、ARE または STE を入力します。その場合は、RD-limit-value を入力するよう求められます。

RD-limit-value

RD-limit-type 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) に含めることができる 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、そのフレームがそこに到達するまでの間に通過したブリッジの数です。フレームがブリッジを 1 つ通過するごとに、1 つの RD がルーティング情報フィールドに追加されます。したがって、RD の数はホップの数に等しくなります。RD (ホップ) 数がこのパラメーターによって許されるホップ数を超える場合、フレームは廃棄されます。

有効値: 0 ～ 14

デフォルト値: 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。各コマンドの説明は、119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。これらのコマンドを使用して、BAN を ASRT ブリッジングまたは DLSw への追加機能として構成することができます。

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>` または `DLSw config` プロンプトで ban コマンドを入力します。118ページの表5 は、BAN 構成コマンドを示しています。

ASRT BAN 構成コマンド (Talk 6)

表 5. BAN 構成コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、BAN 構成に BAN ポートを追加するのに使用します。コマンドでポート番号を指定しないと、ポート番号の入力を求められます。

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

delete コマンドは、BAN 構成から BAN ポートを削除するのに使用します。コマンドでポート番号を指定しないと、ポート番号の入力を求められます。

構文:

delete *port#*

例: delete 3

List

list コマンドは、すべての BAN ポートに関する情報をリストするのに使用します。表示される情報には、BAN ポート番号、BAN DLCI の MAC アドレス、およびそのポートが扱うフレームはブリッジされるのか、あるいは LLC が DLSw によって終端されるのかが含まれます。

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、Tunnel 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では、IP を介してブリッジング・フレームを転送するトンネルのネットワーク・パラメーターを指定することができます。

トンネルの構成コマンドは TNL 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> プロンプトで **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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	IP を介したブリッジングの IP ユニキャストまたはマルチキャスト・アドレッシング構成に参加しているあて先ブリッジの IP アドレスを追加します。
Delete	IP を介したブリッジングの IP ユニキャストまたはマルチキャスト・アドレッシング構成に参加しているあて先ブリッジの 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 を介したブリッジングの IP ユニキャストまたはマルチキャスト・アドレッシング構成に参加しているエンド・ステーションの IP アドレスを表示します。また、IP トンネルを介してルーティングされるブリッジング・パケットのサイズ (バイト数)、およびマルチキャスト・アドレッシングが使用可能であるか使用不可であるかも表示します。
Set	ルーターのマルチキャスト・トンネル伝送の基底マルチキャスト 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。xxixページの『下位レベル操作環境の終了』 を参照してください。

トンネル伝送とマルチキャスト・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・トンネルのいずれかとして定義することができます。ユニキャスト・トンネルを定義するには、**add** コマンドを使用して、トンネルのエンドポイントの IP アドレスを構成します。マルチキャスト・トンネルを定義するには、**set** および **join** コマンドを使用します。マルチキャスト・パケットが含まれてい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) を使用できるネットワーク・セグメント上に存在することが必要です。

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ていません。 このことは、ルーター上でマルチキャスト・トンネル (たとえば、MOSPF トンネル) を定義するときには、以下の条件の 1 つが存在することを確認する必要があることを意味しています。

- 発信元が LAN セグメント・アドレスの 1 つである
- 発信元が内部 IP アドレスである

最初の条件は IP **set router-id** 構成コマンドを使用して確認できます。2 番目の条件は IP **set internal-ip-address** 構成コマンドを使用して確認できます。

すべての環境で、2 番目のオプションが望ましい条件です。最初のオプションは、ネットワーク上の一部のルーターがホスト・アドレスの使用を好まない場合 (これは、混合ベンダー・ネットワークで起こることがあります) にのみ使用すべきです。

Add

add コマンドは、ユニキャスト IP アドレッシング構成に参加しているエンド・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・アドレッシングの場合、トンネル伝送構成であて先ブリッジの IP アドレスを提供する必要があります。ルーター・ソフトウェアは、このレコードを使用して、ソース・ルート・フレーム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、対応するあて先ブリッジの IP アドレスに変換します。透過ブリッジング・フレームの場合は、これはトンネルの反対側のエンドポイントを識別します。

構文: add

address *IP-address*

有効値: 有効な IP アドレス

デフォルト値: 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 IP アドレッシング構成に参加しているブリッジの 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

デフォルト値: 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設定するのに使用します。トンネル・グループは、3 つのタイプ (ピア、クライアント、またはサーバー) のいずれかです。トンネル・グループは、整数タグによって定義されます。ブリッジは、各タグの 1 つのグループにのみ属することができます。たとえば、ブリッジはピアグループ *1* とサーバー・グループ *1* の両方に所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*
指定されたグループ番号のクライアント・グループに結合します。

有効値: 0 ～ 64

デフォルト値: 0

例: `join client-group 3`

peer-group *group-number*
指定されたグループ番号のピア・グループに結合します。

有効値: 0 ～ 64

デフォルト値: 0

例: `join peer-group 5`

server-group *group-number*
指定されたグループ番号のサーバー・グループに結合します。

有効値: 0 ～ 64

デフォルト値: 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・グループ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*
指定されたグループ番号のサーバー・グループから除去します。

有効値: 0 ～ 64

デフォルト値: 0

例: `leave server-group 7`

client-group *group-number*
指定されたグループ番号のクライアント・グループから除去します。

有効値: 0 ～ 64

デフォルト値: 0

例: `leave client-group 3`

peer-group *group-number*
指定されたグループ番号のピア・グループから除去します。

有効値: 0 ～ 64

デフォルト値: 0

例: `leave peer-group 5`

List

list トンネル・コマンドは、IP を介したトンネル伝送の IP ユニキャストまたはマルチキャスト・アドレッシング構成に参加しているブリッジの IP アドレスを表示するのに使用します。また、このコマンドを使用して、トンネルを通して送信される IP パケットのサイズ、および IP が使用可能であるか使用不可であるかも表示できます。

構文:

list address
all

address
IP を介したトンネル伝送の IP ユニキャストまたはマルチキャスト・アドレッシング構成に参加しているブリッジの 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 すべてのユニキャスト 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、ルーターの基底マルチキャスト・アドレスを設定するのに使用します。

IP マルチキャスト・アドレッシングの場合、トンネル伝送構成では、トンネル伝送用に予約されている IP マルチキャスト・アドレスのみが必要です。カプセル化では、3 つのグループの IP マルチキャスト・アドレスが使用されます。最初のグループは全ルート探索 (ARE) フレームの送信用、2 番目のグループはスパンニング・ツリー探索 (STE) フレームの送信用、そして 3 番目のグループは特別ルート・フレーム (SRF) 用です。

構文:

set base-multicast-address

base-multicast-address
マルチキャスト・トンネル伝送の基底マルチキャスト IP アドレスを設定します。

有効値: 最後の 2 バイトが 0 に設定された任意の有効なクラス D IP アドレス

デフォルト値: 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たブリッジングを使用可能にするためには、DLCI 番号 (回線番号とも呼ばれます) とブリッジ・ポートを関連付けることが必要です。これを、フレーム・リレー・ポイント・ポイント・ブリッジ・ポートといいます。フレーム・リレー・インターフェース自身と関連付けられたYou 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。詳細については、59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・ポートを構成した後は、プロトコル・フィルターやアドレス・フィルターを含めて、そのブリッジ・ポートに関連したすべての機能が利用可能になります。

各フレーム・リレー・ポイント・ポイント・ブリッジについて、PVC または 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、関連付けられた DLCI 番号を指定する必要があります。SVC サポートについては、SVC 回線名を提供する必要があります。

ASRT config> プロンプトで、以下のコマンドを使用して、フレーム・リレー・サーキット用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# サーキットに関連付けられている固有のブリッジ特定番号

有効範囲: 1 ～ 254

デフォルト値: なし

Use PVC? 使用しない場合は、SVC が追加されます。

有効値: Yes または No

デフォルト値: No

circuit# ブリッジングが使用可能にされている PVC の DLCI 番号。

circuit-name ブリッジングが使用可能にされている SVC のサーキット名。

このコマンドは、ポート番号を *circuit number* で識別されたフレーム・リレー PVC と関連付け、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。

ASRT 監視環境へのアクセス

ASRT 監視環境にアクセスするには、+ (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。これらのコマンドを使用して、アクティブな監視からパラメーターを表示および変更することができます。監視コマンドを使って変更した情報は、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。

これらのコマンドでは、ブリッジ・メモリー内の構成情報を失うことなく、一時的に構成を変更することができます。すべての ASRT 監視コマンド用として ASRT> プロンプトが表示されます。

NetBIOS の監視コマンドは NetBIOS> 監視プロンプトで入力します。NetBIOS プロンプトは、メジャー ASRT コマンドのサブセットであり、本章で後述する ASRT **netbios** コマンドを入力することによりアクセスします。

NetBIOS の監視コマンドは NetBIOS> 監視プロンプトで入力します。NetBIOS フィルター・プロンプトは、メジャー ASRT コマンドのサブセットです。

注: MAC アドレスを入力する必要があるコマンドの場合、アドレスは次のフォーマットで入力することができます。

IEEE 802 標準ビット順序
00-00-00-12-34-56

IEEE 802 標準ビット順序 (速記フォーマット)
000000123456

IBM トークンリング固有のビット順序 (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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	ブリッジング・ルーターの固定データベースに、固定 (静的) アドレス・エントリーを追加します。
BAN	特定の BAN 監視コマンドを入力するための境界アクセス・ノード (BAN) 監視プロンプトにアクセスすることができます。 詳しい説明については、142ページの表8を参照してください。
Cache	指定されたポートのキャッシュ・エントリーを表示します。
Delete	ブリッジング・ルーター・データベースから MAC アドレス・エントリーを削除します。

表 7. ASRT 監視コマンドの要約 (続き)

コマンド	機能
Flip	MAC アドレスを、標準ビット順序から 802.5 (非標準または IBM) ビット順序に反転します。
List	ブリッジ構成全体または選択された構成オプションに関する情報を表示します。
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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、静的アドレス・エントリーおよびあて先アドレス・フィルターを、ブリッジング・ルーターのデータベースに追加するのに使用します。これらのデータベースへの追加は、ルーターをリスタートすると失われます。

構文:

add destination-address-filter

static-entry

destination-address-filter *mac_address*

あて先アドレス・フィルターを、ブリッジング・ルーターの固定データベースに追加します。コマンドの後に、そのエントリーの MAC アドレスを入力します。

例: add destination-address-filter

```
Destination MAC address [00-00-00-00-00-00]?
```

static-entry *mac_address input_port [output_ports]*

静的アドレス・エントリーを、ブリッジング・ルーターの固定データベースに追加します。コマンドの後に、静的エントリーの MAC アドレスと着信ポート番号を入力します (任意選択の発信ポート番号も入力できます)。複数のポート・マップ (着信ポートごとに 1 つ) を持つ静的エントリーを作成する場合は、このコマンドを数回使用します。

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。**ban** コマンドは ASRT> プロンプトから入力します。

構文: ban

例: ASRT>**ban**

```
BAN>
```

BAN 監視プロンプトにアクセスしたら、特定の監視コマンドの入力を開始できます。**exit** コマンドを入力すれば、いつでも ASRT> プロンプトに戻ることができます。

Cache

cache コマンドは、選択されたブリッジング・ポート・ルーティング・キャッシュのコンテンツを表示するのに使用します。ポートがキャッシュを保持していない場合は、メッセージ `Port X does not have a cache` 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
そのエントリーの 6 バイト MAC アドレス

Entry Type
以下のアドレス・エントリー・タイプの 1 つを指定します。

Reserved - IEEE802.1D 標準によって将来の利用のために確保されているエントリー

Registered - エントリーは、ボックスに接続された専有の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機能によって使用可能にされたマルチキャスト・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たエントリーで、電源オン/オフまたはシステム・リセットの後も存続します。

Static - 監視プロセスでユーザーによって入力されたエントリーで、電源オン/オフまたはシステム・リセットの後は存続せず、エージング・タイマーによる影響を受けません。

Dynamic - ブリッジによって 『動的』 に 『確認』 されたエントリーで、電源オン/オフまたはシステム・リセットの後は存続せず、エントリーに関連付けられた 『エージ』 を持っています。

Free - 自由にアドレス・エントリーを記入できるデータベース内の場所

Unknown - ブリッジには確認不能 (不定) のエントリー・タイプ。バグまたはイリーガル・アドレス (あるいは、その両方) の可能性があります。

Age
各動的エントリーのエージ (秒数)。エージは、レゾリューション間隔ごとに減分されます。

port(s)
そのエントリーに関連付けるポート番号を指定し、インターフェース名を表示します (これは常に、キャッシュを保持しているインターフェースの名前になります)。

Delete

delete コマンドは、ルーターの固定データベースからステーション (MAC を含む) アドレス・エントリー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・ビット順序を 『反転』 させることにより、特定の MAC アドレスを標準および非標準フォーマットで表示します。このコマンドは、典型的な非標準フォーマットの IEEE 802.5 アドレスを、ブリッジ・コンソールおよび ELS で一般的に使用されている標準フォーマットに (および、その逆に) 変換するのに便利です。

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・ルーター構成に関する情報を表示する、あるいは選択された構成またはブリッジング・オプションに関する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]*

ブリッジングのタイプ間で変換を行う SR-TB ブリッジに関する一般情報をリストします。**list adaptive** のもとで表示できる一般的なデータ・グループ・オプションには、さまざまなものがあります。これには、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 ブリッジのカウンターを表示します。
- Database - SR-TB ブリッジ RIF データベースのカウンターを表示します。

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 適応ブリッジの現在の状態を示します。この値は、Enabled (使用可能) または Disabled (使用不可) のいずれかとして表示されます。

Translation database size
SR-TB データベースの現在のサイズを表示します。これには、ソース・ルーティング・ドメインの MAC アドレスと関連の RIF が入っています。

Aging time エージング・タイマーの設定値 (秒数) を表示します。このタイムリミットを超過した SR-TB RIF データベース・エントリーはすべて廃棄されます。

Aging granularity
エージング・タイマーに従ってエントリーの満了を調べるためのスキャン頻度を表示します。

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ているソース・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・セグメントおよび (ATM ポートの場合は) VPI/VCI に接続されている装置を識別します。

State 変換ブリッジ・ポートの現在の状態を示します。

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 の開始まで) 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・テーブルの同じ位置に保管 (ハッシュ) されたアドレスの個数を表示します。この数は累積され、ハッシュ衝突

が発生した合計数を反映します。この数が増大する場合は、潜在的なテーブル・サイズ問題があることを示していることがあります。

Adaptive Database Entry
適応ブリッジ・データベースに現在保管されているエントリーの数を表示します。

Adaptive Database Overflow
変換データベース・テーブルのテーブル・スペースが使い尽くされて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* オプションは、表示する適応ブリッジ RIF データベースの特定部分を選択することができます。これはデータベースのサイズに限界があるためです。表示オプションには、次のものがあります。

- Address - 指定された特定の 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・エントリーを表示します。
- Segment - 指定されたセグメント番号のポートに関連したすべての変換ブリッジ・エントリーを表示します。

list adaptive database コマンド・オプションのそれぞれの例を、以下に示します。

注: これらは、適応ブリッジングが使用可能にされている場合にのみ表示されます。

例: `list adaptive database address` *`mac-address`*

例: `list adaptive database all`

例: `list adaptive database port` *`segment#`*

例: `list adaptive database segment` *`segment#`*

各エントリーは 2 行に表示され、その後に 1 行のブランク行が置かれます。各エントリーでは、以下の情報が表示されます。

Canonical address
このエントリー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 標準 (16 進) フォーマットで表示されます。

Interface このエントリーを確認した (learned) 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・エントリーを確認したポートのポート番号を表示します。

Seg このアドレスを確認したセグメントの番号を表示します。

Age エントリーのエージ (秒数) を表示します。

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 (順方向) または Reverse (逆方向) として表示します。

RIF Length RIF の長さ (バイト) を表示します。

RIF LF RIF に符号化された最大フレーム値を表示します。

IBM MAC Address
このエントリーに対応するノードの MAC アドレスを表示します。これは、通常 802.5 インターフェース上にラベル表示されている 『IBM』 非標準ビット順序で表示され、IP/ARP、IPX、および NetBIOS プロトコルによって使用されます。

RIF このノードから確認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・エントリーをリストします。それぞれの重複 MAC アドレスの 1 次 RIF および 2 次 RIF が表示されます。

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・ルーター構成に関するすべての一般情報をリストします。

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

                                                      Maximum
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・ツリーを決めるのに使用する固有な ID。ネットワーク上の各ブリッジには、固有なブリッジ識別子が割り当てられています。ブリッジ優先順位が 10 進数で示され、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であるか使用不可であるかを示します。

Bridge Type 構成されたブリッジ・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
そのブリッジに構成されたポートの個数を表示します。

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 ブリッジを通してネットワーク・セグメントに接続されている装置を示します。

State ポートの現在の状態を示します。これは UP または DOWN として表示されます。

MAC address そのポートに関連付けられている MAC アドレスを標準ビット順序で表示します。

Modes そのポートのブリッジング方式を表示します。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、適応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上で送受信できる最大フレーム (データ単位) サイズ (MAC ヘッダーは含まれますが、FCS フィールドは含まれません) を指定します。

Segment そのポートに割り当てられているソース・ルーティング・ブリッジ・セグメント番号を表示します (もしあれば)。

SR bridge number
ユーザーが割り当てたソース・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・バーチャル・セグメント番号を表示します (もしあれば)。

Adaptive segment
透過ドメインへのルーティング (変換を介しての) に使用される、ソース・ルーティング・ドメイン内のセグメントの番号を表示します。

conversion *datagroup-option*

- ブリッジがフレーム・タイプに基づいてフレーム・フォーマットを変換する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的なデータ・グループには、さまざまなものがあります。These include the following:
  - 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 タイプの規則を表示します。

以下に list conversion 表示オプションの各例を示します。

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・データベースのコンテンツをリストします。list database コマンドのもとで表示するために選択できるデータ・グループには、さまざまなものがあります。これには、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 (確認された) アドレス・データベース・エントリーを表示します。
- Local - すべてのローカル (予約済み) アドレス・データベース・エントリーを表示します。
- Permanent - すべての固定アドレス・データベース・エントリーを表示します。
- Port - 特定のポートのアドレス・エントリーを表示します。
- Range - 透過ブリッジング・フィルター・アドレス・データベース全体の中のある範囲のデータベース・エントリーを表示します。範囲を定義するために、開始と終了の MAC アドレスを指定します。この範囲内のすべてのエントリーが表示されます。
- Static - アドレス・データベースから静的エントリーを表示します。

以下に list database コマンド・オプションの各例を示します。最初の例には、関連の出力も示されています。

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、すべての **list database** コマンド・オプションで表示されます。

MAC Address
アドレス・エントリーを 12 桁の 16 進フォーマット (標準ビット順序) で表示します。

MC* アドレス・エントリーの後にアスタリスクが付いている場合は、そのエントリーがマルチキャスト・アドレスとしてフラグが付けられていることを示します。

Entry Type
次のタイプの 1 つを指定します。

Reserved IEEE802.1D 標準によって将来の利用のために確保されているエントリー。

Registered エントリーは、ブリッジに参加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機能によって使用可能にされたマルチキャスト・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たエントリーで、電源オン/オフまたはシステム・リセットの後も存続します。

Static 監視プロセスでユーザーによって入力されたエントリーで、電源オン/オフまたはシステム・リセットの後は存続せず、エージレスです。

Dynamic ブリッジによって 『動的』 に 『確認』 されたエントリーで、電源オン/オフまたはシステム・リセットの後は存続せず、エントリーに関連した 『エージ』 を持っています。

Free このタイプは使用されず、まれに見られる監視とブリッジ間の 『レース』 状態の場合を除いて、通常は表示されてはなりません。

Unknown 確認不能 (不定) なエントリー・タイプ。ソフトウェア・バグを示している可能性があります。16 進値のエントリー・タイプをカスタマー・サービスに報告してください。

Age 各動的エントリーのエージ (秒数) を表します。エージは、レゾリューション間隔ごとに減分されます。

Port(s)
そのエントリーの発信ポート番号を指定します。単一ポート・エントリーの場合は、装置タイプもリストされます。IP トンネルの動的エントリーの場合、ポートは IP トンネルの 『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 アドレス機能の構成済みオプションに関する情報を表示します。

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・データベースに関する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的なデータ・グループには、さまざまなものがあります。これには、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・エントリーを表示します。
- 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・エントリーを表示します。
- SAP - SAP プロトコルのフィルター・データベース・エントリーを表示します。
- SNAP - SNAP プロトコル識別子のフィルター・データベース・エントリーを表示します。

以下に list filtering 表示オプションの各例を示します。

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
```

パケットの伝達方法を説明するのに使用される記述子は、次のとおりです。

- Routed - 転送のためにルーティング転送機能に渡されるパケットを記述します。
- Filtered - ユーザー設定のプロトコル・フィルターによって管理的にフィルターに掛けら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機能ではないプロトコル・エンティティーが存在するプロトコル識別子を記述します。この一例は、リンク・レベル・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、登録されたアドレスに送信された場合、ブリッジされ

るか、ローカルに処理されます。登録されたマルチキャスト・アドレスあてのマルチキャスト・パケットは、転送されて、ローカルに処理されます。

これらの記述子はすべて、この Ethertype をもつ 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 または port port#]

マルチアクセス・データベースのコンテンツを表示します。このデータベースは、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

すべてのデータベース・エントリーを表示するよう指定します。

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・ポートを表示します。

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
```

次のものが表示されます。

Segment あて先ソース・ルーティング・セグメント番号です。

Age 秒単位のエントリー活動時間です。

Port このエントリーを作成するマルチアクセス・ブリッジ・ポートのポート番号です。

Interface このエントリーを作成したネットワーク・インターフェースの名前です。

Circuit このエントリーを作成したフレーム・リレー・サーキット番号です。

ASRT 監視コマンド (Talk 5)

port ポート情報を表示します。

```
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
ブリッジを通してネットワーク・セグメントに接続されている装置を示します。

State ポートの現在の状態を示します。これは UP または DOWN として表示されます。

MAC address
そのポートに関連付けられている MAC アドレスを標準ビット順序で表示します。

Modes
そのポートのブリッジング方式を表示します。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、適応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上で送受信できる最大フレーム (データ単位) サイズ (MAC ヘッダーは含まれますが、FCS フィールドは含まれません) を指定します。

Segment
そのポートに割り当てられているソース・ルーティング・ブリッジ・セグメント番号を表示します (もしあれば)。

source-routing
ソース・ルーティング・ブリッジ構成情報を表示します。list source-routing コマンドのもとで表示できる一般的なデータ・グループ・オプションには、さまざまなものがあります。これには、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 - すべての SRB ブリッジのカウンターを表示します。
- State - すべての関連 SR-TB ブリッジ・データベースのコンテンツを表示します。

以下に list source-routing 表示オプションの各例を示します。

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であるか使用不可であるかを示します。

Maximum STE hop count
ソース・ルーティング・ブリッジングに関連した指定のインターフェースのブリッジから転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
ソース・ルーティング・ブリッジングに関連した指定のインターフェースのブリッジから転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 ブリッジング用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付けられているポートの個数

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ているセグメント番号

Interface
関連するインターフェースの名前。SR-TB 機能に参加しているインターフェースには 『Adaptive』 がリストされ、ATM の場合は VPI/VCI、FR の場合は DLCI

State 現在のポートの状態 (Enabled または Disabled)

MTU そのポートに設定された MTU サイズ

STE Forwarding
このポートで受信されたスパンニング・ツリー探索フレームが着信転送 (Yes) であるかどうか、および他のポートからの STE がこのポートから発信されるかどうかを示します。

LNM その特定ポート上の LAN ネットワーク・マネージャー (LNM) エージェントが、使用可能 (ENA) であるか、使用不可 (DIS) であるかを示します。

カウンター・オプションには、さらに情報のサブグループもあり、それらを list source-routing コマンドを用いて表示することができます。これには、次のものが含まれます。

- All-ports - すべてのポートのカウンターを表示します。
- Port - 特定のポート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のカウンターを表示します。

以下に list source-routing 表示オプションの各例を示します。

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付けられているポートの個数をリストします。

Segment
ソース・ルーティング・セグメント番号を 16 進値でリストします。

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 の場合は VPI/VCI、 FR の場合は DLCI。

SRF Frames Received/Sent
このブリッジで受信または送信された特別ルート・フレームの個数をリストします。

STE Frames Received/Sent
このブリッジで受信または送信されたスパンニング・ツリー探索フレームの個数をリストします。

ARE Frames Received/Sent
このブリッジで受信または送信された全ルート探索フレームの個数をリストします。

SR Frames Sent as TB
このインターフェースで受信したソース・ルーティング・フレームのうち、透過型ブリッジ・フレームとして送信されたフレームの個数をリストします。

TB Frames Sent as SR
このインターフェースで受信した透過型ブリッジ・フレームのうち、ソース・ルーティング・フレームとして送信されたフレームの個数をリストします。

Dropped, input queue
このインターフェースに到着したフレームのうち、フロー制御の理由からブリッジされなかったフレームの個数をリストします。転送機能への入力待ち行列が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したフレームのうち、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フレームの個数をリストします。

Dropped, destination address filtering
このインターフェースに到着したフレームのうち、このあて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フレームの個数をリストします。

Dropped, protocol filtering
このインターフェースに到着したフレームのうち、そのプロトコル識別子がフィルターで管理されているものであったためにブリッジされなかったフレームの個数をリストします。

Dropped, invalid RIF length
このインターフェースに到着したフレームのうち、RIF の長さが 2 未満、または 30 を超えていたために廃棄されたフレームの個数をリストします。

Dropped, duplicate segment
このインターフェースに到着したフレームのうち、RIF 内に重複セグメントがあったために廃棄されたフレームの個数をリストします。これは ARE フレームの場合は正常です。

Dropped, segment mismatch
このインターフェースに到着したフレームのうち、発信セグメント番号がこのブリッジ内のどれにも一致しないために廃棄されたフレームの個数をリストします。

Dropped, Duplicate LAN ID or tree error:
重複する LAN ID またはツリー・エラーの個数。これは、旧式の IBM ソース・ルーティング・ブリッジが含まれているネットワークでの問題検出に役立ちます。

Dropped, STE hop count exceeded:
ルーティング情報フィールドが最大ルート記述子長を超えていたために、このポートによって廃棄された探索フレームの個数

Dropped, ARE hop count exceeded:
ルーティング情報フィールドが最大ルート記述子長を超えていたために、このポートによって廃棄された探索フレームの個数

Dropped, no buffer available to copy:
フレームをコピーするために利用できる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 (マルチキャストあて先または確認不能のあて先へのフレームは、転送するためにすべてのアクティブ・ポートでコピーすることが必要です。)

Dropped, MTU exceeded:
サイズ超過のために、このポートによって廃棄されたフレームの個数

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、ループのないトポロジーを形成するために、透過ブリッジによって使用されます。**list spanning-tree-protocol** コマンドのもとで表示できる一般的なデータ・グループ・オプションには、さまざまなものがあります。これには、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 - スパンニング・ツリー・プロトコルの現在の状態情報を表示します。
  - Tree - 現在のスパンニング・ツリー情報 (ポート、インターフェース、およびコスト情報を含む) を表示します。

  以下に list spanning-tree-protocol 表示オプションの各例を示します。

  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* **or** *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できる一般的なデータ・グループ・オプションがあります。これには、以下のものが含まれます。

- 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。

以下に list tunnel 表示オプションの各例を示します。

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> プロンプトでは、NetBIOS 監視コマンドを入力することができます。

NetBIOS 監視コマンドについては、168ページの『NetBIOS コマンド』 を参照してください。

構文:

netbios

注: ユーザーのブリッジング・ルーター・ソフトウェア・ロードで NetBIOS フィルター機能が購入されていない場合、このコマンドを使用しようとすると、次の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** コマンドを使用します。

BAN 監視プロンプトにアクセスするには、DLSw 監視プロンプトの ASRT 監視プロンプトから **ban** コマンドを入力します。たとえば、

```
ASRT> ban
BAN>

   or

DLSw> ban
BAN>
```

BAN 監視プロンプトにアクセスしたら、特定の監視コマンドの入力を開始できます。直前の監視プロンプトに戻るには **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> プロンプトで入力します。

表 8. BAN 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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。xxixページの『下位レベル操作環境の終了』 を参照してください。

List

list コマンドは、すべての BAN ポートに関する情報をリストするのに使用します。表示される情報には、BAN ポート番号、BAN DLCI の MAC アドレス、そのポートが扱うフレームはブリッジされるのか、あるいは LLC が DLSw によって終端されるのか、およびポートの状態が含まれます。

ポートの状態は、3 つの値のいずれかです。

- Init Fail - 構成問題が存在することを示します。
- Up - フレーム・リレー DLCI がアップで、動作していることを示します。
- 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、ブリッジ・ネットワークおよび DLSw ネットワークを介した NetBIOS の IBM における実現方式について説明します。本章には、以下の節が含まれています。

- 『NetBIOS について』
- 145ページの『NetBIOS トラフィックの削減』
- 146ページの『フレーム・タイプ・フィルター』
- 159ページの『NetBIOS ホスト・ネーム・フィルターとバイト・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 上で使用するために設計されたものです。これはルート可能なプロトコルではありませんが、ブリッジしたり、DLSw を使用して交換することが可能です。NetBIOS トラフィックを扱うこれらの方式は両方ともサポートされています。

NetBIOS は、データ転送以外のほとんどの機能が、同報通信 (ブロードキャスト) フレームに依存しています。これは LAN 環境では問題はないかもしれませんが、WAN 環境では、制御されていないと、すぐに問題が起きる可能性があります。

以下の節では、NetBIOS ネームと種々のタイプの NetBIOS 同報通信の通信について説明します。

NetBIOS ネーム

NetBIOS ステーション間の通信でかぎとなるのは NetBIOS ネームです。各 NetBIOS エンティティーには NetBIOS ネームが割り当てられています。他の NetBIOS エンティティーと通信するためには、その NetBIOS ネームを知っている必要があります。ネームは同報通信 NetBIOS フレームの中で使用され、フレームの発信元 NetBIOS エンティティーと、フレームを受信するターゲット NetBIOS エンティティーを表します。

NetBIOS フレーム内のネームはすべて 16 字の ASCII 文字です。NetBIOS ネームには 2 種類があります。

個別 (または固有)

1 つの NetBIOS クライアントまたはサーバーを表します。このネームは NetBIOS ネットワーク内で固有のものでなければなりません。

このネームは、この特定の NetBIOS エンティティーと通信するのに使用します。

グループ

NetBIOS ステーションのグループ (たとえば、OS/2 LAN サーバー・ドメイン) を表します。このネームは、ネットワーク上の個別 NetBIOS ネームのいずれとも同じであってはなりません。

このネームを使用して NetBIOS エンティティーのグループ間で通信することができます。

1 つの NetBIOS ステーション (1 つの MAC アドレス) が、それに関連する複数の個別ネームまたはグループ・ネーム (あるいは、その両方) を持つことができます。これらのネームは、ネットワーク管理者が NetBIOS ステーションで構成した名前に基づいて NetBIOS アプリケーションによって生成されます。

NetBIOS ネームの競合の解決

NetBIOS エンティティーは、個別 NetBIOS ネームをそれ自身のネームとして使用する準備をするときに、ネットワークをチェックして他の NetBIOS ステーションがすでにそのネームを使用していないことを確認します。

NetBIOS ネームのチェックは、特定の NetBIOS UI フレームをすべての NetBIOS ステーションに繰り返し同報通信する方法で行われます。どのステーションも応答しない場合、そのネームは固有のものであると見なされ、使用することができます。ステーションが応答した場合は、新規ステーションはそのネームを使用してはなりません。

NetBIOS セッションの設定手順

データ転送タイプの運用を行うために NetBIOS セッションを設定するには、最初に NetBIOS クライアントは NetBIOS サーバーの MAC アドレスと NetBIOS サーバーへの LLC ルートを解決します。

これは、特定の NetBIOS UI フレームをすべての NetBIOS ステーションに繰り返し同報通信する方法で行われます。このフレームには、このクライアントがセッションを確立しようとしている相手側サーバーの NetBIOS ネームが入っています。サーバーは NetBIOS ネームが入っているこのフレームを受信すると、対応する同報通信 NetBIOS UI フレームをクライアントに送って応答します。クライアントがレスポンス・フレームを受信したとき、フレームには NetBIOS サーバーの MAC アドレスとルートが入っています。

一部の NetBIOS アプリケーションでは、NetBIOS サーバーの探索プロセスは、複数のステップから構成されます。たとえば、最初のステップで、クライアントが使用するドメイン・サーバーを指示するドメイン制御機能を見つけます。次に、クライアントはそのドメイン・サーバーを見つけます。

NetBIOS サーバーの MAC アドレスと NetBIOS サーバーへのルートが見つかると、NetBIOS クライアントは次のアクションのいずれかを取ることができます。

- I フレームを使用してサーバーと通信するために、NetBIOS サーバーとの LLC2 コネクションを確立する。
- 特別にルートされた NetBIOS UI フレームを使用して、NetBIOS サーバーとの通信を開始する。

NetBIOS 同報通信データの流れ

ある種の NetBIOS アプリケーションでは、データ・フレームを定期的に同報通信することが一般的に行われます。たとえば、あるステーションが別の NetBIOS ステーションに送る 1 フレーム分のデータを持っている場合です。この場合、特定の NetBIOS UI フレーム (ターゲット NetBIOS ステーション名がフレームに入っている) をすべての NetBIOS ステーションに同報通信する方法で行います。

もう 1 つは、グループ (または、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です。この場合は、特定の NetBIOS UI フレーム (ターゲット NetBIOS グループ名がフレームに入っている) をすべての NetBIOS ステーションに同報通信する方法で行います。これは広く一般的に行われている動作です。

NetBIOS 状態の流れ

それほど一般的ではない NetBIOS 機能として、他の NetBIOS ステーションから状態を入手する機能があります。これは、特定の NetBIOS フレーム (ターゲット NetBIOS ステーション名がフレームに入っている) をすべての NetBIOS ステーションに同報通信する方法で行います。ターゲット NetBIOS ステーションは、このフレームを受信すると、対応するレスポンス・フレームで応答します。

NetBIOS 全ステーション同報通信フレーム

まれにしか使用されない NetBIOS 機能として、2 つの機能があります。これらの機能は両方とも、すべての NetBIOS ステーションに NetBIOS フレームを同報通信する方法で行われます。フレームにはターゲット NetBIOS ネームは入っていません。2 つの機能は、次のとおりです。

- NetBIOS 一般同報通信機能 - 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 トレース機能終了 - ネットワーク管理者が単一地点からすべての NetBIOS ステーションの NetBIOS トレース機能を終了させることができます。特定の NetBIOS フレームが、ネットワーク上のすべての NetBIOS ステーションに同報通信されます。

NetBIOS トラフィックの削減

ネットワークを安定させるためには、ブリッジ・ネットワークまたは DLSw 交換ネットワークを介し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が必要です。これは 2 通りの方法で行うことができます。

- ブリッジングまたは DLSw 交換の前に、できるだけ多くの同報通信 NetBIOS フレームをフィルターに掛ける。
- フィルターに掛けられなかった NetBIOS UI フレームは、できるだけ少数のブリッジ・ポートまたは DLSw TCP セッションを介して転送する。

表9 は、IBM が提供するフィルターをリストしています。

表 9. NetBIOS フィルター

フィルター・タイプ	フィルターに掛けるもの
MAC アドレス	フレームを発信元またはあて先 MAC アドレスによって
バイト	フレームをバイト・オフセットおよびフィールド長によって
ネーム	フレームを NetBIOS 発信元ネームおよびあて先ネームによって
重複フレーム	重複フレーム
レスポンス	ルーターが NetBIOS 同報通信フレームを転送しなかったレスポンス

ルーターがフレームをフィルターに掛けた後は、NetBIOS ネーム・リストと NetBIOS ネーム・キャッシュおよびルート・キャッシュが、残りのフレームの転送方法を制御します。52ページの『NetBIOS バイト・フィルター』および 51ページの『NetBIOS ホスト・ネーム・フィルター』は、それぞれバイト・フィルターおよびネーム・フィルターについて説明しています。MAC アドレス・フィルターについては、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*で説明しています。

ホスト・ネーム・フィルターおよびバイト・フィルターの概要については、50ページの『NetBIOS ネームおよびバイト・フィルター』を参照してください。

以下の節では、フレーム・タイプ、重複フレーム、レスポンス・フレーム・フィルター、NetBIOS ネーム・リスト、NetBIOS ネーム・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・フィルターは、ブリッジ・トラフィック、 DLSw トラフィック、または DLSw トラフィックとブリッジ・トラフィックの両方を対象にして、特定のカテゴリーの NetBIOS フレームを完全にフィルターに掛けることができます。

フィルターに掛けることができる 3 つのカテゴリーの NetBIOS フレームは、次のとおりです。

- ネーム競合解決フレーム

  これは、使用する NetBIOS ネームがネットワーク内で固有のものであるようにするために使用される同報通信 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側ステーション (通常は、NetBIOS サーバー) の NetBIOS ネームが固有のものであることが非常に重要です。また、同じグループ (または、ドメイン) 内のステーションの個別 NetBIOS ネームも固有のものであることが重要です。しかし、NetBIOS セッションを設定するステーション (通常は NetBIOS クライアント) の NetBIOS ネームが固有のものであることはそれほど重要ではない場合がしばしばあります (特に、ドメイン間にまたがっている場合)。

  この理由から、サーバー・ネームが良く管理されているネットワークでは、ネーム競合解決フレームをフィルターに掛けると有益な場合があります。これは、特に DLSw 交換ネットワークに当てはまります。

  NetBIOS ネーム競合解決フレームには、Add-Name-Query、Add-Group-Name-Query、および Add-Name-Response があります。
- 一般同報通信フレーム

これはネットワーク上のすべての NetBIOS ステーションにデータを同報通信するのに使用される同報通信 NetBIOS フレームです。このフレームはめったに使用されないので、通常はフィルターに掛けることができます。

NetBIOS 一般同報通信フレームは Datagram-Broadcast です。

- トレース終了フレーム

  これは、ネットワーク上のすべての NetBIOS ステーションの NetBIOS トレースを終了させるのに使用される同報通信 NetBIOS フレームです。これらのフレームはめったに使用されないので、通常はフィルターに掛けることができます。

  NetBIOS トレース終了フレームは Terminate-Trace です。

デフォルトでは、ブリッジされた NetBIOS トラフィックは、上記のフレーム・タイプのいずれもフィルターに掛けられず、DLSw 交換 NetBIOS トラフィックは、上記のフレーム・タイプはすべてフレームに掛けられます。ただし、NetBIOS トラフィックが WAN リンク上でブリッジされる場合は、上記のフレーム・タイプをフィルターに掛けると有益な場合があります。

ブリッジングの場合、フレーム・タイプ・フィルターをオンまたはオフにするには **set filters bridge** を入力します。DLSw の場合、フレーム・タイプ・フィルターをオンまたはオフにするには **set filters dlsw** を入力します。

たとえば、次のように入力します。

```
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
```

重複フレームのフィルター

レスポンスが得られる可能性がある同報通信 NetBIOS フレームはすべて、発信元 NetBIOS ステーションによって一定の回数 (デフォルトは 6 回)、一定の間隔 (デフォルトは 1/2 秒間隔) で送信されます。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、得られる可能性のあるレスポンス・フレームを *NetBIOS レスポンス・フレーム* と呼びます。

NetBIOS コマンド・フレームには、次のものがあります。

- ネーム競合解決フレーム - Add-Name-Query および Add-Group-Name-Query
- NetBIOS セッション設定フレーム - Name-Query
- NetBIOS 状態フレーム - Status-Query

コマンド・フレームは、送達に成功する確率を高くするために、何回も送信されます。レスポンス・フレームは、受信した各コマンド・フレームに応答して 1 回だけ送信されます。

NetBIOS の使用

DLSw 交換ネットワークでは、各再試行を WAN セッションを介して転送すると非常にコストが高くなる可能性があります。そのため、最初のコマンド・フレームを受信すると、それを該当する近隣の 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じ 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・ネットワーク用の構成可能な時間枠が 1 つと、DLSw ネットワーク用の構成可能な時間枠が 1 つ用意されています。

ブリッジ・ネットワークの構成可能な時間枠は、2 つのコマンドによって制御されます。

- **enable duplicate-filtering/disable duplicate-filtering**。これは、重複する 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に掛けら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)

  ブリッジ・ネットワークについて重複フレーム・フィルターが使用可能にされる場合、この値は、NetBIOS コマンド・フレームがブリッジされた後に重複 NetBIOS コマンド・フレームが廃棄される期間の長さを指定します。

  タイムアウトが満了した後に重複 NetBIOS コマンド・フレームが受信される場合、フレームはブリッジ・ネットワークまで転送されます。

DLSw ネットワークの構成可能な時間枠は、1 つ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の長さを指定します。

  このタイムアウトが満了した後で重複 NetBIOS コマンド・フレームを受信した場合、そのフレームは DLSw ネットワークに転送されます。

  注: DLSw ネットワークへの重複 NetBIOS コマンド・フレームのフィルターは、常に使用可能です。

NetBIOS コマンド・フレームが DLSw 近隣によって受信されると、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。近隣 DLSw 機能は、構成可能な間隔 (1/2 秒) で構成可能な回数 (デフォルトは 6 回) だけ、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、構成されたブリッジ重複フレーム・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と間隔は、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・ネットワークおよび DLSw ネットワークの転送を実行するためにコマンド・フレームを保管しておく時間の長さを制御する 1 つのパラメーターがあります。

- **set general** ("Duplicate frame detect timeout value in seconds" パラメーター)

このパラメーターは、重複フレームおよびレスポンス・フレームの処理のために、受信した NetBIOS コマンド・フレームを保管しておく時間の長さを指定します。タイムアウトが満了すると、コマンド・フレームは削除され、それに関連した重複フレーム・フィルター・タイマーおよび縮小探索タイマーは取り消されます。タイムアウト期間後に受信した最初の重複コマンド・フレームは、受信した最初のコマンド・フレームとして扱われます。タイムアウト期間後に受信したレスポンス・フレームは、すべて廃棄されます。

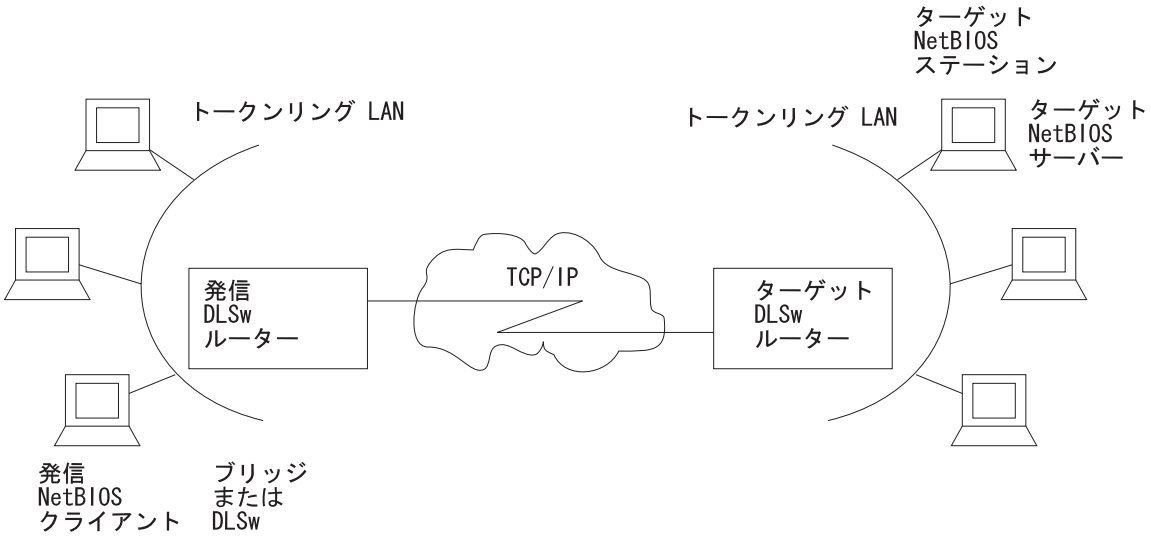
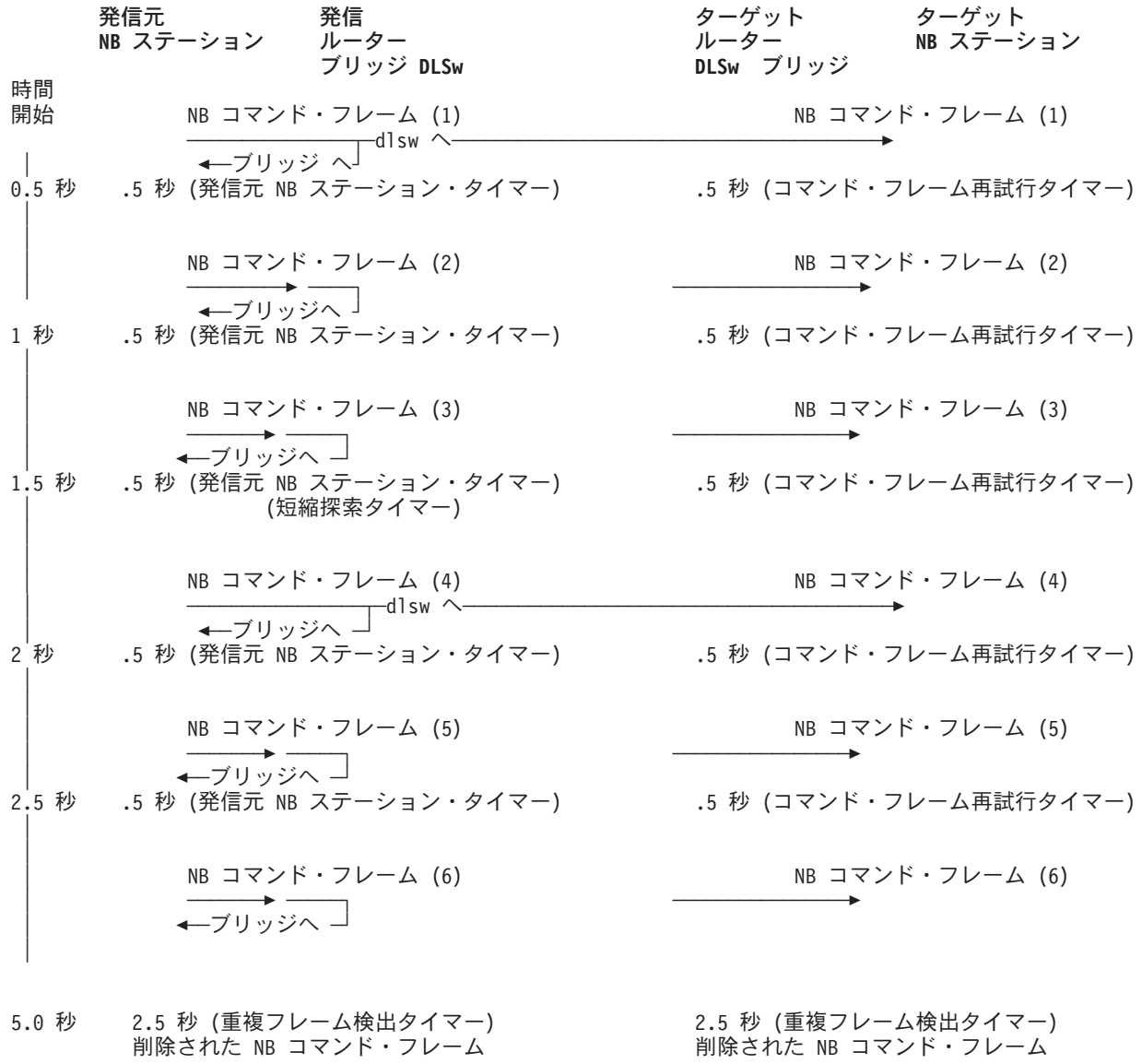


図 24. DLSw を介した NetBIOS セッションの設定. 重複フィルターは DLSw WAN を介して転送される同報通信フレームの数を減らします。

図24 および以下のシーケンスは、デフォルト値を使用してこのプロセスの様子を示します。例を簡単にするために、レスポンス・フレームは受信しなかったものと想定しています。

NetBIOS の使用



イベントのシーケンスは、次のとおりです。

1. 発信元 DLSw ルーターのブリッジ・ポートで、最初の NetBIOS コマンド・フレームを受信する。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なっているので、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は、デフォルトで使用不可になっているので、重複フレーム・フィルター・タイマーはスタートしません。DLSw NetBIOS が使用可能になっているので、フレームは DLSw ネットワークに転送され、縮小探索タイマーがスタートします (デフォルトは 1-1/2 秒)。重複フレーム検出タイマー (デフォルトは 5 秒) もスタートします。
2. ターゲット・ルーター DLSw 機能が、最初の NetBIOS コマンド・フレームを受信する。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なっているので、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は、デフォルトで使用不可になっているので、重複フレーム・フィルター・タイマーはスタートしません。再試行コマンド・タイマー (デフォルトは 1/2 秒) および重複フレーム検出タイマー (デフォルトは 5 秒) がスタートします。

3. 発信ルーターで、2 番目の NetBIOS コマンド・フレーム (最初の再試行) を受信する。ブリッジ・ネットワーク上の重複フィルターは、デフォルトで使用不可になっているので、フレームはブリッジ・ネットワークに転送されます。縮小探索タイムアウトが満了していないので、フレームは DLSw ネットワークに転送されません。
4. ターゲット・ルーターで、DLSw 機能が NetBIOS コマンド・フレーム (ローカルに生成された) の最初の再試行をブリッジ機能に転送する。ブリッジ・ネットワーク上の重複フィルターは、デフォルトで使用不可になっているので、フレームはブリッジ・ネットワークに転送されます。再試行コマンド・タイマー (デフォルトは 1/2 秒) がスタートします。
5. 発信ルーターで、3 番目の NetBIOS コマンド・フレーム (2 番目の再試行) を受信する。
6. ターゲット・ルーターで、NetBIOS コマンド・フレームの 2 番目の再試行が、最初の再試行と同じ方法で処理される。
7. 発信ルーターで、4 番目の NetBIOS コマンド・フレーム (3 番目の再試行) を受信する。ブリッジ・ネットワーク上の重複フィルターは、デフォルトで使用不可になっているので、フレームはブリッジ・ネットワークに転送されます。縮小探索タイムアウトが満了したので、フレームは DLSw ネットワークに転送されます。縮小探索タイマーがリスタートします。
8. ターゲット・ルーターで、DLSw 機能が NetBIOS コマンド・フレーム (ローカルに生成された) の 3 番目の再試行をブリッジ機能に転送する。ブリッジ・ネットワーク上の重複フィルターは、デフォルトで使用不可になっているので、フレームはブリッジ・ネットワークに転送されます。再試行コマンド・タイマー (デフォルトは 1/2 秒) がスタートします。ターゲット・ルーターは、発信元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、重複するのでそれを廃棄します。
9. 発信元ルーターで、5 番目の NetBIOS コマンド・フレーム (4 番目の再試行) が、2 番目の NetBIOS コマンド・フレームと同じ方法で処理される。
10. ターゲット・ルーターで、NetBIOS コマンド・フレームの 4 番目の再試行が、最初の再試行と同じ方法で処理される。
11. 発信元ルーターで、6 番目の NetBIOS コマンド・フレーム (5 番目の再試行) を受信する。ブリッジ・ネットワーク上の重複フィルターは、デフォルトで使用不可になっているので、フレームはブリッジ・ネットワークに転送されます。縮小探索タイムアウトが満了していないので、フレームは DLSw ネットワークに転送されません。
12. ターゲット・ルーターで、DLSw 機能が NetBIOS コマンド・フレーム (ローカルに生成された) の 5 番目の再試行をブリッジ機能に転送する。ブリッジ・ネットワーク上の重複フィルターは、デフォルトで使用不可になっているので、フレームはブリッジ・ネットワークに転送されます。再試行カウントが尽きたので、コマンド再試行タイマーはリスタートしません。
13. 発信元ルーターで 2 ～ 1/2 秒後に、重複フレーム検出タイマーが満了し、保管された NetBIOS コマンド・フレームが削除される。
14. ターゲット・ルーターで 2 ～ 1/2 秒後に、重複フレーム検出タイマーが満了し、保管された NetBIOS コマンド・フレームが削除される。

レスポンス・フレームのフィルター

NetBIOS セッション設定コマンド・フレームおよび NetBIOS 状態コマンド・フレームは、それぞれ対応する NetBIOS レスポンス・フレームを期待します。レスポンス・フレームを受信しない場合は、上記の例のように、コマンド・フレームが再試行されます。

ブリッジ・ネットワーク上のターゲット・ルーターで最初の NetBIOS レスポンス・フレームが受信されると、それが発信元ルーターに送り返され、保管されていた NetBIOS コマンド・フレームが削除されます。それ以降にターゲット・ルーターで受信されたレスポンス・フレームは、対応する NetBIOS コマンド・フレームが見つからないので、すべて廃棄されます。

発信元ルーターでは、受信したレスポンス・フレームをブリッジ・ネットワークに転送し、保管していた NetBIOS コマンド・フレームを削除します。それ以降に発信元ルーターが (DLSw またはブリッジ・ネットワークから) 受信したレスポンス・フレームは、すべて廃棄されます。

NetBIOS ネーム競合コマンド・フレームの場合は、対応する NetBIOS レスポンス・フレームが生成される場合があります (ただし、これは必須要件ではありません)。また、受信されたすべてのレスポンス・フレームが使用されます (複数の競合が存在するかどうかを判別するために)。

したがって、受信された NetBIOS ネーム競合フレームはすべて転送されますが、NetBIOS コマンド・フレームは重複フレーム検出タイマーが満了するまでは削除されません。

NetBIOS ネーム・リスト

NetBIOS ネーム・リストは、NetBIOS UI フレームの転送先の DLSw パートナーの数を制限するための DLSw 専用の機能です。

各ルーターで、ローカル NetBIOS ネーム・リストを構成することができます。このネーム・リストは、DLSw パートナーがアクセス可能な、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すべての NetBIOS ネームを表します。ルーターは、ローカル NetBIOS ネーム・リストを、すべての DLSw パートナーに送ります。パートナーはこのリストを使用して、その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 ネーム・リストは、NetBIOS ネームが良く管理されている環境では有益です。特に、DLSw を介してリモート・アクセスする必要がある環境には便利です。

ローカル NetBIOS ネーム・リストの構成

NetBIOS ネーム・リストは、NetBIOS ネーム・リスト・エントリーの集合です。ローカル NetBIOS ネーム・リストの構成には、次のことが含まれます。

- 最高 30 エントリーをネーム・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 ネームを表しているかどうかを構成する

ネーム・リスト・エントリーの構成は、NetBIOS config> プロンプトで *add name-list* コマンドを使用して行います。各エントリーは、以下の情報から構成されます。

name qualifier (ネーム修飾子)

ネーム修飾子は 1 つまたは複数の NetBIOS ネームを表します。各ネーム修飾子は、最高 16 文字まで使用できます。ネームの中にワイルドカード (埋め込み ? または末尾の *) を使って、複数の NetBIOS ネームを表すことができます。

? (疑問符) は、NetBIOS ネームのその位置の文字が任意の値を取れることを意味します。

ネームの最後の文字としての * (アスタリスク) は、NetBIOS ネームの残りの文字はすべて任意の値を取れ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多数決は、ネーム・リストに必要な名前は、サーバーまたはドメイン (ドメイン) の名前だけです。個々のクライアントの名前は、ネーム・リストに構成する必要はありません。

name qualifier type (ネーム修飾子タイプ)

NetBIOS ネームは、個別ネームまたはグループ・ネームを使用することができます。各ネーム修飾子は、個別 NetBIOS ネームの集合であるか、グループ NetBIOS ネームの集合であるかを表します。ネーム修飾子タイプは、対応するネーム修飾子がどちらのタイプの NetBIOS ネーム (個別またはグループ) を表すのかを指定します。

一般的な規則として、ドメイン名はグループ・ネームであり、クライアントまたはサーバーの名前は個別ネームです。

ネーム・リスト自体には、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があります。その属性は *ネーム・リスト排他性* です。

この属性は、ネーム・リスト・エントリーの集合が、このルーターの DLSw パートナーが到達可能なすべての NetBIOS ネームを表しているのか (排他的)、またはこのルーターの DLSw パートナーが到達可能な NetBIOS ネームの一部を表しているが、必ずしも全部ではないのか (非排他的) を示します。

排他的 (exclusive) ネーム・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最も効果的です。ルーターの排他的ネーム・リストに表示されている NetBIOS ネームあてのフレームだけが、そのルーターに転送されます。

非排他的 (non-exclusive) ネーム・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、排他的ネーム・リストほど効果的ではありません。非排他的ネーム・リストに表示されている NetBIOS ネームあてのフレームは、最初にそのルーターに転送されます。

ルーターが、どのルーターのネーム・リストにも表示されていない NetBIOS ネームあてのフレームを受信した場合、ルーターはそのフレームを非排他的ネーム・リストを持つすべてのルーターに転送します。

特定のルーターがローカル NetBIOS ネーム・リストおよびその DLSw パートナーから受信したネーム・リストを使用する方法は、以下のパラメーターを使用して制御できます。

use local NetBIOS name list (ローカル NetBIOS ネーム・リスト使用)
この機能は、NetBIOS config> プロンプトで **enable name-list local** または **disable name-list local** コマンドを使用して構成します。

「ローカル NetBIOS ネーム・リスト使用」を使用可能にした場合、ルーターはそのルーターで構成されたローカル NetBIOS ネーム・リストをすべての DLSw パートナーに送信します。

「ローカル NetBIOS ネーム・リスト使用」を使用不可にした場合、ルーターはそのルーターで構成されたローカル NetBIOS ネーム・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 (リモート NetBIOS ネーム・リスト使用)
この機能は、NetBIOS config> プロンプトで **enable name-list remote** または **disable name-list remote** コマンドを使用して構成します。

「リモート NetBIOS ネーム・リスト使用」を使用可能にした場合、ルーターは、ルーターの DLSw パートナーから受信したすべての NetBIOS ネーム・リストを使用して、特定の NetBIOS フレームの転送方法を判別します。

「リモート NetBIOS ネーム・リスト使用」を使用不可にした場合、ルーターは、ルーターの DLSw パートナーから受信したすべての NetBIOS ネーム・リストを無視します。

NetBIOS ネーム・リスト変更の認定

すべての NetBIOS ネーム・リスト・パラメーターは、NetBIOS config> プロンプトで固定的に変更することも、NetBIOS> プロンプトで一時的に変更することもできます。

変更が行われる度に、ルーターは各 DLSw パートナーに情報を送らなければならないので、ユーザーは NetBIOS> コマンド・プロンプトで **set name-list** を入力し、ネーム・リストの変更がレディー状態になっていることを示す必要があります。

NetBIOS ネーム・リストの使用

ルーターは NetBIOS ネーム・リストを使用して、次の NetBIOS フレームの転送方法を判別します。

- NetBIOS セッション設定フレーム (Name-Query)
- NetBIOS 状態コマンド・フレーム (Status-Query)
- NetBIOS コネクションレス・データ転送フレーム (Datagram)

排他的 NetBIOS ネーム・リストの効果的な使用: 可能な場合には必ず排他的 NetBIOS ネーム・リストを構成してください。排他的ネーム・リストを構成し、すべての DLSw パートナーに送信した場合、あて先ネームがネーム・リスト・エントリーの 1 つに一致するフレームは、DLSw パートナーから受信した NetBIOS フレームだけになります。

便利な排他的 NetBIOS ネーム・リストの 1 つに、空の NetBIOS ネーム・リストがあります。特定のルーターに、DLSw パートナーがアクセスできる NetBIOS サーバーがない場合は、空の排他的ネーム・リストを使用する必要があります。

非排他的 NetBIOS ネーム・リストの使用: ルーターが多数の DLSw パートナーを持っており、そのすべてがそれぞれ異なるブリッジ・ネットワークに存在する場合には、非排他的ネーム・リストを使用することができます。最も頻繁に使用されるサーバーに対してネーム・リスト・エントリーを構成し、これらのサーバーあてのトラフィックが、最初にこのルーターに送られるようにします。このネーム・リストを非排他的として指定すれば、あまり頻繁に使用されないサーバーにもトラフィックを送ることができるので、頻繁に使用されないサーバーはネーム・リストに構成しなくて済みます。この構成は、NetBIOS ネームが厳重に管理されていないネットワーク、特に DLSw を介してサーバーにリモート・アクセスする場合に使用します。

非排他的 NetBIOS ネーム・リストを使用するもう 1 つの例は、ブリッジされたネットワーク間に並列 DLSw パスが含まれている構成です。同じブリッジ・ネットワーク上に 2 つのルーターが存在する場合、一方のルーターにそのブリッジ・ネットワーク上の DLSw を介してリモート・アクセスする 1 組のサーバーを表す NetBIOS ネーム・リストを構成し、他方のルーターには別の 1 組のサーバーを表す NetBIOS ネーム・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のときは、NetBIOS トラフィックは 2 つのルーターに分散されます。一方のルーターが非アクティブのときは、すべての NetBIOS トラフィックが他方のルーターを通ります。このルーターが非排他的リストを持っているからです。

デフォルトのネーム・リストは、空の非排他的 NetBIOS ネーム・リストです。これは、ルーターが DLSw パートナーに対して、転送不能のすべての NetBIOS トラフィックをそのルーターに送るように指示します。

NetBIOS ネーム・キャッシュとルート・キャッシュ

NetBIOS ネーム・キャッシュとは、NetBIOS ネームのタイプとその NetBIOS ネームに到達するために必要な情報を分類するルーター機能です。この情報を使用して、フィルターに掛けられなかった NetBIOS フレームを、できるだけ少数の DLSw 近隣、およびできるだけ少数のブリッジ・ポートに転送するための最善の方法を判別します。NetBIOS ネーム・タイプと各タイプに保管される情報は、次のとおりです。

Individual remote (個別リモート)
これは、特定の DLSw TCP セッションを介してリモートから到達可能であることが分かっている NetBIOS ネームです。最善の TCP セッションが保管されています。

Individual local (個別ローカル)
これは、ブリッジ・ネットワークを介してローカルに到達可能であることが分かっている NetBIOS ネームです。その名前に関連した MAC アドレスが保管されています。ルート・キャッシュが使用可能になっているときは、ルーターと NetBIOS ステーション間の最善の LLC ルートも保管されています。

Group (グループ)
これはグループ名であることが分かっている NetBIOS ネームです。これは、

リモートまたはローカル (あるいは、その両方) から到達可能であり、複数の NetBIOS ステーションを表す場合もあります。その他の情報は保管されていません。

Unknown (不定)
この NetBIOS ネームに関する情報はまだ不明であり、その名前の探索がまだ完了していないことを示しています。その他の情報は保管されていません。

NetBIOS セッション設定フレームまたはコネクションレス・データ転送フレームを受信するたびに、ネーム・キャッシュを使用して、そのフレームの転送方法が判別されます。ブリッジ・ネットワーク上のルーターがこれらのフレームの 1 つを受信すると、次のアクションが取られます。

- NetBIOS フレーム内のあて先ネームがルーターの NetBIOS ネーム・キャッシュに存在しない場合は、すべての DLSw パートナーのネーム・リストを探索して、一致するものを見つけます。

  グループ・ネーム修飾子との一致が見つかると、ネーム・タイプを *group* とした NetBIOS ネーム・キャッシュ・エントリーが作成されます。フレームは、すべてのブリッジ・ポートで転送され、一致するネーム・リスト・エントリーを含んでいる非排他的ネーム・リストまたは排他的ネーム・リストを持つすべての DLSw パートナーに送られます。

  個別ネーム修飾子との一致が見つかると、ネーム・タイプを *individual remote* とした NetBIOS ネーム・キャッシュ・エントリーが作成されます。フレームは、一致するネーム・リスト・エントリーを持つ各 DLSw パートナーに転送されます。

  一致が見つからなかった場合は、ネーム・タイプを *unknown* とした NetBIOS ネーム・キャッシュ・エントリーが作成されます。フレームは、すべてのブリッジ・ポートで転送され、非排他的ネーム・リストを持つすべての DLSw パートナーに送られます。

- NetBIOS フレームのあて先ネームがルーターの NetBIOS ネーム・キャッシュに存在し、個別リモートとして分類されている場合、フレームは確認された (learned) 最善の DLSw TCP セッションに転送されます。

  確認された同等の最善の TCP セッションが複数ある場合は、異なる NetBIOS 設定フレームに対してそれらが交互に使用されます。

- NetBIOS フレームのあて先ネームがルーターの NetBIOS ネーム・キャッシュに存在し、個別ローカルとして分類されている場合、保管されている MAC アドレスが NetBIOS フレームのあて先 MAC アドレスと置き換えられます。

  ルート・キャッシュが使用不可にされている場合、NetBIOS フレームのルーティング情報はそのまま残され、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の場合は、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を用いて更新され、フレームは正しいブリッジ・ポート (MAC アドレスとルートによって判別された) に転送されます。

- NetBIOS フレームのあて先ネームがルーターの NetBIOS ネーム・キャッシュに存在し、グループまたは不定として分類されている場合、フレームはすべてのブリッジ・ポートで転送され、すべての DLSw 近隣に送られます。

NetBIOS ネームの確認

NetBIOS ネームは、NetBIOS セッション設定フレーム (Name-Query および Name-Recognized) 内の情報から確認 (learned) され、分類されます。

NetBIOS ネーム・キャッシュ・エントリーの構成

個別リモート NetBIOS ネームを構成し、それらを特定の DLSw TCP セッションに関連付けることができます。これにより、探索のオーバーヘッドを大きく削減できます。性能を向上させるために、ルーターのローカル・ブリッジ・ネットワーク上の NetBIOS クライアントによって通常的にアクセスされるリモート NetBIOS サーバーを構成しておくことをお勧めします。

個別ローカル NetBIOS ネームを構成し、それらを特定の MAC アドレスおよびルートに関連付けることはできません。

NetBIOS ネーム・キャッシュ・エントリーには 3 つのタイプがあります。

- 固定エントリーは、NetBIOS 構成プロンプト (`NetBIOS config>`) で追加されるエントリーです。ルーターのリスタート時に、ルーターは固定エントリーを構成に保管します。

  固定エントリーを追加するには、`NetBIOS config>` プロンプトで **add cache-entry** を入力します。NetBIOS ネームと関連の IP アドレスの入力を促されます。
- 静的エントリーは、NetBIOS 監視プロンプト (`NetBIOS>` コンソール) で追加されるエントリーです。ルーターのリスタート時に、ルーターは静的エントリーを保管しません。

  静的エントリーを追加するには、`NetBIOS>` コンソール・プロンプトで **add cache-entry** を入力します。NetBIOS ネームと関連の IP アドレスの入力を促されます。
- 動的エントリーは、NetBIOS 構成または監視プロンプトで追加するのでは**なく**、NetBIOS セッション設定フレームから動的に確認されるエントリーです。ルーターのリスタート時に、ルーターは動的エントリーを保管しません。

ネーム・キャッシュ・パラメーターの構成

1 つのタイプの NetBIOS ネームがネーム・キャッシュ全体を満たしてしまうのを防止するために、2 つの構成可能な NetBIOS ネーム・キャッシュ限界が用意されています。

- ローカル・ネーム・キャッシュ・エントリー最大数は、一度にキャッシュできる個別ローカル NetBIOS ネーム・キャッシュ・エントリーの最大数を指定します。最も古くに使用されたエントリーが、新しいエントリーによってオーバーライドされます。
- リモート・ネーム・キャッシュ最大数は、一度にキャッシュできる個別リモート・ネーム、グループ・ネーム、および不定 NetBIOS ネームを合わせたキャッシュ・エントリーの最大数を指定します。最も古くに使用されたエントリーが、新しいエントリーによってオーバーライドされます。

あるエントリーが構成可能なタイムアウト期間中に参照されなかった場合、そのエントリーは自動的に削除されます。このタイムアウト期間は、非参照エントリー・タイムアウト値です。

NetBIOS ネームと、TCP セッションあるいは MAC アドレスとルートのいずれかとのアソシエーションは、適時に 1 回のインスタンスで行われます。ネットワークは常に変化しており、 NetBIOS ネームへの最善パスも変更される可能性があるので、NetBIOS ネームと TCP セッションあるいは MAC アドレスとルートとのアソシエーションは、構成可能な期間だけ保管されています。この期間が過ぎた後、新たな最善パス・アソシエーションが確認されます。この構成可能な期間を制御するパラメーターは、最善パス・エージング・タイムアウト値です。

もう 1 つの便利な構成パラメーターとして、縮小探索タイムアウト値があります。これは、DLSw ネットワークへの重複コマンド・フレームをフィルターに掛ける時間を制御するだけでなく、NetBIOS ネームの探索を拡張する前に待つ時間の長さも制御します。NetBIOS セッション設定フレームを受信し、あて先 NetBIOS ネームがルーターの NetBIOS ネーム・キャッシュ内で個別リモート・フレームとして見つかった場合、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レスポンスを受け取らない場合は、このパスからはその名前にアクセスできなくなっていることが考えられます。縮小探索タイマーが満了した後に受信した最初の重複 NetBIOS セッション設定フレームを、すべての DLSw TCP セッションに転送し、より良いパスを見つけるための探索を拡張します。

最後のパラメーターは名前の有効文字数を表すもので、NetBIOS ネームの 16 文字のうち、その名前を固有な NetBIOS ネームと見なすために必要な文字数を制御します。一部の NetBIOS アプリケーションでは、NetBIOS ネームの 16 番目の文字を使用して、単一の NetBIOS ネームに関連付けられている特定エンティティー (たとえば、プリント・サーバーとファイル・サーバー) を区別しています。そのような場合には、名前の有効文字数を 15 と指定するのが最良です。これにより、あて先 NetBIOS ネームの最初の 15 文字がルーターの NetBIOS ネーム・キャッシュ・エントリーの最初の 15 文字に一致したフレームが、ネーム・キャッシュ・エントリーの情報に従って転送されることになります。これにより、複数の NetBIOS ネームを単一の NetBIOS ネーム・キャッシュ・エントリーで表すことが可能になります。

上記の NetBIOS ネーム・キャッシュ関連のパラメーターはすべて、次のように **set cache-parms** コマンドを用いて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、168ページの『NetBIOS コマンド』を参照してください。

キャッシュ・エントリーの表示

ルーターは、ユーザーがキャッシュ・エントリーを表示するのに使用できる以下のコマンドを提供しています。NetBIOS 構成プロンプトからは、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	表示するもの . . .
list cache all	すべての固定エントリー。静的エントリーと動的エントリーは表示しません。
list cache entry-number	そのエントリー番号に対応する固定キャッシュ・エントリー
list cache NetBIOS-name	特定の NetBIOS ネームの固定キャッシュ・エントリー
list cache ip-address	特定の IP アドレスの固定キャッシュ・エントリー

NetBIOS 監視プロンプトからは、表11 の list cache コマンドを使用できます。

表 11. NetBIOS List Cache 監視コマンド

コマンド	表示するもの . . .
list cache active	固定、静的、および動的エントリーを含めて、ルーターのネーム・キャッシュ内のすべてのアクティブ・エントリー
list cache config	静的エントリーと固定エントリー。 動的エントリーは表示しません。
list cache group	NetBIOS グループ・ネーム用に存在するエントリー
list cache local	ローカル・キャッシュ・エントリー。ローカル・キャッシュ・エントリーとは、ルーターがブリッジ・ネットワークを介して確認したエントリーです。
list cache name	特定の NetBIOS ネームのキャッシュ・エントリー
list cache remote	リモート・キャッシュ・エントリー。 これらは、ルーターが DLSw WAN を介して確認したエントリーです。
list cache unknown	NetBIOS エントリーのタイプが不定のエントリー。ルーターは、エントリーのタイプを確認するまでは、すべてのエントリーを不定と見なします。

NetBIOS ホスト・ネーム・フィルターとバイト・フィルターの構成手順

以下の節では、NetBIOS フィルターの設定方法の例を示します。最初の例は、ホスト・ネーム・フィルターの作成方法を説明しています。2 番目の例は、バイト・フィルターの構成方法を示しています。これらの例で使用されているコマンドの詳細については、168ページの『NetBIOS コマンド』を参照してください。

ホスト・ネーム・フィルターを作成するには 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・ネーム・フィルターの作成

以下の手順を使用して、ホスト・ネーム・フィルターを作成します。

1. 空のネーム・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. そのネーム・フィルター・リストにフィルター項目を追加する。

   update と入力して、その特定フィルター・リストのプロンプトを表示します。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** コマンドを使用して、フィルター項目をフィルター・リストに追加する。フィルター項目の構成の仕方によって、ブリッジまたは廃棄される NetBIOS パケットが決まります。次のパラメーターを以下の順序で入力して、ホスト・ネーム・フィルター項目を構成します。

   - *Inclusive* (ブリッジ) または *Exclusive* (廃棄)
   - *ASCII* または *HEX* - ホスト・ネームの表し方
   - *host name* - ASCII または 16 進文字列で表された実際のホスト・ネーム (構文は、168ページの『NetBIOS コマンド』を参照してください)

     注: このエントリーは大文字小文字の区別をします。

   - <*LAST-hex-number*> - 16 文字より少ない ASCII 文字列で使用するオプション・パラメーター

   次の例は、ホスト・ネーム **westboro** (ASCII 文字列) が含まれているパケットをブリッジすることができる (*inclusive* として構成) フィルター項目を、ホスト・ネーム・リスト **boston** に追加します。このエントリーに対しては <*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) []?
   ```

   プロンプト指示が出ないようにしたい場合は、コマンド行にすべてのパラメーターを 1 つの文字列として入力しても構いません。必ず各パラメーターの間にスペースを 1 つはさんでください。

4. フィルター項目エントリーを検証する。

   list を入力して、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. 他のフィルター項目をフィルター・リストに追加する。

   最初の 4 つのステップを繰り返して、その他のフィルター項目をフィルター・リストに追加します。ユーザーがフィルター項目を入力する順序によって、ルーターがフィルター項目をパケットに適用する方法が決まるので、この順序は重

要です。ルーターは、最初の一致でフィルター項目の適用を停止し、そのフィルター項目が Inclusive (包含) であるか Exclusive (排他) であるかに基づいて、パケットを転送または廃棄します。

最も一般的なフィルター項目を最初に入力すると、ソフトウェアがリストの先頭で一致を見つける確率が高くなるので、フィルター・プロセスが効率的になります。

パケットがフィルター項目のいずれにも一致しない場合、ルーターはフィルター・リストのデフォルト状態 (Inclusive または Exclusive) を使用します。リストのデフォルト状態を変更したい場合は、フィルター・リスト構成プロンプトで **default inclusive** または **default exclusive** を入力します。たとえば、次のように入力します。

```
NetBIOS Name boston config> default exclusive
```

6. フィルター・リストへのフィルター項目の追加が終了したら、**exit** を入力して NetBIOS Filter config> プロンプトに戻る。

```
NetBIOS Name boston config>exit
NetBIOS Filter config>
```

7. フィルターを構成に追加する。

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。これは **filter-on** コマンドを使用して行います。次のパラメーターを用いてホスト・ネーム・フィルターを構成します (この順序で入力します)。

- *Input* (そのポートで受信するすべての NetBIOS パケットをフィルターに掛ける) または output (そのポートで転送するすべての NetBIOS パケットをフィルターに掛ける)。
- *Port#*、これはルーター上の構成されたブリッジ・ポート番号です。
- *Filter-list*、これは、このフィルターに含めたいフィルター・リスト (フィルター項目が入っている) の名前です。
- オプションの演算子は、大文字で AND または OR として入力します。演算子が存在する場合は、その後にフィルター・リスト名が必要です。複数のフィルター・リストを含むフィルターは、複合フィルターと呼ばれます。

次の例は、ポート #3 に入るパケットに影響を与えるホスト・ネーム・フィルターを追加します。このフィルターは、ホスト・ネーム・フィルター・リスト **boston** から構成されています。ポート #3 に入るパケットはすべて、フィルター・リスト**boston** に含まれているフィルター項目によって定められた規則に従って評価されます。つまり、ポート #3 に入った、ホスト・ネーム **westboro** を含んでいるすべてのパケットはブリッジされることを意味しています。

```
NetBIOS Filter config>filter-on input
Port Number [1]? 3
Filter List []? boston
```

8. 新しく作成されたフィルターを検証する。

エントリーを検証するには **list** を入力します。

```
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。

   ルーター上の 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. ルーターをリスタートして、すべての NetBIOS フィルター構成変更を起動する。

    exit と入力し、**Ctrl-P** を押して、* 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中に行ったすべてのソフトウェア変更を起動します。

```
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際は、以下の手順をガイドラインとして使用してください。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 と入力して、その特定フィルター・リストのプロンプトを表示します。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。フィルター項目の構成の仕方によって、ブリッジまたは廃棄される NetBIOS パケットが決まります。次のパラメーターを用いてバイト・フィルター項目を構成します (この順序で入力します)。

   - Inclusive (ブリッジ) または Exclusive (廃棄)
   - Byte Offset - フィルターに掛けられるパケット内のオフセットを示すバイト数 (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と比較するのに使用される 16 進数。構文規則については、168ページの『NetBIOS コマンド』を参照してください。
- Hex mask - (存在する場合) 16 進パターンと同じ長さであることが必要です。パケット内のバイト・オフセットから始まるバイトと論理 AND された後、その結果が 16 進パターン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、すべてが 2 進 ″1″ であるものとみなされます。

次の例は、バイト・オフセットが 0 で 16 進パターン 0x12345678 を持つパケットがブリッジされるようにする (inclusive として構成) フィルター項目を、バイト・フィルター・リスト **westboro** に追加します。16 進マスクは存在しません。

```
NetBIOS Byte westport config>add inclusive
Byte Offset [0]? 0
Hex Pattern []? 12345678
Hex Mask (<CR> for no mask) []?
```

3. **list** コマンドを使用して、フィルター項目エントリーを検証する。

```
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. 他のフィルター項目をフィルター・リストに追加する。

   最初の 3 つのステップを繰り返して、他のフィルター項目をフィルター・リストに追加します。

5. フィルター・リストへのフィルター項目の追加が終了したら、**exit** を入力して NetBIOS Filter config> プロンプトに戻る。

```
NetBIOS Byte westport config>exit
NetBIOS Filter config>
```

   ユーザーがフィルター項目を入力する順序によって、ルーターがフィルターをパケットに適用する方法が決まるので、この順序は重要です。ルーターは、最初の一致でフィルター項目の適用を停止し、そのフィルター項目が Inclusive (包含) であるか Exclusive (排他) であるかに基づいて、パケットを転送または廃棄します。

   最も一般的なフィルター項目を最初に入力すると、ソフトウェアがリストの先頭で一致する確率が高くなり、リスト全体をチェックする必要がなくなるので、フィルター・プロセスが効率的になります。

   パケットがフィルター項目のいずれにも一致しない場合、ルーターはフィルター・リストのデフォルト状態 (Inclusive または Exclusive) を使用します。リストのデフォルト状態を変更したい場合は、フィルター・リスト構成プロンプトで **default inclusive** または **default exclusive** を入力します。たとえば、次のように入力します。

```
NetBIOS Byte westport config> default exclusive
```

6. フィルターを構成に追加する。

   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。これは **filter-on** コマンドを使用して行います。次のパラメーターを用いてホスト・ネーム・フィルターを構成します (この順序で入力します)。

- *Input* (そのポートで受信するすべてのパケットをフィルターに掛ける) または output (そのポートで転送するすべてのパケットをフィルターに掛ける)
- *Port#* - 構成されたブリッジ・ポート番号
- *Filter-list* - このフィルターに含めたいフィルター・リスト (フィルター項目が入っている) の名前
- オプションの演算子は、大文字で AND または OR として入力します。演算子が存在する場合は、その後にフィルター・リスト名が必要です。複数のフィルター・リストを含むフィルターは、複合フィルターと呼ばれます。これらについては、165ページの『NetBIOS 構成および監視コマンドについて』でさらに詳しく説明しています。

次の例は、ポート #3 から出るパケットに影響を与えるホスト・ネーム・フィルターを追加します。このフィルターは、バイト・フィルター・リスト **westboro** から構成されています。ポート #3 から出るパケットはすべて、フィルター・リスト **westboro** に含まれているフィルター項目によって定められた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. 新しく作成されたフィルターを検証する。

   エントリーを検証するには **list** を入力します。

```
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・ルーター上の 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. ルーターをリスタートして、すべての NetBIOS フィルター構成変更を起動する。

   exit と入力し、**Ctrl-P** を押して、* プロンプトに戻ります。**restart** と入力します。

```
NetBIOS Filter config>exit
ASRT config>exit
Config> Ctrl-P
* restart
```

第8章 NetBIOS の構成および監視

この章では、ブリッジ・ネットワークおよび DLSw ネットワークを介した NetBIOS の IBM による構成および監視について説明します。本章には、以下の節が含まれています。

- 『NetBIOS 構成および監視コマンドについて』
- 168ページの『NetBIOS コマンド』

NetBIOS 構成および監視コマンドについて

NetBIOS 構成コマンドは ASRT/DLSW config> プロンプトで利用可能です。ルーターの構成に加えた変更は、即時には有効になりません。ルーターをリスタートしたときに、ルーターの構成メモリーの一部になります。この章では、構成変更のことを固定 (permanent) と呼びます。

NetBIOS 監視コマンドは、ASRT/DLSW> プロンプトで利用可能です。監視コマンドは即時に有効になりますが、ルーターの不揮発性構成メモリーには保管されません。つまり、監視コマンドはルーターの構成をリアルタイムで変更できますが、これらの変更は一時的なものです。ルーターをリスタートすると、ルーターの構成メモリーがそれらを上書きしてしまいます。本章では、監視プロンプトで行う変更のことを静的 (static) 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 構成環境または DLSw 構成環境から表示することができます。NetBIOS config> プロンプトから行う変更は、ブリッジングと DLSw の両方に影響を与えます。

ASRT 構成環境から NetBIOS config> プロンプトを表示するには、次のように入力します。

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

NetBIOS Support User Configuration

NetBIOS config>
```

DLSw 構成環境から NetBIOS config> プロンプトを表示するには、次のように入力します。

```
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 監視環境または DLSw 監視環境から表示することができます。

NetBIOS> 監視プロンプトで行った変更は、ブリッジングと DLSw の両方に影響を与えます。

ASRT 監視環境から NetBIOS> 監視プロンプトを表示するには、次のように入力します。

```
 + protocol asrt
ASRT>NetBIOS

NetBIOS Support User Console

NetBIOS>
```

DLSw 監視環境から NetBIOS> プロンプトを表示するには、次のように入力します。

```
 + protocol dls
DLSw>NetBIOS

NetBIOS Support User Console

NetBIOS>
```

DLSw 用の NetBIOS の構成

DLSw を介して 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で指定します。

- NetBIOS SAP をオープンする。
- SNA および NetBIOS セッションの優先順位を設定する。
- 最大 NetBIOS フレーム・サイズを設定する。
- NetBIOS UI フレームに割り当てるバイト数を設定する。

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 フレームを転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 および NetBIOS セッションの優先順位の設定

ネットワーク輻輳 (ふくそう) のときに 1 つのタイプのセッションが、利用可能な帯域幅を多く使い過ぎないようにするために、SNA および NetBIOS トラフィックに優先順位を付けることができます。これを行うには **priority** を入力し、SNA セッションと NetBIOS セッションの優先順位を設定します。セッションの優先順位に対応するメッセージ割り当ても設定することができます。

set priority コマンドを使用して、次の例のように指定します。

```
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
```

デフォルトのメッセージ割り当て 4/3/2/1 は、セッションに次のように割り当てます。

4 - Critical (クリティカル)

3 - High (高)

2 - Medium (中)

1 - Low (低)

ルーターは優先順位とメッセージ割り当てを使用して、特定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。たとえば、次の場合を考えてみましょう。

- SNA トラフィックに「クリティカル」の優先順位を割り当て、「クリティカル」セッションのメッセージ割り当てが 4 である場合

  かつ

- NetBIOS トラフィックに「中」の優先順位を割り当て、「中」セッションのメッセージ割り当てが 2 である場合

ルーターは 4 つの SNA フレームを処理し、その後で 2 つの NetBIOS フレームを処理します。2 つの NetBIOS フレームを処理した後、次にルーターは 4 つの SNA フレームを処理するという具合に進められます。

このシナリオでは、利用可能な帯域幅の 3 分の 2 が SNA トラフィック専用に割り当てられます (4 対 2 の割合で)。ルーターがユーザーの指定した優先順位に従って帯域幅を割り当てる際には、バイト数ではなくフレーム数でカウントすることに注意してください。

セッションに対するメッセージ割り当ては、デフォルトの 4/3/2/1 から変更することが可能です。その場合は、必ず 4 桁の数字 (9 から 1 までの) を降順に入力する必要があります。たとえば、SNA の優先順位が「クリティカル」で、NetBIOS トラフィックが「中」の場合、ユーザーがメッセージ割り当てを 8/7/6/5 に変更すると、ルーターは 8 つの SNA フレームを処理し、次に 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** コマンドを使用して、最大 NetBIOS フレーム・サイズを変更することもできます。デフォルトは 2052 です。このパラメーターは、ユーザーが必要と考える最大フレーム・サイズに設定し、それ以上は大きく設定しないでください。フレーム・サイズを必要以上に大きく設定すると、利用可能なバッファー数が減ります。

NetBIOS UI フレームのメモリー割り当ての設定

DLSw **set memory** コマンドを使用して、ルーターが NetBIOS UI フレーム用のバッファーとして割り当てるバイト数を設定します。TCP 転送バッファーが満ぱいになると、ルーターはこのバッファーを NetBIOS UI フレームに使用します。

NetBIOS に割り当てられるバイト数はグローバルであり、セッション単位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 は、NetBIOS 構成および監視コマンドをリストしています。

表 12. NetBIOS 構成および監視コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	キャッシュ・エントリーをルーターのネーム・キャッシュに追加し、ネーム・リスト・エントリーをルーターのローカル・ネーム・リストに追加します。
Delete	**add** コマンドを使用して追加したキャッシュ・エントリーまたはネーム・リスト・エントリーを削除します。
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/リモート NetBIOS ネーム・リストの使用を使用不可にします。
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/リモート NetBIOS ネーム・リストの使用を使用可能にします。
List	構成プロンプトであるか、監視プロンプトであるかに応じて、各種の NetBIOS ネーム・キャッシュおよびネーム・リスト構成情報を表示します。
Set	ネーム・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、およびネーム・リストの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利用可能であり、特定の NetBIOS ネームを、現行の NetBIOS ネーム・キャッシュおよびネーム・リストと照合してテストします。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

新規ネーム・キャッシュをルーターの固定構成または静的構成に追加したり、またはリモート・ステーションのローカル DLSW へのアクセスを制限するのに使用する NetBIOS ネーム・リスト・エントリーを追加します。追加できるのは、 DLSw 近隣のネーム・キャッシュ・エントリーだけです。ASRT トラフィックに対して追加したエントリーは、ルーターによって無視されます。

構文:

add cache-entry

name-list

cache-entry

新規エントリーをルーターのネーム・キャッシュに追加します。

- 構成プロンプトから、固定エントリーを追加します。

- 監視プロンプトから、一時エントリーを追加します。

ユーザーが **set cache-parms** を使用して NetBIOS ネーム内の 16 文字が関係することを指示した場合にのみ、ルーターは 16 進数の 16 番目の文字を入力するよう求めるプロンプトを出します。

1 つの NetBIOS ネームに、異なる IP アドレスを持つ複数のエントリーを追加することも可能です。こうすると、そのネームに複数の DLSw 近隣を介してアクセスすることが可能になります。

注: NetBIOS ネームは大文字小文字の区別をし、ネットワークの NetBIOS ネームの大文字小文字と一致していることが必要です。

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

新規エントリーを、ルーターのローカル・ネーム・リストに追加します。

構成プロンプトから、固定ネーム・リスト・エントリーを追加します。この変更は、ルーターをリスタートするまで、または NetBIOS> プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。

監視プロンプトから、一時ネーム・リスト・エントリーを追加します。この変更は、NetBIOS> プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。ルーターをリスタートすると、この変更は失われます。

NetBIOS ネーム修飾子は、DLSw を介して他のルーターに到達可能にする必要のある、このルーターのローカル・ブリッジ・ネットワーク上で到達可能な 1 つまたは複数の NetBIOS ネームを表します。

NetBIOS ネーム修飾子には、次の 2 種類のワイルドカード文字を含めることができます。

? (疑問符)
実際の NetBIOS ネームの中の 1 文字が任意の値で構わないことを示します。

*** (アスタリスク)**
ネーム修飾子の末尾に付けて、実際の NetBIOS ネームの残りの文字が任意の値で構わないことを示します。

注:

1. ネーム修飾子の末尾にアスタリスクが付いていない場合、ネーム修飾子の残りの部分には、最大 16 文字までヌル (16 進数のゼロ) が埋め込まれます。
2. NetBIOS ネーム修飾子は大文字小文字の区別をし、ネットワークの NetBIOS ネームの大文字小文字と一致していることが必要です。

例: add name-list

NetBIOS コマンド (Talk 6 および Talk 5)

```
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

ネーム・キャッシュ・エントリーまたは NetBIOS ネーム・リスト・エントリーを削除します。

構文:

delete cache-entry

name-list

cache-entry

構成プロンプトから、ルーターの固定構成からネーム・キャッシュ・エントリーを削除します。ルーターはレコード番号を入力するようにプロンプトで指示します。これはユーザーが削除したいエントリーの番号です。エントリー番号のリストを見たい場合は **list cache all** を入力します。

監視プロンプトから、ルーターの静的構成またはアクティブ・キャッシュから、ネーム・キャッシュ・エントリーを削除します。ルーターはキャッシュ・エントリーの名前を入力するように指示します。エントリーのリストを見たい場合は、**list cache conf** または **list cache active** を入力します。

注: NetBIOS ネームは大文字小文字の区別をします。

構成の例: delete cache-entry

```
Enter name cache record number [1]? 2

Name cache entry has been deleted
```

監視の例: 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・ネーム・リストからエントリーを削除します。

構成プロンプトから、固定ネーム・リスト・エントリーを削除します。ルーターはレコード番号 (削除したいエントリーの番号) を入力するように指示します。エントリー番号のリストを見たい場合は **list name-list all** コマンドを入力します。この変更は、ルーターをリスタートするまで、または監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。

監視プロンプトから、ネーム・リスト・エントリーを一時的に削除します。ルーターはレコード番号 (削除したいエントリーの番号) を入力するように指示します。エントリー番号のリストを見たい場合は **list name-list config** コ

マンドを入力します。この変更は、監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。ルーターをリスタートすると、この変更は失われます。

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 ネーム・リストの使用、またはルート・キャッシュを使用不可にします。

構文:

disable duplicate-filtering

name-list local

name-list remote

route-caching

duplicate-filtering

ブリッジングの重複フレーム・フィルターを使用不可にします。DLSw トラフィックの重複フレーム・フィルターは、使用不可にできません。

例: disable duplicate-filtering

```
Duplicate frame filtering is          OFF
```

name-list local

ローカル・ネーム・リストの使用を使用不可にします。ローカル・ネーム・リスト・エントリーは、どの DLSw パートナーにも送信されなくなります。

構成プロンプトから、ローカル・ネーム・リストの使用を固定的に使用不可にします。この変更は、ルーターをリスタートするまで、または監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。

監視プロンプトから、ローカル・ネーム・リストの使用を一時的に使用不可にします。この変更は、監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。ルーターをリスタートすると、この変更は失われます。

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・ネーム・リストの使用を使用不可にします。DLSw から受信した NetBIOS ネーム・リストは使用されなくなります。

構成プロンプトから、リモート・ネーム・リストの使用を固定的に使用不可にします。この変更は、ルーターをリスタートするまで、または監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。

監視プロンプトから、リモート・ネーム・リストの使用を一時的に使用不可にします。この変更は、監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。ルーターをリスタートすると、この変更は失われます。

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 のルート・キャッシュを使用不可にします。ルート・キャッシュというのは、NetBIOS ネーム・キャッシュ内のエントリーを使用して、同報通信フレームを特別ルート・フレーム (SRF) に変換するプロセスをいいます。

例: disable route-caching

```
Route caching is                    OFF
```

Enable

重複フレーム・フィルター、NetBIOS ネーム・リストの使用、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

ブリッジングの重複フレーム・フィルターを使用可能にします。DLSw の重複フレーム・フィルターは常に使用可能です。これを使用可能にしたり、使用不可にしたり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・ネーム・リストの使用を使用可能にします。ローカル・ネーム・リスト・エントリーが、すべての DLSw パートナーに送信されるようになります。

構成プロンプトから、ローカル・ネーム・リストの使用を固定的に使用可能にします。この変更は、ルーターをリスタートするか、監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。

監視プロンプトから、ローカル・ネーム・リストの使用を一時的に使用可能にします。この変更は、監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。ルーターをリスタートすると、この変更は失われます。

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・ネーム・リストの使用を使用可能にします。DLSw から受信したすべての NetBIOS ネーム・リストが使用されます。

構成プロンプトから、リモート・ネーム・リストの使用を固定的に使用可能にします。この変更は、ルーターをリスタートするか、監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。

監視プロンプトから、リモート・ネーム・リストの使用を一時的に使用可能にします。この変更は、監視プロンプトから **set name-list** コマンドを使用して変更を認定するまでは有効になりません。ルーターをリスタートすると、この変更は失われます。

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 のルート・キャッシュを使用可能にします。ルート・キャッシュというのは、NetBIOS ネーム・キャッシュを使用して、同報通信フレームを特別ルート・フレーム (SRF) に変換するプロセスをいいます。

例: enable route-caching

```
Route caching is                        ON
```

List (構成)

すべてのキャッシュ・エントリーを表示するか、またはエントリーのタイプ別にキャッシュ・エントリーを表示します。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 ネーム・リストを表示します。

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

ルーターのネーム・キャッシュ内のすべての固定エントリーを表示します。静的または動的エントリーは表示しません。

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#*

エントリー番号に対応するキャッシュ・エントリーを表示します。エントリー番号のリストを見たい場合は、**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 ネームのキャッシュ・エントリーを表示します。探索を単純化するために、次のワイルドカードを使用することができます。

***** (アスタリスク) は、任意の文字のゼロまたはそれ以上のオカレンスを表します。たとえば、San* は、次のようなものを表すことができます。

- San Francisco
- Santa Fe
- San Juan

? (疑問符) は、任意の 1 文字を表します。

$ (ドル記号) は、NetBIOS ネームの有効文字数が 16 ではなく、しかも探索引き数がアスタリスク (*) で始まっていない場合にのみ有効です。

ワイルドカードは、NetBIOS ネームの最大文字数 (構成によって 15 または 16) まで、必要な数だけ使用できます。

注: NetBIOS ネームは大文字小文字の区別をします。

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 アドレスを持つすべてのエントリーを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 の両方について、フレーム・タイプ・フィルターがオンであるか、オフであるかを表示します。**set filters bridge** コマンドを使用して、これらのフィルターをオンまたはオフにします。

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

フレーム・タイプ・フィルターがオンであるか、オフであるかを表示します。**set filters bridge** を使用して、これらのフィルターをオンまたはオフにします。

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 のフレーム・タイプ・フィルターがオンであるか、オフであるかを表示します。**set filters dlsw** を使用して、これらのフィルターをオンまたはオフにします。

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

固定的に構成されたローカル NetBIOS ネーム・リスト・エントリーを表示します。静的エントリーは表示しません。

例:

```
list name-list all
Entry  Name Qualifier    Type
-----  ----------------  ----------
  1    NY_SERV*          INDIVIDUAL
  2    NY_DOMAIN*             GROUP
```

name-list *entry-number*

特定の固定的に構成されたローカル NetBIOS ネーム・リスト・エントリーを表示します。

例:

```
list name-list entry-number
Enter name list record number [1]? 1

Entry  Name Qualifier    Type
-----  ----------------  ----------
  1    NY_SERV*          INDIVIDUAL
```

List (監視)

種々のタイプのキャッシュ・エントリー、フィルター構成、一般構成情報、NetBIOS ネーム・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

ルーターのネーム・キャッシュ内のすべてのアクティブ・エントリーを表示します。

不等号括弧内の数字は、NetBIOS ネームの 16 番目の文字です。この文字 (キャッシュ・エントリーを作成するときに 16 進数で入力できます) は、一部の NetBIOS アプリケーションによって特殊な目的に使用されます。

Name Type フィールドに LOCAL が指定されていない場合、それはリモート・エントリーです。

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

すべての静的および固定ネーム・キャッシュ・エントリーを表示します。動的エントリーは表示しません。

不等号括弧内の数字は、NetBIOS ネームの 16 番目の文字です。この文字 (キャッシュ・エントリーを作成するときに 16 進数で入力できます) は、一部の NetBIOS アプリケーションによって特殊な目的に使用されます。

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・ネーム用に存在するキャッシュ・エントリーを表示します。

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・エントリーを表示します。ローカル・キャッシュ・エントリーというのは、ルーターがローカル・ブリッジ・ネットワークを介して確認したエントリーのことです。

NetBIOS クライアントの場合、Local Path State (ローカル・パス状態) は常に Unknown (不定) であり、MAC address and Routing information (MAC アドレスおよびルーティング情報) 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・エントリーの数

NetBIOS Name
そのエントリーの NetBIOS ネーム

Loc Path State
ローカル・パス状態

MAC Address
そのエントリーがサーバーの場合、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 ネームのキャッシュ・エントリーを表示します。探索を単純化するために、次のワイルドカードを使用することができます。

***** (アスタリスク) は、任意の文字のゼロまたはそれ以上のオカレンスを表します。たとえば、San* は、次のようなものを表すことができます。

- San Francisco
- Santa Fe
- San Juan

? (疑問符) は、任意の 1 文字を表します。

$ (ドル記号) は、NetBIOS ネームの有効文字数が 16 ではなく、しかも探索引き数がアスタリスク (*) で始まっていない場合にのみ有効です。

ワイルドカードは、NetBIOS ネームの最大文字数 (構成に応じて 15 または 16) まで、必要な数だけ使用できます。

注: NetBIOS ネームは大文字小文字の区別をします。

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 を介して確認したキャッシュ・エントリーを表示します。

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・エントリーの数

NetBIOS Name
そのエントリーの NetBIOS ネーム

Rem Path State
リモート・パス状態。可能な状態は、以下のとおりです。

Best Found ルーターは、このステーションへの最善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善ルートをまだ見つけていません。

Group ルーターは、グループ・ネームに対する最善パスは探しません。

Search Limited
ルーターは、この NetBIOS ネームに対して限定的な探索を行っています。縮小探索についての詳細は、**set cache-parms** コマンドを参照してください。

Search All ルーターは完全な探索を行っています。**set cache-parms** コマンドの縮小探索タイマーが満了すると、ルーターは完全探索を実行します。

IP Address(es)
最善パスが見つかると、その NetBIOS ステーションに到達できる近隣 DLSw に関連した IP アドレス (1 つまたは複数) を表示します。

cache unknown

NetBIOS ネームのタイプが不定のキャッシュ・エントリーを表示します。ルーターは、ネームのタイプを確認するまでは、すべての動的エントリーを Unknown (不定) として入力します。確認されると、それらのエントリーにローカル、リモート、またはグループのマークを付けます。

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

ブリッジングおよび DLSw の両方について、フレーム・タイプ・フィルターがオンであるか、オフであるかを表示します。

set filters bridge および **set filters dlsw** コマンドを使用して、これらのフィルターをオンまたはオフにします。

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
```

NetBIOS コマンド (Talk 6 および Talk 5)

filters bridge

ブリッジングのフレーム・タイプ・フィルターがオンであるか、オフであるかを表示します。**set filters bridge** コマンドを使用して、これらのフィルターをオンまたはオフにします。

例: `list filters bridge`

```
Bridge name conflict filtering is       OFF
Bridge general bcast filtering is       OFF
Bridge trace control filtering is       OFF
```

filters dlsw

両方の DLSw のフレーム・タイプ・フィルターがオンであるか、オフであるかを表示します。**set filters dlsw** コマンドを使用して、これらのフィルターをオンまたはオフにします。

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

ローカルとリモートの両方の、現在アクティブのすべての NetBIOS ネーム・リストを表示します。ローカル・ネーム・リスト・エントリーが未認定の場合、またはローカル・ネーム・リストの使用が使用不可の場合、ローカル・ネーム・リスト・エントリーは、リストに表示されません。リモート・ネーム・リストが使用不可の場合、リモート・ネーム・リスト・エントリーは、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

すべての固定的および一時的に構成されたローカル NetBIOS ネーム・リスト・エントリーを表示します。

Source フィールドには、以下の値の 1 つが入ります。

PERMANENT 固定的に構成されたエントリー

STATIC 一時的に構成されたエントリー

LastMod フィールドには、以下の値の 1 つが入ります。

ADDED ローカル・ネーム・リスト・エントリーが追加されたが、変更がまだ認定されていない。

DELETED ローカル・ネーム・リスト・エントリーが削除されたが、変更がまだ認定されていない。

UNCHANGED ローカル・ネーム・リスト・エントリーが追加され、変更が認定された。

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

現在アクティブのすべてのローカル NetBIOS ネーム・リスト・エントリーを表示します。ローカル・ネーム・リスト・エントリーが未認定の場合、またはローカル・ネーム・リストの使用が使用不可の場合、ローカル・ネーム・リスト・エントリーは、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

特定の DLSw パートナーの現在アクティブのすべてのリモート NetBIOS ネーム・リスト・エントリーを表示します。リモート・ネーム・リストが使用不可の場合、エントリーは何も表示されません。

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

次のようなネーム・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

次のような、ブリッジングのネーム・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

次のような、DLSw のネーム・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

ブリッジングのフレーム・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 のフレーム・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

ネーム・キャッシュ・パラメーターの設定、ブリッジングまたは DLSw のフレーム・タイプ・フィルターのオンまたはオフ、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の調整、および NetBIOS ネーム・リスト・パラメーターの設定を行います。また、 NetBIOS ネームおよびバイト・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スイッチングに適用されるネーム・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 ネームを探索するときに考慮する文字数が 15 文字であるか 16 文字であるかを決めます。15 と入力すると、ルーターは 16 番目の文字を無視します。16 を選択すると、ルーターはキャッシュ・エントリーを探索するときに 16 番目の文字を含めます。

デフォルトは 15 です。

Best path aging timeout

ルーターがネーム・キャッシュ・エントリーのアドレスとルートを、そのステーションへの最善パスとみなす時間の長さ。このタイマーが満了すると、ルーターはそのネーム・キャッシュ・エントリーを削除し、この NetBIOS ネームの新たな最善パスを見つけようと試みます。

最善パスを決めるに際して、ルーターはこれらのノードを接続する可能なすべてのルートについて、ノード間の転送時間だけでなく最大フレーム・サイズも考慮します。パス上で転送される可能性がある最大 NetBIOS フレームを収容できないパスは、適切なパスとはみなしません。

デフォルトは 60 秒です。範囲は 1.0 ～ 100000.0 秒です。

Reduced search timeout

タイムアウト期間内に Name-Query、Status-Query、または Datagram を受信すると、ルーターは現在の NetBIOS ネーム・キャッシュ情報に基づいて探索を実行します。

このタイマーが満了した後で重複フレームを受信した場合、ルーターは前のルートはもはや有効ではないものと想定し、探索を拡大します。ルーターは重複フレームをブリッジと DLS の両方に転送します。DLS は対応する SSP メッセージをすべての可能な DLS パートナーに同報通信します。

デフォルトは 1.5 秒です。範囲は 1.0 ～ 100.0 秒です。

Unreferenced entry timeout

ルーターは、削除する前に、参照されない名前をこの時間の長さだ

けキャッシュ内に保持します。キャッシュが満ぱいになった場合には、ルーターはこの時間より早くエントリーを除去します。

デフォルトは 5000 分です。範囲は 1 〜 100000 分です。

Max nbr local name cache entries

ルーターがネーム・キャッシュに保管する、ローカルで確認したエントリーの最大数

デフォルトは 500 です。範囲は 100 〜 30000 です。この値を低く設定すると、ルーターのメモリーを節約できます。メモリーの使用、プロセッサーの使用、および同報通信トラフィックの量を最適化するために、ローカル・ネーム・キャッシュ・エントリーの数は、このルーターのローカル・ブリッジ・ネットワーク上のアクティブな 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い値に設定してください。

Max nbr remote name cache entries

ルーターがネーム・キャッシュに保管する、リモートで確認されたエントリー、グループ・ネーム・エントリー、および不定エントリーの最大数

デフォルトは 100 です。範囲は 100 〜 30000 です。この値を低く設定すると、ルーターのメモリーを節約できます。メモリーの使用、プロセッサーの使用、および同報通信トラフィックの量を最適化するために、リモート・ネーム・キャッシュ・エントリーの数は、このルーターのローカル・ブリッジ・ネットワーク上の 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% を上乗せした数に設定してください。

filters bridge

ブリッジングのフレーム・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、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、189ページの『第9章 NetBIOS フィルターの構成および監視』で説明しています。

NetBIOS > 監視プロトコルから、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、199ページの『NetBIOS フィルターの監視』で説明しています。

このパラメーターは NetBIOS バイト・フィルターへのアクセスを可能にします。

例: set filters byte

```
NetBIOS Filtering configuration
NetBIOS Filter config>
```

filters dlsw

DLSw トラフィックのフレーム・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、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、189ページの『第9章 NetBIOS フィルターの構成および監視』で説明しています。

NetBIOS > 監視プロトコルから、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、199ページの『NetBIOS フィルターの監視』で説明しています。

このパラメーターは NetBIOS ネーム・フィルターへのアクセスを可能にします。

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とタイムアウトを設定します。重複フレーム・フィルターの機能についての詳細は、147ページの『重複フレームのフィルター』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 が使用可能の場合、ソフトウェアは次のような質問をします。

```
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の場合、ブリッジされる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、ルーターは受信したすべての重複フレームをフィルターに掛けます。

範囲は 0.0 ～ 100.0 秒です。ゼロは、重複フレーム検査を使用不可にします。デフォルトは 1.5 秒です。

Duplicate frame-detect timeout

ブリッジ・トラフィックと DLSw トラフィックの両方に適用されます。ルーターが重複フレーム・フィルター・データベースにエントリーを保管しておく時間の長さ。このタイマーが満了すると、ルーターは受信した新規フレームのために新規エントリーを作成します。

範囲は 0.0 ～ 100.0 秒です。デフォルトは 5 秒です。

Command frame retry count

DLSw トラフィックにのみ適用されます。

ターゲット DLSw ルーターが、ローカル接続している LAN に送信する重複 NetBIOS 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によって指定された間隔で送信されます。

範囲は 0 ～ 10 です。デフォルトは 5 です。

Command frame retry timeout

DLSw トラフィックにのみ適用されます。これは、近隣 DLSw ルーターがローカル・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 ～ 10.0 秒です。デフォルトは 0.5 秒です。

name-list

ローカル NetBIOS ネーム・リストに関連するパラメーターを設定します。現在使用されている唯一のローカル NetBIOS ネーム・リスト関連のパラメーターは、 local NetBIOS name list exclusivity (ローカル NetBIOS ネーム・リスト排他性) です。

構成プロンプトから、ローカル NetBIOS ネーム・リスト・パラメーターを固定的に設定します。この変更は、ルーターをリスタートするか、監視プロンプトから **set name-list** コマンドを使用して変更を認定するまで、有効になりません。

構成プロンプトから、このコマンドはローカル NetBIOS ネーム・リスト・パラメーターを一時的に設定します。また、このコマンドは、構成または監視プロンプトから行われた NetBIOS ネーム・リストの変更の認定も行います。

Test (監視のみ)

実際の NetBIOS ネームを、現行の NetBIOS キャッシュまたは NetBIOS ネーム・リストと照合してテストすることができます。

構文:

test cache

name-list

test cache

指定の NetBIOS あて先ネームを持つ DLSw フレームが転送される現行の DLSw パートナーと、フレームの転送方法を示したリストを表示します。

例 (対応する NetBIOS キャッシュ・エントリーが存在しない場合): 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・エントリーが存在する場合): 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

指定の NetBIOS ネームに一致する NetBIOS ネーム・リスト・エントリー (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 フィルターの構成および監視

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。これらのコマンドを使用して、NetBIOS フィルターを ASRT ブリッジングへの追加機能として構成することができます。構成コマンドには NetBIOS config> プロンプトからアクセスします。

本章には、以下の節が含まれています。

- 『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、次の例の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>
```

DLSw 構成環境から NetBIOS config> プロンプトを表示するには、次のように入力します。

```
 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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Create	NetBIOS フィルターのバイト・フィルターおよびホスト・ネーム・フィルター・リストを作成します。
Delete	NetBIOS フィルターのバイト・フィルターおよびホスト・ネーム・フィルター・リストを削除します。
Disable	ブリッジング・ルーター上の NetBIOS フィルターを使用不可にします。

表 13. NetBIOS フィルター構成コマンド (続き)

コマンド	機能
Enable	ブリッジング・ルーター上の NetBIOS フィルターを使用可能にします。
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。このフィルターを、指定されたポートに着信**または**発信するすべての NetBIOS パケットに適用することができます。
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・ネーム・リストまたはバイト・フィルター・リストに情報を追加したり、情報を削除したりします。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Create

create コマンドは、バイト・フィルター・リストまたはホスト・ネーム・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 フィルターのバイト・フィルター・リスト名を作成します。作成するリストを識別するために、最高 16 文字まで使用できます。*Filter-list* は、以前に **create byte-filter-list** または **create name-filter-list** コマンドで使用されていない固有な名前でなければなりません。

例: `create byte-filter-list newyork`

name-filter-list *filter-list*

NetBIOS フィルターのホスト・ネーム・フィルター・リスト名を作成します。作成するネーム・フィルター・リストを識別するために、最高 16 文字まで使用できます。*Filter-list* は、以前に **create byte-filter-list** または **create name-filter-list** コマンドで使用されていない固有な名前でなければなりません。

例: `create name-filter-list atlanta`

Delete

delete コマンドは、**filter-on input** または **filter-on output** コマンドを使用して作成したバイト・フィルター・リスト、ホスト・ネーム・フィルター・リスト、およびフィルターを削除するのに使用します。このコマンドは、バイトおよびホスト・ネーム・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。新規フィルター・リストの名前としてユーザーが定義した文字列も除去します。

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・リストを識別するのに使用されるユーザー定義の文字列です。

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・ネーム・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・リストを識別するのに使用されるユーザー定義の文字列です。

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、その結果生じたフィルター番号のギャップを埋めます。

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、その結果生じたフィルター番号のギャップを埋めます。

例: delete filter output 2

Disable

disable コマンドは、ルーター上の NetBIOS ネームおよびバイト・フィルターをグローバルに使用不可にするのに使用します。

構文:

disable netbios-filtering

例: disable netbios-filtering

Enable

enable コマンドは、ルーター上の NetBIOS ネームおよびバイト・フィルターをグローバルに使用可能にするのに使用します。

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、特定のポートの着信または発信に割り当てます。

NetBIOS フィルター構成コマンド (Talk 6)

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 . . . >*

このコマンドは、特定のポートの着信パケットに、1 つまたは複数のフィルター・リストを割り当てます。割り当てられたフィルターが、指定のポートに着信したすべての NetBIOS パケットに適用されます。

Port# は、ルーター上の構成されたブリッジ・ポート番号です。ポート番号は、このフィルターを識別します。ポート番号のリストを見たい場合は **list** を入力します。 Filter-list は、**create** コマンドを使用して以前に入力した文字列です。このポートに他のフィルター・リストを追加する場合は、AND または OR をすべて大文字で入力した後、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もできます。複数の演算子を入力する場合は、すべての演算子を同じコマンド行に一度に入力することが必要です。

このコマンドによって作成されたフィルターは、指定のポートに着信するすべての NetBIOS パケットに適用されます。コマンド行上の各フィルター・リストは、存在する演算子も含めて、左から右に評価されます。フィルター・リストの Inclusive (包含) の評価は「真」の状態と同等であり、Exclusive (排他) の評価は「偽」の状態と同等です。フィルター・リストの評価結果が「真」の場合、パケットはブリッジされます。そうでない場合、パケットはフィルター (廃棄) 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、このフィルターのすべてのホスト・ネーム・フィルター・リストは『Inclusive』 「真」と指定されます。指定のポート番号の着信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 input 2 newyork AND boston`

output *port# filter-list <operator filter-list . . . >*

このコマンドは、ポートの発信パケットに 1 つまたは複数のフィルターを割り当てます。このフィルターが、そのポートから発信されるすべての NetBIOS パケットに適用されます。

Port# は、ルーター上の構成されたブリッジ・ポート番号です。ポート番号は、このフィルターを識別します。ポート番号のリストを見たい場合は **list** を入力します。Filter-list は、create コマンドを使用して以前に入力された文字列です。任意選択の演算子は、すべて大文字で AND または OR のいずれかを入力します。演算子が存在する場合は、その後にフィルター・リスト名が必要です。ポート番号は、このフィルターを識別するのに使用します。

注: 複数の演算子を使用することも可能です。これは、複合フィルターを作成します。1 つまたは複数の演算子が存在する場合、それらはすべて同じコマンド行に一度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、指定のポート番号から発信されるすべての NetBIOS パケットに適用されます。コマンド行上の各フィルター・リストは、存在する演算子も含めて、左から右に評価されます。フィルター・リストの Inclusive (包含) の評価は「真」の状態と同等であり、Exclusive (排他) の評価は「偽」の状態と同等です。フィルター・リストの評価結果が「真」の場合、パケットはブリッジされます。そうでない場合、パケットはフィルター (廃棄) 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、このフィルターのすべてのホスト・ネーム・フィルター・リストは『Inclusive』 「真」と指定されます。指定のポート番号の発信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

list NetBIOS フィルター・コマンドは、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のに使用します。

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であるか、使用不可であるかを表示します。

NetBIOS Filter Lists
構成されたフィルター・リストのユーザー定義名 (ハンドル) を表示します。タイプの欄の 『Name』 はホスト・ネーム・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
割り当てられたポート番号と各フィルターの方向 (着信または発信) を表示します。Filter List Handles (フィルター・リスト・ハンドル) は、フィルターを構成しているフィルター・リストの名前を表示します。

Update

update コマンドは、ホスト・ネーム・フィルターまたはバイト・フィルター・リストの情報を追加または削除するのに使用します。フィルター・リストは、以前に create byte (or name) filter-list プロンプトを使用して入力した文字列です。このコマンドは `NetBIOS Byte (or Name) filter-list Config>` プロンプトを表示し、指定のフィルター・リストの更新タスクを実行できるようにします。このプロンプトで、バイトおよびホスト・ネーム・フィルター・リストのフィルター項目を追加、削除、表示、または移動することができます。また、このプロンプトから、各フィルター・リストのデフォルト値を Inclusive または Exclusive に設定することもできます。

add サブコマンドを使用して、フィルター・リスト内のフィルター項目を作成します。最初に作成されたフィルター項目には番号 1 が割り当てられ、次の項目には番号 2 が割り当てられるという具合になります。add サブコマンドの入力を正常に完了すると、ルーターは追加されたばかりのフィルター項目の番号を表示します。

注: フィルター・リストに追加されるフィルター項目が多くなるほど処理時間が増えて (リスト内の各フィルター項目を評価するの時間がかかるため)、NetBIOS トラフィックが多いときには性能に影響が出る可能性があります。

フィルター・リストのフィルター項目を指定する順序は、それによってフィルター項目をパケットに適用する方法が決まるので重要です。最初の一致が見つかると、フィルター項目の適用は中止され、フィルター・リストが Inclusive (包含) または Exclusive (排他) として評価されます (一致したフィルター・リストの Inclusive または Exclusive 指定に基づいて)。フィルター・リストのフィルター項目がどれも一致しなかった場合は、フィルター・リストのデフォルト状態 (Inclusive または Exclusive) が戻されます。

delete サブコマンドは、フィルター・リストから削除するフィルター項目の数を指定します。delete サブコマンドが実行された場合、リストに生じた穴が埋められます。たとえば、フィルター項目 1、2、3、および 4 が存在し、フィルター項目 3 が削除された場合、フィルター項目 4 は 3 に番号変更されます。

default サブコマンドは、フィルター・リストのデフォルト設定を Inclusive または Exclusive に変更することもできます。フィルター・リストが Inclusive として評価された場合、パケットはブリッジされます。そうでない場合、パケットはフィルターに掛けられます。

move サブコマンドは、フィルター・リスト内のフィルター項目の番号を変更するのに使用できます。move サブコマンドの最初の引き数は、移動するフィルター・リストの番号です。move サブコマンドの 2 番目の引き数は、最初のフィルター・リストの移動先のすぐ前のフィルター・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、以前に **create byte-filter-list** コマンドを使用して入力した文字列で

す。このコマンドは、次の NetBIOS BYTE filter-list Config> コマンド・レベルに移動します (例を参照)。このレベルで、指定されたフィルター・リストの更新タスクを行うことができます。

例: update byte-filter-list newyork

```
NetBIOS Byte newyork Config>
```

このプロンプト・レベルでは、いくつかのコマンドを実行できます。利用可能な各コマンドは、『**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*

ネーム・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、ネーム・フィルター・リストを指定することを除けば、byte-filter-list コマンドと同じです。filter-list パラメーターは、以前に create name-filter-list プロンプトを使用して入力した文字列です。このコマンドは、次の NetBIOS Name filter-list Config> コマンド・レベルに移動します (例を参照)。このレベルで、指定されたフィルター・リストの更新タスクを行うことができます。

例: update name-filter-list accounting

```
NetBIOS Name accounting Config>
```

このプロンプト・レベルでは、いくつかのコマンドを実行できます。利用可能な各コマンドは、『**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)

この節には、**update byte-filter-list** コマンドで利用可能なコマンド・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 パケットと一致した場合、それが属するフィルター・リストは Inclusive (真) として評価されます。

- Byte-offset は、フィルターに掛けられるパケット内のオフセットを示すバイト数 (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。
- Hex-pattern は、NetBIOS ヘッダーのバイト・オフセットから始まるバイトと比較するのに使用される 16 進数です。16 進パターンの構文規則は、前に 0x を含まない最大 32 桁の偶数の 16 進数です。
- Hex-mask (存在する場合) は、16 進パターンと同じ長さでなければならず、パケット内のバイト・オフセットから始まるバイトと論理 AND された後、その結果が 16 進パターン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には、すべてが 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とパターンが NetBIOS パケット内に存在しないバイト数を表している場合 (つまり、バイト・フィルター・リストの設定時に予定された長さよりパケットが短い場合)、そのパケットにはフィルター項目は適用されず、パケットはフィルターに掛けられません。1 つの NetBIOS フィルター・リストが一連のバイト・フィルター項目を用いて設定

されている場合、NetBIOS フィルター・リスト内のいずれかのバイト・フィルター項目が、NetBIOS パケット内に存在しないバイト数を表しているときには、フィルター処理のためのパケットのテストは行われません。

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、フィルター項目と NetBIOS パケットの比較結果が一致したときは、フィルター・リストは Exclusive (偽) として評価されることを除いて、add inclusive コマンドと同じです。このコマンドを使用してバイト・オフセットを 4 に、バイト・パターンを 09 に指定することにより、データグラム同報通信パケットを廃棄するように指定することができます。

- Byte-offset は、フィルターに掛けられるパケット内のオフセットを示すバイト数 (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。
- Hex-pattern は、NetBIOS ヘッダーの byte-offset オフセットから始まるバイトと比較される 16 進数です。16 進パターンの構文規則は、前に 0x を含まない最大 32 桁の偶数の 16 進数です。
- Hex-mask (存在する場合) は、16 進パターンと同じ長さでなければならず、パケット内のバイト・オフセットから始まるバイトと論理 AND された後、その結果が 16 進パターン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には、すべてが 2 進数の 1 とみなされます。

バイト・フィルター項目のオフセットとパターンが NetBIOS パケット内に存在しないバイト数を表している場合 (つまり、バイト・フィルター・リストの設定時に予定された長さよりパケットが短い場合)、そのパケットにはフィルター項目は適用されず、パケットはフィルターに掛けられません。1 つの NetBIOS フィルター・リストが一連のバイト・フィルター項目を用いて設定されている場合、NetBIOS フィルター・リスト内のいずれかのバイト・フィルター項目が、NetBIOS パケット内に存在しないバイト数を表しているときには、フィルター処理のためのパケットのテストは行われません。

例: add exclusive

```
Byte Offset  [0] ?
Hex Pattern  [] ?
Hex Mask  (<CR> for no mask)  [] ?
```

default include

フィルター・リストのデフォルト設定を 『inclusive』 に変更します。このコマンドは、フィルター・リスト内のどのフィルター項目も、フィルターの対象となるパケットのコンテンツ (内容) と一致しない場合、フィルター・リストは Inclusive として評価されることを示します。これがデフォルト設定です。

default exclude

フィルター・リストのデフォルト設定を 『exclusive』 に変更します。このコマンドは、フィルター・リストのどのフィルター項目も、フィルターの対象となるパケットのコンテンツと一致しない場合、フィルター・リストは Exclusive として評価されることを示します。

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 command 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を再順序付けします。filter-item1 で指定された番号のフィルター項目が移動され、filter-item2 の直後の番号に変更されます。

exit 直前のコマンド・プロンプト・レベルに戻ります。

Update Name-Filter-List (コマンド・オプション)

以下の節には、update name-filter-list コマンドで利用可能なコマンド・オプションをリストします。

add inclusive *ASCII host-name <LAST-hex number>*

ホスト・ネーム・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・ネーム・フィールドが、このコマンドで指定された host-name と比較されます。次のリストは、比較の方法を示しています。

- ADD_GROUP_NAME_QUERY: 発信元 NetBIOS ネーム・フィールドが調べられます。
- ADD_NAME_QUERY: 発信元 NetBIOS ネーム・フィールドが調べられます。
- DATAGRAM: あて先 NetBIOS ネーム・フィールドが調べられます。
- NAME_QUERY: あて先 NetBIOS ネーム・フィールドが調べられます。

一致している場合 (このコマンドで指定されたワイルドカードも考慮して)、フィルター・リストは Inclusive として評価されます。一致していない場合、そのフィルターのフィルター・リスト (もしあれば) 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 ネーム・フィルターによってサポートされている 4 つのタイプの 1 つでない場合、パケットはブリッジされます。

- Host-name は、最高 16 文字の長さの ASCII 文字列です。疑問符 (?) を host-name 内で使用すると、1 文字をワイルドカードで示すことができます。アスタリスク (*) を host-name の最後の文字として使用すると、host-name の残りの文字をワイルドカードで示すことができます。host-name に含まれている文字数が 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。Host-name には、次のものを除く任意の文字を含めることができます。

  . / \ [ ] : | < > + = ; , <space>

注: Host-name は、大文字小文字の区別をします。

- host-name に含まれている文字数が 16 文字より少ない場合は、LAST-hex-number を使用できます。これは、この値を最後の文字として使用することを示す 16 進数 (前に 0x が付かない) です。16 文字より少ないホスト・ネームに LAST 引き数を指定しない場合には、『?』 ワイルドカードが 16 番目の文字として供給されます。

add inclusive HEX *hexstring*

ホスト・ネーム・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 コマンドと同等です。ただし、ホスト・ネームの表現が異なっています。このコマンドでは、ホスト・ネームを一連の 16 進数 (前に 0x が付かない) として指定します。

- Hexstring は、偶数の 16 進数から構成されていることが必要です。ユーザーが完全に 32 桁の 16 進数を指定しない場合、29 番目と 30 番目の数字には ASCII ブランクが埋め込まれ、31 番目と 32 番目 (16 番目のバイト) の数字としてワイルドカードが供給されます。1 バイトのワイルドカードは **??** によって指定できます。

add exclusive ASCII *host-name <LAST-hex-number>*

ホスト・ネーム・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、パケットがこのフィルター項目に一致するとフィルター・リストが Exclusive の結果になることを除いて、add inclusive ASCII コマンドと同等です。

- Host-name は、最高 16 文字の長さの ASCII 文字列です。疑問符 (?) を host-name 内で使用すると、1 文字をワイルドカードで示すことができます。アスタリスク (*) を host-name の最後の文字として使用すると、host-name の残りの文字をワイルドカードで示すことができます。host-name に含まれている文字数が 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。Host-name には、次のものを除く任意の文字を含めることができます。

  . / \ [ ] : | < > + = ; , <space>

- host-name に含まれている文字数が 16 文字より少ない場合は、LAST-hex-number を使用できます。これは、この値を最後の文字として使用することを示す 16 進数 (前に 0x が付かない) です。16 文字より少ない host-name に LAST 引き数が指定されていない場合には、**?** ワイルドカードが 16 番目の文字として供給されます。

add exclusive HEX *hexstring*

ネーム・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、パケットがこのフィルター項目に一致するとフィルター・リストが Exclusive の結果になることを除いて、add inclusive hex コマンドと機能的に同等です。

- Hexstring は、偶数の 16 進数から構成されていることが必要です。ユーザーが完全に 32 桁の 16 進数を指定しない場合、29 番目と 30 番目の数字には ASCII ブランクが埋め込まれ、31 番目と 32 番目 (16 番目のバイト) の数字としてワイルドカードが供給されます。1 バイトのワイルドカードは **??** によって指定できます。

default include
フィルター・リストのデフォルト設定を 『inclusive』 に変更します。このコマンドは、フィルター・リストのどのフィルター項目も、フィルターの対象となるパケットのコンテンツと一致しない場合、フィルター・リストは Inclusive として評価されることを示します。これがデフォルト設定です。

default exclude
フィルター・リストのデフォルト設定を 『exclusive』 に変更します。このコマンドは、フィルター・リストのどのフィルター項目も、フィルターの対象となるパケットのコンテンツと一致しない場合、フィルター・リストは Exclusive として評価されることを示します。

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 command 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を再順序付けします。filter-item1 で指定された番号のフィルター項目が移動され、filter-item2 の直後の番号に変更されます。

exit 直前のコマンド・プロンプト・レベルに戻ります。

NetBIOS フィルターの監視

この章では、NetBIOS フィルター監視コマンドについて説明します。これらのコマンドを使用して、ASRT ブリッジングへの追加フィーチャーとして NetBIOS フィルター情報を監視および表示することができます。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 の両方に影響を与えます。

ASRT および DLSw NetBIOS フィルター監視環境へのアクセス

ASRT 監視環境から NetBIOS> 監視プロンプトを表示するには、 ASRT> プロンプトから **netbios** コマンドを入力します。

```
+ protocol asrt

ASRT> netbios
NetBIOS Support User monitoring

NetBIOS monitoring> set filters name or byte

NetBIOS filter>
```

NetBIOS フィルター監視コマンド (Talk 5)

DLSw 監視環境から NetBIOS> 監視プロンプトを表示するには、次のように入力します。

```
+ 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・コマンドをリストしています。

表 14. NetBIOS フィルター監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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。xxixページの『下位レベル操作環境の終了』 を参照してください。

List

list NetBIOS フィルター・コマンドは、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のに使用します。

構文:

list byte-filter-lists

filters

name-filter-lists

byte-filter-lists

指定されたバイト・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。

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 状態を判別するときに、フィルター項目は番号順に評価されます。

Inc/Ex フィルター項目のデフォルト状態を指定します。

Byte-offset フィルターに掛けられるパケット内のオフセットを示すバイト数 (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 ヘッダーのバイト・オフセットから始まるバイトと比較するのに使用される 16 進数。16 進パターンの構文規則は、前に 0x を含まない最大 32 桁の偶数の 16 進数です。

Mask 存在する場合、16 進パターンと同じ長さでなければならず、パケット内のバイト・オフセットから始まるバイトと論理 AND された後、その結果が 16 進パターン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には、すべてが 2 進数の 1 と見なされます。

filters 構成されたすべてのフィルターに関連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

指定されたネーム・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。

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 状態を判別するときに、フィルター項目は番号順に評価されます。

Inc/Ex フィルター項目のデフォルト状態を指定します。

Type 『ASCII』 は、ASCII 文字として追加されたホスト・ネーム・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・ネーム・フィルター項目を示します。

Host-name 最高 16 文字の長さの ASCII 文字列。疑問符 (?) を ホスト・ネーム内で使用すると、1 文字をワイルドカードで示すことができます。アスタリスク (*) をホスト・ネームの最後の文字として使用すると、ホスト・ネームの残りの文字をワイルドカードで示すことができます。ホスト・ネームに含まれている文字数が 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・ネームには、次のものを除く任意の文字を含めることができます。

. / \ [ ] : | < > + = ; , <space>

Last char ホスト・ネームに含まれている文字数が 16 文字より少ない場合に使用します。これは、この値を最後の文字として使用することを示す 16 進数 (前に 0x が付かない) です。16 文

字より少ないホスト・ネームに LAST 引き数を指定しない場合には、『?』 ワイルドカードが 16 番目の文字として供給されます。

第10章 LAN ネットワーク・マネージャー (LNM) の使用

この章では、IBM の ASRT LAN ネットワーク・マネージャー (LNM) について説明します。本章には、以下の節が含まれています。

- 『LNM について』
- 『LNM エージェントと機能』
- 206ページの『LNM 構成の制約事項』

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のに使用します。これを用いて、リング、ブリッジ、および個々のリング・ステーションの動作を監視することができます。

ブリッジ上のソフトウェア・エージェントによって収集された情報を LNM 管理ステーションで利用可能になります。もう少し具体的に説明すると、LNM エージェントは収集された情報を IBM 専有プロトコルである LAN 報告機構 (LRM) と呼ばれる別のエージェントを介して転送します。情報の転送は、LAN ネットワーク・マネージャーへの LLC2 コネクションを介して行われます。

LNM エージェントと機能

LNM エージェントとその機能は、次のとおりです。

- 構成報告サーバー (CRS) - リング・トポロジーの変更とリング・ステーションの状態を LNM に報告します。
- リング・パラメーター・サーバー (RPS) - リング・パラメーター情報 (リング番号、ソフト・エラー報告タイマー値、および物理的位置を含む) を求めるリング・ステーションからの要求にサービスします。
- リング・エラー・監視 (REM) - リング・ステーションからエラー報告を収集し、それを分析します。限界値を超過すると、REM はエラー情報を LNM に転送することができます。
- 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。これらのリンクを経由する他のエージェントとの間の情報転送も管理します。

204ページの図25 は、IBM ブリッジ、LNM エージェント、および IBM LNM ステーション間のコネクションを示しています。

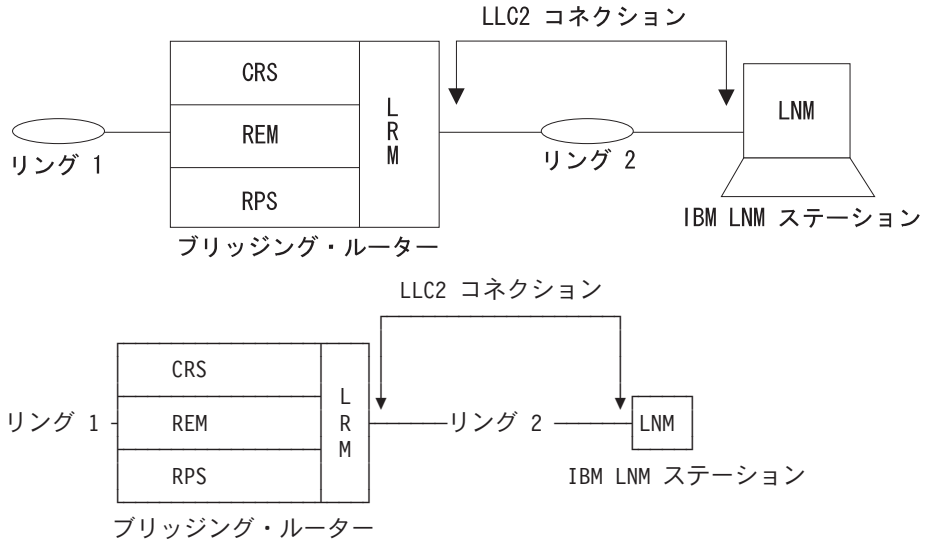


図 25. LNM ステーションとエージェント

以下の節では、各 LNM エージェントについて詳しく説明します。

構成レポート・サーバー

LNM から要求があると、CRS はリング・ステーションの状態を入手して LNM に転送します。CRS は、リング・ステーション・パラメーターを設定したり、リングからステーションを除去したりするのに使用します。

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・ステーションの状態を要求すると、CRS は MAC フレームを作成し、それをステーションに送って情報を入手します。このとき、CRS は次のフレームをリング・ステーションに送ります。

- 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・ステーション接続要求 MAC フレーム

リング・ステーションが応答すると、CRS はその情報を正しくフォーマットされた LLC2 フレームに入れて LNM に転送します。

CRS は、LNM からの要求に応じて、リング・ステーションをリングから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、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、除去に成功したか失敗したかを示すレスポンスを LNM に戻します。

CRS は、新規のアクティブ・モニター報告 MAC フレームを受信すると、その情報を LNM に転送します。NAUN (次のアクティブ・アップストリーム近隣) 変更報告 MAC フレームを受信したときには、この情報も報告します。CRS エージェントは、リング・ステーション MAC レイヤーが MAC フレームを CRS に転送するときに使用できる独自の機能アドレスを持っています。

リング・パラメーター・サーバー

RPS はリング・ステーションをリングに挿入します。リング・ステーションが新たにリングに挿入されると、次のことが起こります。

- 新規ステーションが、初期化要求 MAC フレームをそのリングの RPS に送信します。この MAC フレームには、そのステーションに関するいくつかの情報が入っています。
- RPS は、リング・ステーション初期化 MAC フレーム (リング番号とソフト・エラー報告 MAC フレームの送信間に待つ時間間隔が入っている) で応答します。初期化要求フレームから新たに入手された情報は LNM に渡され、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されます。
- RPS は、LNM からの状態を求める要求にも応答します。リング番号、RPS バージョン情報、およびソフト・エラー報告タイマー値が LNM に戻されます。

RPS 機能は、他のリング・ステーションからこの機能あてに送信された MAC フレームを受信するための関連の機能アドレスを持っています。

重要: ステーションがリングへの挿入を試みるときに、初期化要求 MAC フレームをそのリングのリング・パラメーター・サーバー (RPS) に送信します。このフレームが RPS によって正常にコピーされた場合、ステーションはリング・ステーション初期化 MAC フレームの受信を待ちます。このフレームを受信しなかった場合、ステーションはリングに挿入しません。

LNM 用に構成されている装置がリング・パラメーター・サーバーになり、リング・ステーション初期化 MAC フレームの送信できなくなるような輻輳 (ふくそう) 状態に入った場合、ステーションはリングへの挿入に失敗する可能性があります。この問題の解決策は、影響を受けるポート上の RPS を使用不可に設定することです。RPS が使用可能になっておらず、どのサーバーも初期化要求フレームをコピーしない場合、発信元ステーションはレスポンスを待たずにリングに挿入します。

リング・エラー・モニター

REM は接続されたトークンリングの動作を監視し、ハード・エラーおよびソフト・エラーを検出します。それらを LRM に報告し、エラーの原因を特定するのを助けます。ハード・エラーが検出されると、次のことを行います。

- ハード・エラーは、リング上でビーコン MAC フレームを受信することによって検出されます。
- 障害ドメイン内のステーションは、自動的にリングから離れることにより、問題を訂正しようと試みます。
- REM はハード・エラー状態が訂正されたか否かを判別し、その結果を LNM に報告します。

REM はソフト・エラーを次のようにして監視します。

- ソフト・エラー MAC フレームが定期的にリング・ステーションから REM に送信され、各種の断続的障害 (たとえば、CRC エラーや周波数エラー) が発生した回数が通知されます。

- ステーションのソフト・エラーが所定の限界値を超えると、REM はこの状態を LNM に報告します。
- また、REM はソフト・エラー報告 MAC フレームを監視し、受信側輻輳 (ふくそう) 状態を検出します。受信側輻輳 (ふくそう) とは、受信バッファーの不足のためにリング・ステーションがフレームを廃棄することを示します。
- ステーションが受信側輻輳 (ふくそう) を報告した回数が所定の限界値を超えると、REM はこの状態を LNM に報告します。受信側輻輳 (ふくそう) 状態が正常に戻ると、受信側輻輳 (ふくそう) が終了したことを LNM に通知します。

LAN 報告機構

LRM は、LNM とエージェントのコネクションを制御します。LRM は、それ自体と各接続 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 間の LLC2 コネクションです。

LNM とエージェント間の通信はすべて報告リンクを介して行われます。LRM は報告リンクへの適切なエージェントとの間で管理データをやり取りします。最高 4 つまでの報告リンクがサポートされます。1 つは *制御リンク* として指定され、その他の 3 つは *監視リンク* として指定されます。

制御リンクを介して接続された LNM は、利用可能なすべての動作を実行できます。監視リンクによって接続された LNM は、利用可能な動作うちの限定されたサブセットしか実行できません。

LNM 構成の制約事項

IBM 2212 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。

常に、LNM エージェントと LNM ステーションは、メッセージが 2 パーティー・モデル上で受け渡されるものと想定しています。しかし、LNM は現行構成と整合させるために、ブリッジ・ポート単位で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・ポート上で使用可能にすることができます。LNM が使用可能にされて各ポートに対して LNM のインスタンスが 1 つ作成されます。

2 トークンリング構成では、他方のポートは常に疑似アドレスとして指定されます。これをマルチポート・ブリッジと呼んでいます。これは、バーチャル・リングあるいはシリアル・ライン・インターフェースに相当します。

IBM 2212 ブリッジが 2 つのソース・ルーティング・トークンリング・ポートを持っている場合にのみ、2 ポート・モデル・ブリッジの他方のポートは、実アドレスを持つトークンリングです。

LNM マネージャー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、マネージャー・ステーションによって要求された場合、「パケット転送」および「パケット廃棄」性能データ統計を報告することができます。マネージャー・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・クラス 2 サポート

LAN では、データ・リンク・レイヤーは、媒体アクセス制御 (MAC) とリンク・レイヤー制御 (LLC) の 2 つのサブレイヤーから構成されます。LLC は 2 つのタイプのサービスを提供します。

- LLC1 (タイプ 1) - 非確認形コネクションレス・サービス
- LLC2 (タイプ 2) - 1 組のコネクション型サービス

LAN ネットワーク・マネージャー (LNM) は、LLC2 コネクション型サービスを必要とします。LLC2 は以下の機能を提供します。

- 新規データ・リンク・コネクションを開始する
- データ・リンク・コネクションを管理する
- データを順序通りに (保証された形で) 交換する
- 確立されたコネクション上で、あるレベルのフロー制御を実行する
- サービス利用者から要求されたとき、または回復不能リンク・エラー時に、リンク・コネクションを終了する

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・マネージャー (LNM) の構成および監視

この章では、IBM による LAN ネットワーク・マネージャー (LNM) の ASRT 実現方式について説明します。本章には、以下の節が含まれています。

LNM の構成

この節では、ブリッジング・ルーター上の LNM フィーチャーの基本構成手順の要約を示します。

1. ネットワーク・マネージャー・ソフトウェアに必要な MAC アドレスを入手する。

   ASRT> プロンプトで **list lnm ports** コマンドを入力して、ネットワーク・マネージャー・ステーション上で実行されるネットワーク・マネージャー・ソフトウェアに必要な MAC アドレスを入手します。たとえば、次のように入力します。

   ```
   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、太字体で表示) は、ネットワーク・マネージャーが、ルーター内に存在する LNM エージェントを構成するのに使用します。

   注: これらのアドレスは、出力の表示通りに正確に入力することが必要です。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します。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。たとえば、次のように入力します。

   ```
   LNM config>enable lnm
   Port Number [1]? 1
   ```

   デフォルト設定では、すべての LNM エージェントが使用可能になります。

3. 使用可能にされた LNM エージェントを表示して、構成をチェックします。構成されたポート上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。たとえば、次のように入力します。

   ```
   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 構成コマンドと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、LNM のネットワーク・パラメーターの構成および監視を行うことができます。

構成コマンドは LNM config> プロンプトで入力します。このプロンプトにアクセスするには、次のようにします。

```
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 は、LNM コマンドをリストしています。

表 15. LNM コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Disable	指定のポート上のすべての LNM エージェント、または指定のポート上の指定された LNM エージェント (RPS、CRS、または REM) を使用不可にします。 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を使用不可にします。ブリッジ内の LNM のすべてのインスタンスに対してグローバルに適用されます。 このコマンドは構成にのみ使用されます。
Enable	指定のポート上のすべての LNM エージェント、または指定の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対してグローバルに適用されます。 このコマンドは構成にのみ使用されます。
List	指定のポートの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に使用されます。
Set	指定の報告リンク番号のパスワードを設定します。 このコマンドは構成にのみ使用されます。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Disable

disable コマンドは、指定のポート上のすべての LNM エージェント (RPS、CRS、または REM) を使用不可にするのに使用します。

このコマンドは、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、報告リンク・パスワードの設定も使用不可にします。

構文:

disable *agent port#*

lnm . . .

configuration-remote-change

agent *port#*

指定のポート上の指定された LNM エージェント (RPS、CRS、または REM) を使用不可にします。ポートが構成されていない場合は、メッセージ `LNM not configured for port XX` が表示され、このコマンドは無効です。

例: **disable REM 1**

lnm 指定のポート上の LNM を使用不可にします。LNM 用のポートが構成されていない場合は、メッセージ `LNM not configured for port XX` が表示され、この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・パスワードの設定を使用不可にします。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対してグローバルに適用されます。

例: **disable configuration-remote-change**

```
CONFIGURATION-REMOTE-CHANGE: disabled
```

Enable

指定のポート上のすべての LNM エージェント、または指定のポート上の指定された LNM エージェント (CRS、REM、または RPS) 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、メッセージ `Port number XX is not token-ring` が表示され、コマンドは無効になります。

ポートが構成されていない場合は、メッセージ `Port number XX does not exist` が表示され、コマンドは無効になります。

指定されたエージェントがすでに指定のポートに対して使用可能にされている場合は、メッセージ `Already enabled` が表示されます。

このコマンドは、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、報告リンク・パスワードの設定も使用可能にします。

構文:

enable *agent port#*

lnm . . .

configuration-remote-change

agent *port#*

指定の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#*

指定のポート上のすべての LNM エージェントを使用可能にします。

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・パスワードの設定を使用可能にします。デフォルト設定では、リモートから LNM 構成パラメーターの設定を使用不可にします。

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対して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し、ブリッジに構成されているパスワードも表示します。このコマンドは ASRT> プロンプトで入力します。

構文:

list password

port . . .

password

ブリッジの報告リンクに構成されているパスワードを表示します。リモート LNM アプリケーションによってパスワードを変更できるか否かを表示します。

例: **list password**

```
Reporting Link     Password
0             87654321
1             MADRAS
2             ABC1234
3             123ABC
CONFIGURATION-REMOTE-CHANGE: Disabled
```

port *port#*

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・ポートの場合、指定されたポートで使用可能にされている 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 構成の状態に関する情報を表示します。このコマンドは ASRT> プロンプトで入力します。

構文:

list bridge

lnm ports

source-routing configuration

bridge

指定されたポートの LNM が使用可能にされているかどうかを表示します。

例: **list bridge**

lnm ports

ブリッジング・ルーターで使用可能にされている LNM の構成に関する情報を表示します。

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

指定されたポートの LNM が使用可能にされてい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のパスワードを設定します。リンク番号は 0、1、2、または 3 を使用できます。リンク 0 は、制御リンクに使用します。リンク 1、2、および 3 は、監視リンクに使用します。

パスワードは 6 ～ 8 文字から構成し、LNM がブリッジとの報告リンクを確立するときに使用したパスワードと一致していることが必要です。リンクのパスワードが設定されていない場合は、デフォルト文字列の 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・サービスの構成および監視

この章では、TCP/IP ホスト・サービス (TCP/IP ホスト) プロトコルの構成方法、および TCP/IP ホスト構成コマンドの使用法について説明します。本章には、以下の節が含まれています。

- 『基本構成手順』
- 216ページの『TCP/IP ホスト構成環境へのアクセス』
- 216ページの『TCP/IP ホスト構成コマンド』
- 219ページの『TCP/IP ホスト監視環境へのアクセス』
- 219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を詳しく知りたい場合は、49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 ルーティング用のルーターを構成している場合は、本章を使用しないでください。代わりに、227ページの『第13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は、インターフェースに IP アドレスを構成することはできません。ルーターは IP 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にのみ使用されます。

基本構成手順

以下の節では、2212 上の 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・サービスを最小構成するには、**set ip-host** コマンドを使用して 2212 に IP アドレスを割り当てます。この IP アドレスは、1 つのインターフェースに関連付けられるのではなく 2212 全体に関連します。

デフォルト・ゲートウェイの追加

2212 は、デフォルトのゲートウェイを使用して、2212 が直接接続されているブリッジ・ネットワーク上に存在しないホストおよびゲートウェイと通信します。2212 は、ICMP ルーター・ディスカバリー (本章の **enable router-discovery** コマンドの項を参照) または RIP (本章の **enable rip-listening** コマンドの項を参照) を使用して、動的にデフォルト・ゲートウェイを確認することができます。また、**add default gateway** コマンドを使用して、静的に 1 つまたは複数のデフォルト・ゲートウェイを指定することも可能です。2212 は一度に 1 つだけのデフォルト・ゲートウェイを使用します。その他のデフォルト・ゲートウェイはバックアップ用に使用されます。

割り当てた IP アドレスおよびデフォルト・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** コマンドを使用します。2212 をリスタートした後で、TCP/IP-Host config> プロンプトに戻ります。

TCP/IP ホスト・サービスの使用可能化

2212 IP アドレスおよびデフォルト・ゲートウェイ情報の割り当てと保管が完了したら、**enable services** コマンドを使用して TCP/IP ホスト・サービスを使用可能にします。

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ます。

```
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では、 TCP/IP ホスト・ブリッジのネットワーク・パラメーターを指定することができます。構成コマンドを起動するには、ルーターをリスタートします。TCP/IP 構成コマンドは TCP/IP-Host config> プロンプトで入力します。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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	デフォルト・ゲートウェイを追加します。
Delete	デフォルト・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・ディスカバリー・プロセス、および RIP listen を使用不可にします。
Enable	TCP/IP ホスト・サービス、ルーター・ディスカバリー・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	2212 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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、デフォルト・ゲートウェイ (つまり、ルーター) を構成に追加するのに使用します。

デフォルト・ゲートウェイは、ローカル接続の外の IP あて先にパケットを送信しようとするときに使用されます。その場合、転送 (リダイレクト) 処理を通してルーティング・テーブルが作成されます。見えないルーターを検出するための試みがなされ

ます。ネットワーク上で 2212 がブートされている場合 (TFTP/BootP を介して)、ブート・プロセスからの情報を使用してデフォルト・ゲートウェイが構成されます。

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

delete コマンドは、デフォルト・ゲートウェイを 2212 構成から削除するのに使用します。**delete** コマンドの後に、削除したいデフォルト・ゲートウェイの IP アドレスを入力します。

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

disable コマンドは、以下の TCP/IP 機能を使用不可にするのに使用します。

- TCP/IP ホスト・サービス
- ルーター・ディスカバリー・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不可にします。デフォルトでは、RIP-listening は使用不可です。

例: disable rip-listening

router-discovery

ICMP ルーター・ディスカバリー・メッセージを受信することによりデフォルト・ゲートウェイを確認 (learn) する機能を使用不可にします。デフォルトでは、ルーター・ディスカバリーは使用可能です。

例: disable router-discovery

services

TCP/IP ホスト・サービス・プロトコル全体を使用不可にします。IP ルーティングが使用可能でない場合、TCP/IP ホスト・サービスはデフォルトにより使用可能にされます。

例: `disable services`

Enable

enable コマンドは、以下の TCP/IP 機能を使用可能にするのに使用します。

- TCP/IP ホスト・サービス
- ルーター・ディスカバリー・プロセス
- RIP listen

構文:

enable rip-listening
router-discovery
services

rip-listening

ブリッジが RIP プロトコルを 『listen』 すること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。デフォルトでは、RIP-listening は使用不可にされます。

例: `enable rip-listening`

router-discovery

ICMP ルーター・ディスカバリー・メッセージの受信を通してデフォルト・ゲートウェイを確認することを使用可能にします。デフォルトでは、ルーター・ディスカバリーは使用可能です。

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 ルーティングが使用可能でない場合、TCP/IP ホスト・サービスはデフォルトにより使用可能にされます。

例: `enable services`

List

list コマンドは、現行 TCP/IP ホスト構成に関する情報を表示するのに使用します。

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-Host IP アドレスを表示します。
Address mask	現行の IP-Host IP サブネット・アドレス・マスクを表示します。
Default Gateway IP-address(es)	現行のデフォルト・ゲートウェイ 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であるか使用不可であるかを表示します。
RIP-LISTENING	RIP-LISTENING が使用可能であるか使用不可であるかを表示します。
Router Discovery	ルーター・ディスカバリーが使用可能であるか使用不可であるかを表示します。

Set

set コマンドは、2212 の IP アドレスを設定するのに使用します。前もって 2212 に IP アドレスを割り当てないと、TCP/IP ホスト・サービスを使用可能にすることはできません。

注: まだ IP アドレスが構成されていない場合、(デフォルトにより) ブート情報を使用して設定されます。このプロセスは 2212 が IP ホストとして稼働するネットワーク・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 2212 上の TCP/IP ホスト・サービスを監視する方法について説明します。

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ます。

```
+ 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して、アクティブ端末からパラメーターを表示したり、情報要求を入力したり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。220ページの表17 は、コマンドを要約しています。

表 17. TCP/IP ホスト監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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 2212 の IP アドレスを表示します。
Ping	指定のあて先に継続的に PING し、受信した各レスポンスを 1 行に印刷します。
Traceroute	指定のあて先へのルートをホップごとに表示します。
Routers	2212 が知っているすべての 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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Dump

dump コマンドは、現行の IP ルーティング・テーブルを表示するのに使用します。各あて先につき 1 行が印刷されます。表示されるエントリーの多くは ICMP 転送の結果です。

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導出されたかを示すルート・タイプ

  RIP - ルートは RIP プロトコルを通して確認された

  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
: ルート・コストを表示します。

Age
: RIP ルートの場合、ルートが更新された以降の時間を秒数で表示します。他のタイプのルートの場合、ルートがインストールされた以降の時間を秒数で表示します。

Next Hop
: あて先ホストに向かうパス上の次のルーターの IP アドレスを表示します。パケットを転送するために送信側ルーターによって使用されたインターフェース・タイプも表示されます。

Default gateway
: デフォルト・ゲートウェイの IP アドレスが、ルート・タイプ、コスト、エージ、およびそのエントリーに関連するネクスト・ホップ情報と共に表示されます。

Routing table size	現行テーブルの現行サイズ (ネットワーク数とバイト数) が表示されます。ホストに判明しているネットワークの数 (nets) も識別します。

Interface

interface コマンドは IBM 2212 の IP アドレスを表示するのに使用します。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場合、単一のアドレスが端末で 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 であり、ブリッジを示します。
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・サブネット・マスクを表示します。

Ping

ping コマンドは、ルーターに ICMP エコー要求を指定のあて先に毎秒 1 回送信させ (『pinging』)、レスポンスを監視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の障害を分離するのに使用できます。

このプロセスは連続的に実行され、パケットが追加されるごとに ICMP シーケンス番号が増分されます。対応する受信 ICMP エコー・レスポンスが、シーケンス番号および往復時間と共に報告されます。往復時間の計算の細分性 (タイム・レゾリューション) はプラットフォーム特有であり、通常は約 20 ミリ秒です。

PING プロセスを停止するときは、端末で任意の文字を入力します。このとき、パケット紛失、往復時間、および到達不能 ICMP あて先の数の要約が表示されます。

マルチキャスト・アドレスをあて先として指定した場合は、送信されたパケットに対して複数のレスポンス (各グループ・メンバーにつき 1 つ) が印刷される場合があります。戻された各レスポンスが、応答側の発信元アドレスと共に表示されます。

PING のサイズ (ICMP ヘッダーを除いた、ICMP メッセージ内のデータ・バイト数)、TTL 値、および PING の速度は、すべてユーザーによる構成が可能です。デフォルト値は、サイズが 56 バイト、TTL が 64 、速度は毎秒 1 PING 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

traceroute コマンドは、指定のあて先へのパス全体をホップごとに表示するのに使用します。連続する各ホップごとに、traceroute コマンドは 3 つのプローブを送信し、応答側の IP アドレスとそのレスポンスに関連した往復時間を印刷します。特定のプローブがレスポンスを受信しなかった場合、アスタリスク (*) が印刷されます。ディスプレイの各行はこの 3 つのプローブ・セットに関連しており、左端の数字は、コマンドを実行したルーターからの距離 (ルーター・ホップ数) を示します。

traceroute は、あて先に到着した時点、ICMP Destination Unreachable メッセージを受け取った時点、またはパス長が 32 ルーター・ホップに達した時点で完了します。

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
```

表示で、

TRACEROUTE	あて先エリア・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ってくるまでにかかった往復時間を示す最初のトレース。パケットは 3 回トレースされます。
Destination unreachable	あて先への利用可能なルートがないことを示します。
1 * * * 2 * * *	ルーターはあて先からの何らか形でのレスポンスを期待しているが、あて先は何も応答しないことを示しています。

プローブが予期しない結果を受け取った場合は (前の出力例を参照)、何種類かの表示が印刷されます。これらの表示について、下の表で説明します。

!N ICMP Destination Unreachable (net unreachable) を受信したことを示します。
!H ICMP Destination Unreachable (host unreachable) を受信したことを示します。
!P ICMP Destination Unreachable (protocol unreachable) を受信したことを示します。

! あて先に到達したが、あて先にから受信した応答の TTL が 1 であることを示します。これは通常、あて先のエラーを示しており (UNIX の一部のバージョンでよく見られます)、そのためあて先はプローブの TTL を応答に挿入しています。残念ながら、この結果、最終的にあて先に到達する前にアスタリスクだけから成る多数の行が生じることになります。

Routers

routers コマンドは、IBM 2212 が知っているすべての IP ルーターのリストを表示するのに使用します。ルーターは、以下を通して確認することができます。

- 静的構成 (216ページの『Add』 ページで説明した **add default-gateway** コマンドを使用して)。
- 受信した ICMP 転送
- ICMP ルーター・ディスカバリー・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)

各ルーターが、その発信元、優先順位 (デフォルト・ルートを選択するときに使用した)、および存続時間 (ルーターから再応答がない場合に無効と宣言されるまでの秒数) と共にリストされます。

構文:

routers

例: `routers`

第2部 ルーター・プロトコルの構成および監視

第13章 IP の使用

この章ではインターネット・プロトコル (IP) を構成する方法について説明します。本章には、以下の節が含まれています。

- 『基本構成手順』
- 246ページの『BOOTP/DHCP 転送プロセスの構成』
- 248ページの『UDP 転送の構成』
- 248ページの『バーチャル・ルーター冗長度プロトコルの構成』
- 251ページの『冗長デフォルト IP ゲートウェイの構成』
- 251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 プロトコルを起動して実行するために必要な初期ステップについて概説します。構成変更についての詳細は、本章の他の節で説明しています。個々の構成コマンドについての詳細は、本章のコマンドの節で説明しています。以下のリストは、ルーター上の IP を起動するための初期構成作業の概要を示しています。これらの作業を完了した後で、新規構成を有効にするために、ルーターをリスタートする必要があります。

1. IP 構成環境にアクセスする (255ページの『IP 構成環境へのアクセス』を参照してください)。
2. IP アドレスをネットワーク・インターフェースに割り当てる (228ページの『IP アドレスのネットワーク・インターフェースへの割り当て』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 (231ページの『動的ルーティングの使用可能化』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)。(233ページの『静的ルーティング情報の追加』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)。(236ページの『ARP サブネット・ルーティングの使用可能化』を参照してください。)
6. ARP パラメーターを設定する (必要な場合)。(235ページの『ARP 構成の設定』を参照してください。)
7. IP 構成プロセスを終了する。
8. 構成変更を起動するためにルーターをリスタートする。

以下の節では、それぞれの構成タスクについて詳しく説明します。

IP アドレスのネットワーク・インターフェースへの割り当て

IP 構成 **add address** コマンドは、IP アドレスをネットワーク・インターフェースに割り当てるのに使用します。このコマンドの引き数には、インターフェース番号 (Config> **list devices** コマンドら入手) と、IP アドレスおよび関連のアドレス・マスクが含まれます。

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 と関連のアドレス・マスク 255.255.255.0 (サブネット指定の 3 番目のバイトを使用) が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 1 つのネットワーク・インターフェースに割り当てることも可能です。

デフォルトでは、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、それぞれ異なるネットワークまたはサブネット内に存在しなければなりません。**enable same-subnet** コマンドを使用すれば、この制約を取り除くことができます。

IP は、伝送路に実 IP アドレスを割り当てずに、シリアル・ライン・インターフェースを IP トラフィック用に使用することができます。ただし、各シリアル・ラインに疑似 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、ルーターによってインターフェースを参照するのに使用されますが、外部で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・ラインに 0.0.0.*n* フォーマットのアドレスを割り当てます。ただし、*n* はインターフェース番号 (Config> **list devices** コマンドから入手) です。このアドレス・フォーマットは、該当のインターフェースが *非番号制シリアル・ライン* であることをルーターに知らせます。

インターフェースに IP アドレスを割り当てずに、シリアル・ライン・インターフェース番号 2 の IP を使用可能にするには、次のコマンドを使用します。

```
IP config> add address 2 0.0.0.2
```

IP アドレスのブリッジ・ネットワーク・インターフェースへの割り当て

2212 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 パケットを発送し、ブリッジングが構成されているが、IP アドレスが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。2212 は、ブリッジング・インターフェースから IP データグラムを受信し、IP データグラムをブリッジング・インターフェースに送信し、ブリッジング・インターフェースとルーティング・インターフェース間で IP パケットを発送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、2212 上でこれらの機能を使用可能にすることができます。ブリッジ・ネットワークは、2212 が接続されてい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、**add address** コマンドを使用し、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 アドレスを任意の個別のブリッジング・インターフェースに割り当てるのではなく、実質的にすべてのブリッジング・インターフェースに割り当てます。

ブリッジ・ネットワーク・インターフェースに IP アドレスを割り当てると、 2212 上で物理ネットワーク・インターフェース (物理ポート) の 1 つを解放することができます。これを理解するには、最初に 図26 を検討してください。この図は、それぞれルーター機能とブリッジ機能を実行する別個の装置をもつ IP インターネットワークを示しています。LAN 2 および LAN 3 は、ブリッジによって接続され、ブリッジされたネットワークを形成します。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。

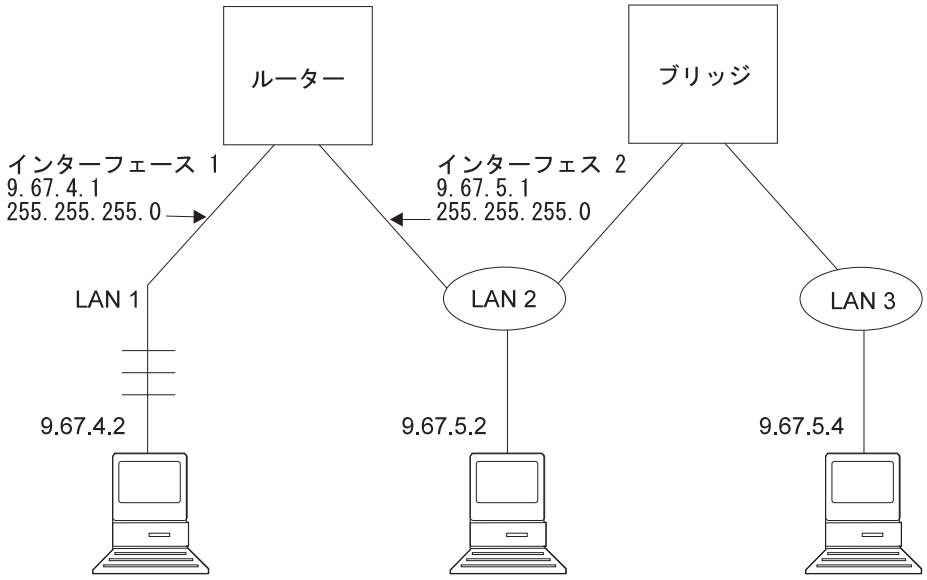


図 26. ブリッジされたネットワークへのルーティング - 選択肢 1

230ページの図27 は、同じインターネットワークだが、ルーター機能とブリッジ機能が単一の装置に結合された場合を示しています。この図では、ルーターは、ブリッジされたネットワークへの、ルーター自体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) をまだ保持しています。

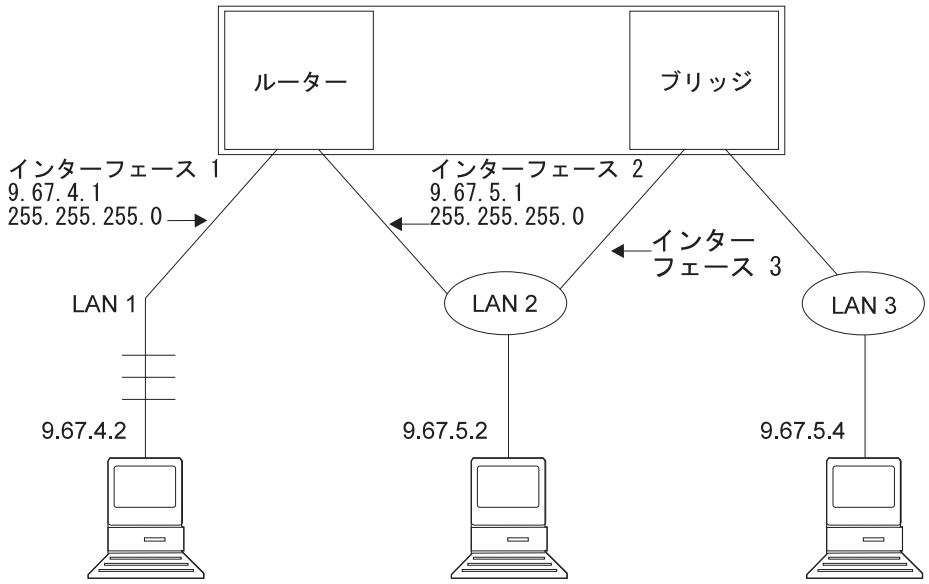


図 27. ブリッジされたネットワークへのルーティング - 選択肢 2

最後に、図28 では、ブリッジされたネットワークへのルーターの物理ネットワーク・インターフェースは、内部インターフェースである、ブリッジ・ネットワーク・インターフェースによって置き換えられています。これは図 図26 および 図27 で示されたのと同じインターネットワークですが、ルーターは、ブリッジされたネットワークへの、それ自体の物理ネットワーク・インターフェースをもはや必要としません。

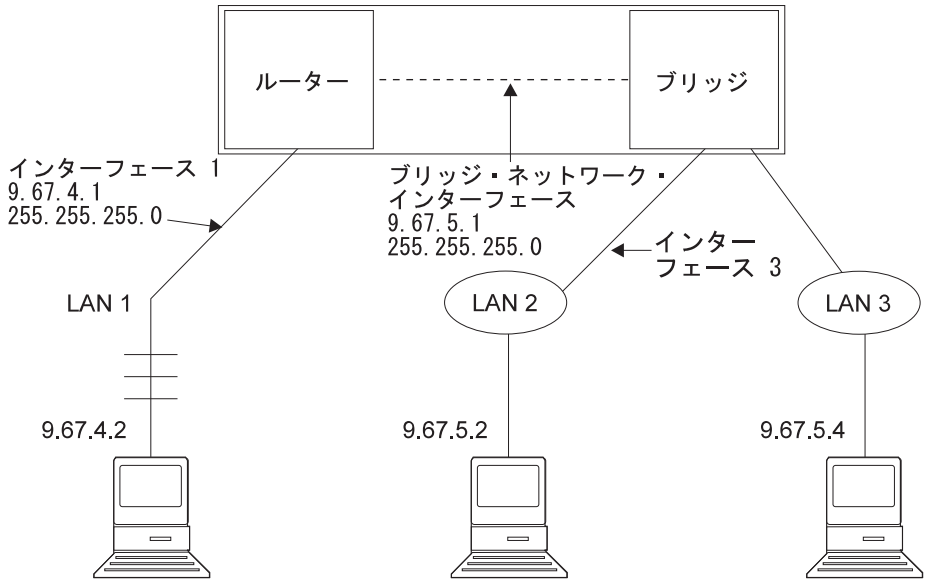


図 28. ブリッジされたネットワークへのルーティング - 選択肢 3

注: ブリッジ・ネットワーク・インターフェースに IP アドレスが構成されている場合には、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・インターフェースには IP アドレスを構成できません。

内部 IP アドレスの設定

これは、どのインターフェースの状態からも独立している IP アドレスであり、どのインターフェースにも関係なく設定されます。一部の IP 構成は IP アドレスを必要とします。詳しくは、300 ページのコマンド **set internal-IP-address** を参照してください。

動的ルーティングの使用可能化

ルーターの動的ルーティングを使用可能にするには、以下の手順で行います。ルーター・ソフトウェアは、OSPF、RIPv1、および RIPv2 の内部ゲートウェイ・プロトコル (IGP) および BGP (これは、外部ゲートウェイ・プロトコル) をサポートします。

すべてのルーティング・プロトコルを同時に実行することが可能です。ただし、通常はほとんどのルーターが 1 つだけのルーティング・プロトコル (IGP の 1 つ) を実行します。OSPF プロトコルは堅固で、しかも追加 IP フィーチャー (等価コスト・マルチパスや可変長サブネットなど) をサポートするので使用が推奨されています。

ルーティング・テーブル・サイズの設定

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めたすべてのソースからのルーティング・テーブルのエントリー数を決めます。デフォルト・サイズは 768 エントリーです。

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ます。ルーティング・テーブル・サイズの設定が小さ過ぎると、ルートが廃棄されてしまいます。設定が大き過ぎると、メモリー資源の使用が非効率的になります。稼働後に、コンソール **dump** コマンドを使用してテーブルのコンテンツを表示し、必要に応じてサイズを調整して、若干の拡張の余地を残した値に設定します。

OSPF プロトコルの使用可能化

OSPF 構成は、専用の構成コンソール (Config> **protocol ospf** コマンドを使用して入ります) を介して行います。OSPF を使用可能にするには、次のコマンドを使用します。

```
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見積もりを入力するように求められます。これは OSPF 用として確保しておく必要があるメモリー量の概略値をルーターに知らせます。ユーザーは、OSPF リンク状態データベースのサイズを見積もるために必要な、次の 2 つの値を供給することが必要です。

- 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・ドメイン内の OSPF ルーターの総数

これらの値は、次のプロンプトで入力します (値の例を記入してあります)。

```
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ます。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
```

一連の動作パラメーターを入力するように促されます。各インターフェースに、コストおよびその他の OSPF 動作パラメーターを割り当てます。

OSPF 以外に他の IP ルーティング・プロトコルも実行している場合は、OSPF と他のプロトコル間のルートの交換を使用可能にすることもできます。これを行うには、次のコマンドを使用します。

```
OSPF Config> enable AS-boundary-routing
```

OSPF 構成プロセスについての詳細は、323ページの『第15章 OSPF の使用』を参照してください。

RIP プロトコルの使用可能化

この節では、RIP プロトコルを最初に構成するときの方法を説明します。RIP プロトコルを構成するときに、各 IP インターフェース上でルーターが公示する、または受け入れる (あるいは、その両方のための) 1 組のルートを指定することができます。

RIP は、X.25 ネットワーク・インターフェース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では、RIP の代わりに OSPF を内部ゲートウェイ・プロトコル (IGP) として使用します。

最初に、次のコマンドを使用して RIP プロトコルを使用可能にします。

```
IP config> enable RIP
```

RIP が使用可能になると、以下のデフォルト動作が設定されます。

- ルーターは、構成された各 IP インターフェースから送信する RIP 更新に、すべてのネットワークおよびサブネットを含める。デフォルト・ルートおよび静的ルートは含めません。
- ルーターは、構成された各 IP インターフェースで受信したすべての RIP 更新を処理する。
- RIP は、デフォルト・ルートおよび静的ルートをオーバーライドしない。

デフォルトの送信/受信動作を変更するには、以下の IP 構成コマンドを使用します。これらは各 IP インターフェースごとに定義します。

```
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 プロトコルの使用可能化

BGP プロトコルは、専用の構成プロンプト 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* の BGP4 の使用および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の追加

この手順は、上記の動的ルーティング・プロトコルのいずれからも入手することができないルーティング情報の場合にのみ必要になります。静的ルーティング情報は電源障害の後も存続し、決して変更されないまたは動的に確認できないルートに使用します。

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*) によって記述します。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。たとえば、IP アドレス 10.0.0.0 およびマスク 255.0.0.0 をもつルートは、10.0.0.0 ～ 10.255.255.255 の IP アドレスに適用されます。あて先へのルートは、ネクスト・ホップ・ルーターの IP アドレス (*next-hop*) およびこのルート上でパケットを転送するコスト (*cost*) によって記述されます。

静的ルートを作成、変更、または削除するには、次のコマンドを使用します。

```
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
```

これらのコマンドでは、1 つの IP あて先につき最高 4 つの静的ルートを定義できるので、1 つまたは複数のルートに障害が起きた場合に代替ルートを使用することが可能です。これらのコマンドは即時に有効になり、ルーターをリブートする必要はありません。

最長の一致規則

ルートのあて先には、IP アドレス・マスクが含まれるので、複数のルートが特定の IP アドレスと一致する可能性があります。たとえば、 IP アドレス 10.1.2.3 の場合、IP アドレス 10.0.0.0 およびマスク 255.0.0.0 をもつルートは IP アドレス 10.1.0.0 およびマスク 255.255.0.0 をもつルートの両方に一致します。どちらのルートを使用するか決定するには、最長の一致規則が適用されます。最長のマスクをもつルート (この場合では、 IP アドレス 10.1.0.0 およびマスク 255.255.0.0 をもつルート) が使用されます。

デフォルト/ネットワーク/サブネット/ホスト・ルート

ルートは、IP アドレスおよびマスクに応じて、*デフォルト*、*ネットワーク*、*サブネット*、または *ホスト* として分類されます。

デフォルト ・ルートは IP アドレス/マスク 0.0.0.0/0.0.0.0 をもちます。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、最長の一致規則により、他に一致するルートがない場合のみ使用されます。次のコマンドにより、静的デフォルト・ルートを作成します。

```
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>
```

静的デフォルト・ルートは、**set default network-gateway** コマンドによって設定することもできます。ただし、このコマンドは即時には有効にならないので、 1 つだけのデフォルト静的ルートを定義することができます。次の例では、上記の **add route** コマンドと同じ静的デフォルト・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 のマスクは、RFC-791 で定義された IP アドレス・クラスによって指定された、ルートのあて先 IP アドレスの値によって異なります。

IP アドレス・クラス	IP アドレス範囲	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

add route、**change route**、および **delete route** コマンドは、あて先 IP アドレスに対応するネットワーク・マスクをデフォルトのマスク値として使用します。次のコマンドにより、静的ネットワーク・ルートを作成します。

```
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** コマンドによって設定することもできます。ただし、このコマンドは即時には有効にならないので、あて先ごとに 1 つだけの静的ルートを定義することができます。次の例では、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>
```

サブセット・ルート のマスクは、ルートのあて先 IP アドレス用のネットワーク・マスクより大きくなります。次のコマンドにより、静的サブネット・ルートを作成します。

```
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 アドレスへのルートで、 255.255.255.255 のマスクをもちます。次のコマンドにより、静的ホスト・ルートを作成します。

```
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の間の相互作用

OSPF および RIP プロトコルを通して動的に確認されたルートは、静的ルートをオーバーライドできます。RIP プロトコルの場合、このオーバーライド機能を使用不可にすることも可能です。**enable/disable override static-routes** コマンドに関しては、本章の RIP の項を参照してください。

OSPF および RIP は両方とも、構成された静的ルートを、これらの動的プロトコルが使用可能になっているインターフェースを介して公示するように構成できます。

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ます。

```
IP config> enable sending static-routes ip-interface-address
```

静的ルートを公示するように 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ます。

```
OSPF Config> enable as boundary
Import static routes? yes
```

ネクスト・ホップ認識

ネクスト・ホップ認識は、近隣ルーターがアップであるかダウンであるかをルーターが検出できるようにします。このオプションが使用可能のときは、ルーターは、近隣ルーターをネクスト・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できます。また、ネクスト・ホップが複数のネットワーク・インターフェース上に定義された IP サブネット内に存在する場合、ルーターは、静的ルートのネクスト・ホップにはどのネットワーク・インターフェースを介して到達できるかを判別することもできます。

特定の IP インターフェース上のネクスト・ホップ認識を使用可能にするには、IP 構成プロンプトで次のコマンドを入力します。

```
IP config> enable nexthop-awareness ip-interface-address
```

特定の IP インターフェース上のネクスト・ホップ認識を使用不可にするには、IP 構成プロンプトで次のコマンドを入力します。

```
IP config> disable nexthop-awareness ip-interface-address
```

ネクスト・ホップ認識は、近隣ルーターが逆 ARP をサポートするフレーム・リレー・ネットワーク上でのみサポートされます。

ARP 構成の設定

アドレス解決プロトコル (ARP) は、ルーターがパケットを転送する前に、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のに使用されます。ARP はルーター上で常にアクティブなので、デフォルト特性を使用して使用可能にする場合は、追加構成は何も必要ありません。ただし、ARP 構成パラメーターを変更する必要

がある場合 (たとえば、デフォルト・リフレッシュ・タイマーを変更する **enable auto-refresh** または **set refresh-timer**)、あるいは固定アドレス・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、579ページの『第26章 ARP の使用』を参照してください。

インターフェース上で LAN エミュレーションが構成されている場合は、デフォルトが適用されます。何も変更しなくても、ARP プロトコルを効果的に使用できます。

ARP サブネット・ルーティングの使用可能化

接続されたサブネット・ネットワーク上に、IP サブネット化をサポートしないホストが存在する場合は、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 で説明) を使用します。ルーターは、ARP サブネット・ルーティング用に構成されている場合、あて先 (つまり、ルーター自身があて先への最善ルートであり、あて先が発信元と同じナチュラル・ネットワーク上に存在する場合は、LAN の外) の ARP 要求に対してプロキシーによって応答します。正しく動作するためには、サブネット化をサポートしないホストが含まれている LAN に接続されたルーターはすべて、ARP サブネット・ルーティング用に構成することが必要です。

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ます。

```
IP config> enable arp-subnet-routing
```

ARP ネットワーク・ルーティングの使用可能化

一部の IP ホスト ARP は、あて先が発信元と同じナチュラル・ネットワーク内に存在するかどうかに関係なく、すべてのあて先に適用されます。このようなホストの場合は、ARP サブネット・ルーティングでは不十分なので、そのあて先がルーターから到達可能であり、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、ルーターがどの ARP 要求に対してもプロキシーによって応答するように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ます。

```
IP config> enable arp-network-routing
```

IP フィルター

フィルターは、ルーターがパケット転送を制御するのに使用する特定の基準を指定することができます。ユーザーのセキュリティーおよび管理上の目的を達成するのに役立つように、次の 2 種類のフィルターが提供されています。

- アクセス制御
- ルート・フィルター

アクセス制御

アクセス制御では、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することができます。

- 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
- 優先順位およびサービス・タイプ (TOS) フィルター

アクセス制御は、IP ホストとサービスの特定の組み合わせが相互に通信する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できます。1 つのグローバル・リストと、インターフェース当たり 2 つのリストを指定できます。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・フィルターとも呼ばれます) は、名前が割り当てられており、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では、一方のリストは着信パケットに適用され、もう一方は発信パケットに適用されます。リストは相互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* することができても、グローバル・リストによって *廃棄* されることもあります。

図29 は、転送される前にパケットが通過する必要がある一連のアクセス制御リストを示しています。

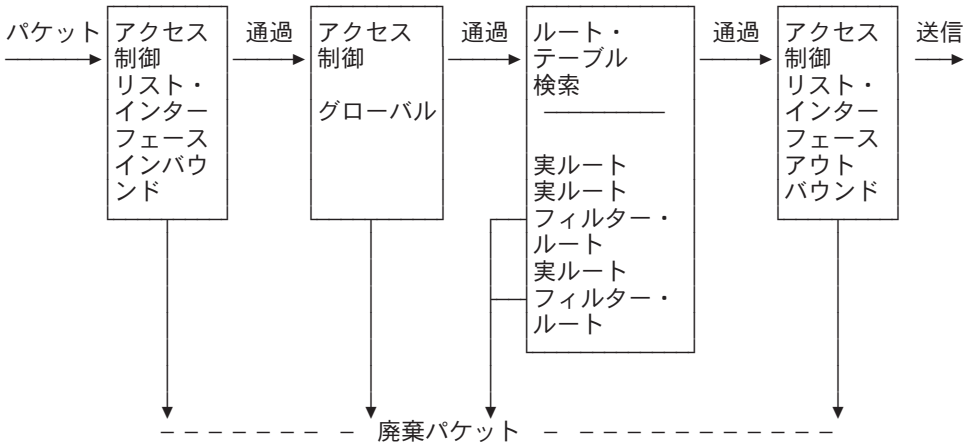


図 29. パケット転送パスにおけるアクセス制御リスト

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した 1 つまたは複数のアクセス制御規則から成っています。一部の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影響を与えるグローバル・フィルターを定義し、その他の規則はインターフェースに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る) を定義します。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されます。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されます。つまり、フィルターを定義するには **add packet-filter** コマンドを、フィルターを構成するには **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過するときに、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。規則内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している場合、パケットは規則に一致します。パケットが規則に一致し、規則が「包含」の場合、そのパケットは *通過* します。規則が「排他」の場合は、パケットは *廃棄* され、ルーターはそれ以上の処理を行いません。リスト全体を照合し終わっても一致する規則がなかった場合にも、パケットは廃棄されます。

アクセス制御リストにレコードを定義する際には、以下の情報に注意することが大切です。

- リスト内のレコードの順序は重要です。リスト内のレコードの順序を変更するための構成コマンドが用意されています。
- 少なくとも 1 つのアクセス制御規則を含む各リストには、任意のパケットがそのリストを通過できるようにするための包含規則が存在することが必要です。指定された規則のどれにも一致しないパケットが通過できるようにするための 1 つの方法は、次のワイルドカード規則を、リストの最後の規則として含めることです。

```
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]):
```

アクセス制御の使用可能化

IP アクセス制御 (グローバル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** コマンドを使用し、使用不可にするには **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されているときに、特定のパケットを使用可能および使用不可にするには、**enable packet-filter** コマンドおよび **disable packet-filter** コマンドを使用することができます。

IP アクセス制御が使用可能になっている場合、ルーターが発信および受信するパケットに注意する必要があります。ルーターによって発信または受信される RIP または OSPF パケットを、フィルターで除去してしまわないようにします。そのための最も簡単な方法は、ワイルドカード包含規則を、アクセス制御リストの最後に追加することです。代わりに、RIP および OSPF 用の特定の規則を (限定的なアドレスとマスクを指定して) 追加する方法を取ることもできます。一部の OSPF パケットは、クラス D マルチキャスト・アドレス 224.0.0.5 および 224.0.0.6 あてに送信されることに

注意してください。これは、ルーティング・プロトコルに対してアドレス検査が実行される場合に重要になります。アクセス制御の詳細については、 **add** コマンドの項を参照してください。

グローバル・アクセス制御リストの定義

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表示、移動、または削除することができます。詳細については、これらのコマンドの説明を参照してください。

パケット・フィルターの定義

インターフェースに固有のパケット・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、フィルターの名前、方向 (入力または出力)、および適用するインターフェース番号を入力するよう求めます。

```
IP config> add packet filter
Packet-filter name [ ]?  test
Filter incoming or outgoing traffic? [IN]? in
Which interface is this filter for [0]? 1
```

list packet-filter コマンドを使用すれば、ルーターに構成されているすべてのインターフェース専用アクセス制御リストを表示することができます。

パケット・フィルター用のアクセス制御規則のセットアップ

定義された各リスト (パケット・フィルター) に対して、アクセス制御規則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、着信または発信トラフィックに対して何も効果がありません。アクセス制御規則を定義するには、 IP config> プロンプトで **update packet-filter** コマンドを使用します。ルーターは最初に、更新したいパケット・フィルターの名前を入力するよう指示します。すると、IP config> プロンプトは Packet-filter 'name' Config> に代わります。ただし、'name' は、ユーザーが入力したリスト名です。

```
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変更するのに使用されるコマンドと同様です。

アクセス制御規則用のパラメーター

アクセス制御規則は複数のパラメーターから構成されます。一部のパラメーターは、すべてのアクセス制御規則で指定することができるのに対し、その他のパラメーターはパケット・フィルター用の規則でのみ指定することができます。以下のパラメーターは、すべてのアクセス制御規則で指定することができます。

- タイプ (inclusive、exclusive)

- IP 発信元アドレスおよびマスク
- IP あて先アドレスおよびマスク
- IP プロトコル番号の範囲
- TCP/UDP あて先ポート番号の範囲
- TCP/UDP 発信元ポート番号の範囲
- TCP SYN フィルター
- ICMP メッセージ・タイプおよびコード
- 優先順位および TOS フィルター・サポート
- ポリシーに基づいたルーティング (次のホップ・ゲートウェイの選択)
- セキュリティー・ログ・オプション

以下のパラメーターはパケット・フィルター専用です。

- パケット・フィルター名
- 発信元アドレスの検証
- 追加のタイプ: IP セキュリティー (IPsec) およびネットワーク・アドレス変換 (NAT)
- IPsec トンネル ID

Type

アクセス制御規則のタイプは、それに一致するパケットに何を行うかを定義します。*exclusive* (E) 規則はパケットを廃棄します。*inclusive* (I) 規則は、パケットがルーターによってさらに処理されることができるようにします。ネットワーク・アドレス変換 *(network address translation)* または NAT (N) 規則は、パケットを NAT に通過させて、アドレス変換させます。出力パケット・フィルター内の *IP* セキュリティー *(IP security)* または IPsec (S) 規則は、パケットを IPsec に通過させて IPsec トンネル内でカプセル化させるか、場合によっては暗号化させます。入力パケット・フィルター内の IPsec 規則は、パケットが正しい IPsec トンネルを通じて受信されたことを検証します。NAT および IPsec 規則は、パケット・フィルター内でのみ、かつ包含 (inclusive (IN または IS)) と組み合わせて指定されたときのみ有効です。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。

さらに、NAT および IPsec は、同じ規則 (INS) 内で指定することができます。出力パケット・フィルター内の INS 規則は、一致するパケットが最初は NAT によって、次は IPsec によって処理されるようにします。入力パケット・フィルター内の INS 規則は、最初に、一致するパケットが正しい IPsec トンネルから受信されたことを検証し、次に NAT によって処理されるようにします。

IP 発信元およびあて先アドレス

各規則には、IP 発信元アドレスとあて先アドレスの両方について、IP アドレスとマスクの組みが入っています。IP パケットがアクセス制御レコードと比較されるときに、パケット内の IP アドレスが規則内のマスクと AND され、その結果が規則内のアドレスと比較されます。たとえば、アクセス制御規則内の発信元アドレスが 26.0.0.0 で、マスクが 255.0.0.0 のときは、最初のバイトが 26 のすべてのIP 発信元アドレスと一致します。あて先アドレスが 192.67.67.20 で、マスクが 255.255.255.255 のとき

は、IP あて先ホスト・アドレス 192.67.67.20 としか一致しません。アドレスが 0.0.0.0 でマスクが 0.0.0.0 は、どの IP アドレスとも一致するワイルドカードです。

IP プロトコル番号

各レコードには、IP プロトコル番号範囲も含めることができます。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 の範囲を指定した場合は、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 発信元およびあて先ポート番号

IP プロトコル番号範囲に 6 (TCP) または 17 (UDP) が含まれる場合、TCP/UDP ポート番号範囲も、発信元ポートおよびあて先ポートの両方について、アクセス制御規則内で指定することができます。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。指定の範囲 (最初と最後の番号を含む) 内のポート番号値が一致することになります。IP パケットが TCP または UDP パケットでない場合、これらのフィールドは無視されます。0 ～ 65535 の範囲を指定した場合は、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のリストは、RFC 1700 (割り当て番号) を参照してください。

TCP コネクション確立 (SYN) フィルター

プロトコル番号範囲に 6 (TCP の場合) が含まれ、フィルター・タイプが排他 (exclusive) である場合、TCP コネクション確立フィルターを設定することができます。TCP コネクション確立フィルターが使用可能にされるとき、アクセス制御規則が TCP パケットに適用されるのは、そのパケットが TCP コネクションを確立する場合のみです。(これらは TCP SYN ビットが 1 で、ACK ビットが 0 であるパケットです。)

ICMP メッセージ・タイプおよびコード

プロトコル番号範囲に 1 (ICMP の場合) が含まれている場合には、ICMP メッセージ・タイプおよびコードを指定することができます。デフォルトは、アクセス制御規則をすべての ICMP メッセージ・タイプおよびコードに適用することです。

優先順位および TOS フィルター・サポート

TOS をサポートするルーターは、要求されたレベルのサービスを提供する特定ルートの識別を済ませています。このルーターは、TOS ビットの設定に応じて、ルートを介してパケットを送信します。

IP に TOS が入っていると、特定のサービス・タイプが保証されるのではなく、要求したサービス・タイプの提供がルーターに要求されます。たとえば、最大スループットを必要とする TOS フィールドをもつパケットを、異なる帯域幅をもついくつかのホップを介して送信することができます。そのようなパケットが TOS をサポートしないルーターによって管理されるホップを介して渡された場合には、通常のサー

ビスが行われます (つまり、特別な処理は行われません)。これらのパラメーターの説明については、256 ページの **add access-controls** コマンドを参照してください。

帯域幅予約 (BRS) 機能を使用して、TOS ビットに基づいて QoS を提供するようフィルターを設定することもできます。BRS は、PPP およびフレーム・リレー・インターフェースと一緒に使用します。*AIS 機構の使用と構成*の 『帯域幅予約と優先待ち行列の使用』 および 『帯域幅予約の設定と監視』 を参照してください。

TOS に基づくルーティング・サポートのパラメーター: ルーターが TOS ビットを解釈し、それらのビットに従ってパケットのルートを定められるようにするために、アクセス制御規則を作成すると、ルーターは、その規則に従って、フィルターとサービス・タイプのルーティング用に TOS パケットを受け取ります。この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。ルーターが比較する TOS ビットを定義するのに使用されるパラメーターは、次のものです。

- TOS バイト・ビットの範囲開始値
- TOS バイト・ビットの範囲終了値
- 範囲に含まれる TOS バイトのビットを判別するためのフィルター・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、グローバル・アクセス制御規則を作成すると、ルーターは、この規則に従って、変更される TOS パケットを受け取ります。TOS ビットの値の変更は、それら値の解釈とパケットのルーティングとはベルのアクティビティーです。解釈と変更の両方が設定されている場合、解釈の後で変更が行われます。変更される TOS ビットを定義するのに使用されるパラメーターは、次のものです。

- TOS ビットの新しい値
- 変更される TOS バイトのビットを判別するための変更マスク

ポリシーに基づくルーティング (ネクスト・ホップ・ゲートウェイの選択)

インバウンド・パケットにフィルターを掛けて、そのあて先を、手動で選択したネクスト・ホップ・ゲートウェイ・アドレス (ポリシー・ベース・ルーティングと呼ばれます) に指定することができます。これを行うには、ルーターについては、包括的なインバウンド・アクセス制御規則をグローバルに作成するか、特定のインターフェースについては、以下のパラメーターを提供してください。

- ポリシー・ベース・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・ホップが使用不可な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どうか

SysLog 機能オプション

SysLog とは、リモート・ログ・サーバーに SysLog メッセージを生成するログ・オプションです。SysLog が使用可能にされている場合、SysLog 機能オプションは、リモート・ログ用に使用されている SysLog 機能を指定します。デフォルトが *User* である、このオプションは、リモート・ログ・ファイルを定義します。このファイルに

SysLog メッセージを保管し、後で分析することができます。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することができます。

セキュリティー・ログ・オプション

セキュリティー・ログを使用可能にする場合、以下のログ・オプションのいずれかまたはすべてを指定することができます。

- ELS メッセージ
- SNMP トラップ
- SysLog

指定された場合、ELS メッセージおよび Syslog は *short (短い)* または *long (長い)* メッセージ・フォーマットを使用することができます。SNMP トラップは、*enabled (使用可能)* または *disabled (使用不可)* にすることができます。ログ・オプションが指定されない場合、セキュリティー・ログが使用不可にされます。

SysLog 優先順位も構成することができます。これは、 *Emergency (緊急)* 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。default (デフォルト) は、ルーター・システムのデフォルト値です。 SysLog 優先順位レベルは、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することができます。

SysLog メッセージは、リモート・サーバーに送信され、現行の SysLog 機能オプションの SysLog ファイルに保管されます。

パケット・フィルター名

このインターフェース専用パラメーターは、任意の名前で構成することができます。名前は、最大 16 文字の長さで、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・フィルター名ごとに最大 2 つのアクセス制御レコード・リストを構成することができます。1 つは発信パケット用、1 つは着信パケット用です。

発信元アドレスの検証

この入力パケット・フィルター・オプションは、受信されたパケットの発信元 IP アドレスが、 IP ルーティング・テーブルに基づき、パケットがそこから受信されたインターフェースと矛盾していないことを検証します。このオプションは、IP ホストに属していない発信元 IP アドレスを使用している (スプーフィング と呼ばれる動作) 不正な動作を行う IP ホストからのパケットの転送を防ぐのに役立ちます。

IPsec トンネル 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・フィルターでは、一致するパケットが送信されるときに通過する IPsec トンネルの ID を指定します。入力パケット・フィルターでは、一致するパケットがそれを通じて受信されなければならなかった IPsec トンネルの ID を指定します。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、任意のホストが 192.67.67.20 の SMTP TCP ソケットにパケットを送信できます。

```
add access-control inclusive 0.0.0.0 0.0.0.0 192.67.67.20 255.255.255.255 6 6 25 25
```

次の例は、クラス B ネットワーク 150.150.0.0 のサブネット 1 上のホストは、クラス B 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ないようにします (1 バイト・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
```

このコマンドは、ルーターがすべての RIP パケットを送信および受信できるようにします。

```
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。IP アドレス 9.1.2.3 から到着したパケットの TOS ビットを解釈できるようにし、パケットを送信する前にこれらのビットの値を変更できるようにする値を入力します。TOS フィルターおよびポリシー・ベース・ルーティングを作成するパラメーターの意味については、256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 (route) フィルターは、ルーティング・テーブルのコンテンツ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、柔軟性に欠けます。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処理は、上述のアクセス制御を使用してのみ行うことができます。

このルーターは、次の方法を用いて、ルーティング・テーブルのコンテンツに影響を与えます。

- 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・ルートの定義

IP あて先をフィルター・ルート としてルーティング・テーブルに挿入するように指定することができます。これらのあて先に対しては IP パケットは転送されず、それらに関するルーティング情報は公示されません。ネットワーク上で OSPF が使用されている場合には、フィルター・ルートの使用は推奨***できません***。OSPF によって確認された内部ルートが、ルーティング・テーブル内のフィルターされたルートをオーバーライドしてしまうからです。

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ます。

```
IP config>  add filter  dest-IP-address  address-mask
```

dump コマンドを使用して IP ルーティング・テーブルを表示すると、フィルター・ルートはタイプ *fltr* のエントリーとしてリストされます。

注: より具体的なルートが利用可能な場合には、パケットは転送されます。たとえば、ネットワーク 9.0.0.0 (マスク 255.0.0.0) に対してフィルター・ルートが定義されており、そのネットワークのサブネット (たとえば、9.1.0.0、マスク 255.255.0.0) あてのルートが確認された場合、パケットはサブネット 9.1.0.0 に転送されますが、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 入力フィルターの定義

動的ルーティング・プロトコルとして RIP が使用されている場合、特定のインターフェースに対して、RIP 更新内のルートを無視するように構成することができます。

次のコマンドを使用すると、インターフェースで受信されたすべての RIP 更新が無視されます。

```
IP config>  disable receiving rip  ip-interface-address
```

次のコマンドを使用すると、インターフェースで受信された特定タイプのルートが無視されます。

```
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
```

後者のコマンド・グループを使用した場合、次のコマンドを使用すると、特定のルートを受け入れることができるようになります。

```
IP config> add accept-rip-route ip-network/subnet/host
```

ルート・テーブル・フィルターの定義

ルート・テーブル・フィルターが使用可能であり、ルート・フィルターが定義されている場合、ルートを IP ルーティング・テーブルに追加する前に、検査が行われます。追加するルートが包含ルート・フィルターに一致した場合、そのルートは IP ルート・テーブルに追加されます。排他ルート・フィルターに一致した場合、そのルートは IP ルート・テーブルに追加されません。直接ルートおよび静的ルートは、フィルターに掛けられることはありません。

ルーティング・プロトコルによってすべてのルートが利用可能として公示されるのをネットワーク管理者が望まないといった状況のときには、この機能を使用して、ルートが IP ルート・テーブルに追加されるのを防止することができます。また、サービス提供者環境で、ユーザーが相互のネットワークにアクセスするのを防止するためにこの機能を利用することもできます。

BOOTP/DHCP 転送プロセスの構成

BOOTP (RFC 951 および RFC 1542 に文書化) は、ディスクレス・ワークステーションが、その IP アドレス、ブート・ファイルの場所およびブート・サーバー・ネームを確認するために使用するブートストラップ・プロトコルです。 動的ホスト構成プロトコル (DHCP) (RFC 1541 に文書化) を使用して、再使用可能なネットワーク・アドレスおよびホスト専用構成パラメーターをサーバーから割り振ります。

BOOTP/DHCP 転送プロセスの説明では、以下の用語が役立ちます。

- *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* - これらのサービスを提供するブート・ホスト (UNIX デーモン bootpd、FTP ソフトウェアから利用可能な DOS バージョン、または OS/2 を搭載) またはその他の 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 転送機能* - クライアントとサーバー間で交換される要求/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。

以下のステップは、BOOTP 転送プロセスの例を概説しています。(DHCP 交換も同様の方法で進められます):

1. クライアントがそのイーサネット・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 に同報通信する。BOOTP は UDP の上で稼働します。
2. ローカル BOOTP リレー・エージェントが、パケットを受信し、パケットをチェックして、そのフォーマットが正しいかどうか、およびアプリケーション・ホップの最大数に達していないかを調べる。クライアントの試行時間が十分であるかもチェックします。

   注: BOOTP エージェントに到達する前に複数のホップが必要な場合、パケットは IP を介して正常にルーティングされます。他のルーターはすべて、そのパケットが BOOTP パケットであるかどうかを調べません。
3. ローカル BOOTP エージェントが、構成された各サーバーに対して個別に BOOTP 要求を転送する。この BOOTP 要求は、新規 IP ヘッダーを持ち、リレー・エージェントの IP アドレスが BOOTP 要求の本体部分にコピーされている以外は、最初にクライアントから送信されたものと同じです。
4. サーバーが要求を受信し、クライアントのハードウェア (たとえば、イーサネット) アドレスをデータベースで探す。見つかると、クライアントの IP アドレス、そのブート・ファイルの場所、およびブート・サーバー・ネームが入っている BOOTP 応答をフォーマットします。この応答を BOOTP リレー・エージェントに送信します。

5. BOOTP リレー・エージェントが応答を受信し、その ARP テーブルにクライアントのエントリーを作成して、応答をクライアントに転送する。
6. クライアントは BOOTP 応答パケット内の情報を使用し、TFTP を用いてブートを継続する。

BOOTP 転送の使用可能化/使用不可化

ルーター上の BOOTP 転送を使用可能または使用不可にするには、IP 構成プロンプトで、次のコマンドを入力します。(BOOTP 転送を使用可能にすると、ルーターは、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とサーバー間で、BOOTP または DHCP (あるいは、その両方の) 要求と応答を転送できるようになります。)

```
IP config> enable/disable bootp
```

BOOTP を使用可能にするときには、次の値を入力するように促されます。

- BOOTP 要求が送られるアプリケーション・ホップの最大数。これは、パケットを転送できる BOOTP リレー・エージェントの最大数です。サーバーまでの IP ホップの最大数では***ありません***。このパラメーターの標準値は 1 です。
- BOOTP 要求を転送する前にクライアントが再試行する秒数。このパラメーターは、*通常は使用されません。* このパラメーターの標準値は 0 です。

BOOTP 要求を受け入れた後、ルーターは BOOTP 要求を各 BOOTP サーバーに転送します。複数のサーバーが BOOTP 用に構成されている場合、ルーターはパケットを複写します。

BOOTP/DHCP サーバーの構成

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

```
IP config> add bootp-server server-IP-address
```

複数のサーバーを構成することも可能です。また、サーバーのネットワーク番号しか分からない場合、あるいは同じネットワーク・セグメント上に複数のサーバーが存在する場合にのみ、サーバーに対して同報通信アドレスを構成することができます。

IP と SNA の統合

TN3270E を使用すると、IP と SNA を統合することができます。TN3270E の詳細については、*プロトコルの構成と監視 解説書 第 2 巻* の 『APPN の使用』 という表題の章および *プロトコルの構成と監視 解説書 第 2 巻* の 『APPN の構成と監視』という表題の章を参照してください。

UDP 転送の構成

ユーザー・データグラム・プロトコル (UDP) (RFC 768 に文書化) は、インターネット・プロトコルを使用してコネクションレス・サービスを提供する、トランスポート・レイヤー・プロトコルです。UDP 転送を使用すると、ローカルに送達された UDP パケット (IBM 2212 に接続された LAN 上の UDP 同報通信など) を、特定の IP あて先に転送したり、指定同報通信 (directed broadcast) としてあて先ネットワークに転送したりすることができます。

たとえば、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 Name-Query パケットを同報通信します。ユーザーが UDP 転送を設定しない限り、ルーターはこれらのパケットを廃棄します。したがって、ルーターは同報通信パケットをローカル・ネットワークより先には転送しません。

UDP 転送の構成は、以下の手順で行います。

1. UDP あて先ポート番号と IP アドレスを追加する。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 転送を使用可能にする。

```
IP config>enable udp-forwarding
For which UDP port number [-1] 36
```

上の例では、ルーターは UDP ポート 36 で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 転送構成を表示して見たい場合は **list udp-forwarding** を入力します。

UDP 転送の使用可能化/使用不可化

ルーターの UDP 転送を使用可能または使用不可にするには、IP 構成プロンプトから、次のコマンドを入力します。(UDP 転送を使用可能にすると、ルーターは UDP 同報通信パケットを指定のアドレスに UDP ポート単位で転送することができます。)

```
IP config> enable/disable udp-forwarding port-number
```

UDP あて先の追加

UDP 転送のあて先の追加は、パケットの転送先の IP アドレスを指定し、その後にポート番号を指定して行います。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・ルーター冗長度プロトコルの構成

ホスト IP 構成では静的に構成されたデフォルト・ルートを使用するのが一般的です。これは、構成および処理のオーバーヘッドが最小限に抑え、ほとんどすべての IP 実現方式によりサポートされています。この操作モードは、一般的にエンド・ホスト IP アドレスおよびデフォルト・ゲートウェイ用の構成を提供する動的構成プロトコル

が展開される場合に使用される確率が高いようです。ただし、これから 1 つの障害点が発生します。デフォルトのルーターが失われると、破滅的な事象が発生し、使用可能な代替パスを検出することができないすべてのエンド・ホストを分離します。

バーチャル・ルーター冗長度プロトコル (VRRP) は、静的なデフォルトのルート指定環境に固有な単一の障害点を取り除くために設計されています。VRRP は、1 組のルーターが動的に相互をバックアップできるようにする選択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、これらの IP アドレスに送信されたパケットを転送します。マスターが使用できなくなるような場合、選択プロセスは転送任務での動的な引き継ぎを提供します。その場合、バーチャル・ルーター上の任意の IP アドレスがエンド・ホストにより、デフォルトの最初のホップ・ルーターとして使用されます。VRRP を使用することから得られる利点は、あらゆるエンド・ホスト上で動的ルーティングの構成またはルーター・ディスカバリー・プロトコルを必要とすることなく、より高い可用性のデフォルト・パスが得られることです。

VRRP を使用し、構成するためには、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) を最初に定義する必要があります。各 VRRP ごとに、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デフォルトの IP アドレスの所有者になります。このルーターはそのアドレスあての ARP 要求に応答し、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は、IP アドレスを所有するルーターをバックアップするよう構成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に中断を最小限に抑えるために共通 MAC アドレスが必要です。以下は、非常に単純な VRRP トポロジーの例です。

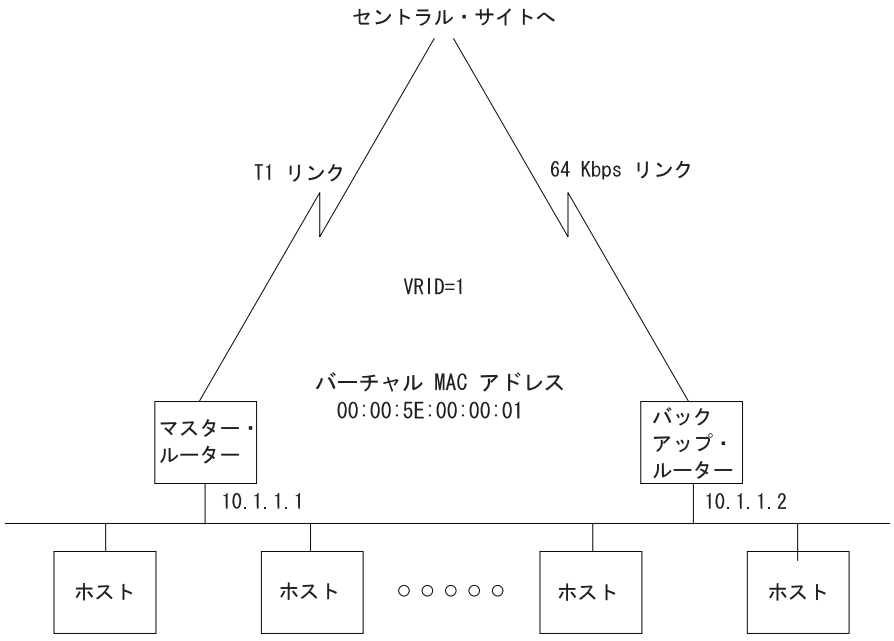


図 30. サブネット 10.1.1.0/255.255.255.0 を持つイーサネット LAN。すべてのホストはデフォルト・ゲートウェイ 10.1.1.1 を使って構成

1. すべてのホストはデフォルトのゲートウェイ 10.1.1.1 を使って構成されます。

2. マスター・ルーターは 10.1.1.1 にあてられたすべての ARP 要求にバーチャル MAC アドレス 00:00:5E:00:00:01 で応答します。
3. マスター・ルーターは、バーチャル MAC アドレスにあてら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は、バックアップが VRRP 公示が存在しないことを介してこのことを判別し、バーチャル MAC アドレスにあてられたパケットの受信を開始します。バックアップは 10.1.1.1 あての ARP 要求にも応答します。

複雑なトポロジーは、複数の VRRP ルーターがあるトポロジーであり、要望はルーター間での負荷のバランスを取ることですが、まだ完全なバックアップ機能も備えています。この事例では、2 つの VRID を定義する必要があり、各ルーターは一方のマスターであり、他方のバックアップになります。この図を以下に示します。

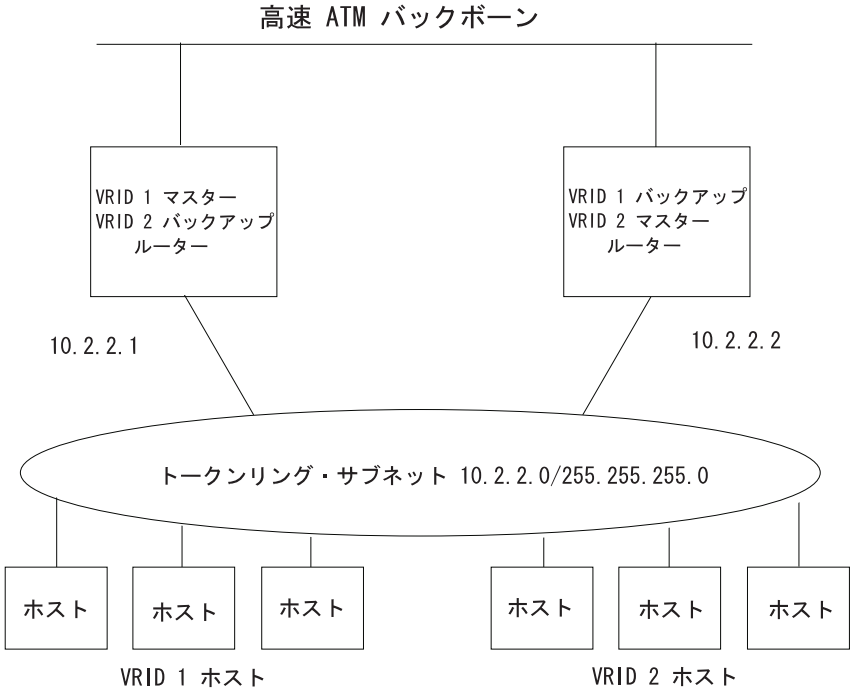


図 31. 複数の VRRP ルーター

1. すべての VRID 1 ホストはデフォルトのゲートウェイ・アドレス 10.2.2.1 を使って構成されています。
2. すべての VRID 2 ホストはデフォルトのゲートウェイ・アドレス 10.2.2.2 を使って構成されています。
3. VRID 1 マスター・ルーターはアドレス 10.2.2.1 あての ARP 要求にバーチャル MAC アドレス C0:00:00:10:00:00 を使って応答します。このルーターは、バーチャル MAC アドレス C0:00:00:10:00:00 あてのパケットも受信し、転送します。
4. VRID 2 マスター・ルーターは、アドレス 10.2.2.2 あての ARP 要求にバーチャル MAC アドレス C0:00:00:20:00:00 で応答します。このルーターは、バーチャル MAC アドレス C0:00:00:20:00:00 あてのパケットも受信し、転送します。
5. どちらのルーターも利用可能でない場合は、他のルーターが引き継ぎます。

6. ルーターが利用可能にならず、その外側の接続可能性を失う場合、そのルーターは ICMP 転送を使って他のルーターを通じてトラフィックを転送します (これは、2 つのルーターが、RIP または OSPF などのルーティング・プロトコルを介してルートを交換していると想定します)。

VRRP は、イーサネット、高速イーサネット、およびトークンリング上でサポートされます。

発信元でルートされた LAN がブリッジされたネットワークの部分であるとき、マルチキャスト VRRP はブリッジ・ネットワーク上でサポートされません。この制約事項は、IP がブリッジ・ネットワーク上で構成されているトポロジーでのみ適用されます。

冗長デフォルト IP ゲートウェイの構成

この節では、ELAN 上に冗長デフォルト IP ゲートウェイを構成するのに使用するステップを概説します。冗長ゲートウェイを構成すると、手動で構成されたデフォルト・ゲートウェイを持つエンド・ステーションは、1 次ゲートウェイがダウンした後も他のサブネットにトラフィックを渡し続けることができます。

1 次ゲートウェイまたはバックアップ・ゲートウェイを持つ装置を構成するには、次のようにします。

1. エンド・ステーションがデフォルト・ゲートウェイとして使用する IP アドレスを決める。
2. ELAN 上のインターフェースによって使用されていない MAC アドレスを調べる。どの MAC アドレスが使用されているかを調べるには、*ソフトウェア使用者の手引き*で 『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』 を参照してください。
3. 1 次ゲートウェイを持つ装置を選択する。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持っていることが必要です。
4. バックアップ・ゲートウェイを持つ 1 台または 1 組の装置を選択する。この装置または装置セットは、エンド・ステーションの ELAN 上に LEC インターフェースを持っていることが必要です。
5. IP の 『Add』 オプションを使用して、各装置に冗長ゲートウェイを構成する。

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 マルチキャスティングの拡張です。これは IP ホストが 1 つのデータグラム (IP マルチキャスト・データグラムと呼ばれます) を送信し、それを複数のあて先に送達する機能です。IP マルチキャスト・データグラムは、あて先がクラス D IP アドレス (つまり、最初のバイトが 224 ～ 239 の範囲内) であるパケットとして識別されます。各クラス D アドレスは、マルチキャスト・グループを定義します。

IP ホストが IP マルチキャスティングに参加するために必要な拡張は、RFC 1112 (IP マルチキャスティングのホスト拡張) に指定されています。この文書は、ホストが動的にマルチキャスト・グループに加わったり、離れたりすることを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) を定義しています。

このルーターは IGMP プロトコル機能を実装しており、「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って、ローカル物理 LAN およびエミュレート LAN 上の IP グループのメンバーシップを追跡することができます。

ルーターには、発信元と (複数の) あて先ホスト間で IP マルチキャスト・データグラムをルーティングする機能も必要です。このルーターは、RFC 1584 によって定義されたマルチキャスト最短パス優先オープン (MOSPF) プロトコル (OSPF のマルチキャスト拡張)、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) をサポートしています。

MOSPF ルーターは、新しいタイプのリンク状態公示 group-membership-LSA (タイプ 6) をフラッディング (全ポートにパケットを送出) することにより、ルーティング・ドメイン全体にグループ位置情報を配布します。これにより、MOSPF ルーターは最も効率的にマルチキャスト・データグラムを複数のあて先に転送できるようになります。各ルーターは、ルート (根) がデータグラム発信元で、端末ブランチがグループ・メンバーを含む LAN である 1 つのツリーとして、マルチキャスト・データグラムのパスを計算します。詳細については、325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) から導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 に対するサポートを提供するので、マルチキャスト・ルーティング情報を、MOSPF をサポートしない他のルーティング・エンティティーと交換することができます。また、このルーターの DVMRP 実現により、DVMRP 情報を MOSPF 可能なネットワークおよびマルチキャスト不能の IP ネットワークを介してトンネル伝送することも可能です。

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』 することもできます。マルチキャスト・グループのメンバーとして、ルーターは 『PING』 およびグループ・アドレスあての SNMP 照会 (1 つのコマンドを使用して複数のルーターを照会できます) に応答します。

さらに、装置の IP マルチキャスト・サポートは、DLSw グループの設定および管理にも使用できるので、DLSw に必要な構成の量を減らすことができます。詳細については、479ページの『第24章 DLSw の使用』を参照してください。

IP マルチキャスト用のルーターの構成

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できるようにするためには、MOSPF、DVMRP、または MOSPF と DVMRP の両方 を使用可能にする必要があります。

DVMRPの使用可能化

DVMRP を使用可能にするには、次のようにします。

1. ルーター上の DVMRP を使用可能にする。

```
DVMRP config> dvmrp on
```

2. DVMRP を実行する LAN インターフェースを設定する。

```
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は、IGMP ポーリング間隔およびタイムアウトは変更できません。これらの値は、それぞれ 125 秒と 270 秒です。

これらのコマンド、および DVMRP と MOSPF 間 (ルーター上で両方ともアクティブの場合) の相互接続を設定するために使用するその他の構成コマンドについての詳細は、*プロトコルの構成と監視 解説書 第 2 巻* の中の 『DVMRP の構成』 の節を参照してください。

IP マルチキャスト・グループへのルーターの登録

ルーター自体が 1 つまたは複数のマルチキャスト・グループに加わる場合は、次の join/leave コマンドを使用します。

- **join multicast-group-address**
- **leave multicast-group-address**

これらの **join** および **leave** コマンドには、OSPF Config プロンプトおよび OSPF 監視プロンプトからアクセスできます。また、DVMRP 監視コンソールからも利用可能です。

これらのコマンドは、ルーターが 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がないことに注意してください。これらはルーターをグループに追加し、『PING』 およびこれらのグループあての SNMP 照会に応答できるようにするのに使用します。

第14章 IP の構成および監視

この章では、IP 構成コマンドおよび監視コマンドについて説明します。本章には、以下の節が含まれています。

- 『IP 構成環境へのアクセス』
- 『IP 構成コマンド』
- 307ページの『IP 監視環境へのアクセス』
- 307ページの『IP 監視コマンド』

IP 構成環境へのアクセス

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

```
Config> 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、IP プロトコルの動作をユーザー特有の要件に適合するように変更できます。IP ルーターが完全に機能するようにするためには、いくらかの構成が必要です。IP 構成コマンドは IP config> プロンプトで入力します。

表 18. IP 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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・フィルターと共に追加することができます。
Change	**add** コマンドを使用して入力された情報を変更します。
Delete	**add** コマンドを使用して入力された 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 IP フィーチャーを使用不可にします。
Enable	ARP サブネット・ルーティング、UDP 転送、デフォルト生成、同報通信、BOOTP、RIP 情報の送受信を制御する各種の RIP フラグ、および route-table-filtering 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順序を変更します。
Set	アクセス制御の使用や同報通信アドレスのフォーマットなどの IP 構成モードを設定します。また、ルーターによって発信されたパケットの TTL (time-to-live)、 IP ルーティング・テーブルのサイズ、および RIP インターフェース・メトリックなどの IP パラメーターも設定、さらに、IGMP 構成パラメーターも設定します。
Update	パケット・フィルターにアクセス制御エントリーを割り当てるのに使用します。

表 18. IP 構成コマンドの要約 (続き)

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

Add

add コマンドは IP 情報を構成に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*

インターフェースの入力 RIP フィルターが使用可能の場合、インターフェースは RIP ルートを受け入れることができます。**list rip-routes-accept** コマンドを使用すれば、すでに入力されたのネットワーク/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 インターフェース単位で使用可能にできます。これは、ネットワーク・レベル・ルート (たとえば、10.0.0.0 へのルート)、サブネット・レベル・ルート (たとえば、128.185.0.0 へのルート)、およびホスト・レベル・ルート (たとえば、128.185.123.28) に対して別々に行います。IP インターフェース上の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** コマンドを使用します。

IP network/subnet

有効値: 任意の有効な IP アドレス

デフォルト値: 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して、アクセス制御レコードをグローバル・アクセス制御リストの最後に追加します。Packet-filter '*packet-filter-name*' Config> プロンプトから、このコマンドを使用して、アクセス制御規則をパケット・フィルターアクセス制御リストの最後に追加します。アクセス制御では、アクセス制御規則に指定されたパケット値に基づき、転送、排除、IP セキュリティーを使っての処理、またはネットワーク・アドレス変換を使っての処理を行うパケットのカテゴリーを定義することができます。アクセス制御リストの長さと順序は、IP パケットの転送性能に影響を与えることがあります。

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ことはありません。**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には、**add packet-filter** 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一致するパケットに何が行われるかを示します。

- **E** Exclusive (排他); 一致するパケットは廃棄されます。
- **I** Inclusive (包含); 一致するパケットはルーターによってさらに処理されます。
- **N** ネットワーク・アドレス変換 (NAT); 一致するパケットは NAT に渡され、アドレス変換を受けます。このタイプは、包括と組み合わせて指定されたときのみ (たとえば、 *IN*) 有効です。NAT および IPsec のタイプは、同じ規則内で指定することができます (たとえば、*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** コマンドによってアクセスされる) 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・フィルターでは、一致するパケットは IPsec に渡され、IP セキュア (IPsec) トンネル内にカプセル化されるか、場合によっては暗号化されます。入力パケット・フィルターでは、一致するパケットは正しい IPsec トンネルを通じて受信されたものか検証されます。このタイプは、包含と組み合わせて指定されたときのみ (たとえば、*IS*)、有効です。NAT および IPsec のタイプは同じ規則内で指定することができます (たとえば、*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** コマンドによってアクセスされる) 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、受信された発信元 IP アドレスとビットが AND され、規則が発信元 IP アドレスの範囲と一致するようにすることができます。発信元マスクのビットが 0 の場合、IP 発信元アドレスの対応するビットも 0 である必要があります。

有効値: 0.0.0.0 ～ 255.255.255.255

デフォルト値: 発信元 IP アドレスの場合は 0.0.0.0。発信元マスクのデフォルトは、構成された 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。dest-mask (あて先マスク) は受信されたあて先 IP アドレスとビットが AND され、規則があて先 IP アドレスの範囲と一致するようにすることができます。あて先マスクのビットが 0 の場合、あて先 IP アドレスの対応するビットも 0 である必要があります。

有効値: 0.0.0.0 ～ 255.255.255.255

デフォルト値: あて先 IP アドレスの場合は 0.0.0.0。あて先マスクのデフォルトは、構成された 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。

一般的な IP プロトコル番号は次のとおりです。

ICMP は 1

TCP は 6

UDP は 17

OSPF は 89

有効値: 0 ～ 255

デフォルト値: 最初のプロトコルの場合は 0、最後のプロトコルの場合は 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であるのは、IP プロトコル番号の範囲に 6 (TCP の場合) または 17 (UDP の場合) 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 であるパケットの場合は無視されます。

一般的に使用されるポート番号は、次のとおりです。

FTP は 21

Telnet は 23

SMTP は 25

rlogin は 513

RIP は 520

有効値: 0 ～ 65535

デフォルト値: 最初のあて先ポートの場合は 0、最後のあて先ポートの場合は 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であるのは、IP プロトコル番号の範囲に 6 (TCP の場合) または 17 (UDP の場合) 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 であるパケットの場合は無視されます。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

デフォルト値: 最初の発信元ポートの場合は 0、最後の発信元ポートの場合は 65535

tcp-syn

このパラメーターは、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 である TCP パケット) に一致します。このパラメーターが有効であるのは、IP プロトコル番号に 6 (TCP の場合) が含まれ、規則タイプが exclusive (排他) である場合だけです。このパラメーターは、タイプ IPsec および NAT (これらは常に inclusive (包含) です) の場合は無効です。このパラメーターは、IP プロトコル番号が 6 でないパケットの場合は無視されます。

有効値: Yes または No

デフォルト値: No

icmp-type

ICMP タイプを定義するこのパラメーターが有効であるのは、IP プロトコル番号の範囲に 1 (ICMP の場合) 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 パケットがアクセス規則に一致することができるのは、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だけです。デフォルト値 -1 が指定されている場合、すべての ICMP タイプ値はアクセス規則に一致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 でないパケットの場合は無視されます。

有効値: -1 〜 255

デフォルト値: -1 (すべての ICMP タイプ)

icmp-code

ICMP コードを定義するこのパラメーターが有効であるのは、IP プロトコル番号の範囲に 1 (ICMP の場合) 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 パケットがアクセス規則に一致することができるのは、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だけです。デフォルト値 -1 が指定されている場合、すべての

ICMP コード値は一致してい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 でないパケットの場合は無視されます。

有効値: -1 ～ 255

デフォルト値: -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たフィルターが可能になります。*Tos-mask* は、フィルターに掛ける優先順位 /TOS バイト内のビットを識別します。たとえば、*tos-mask* が X'E0' (B'11100000') の場合、フィルターは、TOS バイト内の 3 つの優先順位ビット (TOS バイト内の最上位 3 ビット) にのみ適用されます。

tos-range-low および *tos-range-high* は、選択されたビット内の連続する値を定義します。優先順位ビットの 8 個の値すべて (10 進数 0 ～ 7) をフィルターに掛けたい場合には、*tos-range-low* は X'00' (B'00000000') で、*tos-range-high* は X'e0' (B'11100000' は、フィルター用に選択された 3 ビット内に 10 進数 7 を定義します) とします。3 つの優先順位ビットの 2 進値 B'000'、B'001'、B'010'、および B'011' (10 進数 0 ～ 3) をフィルターに掛けたい場合は、*tos-range-low* は X'00' (B'00000000') で、*tos-range-high* は X'60' (B'01100000') とします。

連続する値のシーケンスを作成しないビット・パターンをフィルターに掛ける必要がある場合は、それぞれ必要な範囲ごとに別個のアクセス制御規則を定義する必要があります。たとえば、B'010' (10 進数 2) をフィルターに掛けずに 2 つの優先順位ビット値 B'001' (10 進数 1) と B'011' (10 進数 3) をフィルターに掛けるためには、*tos-mask* を X'e0' に、また、*tos-range-low* と *tos-range-high* の両方を X'20' に設定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。その場合、2 番目のアクセス制御規則は、*tos-mask* を X'e0' に、また、*tos-range-low* と *tos-range-high* の両方を X'60' に設定して定義する必要があります。

tos-mask **の有効値**: X'00' ～ X'FF'

デフォルト値: なしの場合は 0

tos-range-low **の有効値**: X'00' ～ X'FF'

デフォルト値: 0

tos-range-high **の有効値**: X'00' ～ X'FF'

デフォルト値: 構成された *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ルーターが変更できるようになります。*tos-mod-mask* は、変更される TOS バイト内のビットを識別します。*new-tos-value* は、選択されたビットの新しい値を定義します。たとえば、*tos-mod-mask* が X'1e' で、*new-tos-value* がX'00' の場合、TOS フィールドの 4 ビット (バイト内で *tos-mod-mask* 値 X'1e' [B'00011110'] によって識別されたビット)

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') に設定するためには、 *tos-mod-mask* X'1e' および *new-tos-value* X'08' (B'00001000') を使用してください。

tos-mod-mask **の有効値**: X'00' ～ X'FF'

デフォルト値: なしの場合は 0

new-tos-value **の有効値**: X'00' ～ X'FF'

デフォルト値: 0

policy-based-routing、next-hop-gateway、use-default-route

これらのパラメーターを指定すると、ポリシー・ベース・ルーティングが使用可能になります。これは、フィルターに掛けられた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する機能です。*policy-based-routing* パラメーターを Yes に設定すると、フィルターに掛けられたパケットを定義されたネクスト・ホップ・ゲートウェイに送信するよう計画しているものと指示されます。*Next-hop-gateway* は、これらのパケットの送信先となるネクスト・ホップ・ゲートウェイのアドレスです。

use-default-route を Yes に設定すると、定義されたゲートウェイが使用不可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することができます。このパラメーターを No に設定すると、定義されたゲートウェイが使用不可になった場合にパケットは廃棄され、その廃棄されたパケットの発信元アドレスには ICMP *unreachable* メッセージが送信されます。

policy-based-routing **の有効値**: Yes または No

デフォルト値: No

next-hop-gateway **の有効値**: 有効な IP アドレス

デフォルト値: なし

use-default-route **の有効値**: Yes または No

デフォルト値: Yes

IPsec-tunnel-ID

このパラメーターが有効なのは、規則タイプが IPsec である場合だけです。出力パケット・フィルターでは、このパラメーターは、パケットが送信されるときに通過する IP セキュア (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、パケットがそこから受信された 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** コマンドによってアクセスされる) でのみ有効です。

有効値: 1 ～ 65535

デフォルト値: 1

log ログを使用可能にします。

有効値: Yes または No

デフォルト値: No

els
ログが使用可能にされる場合は、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

デフォルト値: No

snmp-trap
ログが使用可能にされる場合は、このアクセス制御規則について SNMP トラップを送信することを可能にします。

有効値: Yes または No

デフォルト値: No

syslog
ログが使用可能にされる場合は、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、接続されたリモート・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

デフォルト値: No

syslog-level
SysLog が使用可能にされる場合、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

デフォルト値: ルーター・システムのデフォルト値

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*
IP アドレスを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 アドレスを持つまでは IP パケットを受信または送信しません。IP アドレスをそのサブネット・マスクと共に指定する必要があります。たとえば、アドレスがクラス B ネットワーク上にあり、3 番目のバイトをサブネット用に使用している場合、マスクは 255.255.255.0 になります。該

当するコマンドのインターフェース番号を入手するには **list devices** コマンドを使用します。シリアル・ラインの場合は、アドレスは必要ありません。この種の伝送路は、非番号制と呼ばれます。ただし **add address** コマンドを使用して IP トラフィック用に使用可能にしておくことは必要です。その場合に使用するアドレスは 0.0.0.*n* になります。ただし、*n* は *interface-number* です。

注: 2212 のブリッジ・ネットワークに IP アドレスを割り当てるには、*interface number* 用の**ブリッジ**を指定します。詳細については、228ページの『IP アドレスのブリッジ・ネットワーク・インターフェースへの割り当て』を参照してください。

IP アドレスをそのサブネット・マスクと共に指定する必要があります。たとえば、アドレスがクラス B ネットワーク上にあり、3 番目のバイトをサブネット用に使用している場合、マスクは 255.255.255.0 になります。該当するオプションの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ます。

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**ブリッジ**

デフォルト値: なし

ip-address

有効値:

クラス A 範囲は 1.0.0.1 ～ 126.255.255.254

クラス B 範囲は 128.0.0.1 ～ 191.255.255.254

クラス C 範囲は 192.0.0.1 ～ 223.255.255.254

非番号制シリアル・ライン・インターフェースの場合は 0.0.0.n。ただし *n* はインターフェース番号

デフォルト値: なし

address mask

有効値: 0.0.0.0 ～ 255.255.255.255

デフォルト値: 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、BOOTP/DHCP 要求を転送する先のサーバーのリストに追加します。詳細については、246ページの『BOOTP/DHCP 転送プロセスの構成』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

デフォルト値: なし

例: add bootp-server 128.185.123.22

filter *dest-IP-address address-mask*

IP あて先をフィルターに掛けることを指示します。フィルターに掛けられたあて先には IP パケットは転送されず、そのようなあて先に関するルーティン

グ情報も配布されません。フィルターに掛けられたあて先へのパケットは、廃棄されるだけです。フィルターに掛けるあて先は、 IP アドレスとそのサブネット・マスクを使用して指定する必要があります。たとえば、3 番目のバイトをサブネットに使用しているクラス B ネットワークのサブネットをフィルターに掛ける場合、マスクは 255.255.255.0 になります。フィルター・メカニズムは、IP アクセス制御を使用するより効率的ですが、柔軟性に劣ります。また、フィルターは、アクセス制御とは異なり、IP ルーティング・プロトコルの動作にも影響を与えます。フィルターに掛けられるネットワーク/サブネットは、 OSPF ルーティング・プロトコルを使用して確認された場合にオーバーライドされます。

このコマンドの効果は即時です。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

デフォルト値: なし

address mask

有効値: 0.0.0.0 〜 255.255.255.255

デフォルト値: 0.0.0.0

例: `add filter 127.0.0.0 255.0.0.0`

packet-filter *filter-name type interface-number*

ルーター構成内のパケット・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。

名前には、ダッシュ (-) と下線 (_) を含めることができます。

デフォルト値: なし

type *IN* 着信トラフィックをフィルターに掛けます。

OUT 発信トラフィックをフィルターに掛けます。

interface-number

有効値: 任意の定義済みインターフェース、またはブリッジ・ネットワーク・インターフェース用の**ブリッジ**

デフォルト値: 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*

冗長デフォルト・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ネット番号を指定します。

有効値: LEC インターフェースのネット番号

デフォルト値: なし

gateway-IP-address

エンド・ステーションのデフォルト・ゲートウェイを指定します。

有効値: デフォルト・ゲートウェイとして使用される IP アドレス

デフォルト値: 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 ネットワーク・マスク

デフォルト値: 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な MAC アドレス

デフォルト値: 00.00.00.00.00.00

primary-gateway

ゲートウェイが 1 次ゲートウェイとして使用されるのか、バックアップ・ゲートウェイとして使用されるのかを指定します。

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運用時にアクティブになる 1 次ゲートウェイであるのか、あるいは 1 次ゲートウェイを持つ LEC インターフェースが動作不能のときアクティブになるバックアップ・ゲートウェイであるのかを尋ねます。**Yes** と応答すると、1 次ゲートウェイとして構成されます。1 次ゲートウェイは、各 ELAN につき 1 つだけでなければなりません。

有効値 Yes または No

デフォルト値: 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。特定のあて先の動的ルーティング情報が得られない場合に、静的ルートが使用されます。

あて先は、IP アドレス (*dest-addr*) とアドレス・マスク (*dest-mask*) によって指定します。あて先 IP アドレスがネットワーク・アドレスの場合、dest-mask 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・アドレスの場合、 dest-mask はサブネット・マスクでなければなりません。また、あて先 IP アドレスがホスト・アドレスの場合、dest-mask はホスト・マスクでなければなりません (つまり、有効値は 255.255.255.255 だけです)。dest-mask は正確に指定することが必要です。そうでないと、静的ルートは受け入れられません。

あて先へのルートは、ネクスト・ホップの IP アドレス *(next-hop)* と、パケットをあて先にルーティングするコスト *(cost)* によって指定します。ネクスト・ホップは、ルーターが直接接続されているインターフェースのうちの 1

つと同じ (sub)net 上になければなりません。静的ルートは常に、OSPF を介して確認されたルートによってオーバーライドされます。デフォルトでは、静的ルートは RIP を介して確認されたルートによってもオーバーライドされますが、これは **enable/disable override static-routes** コマンドを使用して変更することができます。このコマンドの効果は即時です。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

デフォルト値: なし

dest-mask

有効値: 0.0.0.0 ～ 255.255.255.255

デフォルト値: なし

next-hop1、next-hop2、next-hop3、next-hop4

有効値: 任意の有効な IP アドレス

デフォルト値: なし

cost1、cost2、cost3、cost4

有効値: 0 ～ 255 の範囲の整数

デフォルト値: 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]*

ルート・テーブル・フィルターを指定されたルートに追加します。**route-table-filtering** が使用可能のときは、route-table-filter は IP ルート・テーブルに追加されたルートと照合されます。route-table-filters 内の順序は重要ではありません。最も具体的に一致している route-table-filter が選択されます。一致するものが見つからなかった場合、そのルートはルート・テーブルに追加されます。**exact** が指定されている場合は、ルートのあて先およびマスクが route-table-filter のあて先およびマスクと正確に同じでなければ、一致と見なされません。**more-specific** が指定されている場合は、ルートのあて先とマスクは、route-table-filter のあて先とマスクの範囲内でなければなりません。**both** の指定は、exact と more-specific の両方のスーパーセットです (つまり、exact 一致と more-specific 一致の両方の場合に一致と見なされます)。route-table-filter

が **include** を示している場合は、ルートは IP ルート・テーブルに追加されます。route-table-filter が **exclude** を示している場合は、ルートは IP ルート・テーブルに追加されません。静的ルートと直接ルートは、決して IP ルート・テーブルから除外されません。

destination mask

有効値: 任意の有効な IP マスク

デフォルト値: 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 ポート番号を持つ UDP データグラムが指定された IP アドレスに転送されます。

同報通信またはユニキャスト IP アドレスを入力できます。

同じ UDP ポートに複数の IP アドレスを追加する場合は、このコマンドを繰り返します。これにより、ルーターはそれぞれの IP アドレスにパケットを転送するようになります。

port-number

有効値: 0 〜 65535

デフォルト値: なし

address

有効値: 任意の有効な IP アドレス

デフォルト値: 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 ルーター用のバーチャル・ルーター ID 定義を追加します。

interface-ip-address

この VRID が定義されている IP インターフェースを示します。

有効値: 任意の構成済みの IP インターフェース

デフォルト値: なし

vrid バーチャル・ルーター ID。*ip-interface-address* および *vrid* の組み合わせは、 VRID を一意的に定義します。複数の物理インターフェース上で同じ *vrid* を使用することができます。

有効値: 1 〜 255

デフォルト値: なし

advertisement-interval

VRRP 公示間の間隔。

有効値: 1 〜 255

デフォルト値: 1

backup-router

このルーターが、この VRID 用のマスター・ルーターであるか、バックアップ・ルーターであるかを示します。

有効値: Yes または No

デフォルト値: No

backup-ip-address

この VRID 用のバックアップである最初の IP アドレスを示します。複数のサブネットをサポートしている LAN セグメントでは、*add vr-address* コマンドを使用してさらにアドレスを追加することができます。*バックアップ・ルーター* について **No** が構成された場合は、これは適用されません。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

priority

バックアップ・ルーターについての VRRP 優先順位を示します。バックアップ・ルーターが 1 次ルーターを引き継ぐ場合、その VRRP 公示でこの優先順位を使用します。*バックアップ・ルーター* について **No** が構成された場合は、これは適用されません。マスター・ルーターは常に、優先順位 255 を公示します。

有効値: 1 〜 254

デフォルト値: 100

functional/group-mode

マルチキャスト MAC アドレスが VRID バーチャル MAC アドレスとして使用されるかどうかを示します。VRRP が正しく機能するためには、この VRID 用に構成されたすべてのルーターは、このパラメーターについて同じ値を持つ必要があります。

有効値: Yes または No

デフォルト値: No

authentication-type

VRRP 公示に使用される認証のタイプを示します。認証タイプの選択値は 1 (簡易パスワードを示す) または 0 (認証が使用されないことを示す) です。

有効値: なし、simple

デフォルト値: なし

authentication-key

この VRID 用のパスワードを定義するパラメーター。パスワードの認証が使用されている場合、正しい認証キーを持つパケットのみが受け入れられます。*なし* が指定されるか、デフォルトで *認証タイプ* が使われるときは、*認証キー* は適用されません。

有効値: 任意の 1 〜 8 の文字

デフォルト値: ヌル文字列

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 ルーター用のバーチャル・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 用の VRRP 公示に含まれます。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、そのサブネット用のデフォルトのゲートウェイ・アドレスを指定します。ルーターがマスター・ルーターである場合、*add vr-address* コマンドを使用して追加されたアドレスが、 VRID 用の *ip-interface-address* に加えて公示されます。ルーターが VRID 用のバックアップ・ルーターである場合、*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* に加えて公示されます。

interface-ip-address

VRID 用の IP インターフェース

有効値: 任意の構成済みの IP インターフェース

デフォルト値: なし

vrid バーチャル・ルーター ID。*ip-interface-address* および *vrid* の組み合わせは、 VRID を一意的に定義します。VRID は、その定義に追加されるアドレスについて構成する必要があります。

有効値: 1 〜 255

デフォルト値: なし

ip-address

VRID 用の VRRP 公示に含まれる追加の IP アドレス

有効値: 任意の IP アドレス

デフォルト値: 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** コマンドを使用して導入した IP 構成項目を変更するのに使用します。通常は、**add** コマンドで項目を指定したときと同様に、変更する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変更します。**list access-control** コマンドを使用すると、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ことができます。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 つを変更します。各新規アドレスを新規アドレスのサブネット・マスクと共に指定することが必要です。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:

- クラス A 範囲は 1.0.0.1 〜 126.255.255.254
- クラス B 範囲は 128.0.0.1 〜 191.255.255.254
- クラス C 範囲は 192.0.0.1 〜 223.255.255.254
- 非番号制シリアル・インターフェースの場合は 0.0.0.n。ただし n はハードウェア・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

デフォルト値: なし

new-address

有効値: 任意の IP アドレス

デフォルト値: なし

new-mask

有効値: 0.0.0.0 〜 255.255.255.255

デフォルト値: 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]]]*

指定のあて先への構成された静的ルートに関連するネクスト・ホップまたはコストを変更します。このコマンドの効果は即時です。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

デフォルト値: なし

dest-mask

有効値: 0.0.0.0 ～ 255.255.255.255

デフォルト値: 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

デフォルト値: なし

new-cost1、new-cost2、new-cost3、new-cost4

有効値: 0 ～ 255 の範囲の整数

デフォルト値: 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、以前に **add** コマンドを使用して導入した IP 構成項目を削除するのに使用します。一般的に、**add** コマンドで項目を指定したときと同様に、削除する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*

RIP プロトコルが常に受け入れるネットワークのリストからルートを除去します。

有効値: 受け入れられる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

デフォルト値: 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

デフォルト値: なし

例: delete address 128.185.123.22

bootp-server *server-IP-address*

BOOTP サーバーを IP 構成から除去します。

有効値: 任意の構成済みの BOOTP サーバー IP アドレス

デフォルト値: 0.0.0.0

例: delete bootp-server 128.185.123.22

default network/subnet-gateway *[ip-network-address]*

指定されたサブネット・ネットワークのデフォルト・ゲートウェイまたはデフォルト・サブネット・ゲートウェイを削除します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

例: delete default subnet-gateway 128.185.0.0

filter *dest-addr dest-mask*

ルーターのフィルターに掛けられるネットワークの 1 つを削除します。このコマンドの効果は即時です。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

デフォルト値: 0.0.0.0

dest-mask

有効値: 0.0.0.0 ～ 255.255.255.255

デフォルト値: なし

例: `delete filter 127.0.0.0`

```
Address mask [0.0.0.0]? 255.0.0.0
```

packet-filter *filter-name*

指定された packet-filter をルーターの構成から削除します。

有効値: 任意の 16 文字の名前

名前には、ダッシュ (-) と下線 (_) を含めることができます。

デフォルト値: 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*

冗長 IP ゲートウェイを LEC インターフェースから削除します。

interface-number

有効値: 冗長デフォルト IP ゲートウェイを持つ LEC のインターフェース番号

デフォルト値: 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]]]]*

装置の構成された静的ルートの 1 つを削除します。このコマンドの効果は即時です。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

デフォルト値: なし

dest-mask

有効値: 任意の有効な IP マスク

デフォルト値: なし

delete-next-hop

有効値: Yes または No

デフォルト値: 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ルート・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。コマンド拡張の定義については、 266 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

デフォルト値: なし

mask **有効値**: 任意の有効な IP マスク

デフォルト値: なし

mask-definition

有効値: 任意の有効な IP マスク

デフォルト値: 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 転送の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送達 UDP データグラムは、指定された IP アドレスに転送されなくなります。

port-number

有効値: 0 〜 65535 の範囲の整数

デフォルト値: なし

address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

例:

```
delete udp-destination 36 20.1.2.2
```

vrid *interface-ip-address vrid*

VRRP ルーター用の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 が削除されている IP インターフェースを示します。

有効値: 任意の構成済みの IP インターフェース

デフォルト値: なし

vrid バーチャル・ルーター ID。*ip-interface-address* および *vrid* の組み合わせは、 VRID を一意的に定義します。これは、削除されようとしている VRID を識別するのに使用します。

有効値: 1 〜 255

デフォルト値: 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 用の IP インターフェース

有効値: 任意の構成済みの IP インターフェース

デフォルト値: なし

vrid バーチャル・ルーター ID。*ip-interface-address* および *vrid* の組み合わせは、 VRID を一意的に定義します。VRID は、その定義から削除されるアドレスについて構成する必要があります。

有効値: 1 〜 255

デフォルト値: なし

ip-address

VRRP 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

デフォルト値: 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可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。これが使用可能のときは、ルーター経由で最善のルートで到達できるリモートあて先へのすべての

ARP 要求に対して、ルーターはプロキシーによって応答します。これがデフォルト設定であり、一般的に推奨される設定です。

例: disable arp-net-routing

arp-subnet-routing

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。これが使用可能のときは、IP サブネット化をサポートしないホストに対処します。これがデフォルト設定であり、一般的に推奨される設定です。

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

無クラス・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・プロトコルに対するサポートを使用不可にします。ネットワーク・マスク (たとえば、RIPv1) を公示しないプロトコルでは、公示のためのナチュラル・ネットワーク・ルート (たとえば、クラス A、B、または C ルート) は自動的に生成されません。

例: disable classless

directed-broadcast

あて先が非ローカル (たとえば、リモート LAN) 同報通信アドレスである IP パケットの転送を使用不可にします。発信元ホストはパケットをユニキャストとして生成し、それをユニキャストとしてあて先サブネットに転送し、そこで 『分解』 されて同報通信されます。このようなパケットは、ネットワーク・サーバーを見付けるのに使用できます。

注: 転送と分解を別々に使用不可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可にします。これにより、ルーターのインターフェースに送信される PING は応答を生成しなくなります。ルーターのデフォルト設定では echo-reply は使用可能です。

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可にします。この検査が使用可能にされると、ルーターは各フラグメントを検査して、 2 次フラグメントが最初のフラグメントの負荷の最初の 8 バイトをオーバーレーしていないか調べます。デフォルトでは、この検査が使用不可にされます。

icmp-redirect *ip-interface-address*

ルーターが指定の IP インターフェースに ICMP 転送メッセージを送信するのを使用不可にします。IP インターフェース・アドレスの入力を促されたと

きにユーザーが何も入力しないと、ルーターはすべての IP インターフェースへの ICMP 転送メッセージの送信が使用不可にされます。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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 によって受信されたデフォルトのルートが、IP ルーティング・テーブルにすでに導入済みのデフォルトのルートを置き換えないようにします。**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オーバーライドするのを防止します。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

例: disable override default 128.185.123.22

nexthop-awareness *ip-interface-address*

IP インターフェースのネクスト・ホップ認識を使用不可にします。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

例:

```
IP config>disable nexthop-awareness 1.1.1.1
IP config>disable nexthop-awareness
Interface address []? 2.2.2.2
IP config>
```

packet-filter *filter-name*

指定されたインターフェース専用アクセス制御リスト (packet-filters) を使用不可にします。

filter-name

有効値: 任意の 16 文字の名前 名前には、ダッシュ (-) と下線 (_) を含めることができます。

デフォルト値: なし

例: disable packet-filter pf-in-0

per-packet-multipath

per-packet-multipath が使用不可のとき、ルーターはあて先への最初の利用可能なパスを選択します。このフィーチャーのデフォルトは、使用不可です。

例: disable per-packet-multipath

receiving rip *ip-interface-address*

RIP がインターフェース *ip-interface-address* で受信された RIP 更新を処理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

デフォルト値: なし

例: `disable receiving rip 128.185.123.22`

receiving dynamic all/hosts/nets/subnets *ip-interface-address*

disable receiving dynamic nets コマンドは、インターフェース *ip-interface-address* で RIP 更新が受信された場合、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・レベルのルートのみを受け入れるようにします。**disable receiving dynamic subnets** コマンドは、サブネット・ルートに対して、これと同様の働きをします。**disable receiving dynamic host** は、ホスト・ルートに対して同様の働きをします。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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 パケットを受信または転送できないようにします。デフォルトでは、ルーターはこれらのパケットを受信および転送します。

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の RIP2 モードを使用不可にします。

ip-interface-address

有効値: RIP2 が使用可能なインターフェースの任意の有効な IP アドレス

デフォルト値: なし

例: `disable rip2 128.185.123.22`

route-table-filtering

ルートがルーティング・テーブルに追加されるときの route-table-filters の適用を使用不可にします。

例: `disable route-table-filtering`

same-subnet

same subnet (同一サブネット) オプションを使用不可にします。ルーターをリブートしたときに、同じサブネットに複数の IP インターフェースを導入することはできません。これがデフォルトです。

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 ルートのみを公示しないようにします。

ip-interface-address

有効値: RIP2 が使用可能なインターフェースの任意の有効な IP アドレス

デフォルト値: 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、ip-interface-address を使用して送信された RIP 更新内の指定されたタイプのルートを公示するのを防止します。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の他のフラグとしては、**host-routes**、**static-routes**、 **net-routes**、および **subnet-routes** があります。これらは、個別にオフにすることができます。使用可能フラグによって指定されている場合、その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

デフォルト値: なし

例: `disable sending net-routes 128.185.123.22`

sending outage-only *interface-IP-address*

類似の enable コマンドで指定されたルートの存在を条件として RIP 更新の送信を使用不可にします。この機能が使用不可にされると、 RIP 公示が無条件に送信されます。

interface-IP-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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、受信されたパケットの発信元 IP アドレスが、 IP ルーティング・テーブルに基づき、パケットがそこから受信されたインターフェースと矛盾していないことを検証します。このオプションは、IP ホストに属していない発信元 IP アドレスを使用している (スプーフィング と呼ばれる動作) 不正な動作を行う IP ホストからのパケットの転送を防ぐのに役立ちます。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** コマンドによってアクセスされる) でのみ有効です。

source-routing

ルーターがソース・ルート・パケット (つまり、source-route オプションを含んでいる IP パケット) を転送するのを防止します。このオプションのデフォルトは source-routing 使用可能です。

例: `disable source-routing`

tftp-server

ルーターがネットワークからの TFTP GET または PUT 要求を受け入れるのを防止します。これにより、誤って別の装置から構成ファイルまたはロード・イメージがオーバーレーされるのを防止できます。ただし、GET または PUT は、直接接続された端末または装置との Telnet セッションを通して実行することができます。

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 パケットを受信または転送できないようにします。デフォルトでは、ルーターはこれらのパケットを受信および転送します。

udp-forwarding *port-number*

ルーターが受信した指定の UDP あて先ポート番号を持つパケットの UDP 転送を使用不可にします。

デフォルト: すべてのポート番号への UDP 転送が使用不可にされます。

port-number

有効値: 0 〜 65535 の範囲の整数

デフォルト値: 0

例: `disable udp-forwarding 36`

vrrp バーチャル・ルーター冗長度プロトコルを使用不可にします。

例: `disable vrrp`

Enable

enable コマンドは、IP 構成に追加された IP 機構、機能、および情報を起動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。これが使用可能のときは、ルーター経由で最良のルートで到達できるリモートあて先へのすべての ARP 要求に対して、ルーターはプロキシーによって応答します。このコマンドは、ローカルあて先だけでなく、すべてのあて先をアドレス変更する LAN 上のホストが存在するときに使用します。

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 とも呼ばれます) 機能をオンにします。この機能は、サブネット化を認知しないホストが、直接接続された IP サブネットに接続されている場合に使用します。サブネッ

ト機能を持たないホストが存在する直接接続されたサブネットでは、このフィーチャーを有効にするためには ARP を使用する必要があります。

ARP サブネット・ルーティングは、次のように働きます。サブネット不能ホストが 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、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認識できません。そのため、サブネット不能ホストは単に ARP 要求を同報通信します。この ARP 要求がルーターによって受信されます。ルーターは、arp-subnet-routing が使用可能にされており、かつあて先へのネクスト・ホップが ARP 要求を受信したインターフェース以外のインターフェースを経由する場合に、あて先として応答します (これが、プロキシーという名前の由来です)。

LAN 上に “サブネット不能” ホストが存在しない場合には、ARP-subnet routing を使用可能にしないでください。LAN 上で ARP サブネット・ルーティングが必要な場合、その LAN 上のすべてのルーターでこれを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 転送を使用するためには、**add bootp-server** コマンドを使用して、1 つまたは複数の BOOTP サーバーを追加する必要があります。

例: `enable bootp-forwarding`

```
Maximum number of forwarding hops [4]?
Minimum seconds before forwarding [0]?
```

Maximum number of forwarding hops

クライアントからサーバーに BOOTP 要求を転送することができる BOOTP エージェントの最大数 (これは、サーバーへの IP ホップの最大数ではありません)。

デフォルト: 4

Minimum seconds before forwarding

このパラメーターは、通常は使用しません。クライアントとサーバー間に冗長パスが存在し、2 次パス (1 つまたは複数) をスタンドバイとして使用したい場合に、このパラメーターを使用します。

デフォルト値: 0

classless

ルーターが無クラス IP アドレッシング環境で動作することを示します。IBM 2212 は、このオプションを使用可能にせずに、RFC 1817 に記述されている CIDR アドレッシングを完全にサポートします。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ナチュラル・ネットワーク・ルート (たとえば、クラス A、B、または C ネットワーク・ルート) が自動的に生成されるのを防止します。RIPv1 を実行していない場合は、ナチュラル・ネットワーク・ルートは必要ありません。

例: `enable classless`

directed-broadcast

あて先がネットワーク指定またはサブネット指定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

ニキャストとして生成され、ユニキャストとしてあて先サブネットに転送され、そこで 『分解』 されて 同報通信されます。このようなパケットは、ネットワーク・サーバーを見付けるのに使用できます。このコマンドは、指定同報通信 (directed broadcast) の転送と分解の両方を使用可能にします。IP パケット転送機能は、クラス D IP アドレスに対応していない限り、リンク・レベルの同報通信/マルチキャストの転送は行いません。(OSPF **enable multicast-routing** コマンドの項を参照してください。) このフィーチャーのデフォルト設定は、使用可能です。

注: 転送と分解を個別に実現することはできません。また、ルーターは all-subnets IP 同報通信も転送しません。

例: `enable directed-broadcast`

echo-reply

ICMP エコー要求に応答して ICMP 応答を作成し、送信すること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 である (つまり、TCP)、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。フラグメント・オフセットが 1 のパケットは除去されます。デフォルトでは、この検査が使用不可にされます。

注: この機能は、使用不可にされていると、他の IP 機能に影響を与えずに起動することができます。詳細については、Talk 5 **reset IP** コマンドを参照してください。

icmp-redirect *ip-interface-address*

ルーターが指定された IP インターフェースに ICMP 転送メッセージを送信するのを使用可能にします。ユーザーが IP インターフェース・アドレスの入力を促されたときに何も入力しないと、装置はすべての IP インターフェースへの ICMP 転送メッセージの送信が使用可能にされます。

ip-interface-address

有効値: 任意の有効な IP アドレス、または、すべての IP アドレスの場合は何も入力しません。

デフォルト値: 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

デフォルト値: 使用不可

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・テーブルで導入済みのデフォルト・ルートをオーバーライドすることができるようにします。このコマンドは、IP インターフェース単位で起動されます。**enable override default** コマンドが起動されている場合、インターフェース ip-interface-address で受信されたデフォルト RIP ルートがルーターの現行デフォルト・ルートを上書きします (新規デフォルトのコストの方が安い場合)。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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一部をオーバーライドすることを使用可能にします。このコマンドは、IP インターフェース単位で起動されます。**enable override static-routes** コマンドが起動されている場合、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・ルートを上書きします (RIP 情報のコストの方が安い場合)。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

例: `enable override static-routes 128.185.123.22`

packet-filter *filter-name*

指定されたインターフェース専用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。名前には、ダッシュ (-) と下線 (_) を含めることができます。

デフォルト値: なし

例: `enable packet-filter pf-in-0`

per-packet-multipath

per-packet-multipath が使用可能にされ、あて先への同一コストのパスが複数ある場合、ルーターはラウンドロビン方式で、各パケットを転送するパスを選択します。この機能のデフォルトは、使用不可です。

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、類似の 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。) このコマンドは、デフォルトでは使用可能です。

disable receiving rip コマンドを起動すると、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なくなります。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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た RIP 更新の処理を変更します。このコマンドには、類似の 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。) このコマンドは、デフォルトでは使用可能です。

disable receiving dynamic nets コマンドを起動した場合、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** コマンドで指定されていない限り、ネットワーク・レベルのルートを受け入れなくなります。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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た RIP 更新の処理を変更します。このコマンドには、類似の 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。) このコマンドは、デフォルトでは使用可能です。

disable receiving dynamic subnets コマンドを起動した場合、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** コマンドで指定されていない限り、サブネット・レベルのルートを受け入れなくなります。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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 パケットを受信または転送できるようにします。これがデフォルトです。

注: この機能は、使用不可にされていると、他の IP 機能に影響を与えずに起動することができます。詳細については、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 が使用可能になると、以下のデフォルト動作が設定されます。

- ルーターは、構成された各 IP インターフェースから送信する RIP 更新に、すべてのネットワークおよびサブネットを含める。
- ルーターは、構成された各 IP インターフェースで受信したすべての RIP 更新を処理する。

デフォルトの送信/受信動作を変更するには、IP 構成コマンドを使用します。これらは、各 IP インターフェースごとに定義します。

例: enable rip

rip2

インターフェース上の RIP2 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。インターフェースで RIP2 が使用可能になっている場合、認証キーを設定するかどうかを尋ねられます。N (No) と応答すると、RIP2 パケット公示で認証は行われません。Y (Yes) と応答すると、認証キーを入力するように指示されます。この認証キーは、検証のために 2 度入力する必要があります。認証キーは、指定されたインターフェースから発信される RIP2 公示パケットに組み込まれます。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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すべての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 most-specific match (最も具体的に一致するもの) に基づいて適用されます。ルート・テーブル・フィルターは、直接ルートまたは静的ルートに適用されることはありません。

例: enable route-table-filtering

same-subnet

same subnet (同一サブネット) オプションを使用可能にします。装置をリブートしたときに、同じサブネットに複数の IP インターフェースを導入することができます。複数の IP インターフェースを同じサブネットに導入すると便利なのは、次の条件の場合だけです。

- 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。
- 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されており、IP インターフェースを経由するルートとして静的ルートが定義されている。

デフォルトでは、このオプションは使用不可です。

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 更新のコンテンツを決めます。

このコマンドには、類似の 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** コマンドの効果は加算的です。個別の enable sending コマンドによって、特定の 1 組のルートを特定インターフェースから公示する必要があることを指定します。ルートは、少なくとも 1 つの enable sending コマンドによって組み込まれている場合にのみ RIP 更新に組み込まれます。**enable sending default-routes** コマンドは、インターフェース ip-interface-address から送信される RIP 更新にデフォルト・ルート (存在する場合) を組み込むことを指定します。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

例: `enable sending default-routes 128.185.123.22`

注: enable sending ... コマンドの一部の設定値は冗長です。たとえば、特定のインターフェースに対して **enable sending net-routes**、**enable sending subnet-routes**、および **enable sending host-routes** を起動した場合、さらに **enable sending static-routes** も指定する必要はありません (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・ルートであるからです)。デフォルトでは、最初に RIP を使用可能にしたときに、enable RIP, sending net-routes, sending subnet-routes, および sending host-routes は各インターフェースに対して使用可能にされ、sending static-routes および sending default は使用不可にされます。

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 更新のコンテンツを決めます。このコマンドには、類似の 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 コマンドの効果は加算的です。個別の **enable sending** コマンドによって、特定の 1 組のルートを特定インターフェースから公示する必要があることを指定します。ルートは、少なくとも 1 つの **enable sending** コマンドによって組み込まれている場合にのみ RIP 更新に組み込まれます。**enable sending network-routes** コマンドは、インターフェース ip-interface-address から送信される RIP 更新に、すべてのネットワーク・レベル・ルートを含める必要があることを指定します。ネットワーク・レベル・ルートというのは、単一のクラス A、B、または C 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

デフォルト値: 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* によって指定されている IP ルートの存在を条件として、*interface-ip-address* によって指定されたインターフェース上で 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上で無条件に送信され

ます。さらに、指定されたルートが存在するとき、RIP 更新は outage のみの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・ダイヤル・サーキットがダイヤル・オンデマンド回線として構成されているバックアップ・シナリオで便利な場合があります。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

outage-network

有効値: 任意の有効な IP アドレス

デフォルト値: none

outage-network-mask

有効値: 任意の有効な IP マスク

デフォルト値: none

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、10.50.0.0/255.255.0.0 ルートがルーティング・テーブルにない場合、 RIP 公示は非番号制インターフェース上でのみ送信されます。

sending poisoned-reverse-routes *ip-interface-address*

ルートが変更された場合にコンバージェンス・タイムを改善するために 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大きくなります。コンバージェンスがいくらか遅くなっても、ルーティングのオーバーヘッドを最小化する方がよい場合もあります。**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から送信される RIP 更新には、有害な逆ルートを含めないことを指定します。

デフォルト: 使用可能

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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 が使用可能なインターフェースの任意の有効な IP アドレス

デフォルト値: 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 更新のコンテンツを決めます。

このコマンドには、類似の 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** コマンドの効果は加算的です。個別の **enable sending** コマンドによって、特定の 1 組のルートを特定インターフェースから公示する必要があることを指定します。ルートは、少なくとも 1 つの enable sending コマンドによって組み込まれている場合にのみ RIP 更新に組み込まれます。**enable sending subnet-routes** コマンドは、インターフェース ip-interface-address から送信される RIP 更新にすべてのサブネット・ルートを含める必要があることを指定します。ただし、サブネット・ルートは、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のみ組み込まれます。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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 更新のコンテンツを決めます。このコマンドには、類似の 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** コマンドの効果は加算的です。個別の **enable sending** コマンドによって、特定の 1 組のルートを特定インターフェースから公示する必要があることを指定します。ルートは、少なくとも 1 つの enable sending コマンドによって組み込まれている場合にのみ RIP 更新に組み込まれます。**enable sending static-routes** コマンドは、インターフェース ip-interface-address から送信される RIP 更新に、すべての静的構成ルートおよび直接接続ルートを組み込むことを指定します。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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 更新のコンテンツを決めます。このコマンドには類似の **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** コマンドの効果は加算的です。個別の **enable sending** コマンドによって、特定の 1 組のルートを特定インターフェースから公示する必要があることを指定します。ルートは、少なくとも 1 つの **enable sending** コマンドによって組み込まれている場合にのみ RIP 更新に組み込まれます。**enable sending host-routes** コマンドは、インターフェース ip-interface-address から送信される RIP 更新にすべてのホスト・ルートを含める必要があることを指定します。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: 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、受信されたパケ

ットの発信元 IP アドレスが、 IP ルーティング・テーブルに基づき、パケットがそこから受信されたインターフェースと矛盾していないことを検証します。このオプションは、IP ホストに属していない発信元 IP アドレスを使用している (スプーフィング と呼ばれる動作) 不正な動作を行う IP ホストからのパケットの転送を防ぐのに役立ちます。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** コマンドによってアクセスされる) 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 パケットを送信できるようにします。

例: `enable source-routing`

tftp-server
ルーターが、ネットワークからの構成ファイルまたはイメージ・ロードに対する TFTP GET または PUT 要求を受け入れることができるようにします。

例: `enable tftp-server`

timestamp
ルーターが、Timestamp IP オプションを含む IP パケットを受信および転送できるようにします。これがデフォルトです。

注: この機能は、使用不可にされていると、他の IP 機能に影響を与えずに起動することができます。詳細については、Talk 5 **reset IP** コマンドを参照してください。

udp-forwarding *port-number*
ルーターが受信した指定の UDP あて先ポート番号を持つパケットの UDP 転送を使用可能にします。

デフォルト: すべてのポート番号への UDP 転送が使用不可にされます。

port-number
有効値: 0 ～ 65535 の範囲の整数

デフォルト値: 0

例: `enable udp-forwarding 36`

vrrp バーチャル・ルーター冗長度プロトコルを使用可能にします。

例: `enable vrrp`

List

list コマンドは、起動された特定のサブコマンドに対応する種々の IP 構成データ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
構成されたアクセス制御モード (使用可能または使用不可) および構成されたグローバル・アクセス制御レコードのリストを表示します。各レコードがそのレコード番号と共に表示されます。このレコード番号は、IP **move access-control** コマンドを使用してリストの順序を変更するときに使用できます。

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、それぞれに構成された同報通信フォーマットと共に表示します。*BDG/0* によって識別された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 転送が使用可能であるか使用不可であるかを示し、構成された BOOTP サーバーのリストを表示します。

例: `list bootp`

icmp-redirect
ICMP 転送メッセージの送信が各 IP インターフェースで使用可能にされるのか、使用不可にされるのかをリストします。

igmp IGMP 構成を表示します。

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 構成済みの MTU 値をリストします。

nexthop-awareness

すべての IP インターフェースのネクスト・ホップ認識の設定値をリストします。

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。名前を指定すると、そのフィルターに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と、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でパケット・フィルターを構成してある場合は、そのインターフェースは *BDG/0* によって識別されます。

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

same subnet を含めて、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

構成された IP ルーティング・プロトコル (OSPF、RIP、BGP) の状態を、他の一般的な構成設定値と共に表示します。

例: `list protocols`

redundant-default-gateway

構成された各インターフェースの冗長デフォルト IP 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 1 組のルートを表示します。詳細については、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

構成された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、再組み立てバッファー・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 RIP 情報に関連するインターフェース別のタグを表示します。これらのタグは、後に BGP を介して再公示するためにルートをグループ化するのに使

用できます。この場合、タグはルートの発信元の自律システム (AS) 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

すべてのポートおよびすべての IP アドレスを含めて、UDP 転送機能に構成されたすべての情報を表示します。

例: list udp-forwarding

vrid 構成済みの VRRP 状態、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順序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 from# をレコード番号 to# の直後に置きます。レコードを移動すると、直ちに新しい順序を反映するように番号が付け直されます。

ルーターは作成された順序で、リスト内のアクセス制御レコードを適用します。インターフェースで受信した各パケットに対して、ルーターは一致が見つかるまで、各アクセス制御レコードを順番に適用します。パケットに一致した最初のレコードによって、そのパケットが廃棄されるのか、指定のあて先に転送されるのかが決まります。

そのため、アクセス制御レコードの順序は非常に重要です。順序が間違っていると、ユーザーの意図に反して、特定のパケットが除去されたり、ブロックされたりすることになります。

たとえば、アクセス制御レコード 1 の規則が *このインターフェースでは、ネットワーク 10.0.0.0 からのすべてのパケットをブロックする*であるとします。これに対して、アクセス制御レコード 2 は、 *ネットワーク 10.0.0.0 のサブネット 10.5.5.0 からの、アドレス 1.2.3.4 あてのパケットは通過を許可する*であるとします。この順序で指定された場合、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許可しているにもかかわらず、これらのレコードは 10.0.0.0 からのすべてのトラフィックをブロックすることになります。

この例では、レコード 1 がレコード 2 を無効にしています。特定のパケットを転送するというレコード 2 の意図にもかかわらず、レコード 1 はルーターが 10.0.0.0 からのすべてのパケットを廃棄することを保証しています。このタイプの問題を修正するためのかぎは、アクセス制御レコードの順序にあります。順序を修正することにより、サブネット 10.5.5.0 内のアドレス 1.2.3.4 あてのパケットはインターフェースを通過するようになります。ルーターはユーザーの意図通りに 10.0.0.0 からのその他のパケットをすべて廃棄します。

構文:

move access-control *from# to#*

例: move 5 2

Set

set コマンドは、IP 構成内の特定の値、ルート、およびフォーマット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*

ルーターの IP アクセス制御を使用可能または使用不可に構成することができます。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およびインターフェース専用リストが使用可能になります。*off* に設定すると、すべてのリストを使用不可にしますが、削除することはありません。

例: set access-control on

access-control log-facility *log-facility*

アクセス制御の Syslog 機能を設定します。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、使用不可にされていると、他の IP 機能に影響を与えずに起動することができます。詳細については、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

デフォルト値: 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から同報通信パケットを送信するときに使用する IP 同報通信フォーマットを指定します。IP 同報通信が最も一般的に使用されるのは、ルーターが RIP 更新パケットを送信するときです。

style パラメーターは、local wire または network の値を取ることができます。Local-wire 同報通信アドレスは、オール 1 (255.255.255.255) またはオール 0 (0.0.0.0) です。Network 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部分から始まります。

fill-pattern 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、もしあれば、ネットワークおよびサブネット以外の部分) をオール 1 に設定するのか、オール 0 に設定するのかを示します。

受信時に、ルーターはすべての形式の 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

デフォルト値: なし

style **有効値**: *local-wire* または *network*

デフォルト値: local-wire

fill-pattern

有効値: *0* または *1*

デフォルト値: 1

下の例は、同報通信アドレス 255.255.255.255 を構成します。2 番目の例は、ネットワーク 192.9.1.0 はサブネット化されていないものと想定して、同報通信アドレス 192.9.1.0 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・エントリーの最大数を構成します。このキャッシュは、ルーターが最近パケットを転送した特定の IP アドレスに関する情報を保管します。キャッシュは、複数のパケットを同一のあて先に転送するのにかかる処理時間を減らします。

このキャッシュと対照的に、IP ルーティング・テーブル は、すべてのアクセス可能なネットワークに関する情報を保管しますが、特定の IP あて先アドレスは保管しません。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** コマンドを使用します。

有効値: 64 ～ 10000

デフォルト値: 64

例: set cache-size 64

default network-gateway *next-hop cost*

権限ルーター (デフォルト・ゲートウェイ) へのルートを構成します。ルーターのデフォルト・ゲートウェイは、ルーター自体よりも完全なルーティング情報を持っているものと想定します。

ルートは、ネクスト・ホップ (next-hop) の IP アドレスと、デフォルト・ゲートウェイまでの距離 (cost) によって指定されます。

不定のあて先を持つパケットはすべて、権限ルーター (デフォルト・ゲートウェイ) に転送されます。

nexthop

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0 ゲートウェイ・コスト 1

cost **有効値**: 0 ～ 255 の範囲の整数

デフォルト値: 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ルーター (デフォルト・サブネット・ゲートウェイ) へのルートを構成します。各サブネット・ネットワークごとに別々のデフォルト・サブネット・ゲートウェイを構成できます。

ネクスト・ホップ (next-hop) の IP アドレスと、デフォルト・ゲートウェイまでの距離 (cost) が、ルートを指定します。

既知のサブネット・ネットワークの不定のサブネットあてのパケットはすべて、サブネット・ネットワークの権限ルーター (デフォルト・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

デフォルト値: 0.0.0.0

next-hop

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

cost

有効値: 0 ～ 255 の範囲の整数

デフォルト値: 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) パラメーターを構成します。以下のパラメーターに値を指定できます。

query interval *net interval*

IGMP 一般照会の間隔を変更します。

net 構成されるインターフェースのネットワーク番号を指定します。

有効値: 任意の有効なネットワーク番号

デフォルト値:なし

interval

一般照会の伝送間の秒数を指定します。

有効値: 1 ～ 3600

デフォルト値: 125

response-interval *net interval*

IGMP 一般照会に差し込まれる最大応答時間を変更します。

net 構成されるインターフェースのネットワーク番号を指定します。

有効値: 任意の有効なネットワーク番号

デフォルト値:なし

interval

照会とレスポンスで IGMP レポートを送信するホストの伝送間の秒数を指定します。

有効値: 1 ～ 60

デフォルト値: 10

robustness-variable *net variable*

ネットワークの耐性変数を変更します。

net 構成されるインターフェースのネットワーク番号を指定します。

有効値: 任意の有効なネットワーク番号

デフォルト値:なし

variable

ネットワーク上でパケットが失われないように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

デフォルト値: 2

leave-interval *net interval*

IGMP 特定照会に差し込まれる最大応答時間を変更します。

net 構成されるインターフェースのネットワーク番号を指定します。

有効値: 任意の有効なネットワーク番号

デフォルト値:なし

interval
特定の照会とレスポンスで IGMP レポートを送信するホストの伝送間で許される秒数を指定します。

有効値: 1 〜 60

デフォルト値: 1

version *net vernum*
ネットワーク上で実行中の IGMP のバージョンを変更します。

net 構成されるインターフェースのネットワーク番号を指定します。

有効値: 任意の有効なネットワーク番号

デフォルト値:なし

vernum
ネットワーク上で実行するバージョン番号を指定します。

有効値: 1 または 2

デフォルト値: 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ている 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と見なされます。内部アドレスを定義する主な理由は、インターフェースが非アクティブになっても非アクティブにならない TCP コネクションに対してアドレスを提供することです。このアドレスはデータ・リンク交換 (DLSw) に使用され、代替パスの使用を可能にして、インターフェースが非アクティブになったときに DLSw コネクションが破壊されるのを回避します。内部アドレスはアクティブのままであり、OSPF はこのあて先へのアクティブ IP ルートを維持しているので、IP ルーティングは TCP コネクションをダウンにしたり、DLSw の上で実行されている SNA セッションを破壊することなく、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、非番号制インターフェースが使用されている場合にも貴重です。これは、このルーターによって発信され、非番号制インターフェースを介して転送されるパケットの発信元アドレスとしての第 1 の選択肢です。このアドレスの安定度が、この種のパケットの追跡を容易にします。ルーター ID と内部アドレスに同じ IP アドレスを使用すれば、混乱の確率はさらに小さくなります。そのため、ルーター ID のデフォルトは内部アドレスになっています。

内部アドレスが定義されている場合、これは OSPF によってルーターに直接接続されているすべてのエリアへのホスト・ルートとして公示されます。

有効な値: 任意の有効な IP アドレス

デフォルト値: 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

デフォルト値: ネットワーク上のすべての非ゼロ MTU

originate-rip-default

RIP でこのルーターがデフォルト・ゲートウェイとして公示されます。このコマンドは、次の環境で使用します。

- このルーターのルーティング・テーブル内の IP ルートが、多数のプロトコルによって決められている。
- RIP がそれらのプロトコルの 1 つである。
- ほとんどの部分ルーティング情報が、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。

RIP ネットワーク内の RIP が知らないあて先へのトラフィックは、このルーターへのデフォルト・パスを通します。次に、このノードのルート・テーブル内のより完全なルーティング情報を使用して、トラフィックを適切なパスを通してあて先へ転送することができます。RIP ネットワークには公示されないルートをこのルーターが知っている場合にのみデフォルトを発信するように、ルーターを構成することも可能です。

このコマンドを発行すると、ルーターは常に RIP デフォルトを発信するのか、あるいは他のプロトコルからのルートが利用可能な場合にのみ RIP デフォルトを発信するのかを尋ねられます。

このデフォルト・ルートは、RIP 以外のネットワークあてのトラフィックを境界ルーターに送ります。単一のデフォルト・ルートを発信することは、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、自身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ています。

from AS number

有効値: 0 ～ 65535 の範囲の整数

デフォルト値: なし

to network number

有効値: 任意の有効な IP アドレス

デフォルト値: なし

default cost

有効値: 0 ～ 255 の範囲の整数

デフォルト値: 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』 質問に 『Yes』 と応答すると、デフォルト・ルートが常に発信されます。

- 『BGP』 質問に 『Yes』 と応答すると、ルーティング・テーブル内に BGP ルートが存在するときにデフォルトが発信されます。
- 『if OSPF routes available』 質問に 『Yes』 と応答すると、ルーティング・テーブル内に OSPF ルートが存在するときに RIP デフォルトが公示されます。
- RIP デフォルトを発信することに決める場合、ルーターは 『original default cost』 の数値を使用します。
- BGP ルートの AS (自律システム) 番号として 0 が指定される場合、任意の AS からのネットワーク基準に合うルートによって、RIP デフォルトが発信されます。
- BGP または OSPF ネットワーク基準に 0.0.0.0 が指定される場合、AS 基準に合うどの BGP ルートによっても、RIP デフォルトを発信させることができます。

reassembly-size *bytes*

分割された IP パケットの再組み立て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

デフォルト: 12000

例: set reassembly-size 12000

rip-in-metric *ip-interface-address metric*

ルーティング・テーブルに導入する前に、メトリックの構成をインターフェースの RIP ルートに追加することを可能にします。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

metric

有効値: 1 〜 15 の範囲の整数

デフォルト値: 1

例: set rip-in-metric 128.185.120.209 1

rip-out-metric *ip-interface-address metric*

RIP または RIP2 ルートを公示するように構成されたインターフェースで公示される RIP ルートに、メトリックの構成を追加することを可能にします。

ip-interface-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

metric

有効値: 1 〜 15 の範囲の整数

デフォルト値: 0

例: set rip-out-metric 128.185.120.209 0

router-id *ip-address*

各種の IP パケットを発信するときにルーターによって使用されるデフォルト IP アドレスを設定します。このアドレスは、マルチキャスティングおよび OSPF では特に重要です。

ルーター ID は、ルーターの構成済み IP インターフェース・アドレスの 1 つ、または構成済み内部 IP アドレスに一致していることが必要です。そうでない場合は無視されます。無視された場合、あるいは単に構成されていない場合、ルーターのデフォルト IP アドレス (および、その OSPF ルーター ID) は、内部 IP アドレス (構成されている場合) またはルーターの構成内の最初の 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

デフォルト値: 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。デフォルト・サイズは 768 エントリーです。ルーティング・テーブル・サイズの設定が小さ過ぎると、ルートが廃棄されてしまいます。ルーティング・テーブル・サイズの設定が大き過ぎると、ルーターのメモリー資源が無駄になります。テーブル・サイズの詳細については、318ページの『Sizes』を参照してください。

有効値: 64 ～ 65535 の範囲の整数のエントリー数

デフォルト値: 768 エントリー

例: `set routing table-size 1000`

tag

受信した RIP 情報に関連するインターフェース別のタグを構成します。これらのタグは、後に BGP を介して再公示するためにルートをグループ化するのに使用できます。この場合、タグはルートの発信元の自律システム (AS) 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』 という章に記載されているポリシーの発信、送信、および受信に関する情報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 の範囲の整数

デフォルト値: 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の time-to-live (存続時間) を指定します。

有効値: 1 ～ 255 の範囲の数値

デフォルト値: 64

例: `set ttl 255`

Update

update *packet-filter-name*

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。これはこのコマンドの例です。

```
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した任意のパケット・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、以下のコマンドを入力することができます。

構文:

add access-control

change access-control

delete access-control

disable

enable

list access-control

move access-control

Packet-filter '*filter-name*' Config> プロンプト用の **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> プロンプトで表示される **access-control** パラメーターの下のパラメーターの説明を参照してください。たとえば、**update packet-filter add access-control** コマンド用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。

disable および **enable** コマンドについては、キーワード **source-addr-verification** は、Packet-filter '*filter-name*' Config> プロンプトからだけ構成することができます。

以下の節では、**update packet-filter** コマンド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るが、ルーター全体のフィルターには適用されず、Packet-filter '*filter-name*' Config> プロンプトでのみ入力されるパラメーターです。

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、パケットを NAT に通過させて、アドレス変換させます。このタイプは、パケット・フィルターでのみ、かつ包括 (inclusive) と組み合わせて指定されたときのみ (たとえば、***IN***) 有効です。NAT および IPsec のタイプは、同じ規則内で指定することができます (たとえば、***INS***)。詳細については、アクセス・インテグレーター・サービス ソフトウェア

*使用者の手引き*に記載されている NAT 機能の説明を参照してください。 NAT のアクセス制御フィルターの例は、*アクセス・インテグレーター・サービス 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。

デフォルト値: N

デフォルト値: なし

IP Secure Tunnel (IPsec)

アウトバウンド・パケット・フィルターにあるこのタイプのアクセス制御規則は、パケットを IPsec に通過させ、IPsec トンネル内でカプセル化するか、場合によっては暗号化します。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 セキュア・トンネルを通じて受信されたことを検証します。このタイプは、パケット・フィルターでのみ、かつ包括 (inclusive) と組み合わせて指定されたときのみ (たとえば、***IS***) 有効です。NAT および IPsec のタイプは、同じ規則内で指定することができます (たとえば、***INS***)。 IPsec 用のアクセス制御フィルターの例は、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きで IP セキュリティー機能の使用についての章に記載されています。

有効値: S

デフォルト値: なし

add/change access-control *IPsec-tunnel-ID*

このパラメーターが有効なのは、規則タイプが IPsec である場合だけです。出力パケット・フィルターでは、このパラメーターは、パケットが送信されるときに通過する IP セキュア (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、パケットがそこから受信された IPsec トンネルを指定します。

有効値: 1 〜 65536

デフォルト値: 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、受信されたパケットの発信元 IP アドレスが、 IP ルーティング・テーブルに基づき、パケットがそこから受信されたインターフェースと矛盾していないことを検証します。このオプションは、IP ホストに属していない発信元 IP アドレスを使用している (スプーフィング と呼ばれる動作) 不正な動作を行う IP ホストからのパケットの転送を防ぐのに役立ちます。

例:

```
Packet-filter 'filter-name' Config> enable source-addr-verification
```

例:

以下の例は、パケット・フィルター用のさまざまなアクセス制御規則を構成する方法を示しています。NAT および IPsec 用のアクセス制御規則の例については、アクセス・インテグレーター・サービス ソフトウェア使用者の手引きで IP セキュリティー機能の使用についての章を参照してください。

例 1--Exclusive タイプのアクセス制御規則

この例は、ネットワーク 128.185.0.0 から発信され、インターフェース 0 で受信されたすべての着信パケットを除外する方法を示しています。

```
    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--アクセス制御規則の削除

アクセス制御インデックス番号を見付けるには、**list access control** コマンドを使用します。

```
    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して応答します。

```
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 コマンドを使用すれば、各パケット・フィルター用に構成されているアクセス制御を表示することができます。

```
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

パケット・フィルターのアクセス制御レコードの順序を変更する場合は、**move access-control** コマンドを使用して、次のように指定します。

```
    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には、次の手順を使用します。このプロセスにより IP *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** を入力する。 (このコマンドの詳細については、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*の “OPCON プロセス” の章を参照してください。)たとえば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、端末に GWCON プロンプト (+) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. + プロンプトで **protocol ip** コマンドを入力して、IP> プロンプトを表示する。

   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 では、IP 監視コマンドをリストします。これらのコマンドを用いて、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、次のものが含まれます。すなわち、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を表示する機能、IP ルーティング・テーブルの現在の状態を 表示する機能、および IP ルーティング・エラーのカウントをリストする機能があります。

表 19. IP 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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、構成されたアクセス制御レコードと共にリストします。
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・エラーの数および廃棄されたパケットの数を含めた、種々の IP 統計をリストします。
Dump routing tables	IP ルーティング・テーブルのコンテンツをリストします。
IGMP	IGMP 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 packet-filter、またはすべてのフィルターに定義されたアクセス制御情報を表示します。
Parameters	さまざまな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、レスポンスを監視します。このコマンドは、インターネットワーク環境の障害を分離するのに使用できます。
Redundant Default Gateway	冗長デフォルト・ゲートウェイが存在するかどうか、および存在する場合は、アクティブか非アクティブかをリストします。
Reset	IP/RIP 構成をリセットすることができるようにします。

表 19. IP 監視コマンドの要約 (続き)

コマンド	機能
RIP	RIP プロトコルの状態を表示します。
Route	特定のIP あて先へのルートが存在するかどうかを示し、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・エントリーをリストします。
Route-table-filtering	定義されたルート・フィルターをリストし、route-filtering が使用可能であるか使用不可であるかを示します。
Sizes	特定の IP パラメーターのサイズを表示します。
Static routes	構成された静的ルートを表示します。これにはデフォルト・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を (ホップごとに) 表示します。
UDP-Forwarding	**add** コマンド または **enable** コマンドを使用して追加した UDP ポート番号とあて先 IP アドレスを表示します。
VRID	特定の VRID についての詳しい情報を表示します。
VRRP	VRRP プロトコルについての要約状態をリストします。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Access Controls

access controls コマンドは、使用されるグローバル・アクセス制御モードを、構成されたグローバル・アクセス制御規則のリストと共に印刷するのに使用します。

アクセス制御は、使用不可 (アクセス制御は実行されず、アクセス制御規則は無視されることを意味する) または使用可能 (アクセス制御が実行され、アクセス制御規則は認知されることを意味する) 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一致するパケットは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一致するパケットは転送されることを意味します。アクセス制御が使用可能の場合、どのアクセス制御レコードにも一致しないパケットは廃棄されます。*Prot* (プロトコル) は IP プロトコル番号を示します。*Sports* は、TCP/UDP 発信元ポート番号の範囲を示します。*Dports* は、TCP/UDP あて先ポート番号の範囲を示します。*SYN* は TCP コネクション確立フィルターを示します。*T/C* は ICMP タイプおよびコードを表します。*SLOG* は SysLog を表します。

Use フィールドは、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照合した回数、たとえば、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起動された回数を指定します。

この例では、TOS フィルターはアクセス制御規則番号 4 によって起動されています。TOS パラメーターを示します。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、最近ルートされたあて先が入っている 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内に存在しない場合、ルーターはルーティング情報テーブルでそのあて先を探し、転送を決定します。

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 最近、あて先ホストに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。送信側ルーターがパケットの転送に使用す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

counters コマンドは、IP 転送プロセスに関連する統計を表示するのに使用します。これには、ルーティング・エラーの数や輻輳 (ふくそう) のために廃棄されたパケットの数が含まれます。

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・テーブルが満ぱいのために廃棄されたルートの数をリストします。

Net unreachable
あて先が不定のために転送できなかったパケットの数を示します。権限ルーター (デフォルト・ゲートウェイ) に転送されたパケットの数はカウントされません。

Bad subnet number
受信したイリーガル・サブネット (オール 1 またはオール 0) あてのパケットまたはルートの数をカウントします。

Bad net number
受信したイリーガル IP あて先 (たとえば、クラス E アドレス) あてのパケットまたはルートの数をカウントします。

Unhandled broadcasts
受信した (非ローカル) IP 同報通信 (これらは転送されません) の数をカウントします。

Unhandled multicasts
受信したが、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) の数をカウントします。

Unhandled directed broadcasts
このタイプのパケットの転送が使用不可にされているときに受信した、指定 (非ローカル) IP 同報通信の数をカウントします。

Attempted forward of LL broadcast
非ローカル IP アドレスを持っているのにリンク・レベル同報通信アドレスに送信された、受信パケットの数をカウントします。これらのパケットは廃棄されます。

Packets discarded through filter
フィルター・ネットワーク/サブネットにアドレス指定された受信パケットの数をカウントします。これらは通知せずに廃棄されます。

IP multicasts accepted
受信され、ルーターによって正常に処理された IP マルチキャストの数をカウントします。

IP packet overflows
転送側の入力待ち行列の輻輳 (ふくそう) のために廃棄されたパケットの数をカウントします。これらのカウントは受信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/サブネットごとに、個別のエントリーが印刷されます。使用されている IP デフォルト・ゲートウェイ (存在する場合) が、ディスプレイの最後にリストされます。

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 そのルートがどのように導出されたかを示します。

Sbnt - ネットワークがサブネット化されていることを示します。この種のエントリーは、プレースホルダーとしてのみ使用されます。

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 プロトコルを通して確認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 - BGP プロトコルを通して確認されたルートを示します。

BGPR - BGP プロトコルを通して確認され、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 - ルートは OSPF エリア内ルートであることを示します。

SPIA - これは OSPF エリア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 とタイプ 2) を示します。

Rnge - アクティブ OSPF エリア・アドレス範囲を表し、パケット転送には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・エントリーが前回に更新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。パケットを転送するために送信側ルーターによって使用された 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・タイプには静的または直接接続されたバックアップがあることを示します。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/サブネットでは RIP 更新が常に受け入れられることを示します。

欄の最後の括弧内の数字は、そのあて先への等価コスト・ルートの数を示します。これらのルートに属する最初のホップは IP **route** コマンドを用いて表示することができます。

IGMP

igmp コマンドは、IGMP カウンターおよび IGMP の稼働パラメーターを表示するのに使用します。

構文:

igmp counters

parameters

counters

総受信される 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 装置が指定のネットワーク上で照会を行うかどうかを指定します。

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
装置の付加インターフェースの操作可能 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
指定インターフェースの耐性変数

Query interval
この装置が指定の IGMP 照会を行う場合、そのネットワーク上での IGMP 一般照会間の秒数

Response interval
この装置が指定の IGMP 照会を行う場合、そのネットワーク上での IGMP 一般照会に差し込まれる最大応答時間

Leave query interval
この装置が指定の IGMP 照会を行う場合、そのネットワーク上での IGMP 特定照会に差し込まれる最大応答時間

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。各アドレスが、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・マスクと共に表示されます。同じインターフェース上でのブリッジングと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* によって識別されます。

IP インターフェース・アドレスが構成されていないハードウェア・インターフェースは、IP 転送プロセスによって使用されず Not an IN net としてリストされます。ただし、例外が 1 つあります。シリアル・ラインは、IP トラフィックを転送するために IP インターフェース・アドレスが割り当てられている必要はありません。このようなシリアル・ラインは、非番号制と呼ばれています。これらは、アドレス 0.0.0.0 として表示されます。

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定義されている情報を表示するのに使用します。Packet-filters は、アクセス制御レコードのインターフェース特定リストです。インターフェースはインターフェース番号によって識別されます。ただし、同じインターフェース上でのルーティングとブリッジングに使用されるブリッジ・インターフェースは例外です。これは *BDG/0* によって識別されます。

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、さまざまな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 エコー・メッセージを指定のあて先に送信させ、(つまり、『PING』 して) レスポンスを監視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の障害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 プロセスは連続的に実行され、パケットが追加されるごとに ICMP シーケンス番号が増分されます。一致する ICMP エコー・レスポンスを受信すると、そのシーケンス番号と往復時間が報告されます。往復時間の計算の細分性 (タイム・レゾリューション) は、通常は約 20 ミリ秒ですが、プラットフォームによって異なります。

PING プロセスを停止するときは、コンソールで任意の文字を入力します。このとき、パケット紛失、往復時間、および到達不能 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・アドレスをあて先として指定した場合は、送信されたパケットに対して複数のレスポンス (各グループ・メンバーにつき 1 つ) が印刷される場合があります。戻された各レスポンスが、応答側の発信元アドレスと共に表示されます。

PING のサイズ (ICMP ヘッダーを除いた、ICMP メッセージ内のデータ・バイト数)、データの値、存続時間 (TTL) 値、PING の速度、および設定する TOS ビットを指定することができます。発信元 IP アドレスも指定することができます。IP アドレス を指定していない場合、ルーターは指定のあて先への発信インターフェースのローカル・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からあて先への接続可能性を検査する場合は、そのインターフェースの IP アドレスを発信元アドレスとして入力します。

あて先パラメーター (destination) だけは指定が必須です。他のすべてのパラメーターの指定は任意です。デフォルトでは、サイズは 56 バイト、TTL は 64、速度は秒当たり 1 PING、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されます。デフォルトでは、残りのデータは、値が X'04' から始まって 1 ずつ増分され、 X'FF' から X'00' へと循環する一連のバイトです (たとえば、X'04 05 06 07 . . . FC FD FE FF 00 01 02 03 . . .')。これらの値は、デフォルトが使用されるときだけ増分されます。データ・バイト値が指定される場合、ICMP データのすべて (最初の 4 バイトを除く) はその値に設定され、その値は増分されません。たとえば、データ・バイト値を X'FF' に設定する場合は、ICMP データは X'FF FF FF . . .' の値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対して構成された冗長デフォルト 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: タイプは 『Primary』 または 『Backup』 です。状態は 『 Active』 または 『Standby』 です。

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>
```

以下の機能は、**reset ip** コマンドによってサポートされます。

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 プロトコル状態の詳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、指定の IP あて先へのルート (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、ネクスト・ホップの IP アドレスが、照合ルーティング・テーブル・エントリーに関する詳細情報と共に表示されます。(IP **dump** コマンドの項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であるかどうかを表示し、定義されたルート・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、構成された特定 IP パラメーターの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
構成された、ルーティング・テーブルが維持するエントリーの数

Table entries used
ルーティング・テーブルから使用されたエントリーの数。この数には、アクティブおよび非アクティブの両方のエントリーが含まれます。“dump” コマンドによって “xx nets known” として表示された値は、アクティブ・ルーティング・テーブル・エントリーの数です。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・エントリーを維持するとともに、他の予想されるルーティング・エントリーも維持できる十分な大きさであることが必要です。

Reassembly buffer size
分割された IP パケットを再組み立てするために使用される、再組み立てバッファーの構成されたサイズ

Largest reassembled pkt
このルーターが再組み立てする必要がある最大 IP パケット

Size of routing cache
構成されたルーティング・キャッシュのサイズ

# of cache entries in use
現在キャッシュから使用されているエントリーの数

Static Routes

static routes コマンドは、構成済みの静的ルートのリストを表示するのに使用します。構成されたデフォルト・ゲートウェイおよびデフォルト・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 address-mask と組みで指定されます。デフォルト・ゲートウェイは、あて先が 0.0.0.0 でマスクが 0.0.0.0 の静的ルートとして表示されます。デフォルト・サブネット・ゲートウェイは、全 IP サブネット・ネットワークへの静的ルートとして表示されます。

次の例は、構成されたデフォルト・ゲートウェイ、構成されたデフォルト・サブネット・ゲートウェイ (128.185.0.0 がサブネット化されているものと想定)、およびネットワーク 192.9.10.0 への静的ルートを表示します。

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 ルートの着信マスク

Cost このルートを使用するコスト

Next Hop パケットがこのルートを使用して通過する次のルーター

Traceroute

traceroute コマンドは、指定のあて先へのパス全体をホップごとに表示するのに使用します。連続する各ホップに対して、**traceroute** コマンドは 3 つのプローブのデフォルトを送信し、応答側の IP アドレスとそのレスポンスに関連する往復時間を印刷します。特定のプローブがレスポンスを受信しなかった場合、アスタリスクが表示されます。ディスプレイの各行はこの 3 つのプローブ・セットに関連しており、左端の数字は、コマンドを実行したルーターからの距離 (ルーター・ホップ数) を示します。

traceroute は、あて先に到着した時点、ICMP Destination Unreachable を受け取った時点、またはパス長が 32 ルーター・ホップのデフォルト最大値に達した時点で完了します。

プローブが予期しない結果を受信したときには、何種類かの表示が示されます。『!N』 は、ICMP Destination Unreachable (net unreachable) を受信したことを示します。『!H』 は、ICMP Destination Unreachable (host unreachable) を受信したことを示します。『!P』 は、ICMP Destination Unreachable (protocol unreachable) を受信したことを示します。プローブは不明のポートに送信された UDP パケットなので、ポートに到達不能であることは予想されます。『!』 は、あて先に到達したが、あて先から受信した応答の TTL が 1 であったことを示しています。これは通常、あて先のエラーを示しており (UNIX の一部のバージョンではよく見られます)、そのためあて先はプローブの TTL を応答に挿入しています。残念ながら、この結果、最終的にあて先に到達する前に、アスタリスクだけから成る行が多数生じることになります。

構文:

traceroute *dest-addr [src-addr data-size probes wait tos max-ttl]*

dest-addr ルートの反対側のアドレス

src-addr トレースが発信する発信元アドレス

data-size traceroute メッセージのデータ・フィールドのバイト単位のサイズ。データ・フィールドに、UDP ヘッダーは含まれません。

probes 各ホップから送信された UDP traceroute メッセージの数

wait 再試行の間隔 (秒単位)

tos UDP メッセージ内の TOS ビットの設定値。たとえば、値 X'10' (B'00010000') の場合、TOS ビットは B'1000' に設定されます。デフォルトは 0 で、この場合、TOS ビットは B'1000' に設定されます。

max-ttl 各メッセージの秒数単位の最大活動時間

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
あて先エリア・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 と、パケットがあて先に到達するまでにかかった時間を表示した最初のトレース。パケットは 3 回トレースされます。

Destination unreachable
あて先への利用可能なルートがないことを示します。

3 * * *
ルーターはあて先からの何らか形でのレスポンスを期待しているが、あて先は何も応答しないことを示しています。

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 ポートと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・ルーターの詳しい状態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15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・テーブルを 作成するために、次の IGP をサポートしています。すなわち、最短パス最優先オープン (OSPF) プロトコルおよび RIP プロトコルです。OSPF は、リンク状態テクノロジーまたは最短パス優先 (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。

本章には、以下の節が含まれています。

- 『OSPF ルーティング・プロトコル』
- 326ページの『OSPF の構成』
- 343ページの『OSPF 構成環境へのアクセス』
- 343ページの『OSPF 構成コマンド』
- 334ページの『マルチキャスト転送』

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・プロトコルは、内部ゲートウェイ・プロトコル (IGP) と呼ばれます。IGP は ネットワーク到達可能性および AS 内のルーティング情報を動的に検出し、その情報を使用して IP ルーティング・テーブルを作成します。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。同時に実行する場合は OSPF ルートが優先されます。一般的には、その堅固さ、応答性、および帯域幅の所要量の少なさから、OSPF プロトコルを使用することが推奨されます。

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) に指定されている OSPF ルーティング・プロトコルを完全に実現しています。OSPF は、到達可能なあて先への最善ルートを検出および確認するリンク状態動的ルーティング・プロトコルです。OSPF は AS のトポロジー変更を速やかに検出し、短いコンバージェンス期間の後、新規ルートを計算することができます。OSPF プロトコルは、IP パケットのカプセル化は行わず、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) あて先への最善ルートを検出および確認するリンク状態動的ルーティング・プロトコルです。OSPF は AS のトポロジー変更を速やかに検出し、短いコンバージェンス期間の後、新規ルートを計算することができます。OSPF プロトコルは、IP パケットのカプセル化は行わず、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

ルーターは初期化されると、ハロー・プロトコルを使用してハロー・パケットを近隣 (neighbor) に送信し、近隣はそれぞれのパケットをルーターに返送します。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、ルーターはハロ

ー・パケットをマルチキャスト・アドレス *ALLSPFRouters (224.0.0.5)* あてに送信することによって、*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の場合は、ルーターが *近隣* を発見するのを助ける情報をユーザーが構成する必要があります。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の*指定ルーター* も選出します。

次に、ルーターはそれぞれのトポロジー・データベースを同期化するために、近隣との隣接 (adjacencies) の形成を試みます。隣接は、ルーティング・プロトコル・パケットの配信 (送信と受信) およびトポロジー・データベース更新の配信を制御します。マルチアクセス・ネットワークでは、指定ルーターが隣接 (adjacent) になるルーターを決めます。

ルーターは、定期的にその状態またはリンク状態を隣接に公示します。*リンク状態*公示 (LSA) は、エリア全体にフラッディング (全ポートにパケットを送出) され、すべてのルーターが正確に同じトポロジー・データベースを持つようにされます。このデータベースは、あるエリア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、各ルーターは自身をルート (根) として指定し、最短パスのツリーを計算することができます。この最短パス・ツリーが、ルーティング・テーブルを生成します。

OSPF は、RIP では得られないサービスが提供さ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含まれています。

- *最小コスト・ルーティング。* 任意の組み合わせのネットワーク・パラメーターに基づいて、パス・コストを構成することができます。たとえば、帯域幅、遅延、およびドル・コストなどです。
- *ルーティング・メトリックに対する制限がない。* RIP ではルーティング・メトリックが 16 ホップに制限されますが、OSPF には制限がありません。
- *マルチパス・ルーティング。* 同一ポイントを接続する等価コストの複数のパスを使用することが可能です。これにより、これらのパスを使用して負荷を分散できるので、ネットワークの帯域幅をより効率的に使用できるようになります。
- *エリア・ルーティング。* プロトコルによる資源 (メモリーおよびネットワーク帯域幅) の消費を削減し、ルーティング保護レベルを向上します。
- *可変長サブネット・マスク。* IP アドレスを中断して可変サイズ・サブネットに入れることができるので、 IP アドレス・スペースを節約できます。
- *ルーティング認証。* ルーティング・セキュリティーを強化します。

OSPF は、以下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。* 通信回線を使用して 1 対のルーターを結合するネットワーク。2 つのルーターを接続する 56-Kbps シリアル・ラインは、ポイント・ポイント・ネットワークの例です。
- *同報通信。* 3 つ以上の接続ルーターをサポートし、1 つの物理メッセージをすべての接続ルーターにアドレッシング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例です。
- *非同報通信マルチアクセス (NBMA)。*3 つ以上の接続ルーターをサポートしますが、同報通信機能はないネットワーク。X.25 公衆データ・ネットワークは、非同報通信ネットワークの例です。OSPF が正しく機能するためには、このネットワークは非同報通信ネットワークに 接続された他の OSPF ルーターに関する追加の構成情報が必要です。

- *ポイント・マルチポイント。* 3 つ以上の接続ルーターをサポートし、同報通信機能がなく、部分メッシュのネットワーク。すべての接続ルーター間に PVC が存在するわけではないフレーム・リレーネットワークは、ポイント・マルチポイント・ネットワークの例です。非同報通信ネットワークと同様に、このネットワークに接続された他の OSPF ルーターに関する追加の構成情報が必要です。

指定ルーター

それぞれの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、ルーティング・プロトコルの 2 つの主要な機能 (すなわち、ネットワーク・リンク公示を発信すること、およびネットワーク上の他のすべてのルーターの隣接になること) を行う指定ルーターが存在します。

指定ルーターは、ネットワーク・リンク公示を発信するときに、そのネットワークに現在接続されているすべてのルーター (自身を含む) をリストします。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・アドレスになります。指定ルーターは、サブネット/ネットワーク・マスクを使用して、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を同期化する働きをします。

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調べて、指定ルーターを選出します。ルーターのインターフェースが最初に動作可能になったとき、ルーターは現在そのネットワークに指定ルーターが存在するかどうかをチェックします。存在する場合は、そのルーターの優先順位には関係なく、その指定ルーターを受け入れます。存在しない場合は、自身を指定ルーターとして宣言します。ルーターが自身を指定ルーターとして宣言したときに、同時に他のルーターも宣言した場合には、ルーター優先順位 (*Rtr Pri*) が高い方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、ルーター ID の高い方が選出されます。

指定ルーターが選出されると、それが多数の隣接のエンドポイントになります。同報通信ネットワークでは、指定ルーターは各隣接を介して個別にパケットを送信するのではなく、リンク状態更新パケットをアドレス ALLSPFRouters (224.0.0.5) あてにマルチキャストできるので、フラッディング手順が最適化されます。

マルチキャスト OSPF

マルチキャスティングは、1 つのパケットのコピーを選択されたサブネットのすべての可能なあて先に渡すことができる LAN 技法です。一部のハードウェア (たとえば、イーサネット) は、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・グループに所属できるようにすることにより、マルチキャストをサポートしています。ルーターの IP マルチキャスティング・サポートについての詳細は、251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 のマルチキャスト拡張 (MOSPF) を介した IP マルチキャスト・ルーティングをサポートします。

OSPF の使用

MOSPF ルーターは、新規タイプ (タイプ 6) のリンク状態公示 group-membership-LSA をフラッディングすることによって、ルーティング・ドメイン全体にグループ位置情報を配信します。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、マルチキャスト・データグラムのパスを 1 つのツリー (そのルート (根) はデータグラム発信元で、末端の分岐 (支局) はグループ・メンバーを含む LAN) として計算することにより、これを実行します。

MOSPF の実行時には、マルチキャスト・データグラム転送は、次のような方法で行われます。

- IP マルチキャストの転送は高信頼性ではありませんが、IP マルチキャスト・データグラムは、IP ユニキャストの配信と同じベスト・エフォートを用いて送達されます。
- 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あて先の間の最短パス (OSPF リンク状態コスト) を移動します。このようになるのは、各データグラム発信元とあて先グループの組みごとに別々のツリーが作成されるためです。
- マルチキャスト・データグラムは、各ホップでデータ・リンク・マルチキャストとして着信転送されます。ARP プロトコルは使用されません。あるネットワーク技術では、IP クラス D アドレスとデータ・リンク・マルチキャスト間でマッピングが行われ、別のネットワーク技術では、クラス D IP アドレスはデータ・リンク同報通信アドレスにマップされます。
- データグラム発信元から 2 つの別々のグループ・メンバーへのパスが最初の共通セグメント部分を共用している場合、パスが別々の方向に向かう地点までは、単一のデータグラムが転送されます。パスは、ルーター部分またはネットワーク部分で分割できます。パスがルーター部分で分割されている場合、ルーターは送信する前にパケットを複写します。パスがネットワーク部分で分割されている場合、ネットワークはデータ・リンク・マルチキャストによって複写します。
- ネットワーク構成には、MOSPF ルーターとマルチキャスト拡張を持たないルーターの両方を含めることも可能です。このような構成では、すべてのルーターがユニキャスト・ルーティングの形で相互動作します。これにより、ユーザーはマルチキャスト機能を徐々にインターネットワークに導入することが可能になります。

  MOSPF と非 MOSPF ルーター構成の一部では、マルチキャスト・ルーティングに予期しない障害が発生する場合があります。
- 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って、SNMP トラップをマルチキャスト・グループ・アドレスあてに送信するように構成できます。

OSPF の構成

以下の節では、OSPF プロトコルの初期構成の方法について説明します。この情報は、OSPF プロトコルを起動して実行するのに必要なタスクの概要です。構成を変更する方法については、343ページの『OSPF 構成コマンド』で説明しています。

以下のステップは、OSPF プロトコルを起動し、実行するのに必要なタスクの概要です。後続の各節で、それぞれのステップについて、例を含めて詳しく説明しています。

OSPF プロトコルを実行する前に、以下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。そのためには、OSPF ルーティング・ドメインの最終サイズを見積もることが必要です。(『OSPF プロトコルの使用可能化』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ていないネットワーク・テクノロジー (たとえば、フレーム・リレー) の場合、マルチキャスト・データグラムはルーターによって複写され、データ・リンク・ユニキャストとして転送される必要があります。(328ページの『OSPF ルーター ID の設定』 を参照してください。)
3. ルーターに接続されている OSPF エリアを定義する。OSPF エリアが定義されていない場合は、単一のバックボーン・エリアが想定されます。(328ページの『バックボーンと接続された OSPF エリアの定義』 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にパケットを送信するコストと、一連の OSPF 動作パラメーターを設定します。(332ページの『OSPF インターフェースの設定』 を参照してください。)
5. IP マルチキャスト (IP クラス D 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する。(334ページの『マルチキャスト転送』 を参照してください。)
6. ルーターが非同報通信ネットワーク(X.25、またはフレーム・リレー) にインターフェースする場合は、追加のインターフェース・パラメーターを設定する。(335ページの『非同報通信ネットワーク・インターフェース・パラメーターの設定』および 335ページの『広域サブネットワークの構成』を参照してください。)
7. ルーターが、このルーター上で実行されている他のルーティング・プロトコルから確認されたルート (BGP、RIP、または静的に構成されたルート) をインポートしたい場合は、AS 境界ルーティングを使用可能にする。また、ルートをタイプ 2 外部またはタイプ 1 外部のいずれとしてインポートするのかも定義する必要があります。(337ページの『AS 境界ルーティングの使用可能化』 を参照してください。)
8. 接続されたポイント・ポイントまたはポイント・マルチポイント・インターフェースを介して近隣ルーターによってブートしたい場合は、近隣の IP アドレスを構成する必要があります。これはポイント・ポイント・インターフェースの OSPF 近隣を追加することによって行います。

OSPF プロトコルの使用可能化

OSPF ルーティング・プロトコルを使用可能にする場合、OSPF ルーティング・ドメインの最終サイズを見積もるために、ユーザーは次の 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 外部ルートの合計数。別々の AS 境界ルーターによってインポートされる場合、1 つのあて先が複数の外部ルートに通じている場合があります。たとえば、OSPF ルーティング・ドメインに 2 つの AS 境界ルーターが存在し、両方が同じ 100 のあて先へのルートをインポートする場合、AS 外部ルートの数は 200 に設定します。
- ルーティング・ドメイン内の OSPF ルーターの合計数

この 2 つの値は、すべての OSPF ルーターで同値に構成します。OSPF プロトコルを実行する各ルーターは、ルーティング・ドメインのマップを記述したデータベースを持っています。このデータベースは、参加しているすべてのルーターで同一です。このデータベースから、ルーター自身をルート (根) とする最短パス・ツリーを構築することにより、IP ルーティング・テーブルが作成されます。ルーティング・ドメインは、OSPF プロトコルを実行している AS を表します。

OSPF ルーティング・プロトコルを使用可能にするには **enable** コマンドを使用して、次の例のように指定します。

```
OSPF Config> enable ospf
Estimated # external routes[100]? 200
Estimated # OSPF routers [50]? 60
Maximum Size LSA [0]? 2048
```

通常は、ルーターによって生成されるリンク状態公示 (LSA) 用としては 2048 バイトの大きさで十分です。ただし、多数の OSPF ダイヤル・リンク (たとえば、 ISDN ダイヤル・リンク) を持つルーターは、これより大きい LSA が必要になる可能性があります。このような状況では、一般構成の **packet-size** も大きくすることが必要になります。

OSPF ルーター ID の設定

OSPF ルーティング・ドメイン内の各ルーターには、固有な 32 ビットのルーター ID を割り当てることが必要です。OSPF ルーター ID に使用する値の選択は、次のように行います。

- IP 構成 **set router ID** コマンドを使用する場合、構成された値が OSPF ルーター ID として使用されます。
- IP 構成 **set internal address** コマンドを使用する場合、構成されたアドレスが OSPF ルーター ID として使用されます。定義する場合は、ルーター ID と内部アドレスに同じ値を使用することが推奨されます。
- IP 構成時にルーター ID も内部アドレスも構成しなかった場合は、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。

バックボーンと接続された OSPF エリアの定義

330ページの図32 は、OSPF ルーティング・ドメインのサンプル構成図を示しています。1 つの区分は、OSPF ドメイン内部の IP サブネットワークと OSPF ドメイン外部の IP サブネットワークとの間にあります。OSPF ドメイン内部に含まれているサブネットワークは、エリア と呼ばれる区域に細分化されています。OSPF エリアは、隣接するIP サブネットワークの集合です。エリアの機能は、異なるエリア内のあて先へのルートを見つけるのに必要な OSPF のオーバーヘッドを減らすことです。オーバーヘッドの削減は、ルーター間で交換される情報が少なくなること、およびルート・テーブルの計算が複雑でなくなり、必要な CPU サイクル数が減ることの両方によって実現されます。

各 OSPF ルーティング・ドメインには、少なくとも 1 つのバックボーン・エリア が必要です。バックボーンは常にエリア番号 0.0.0.0 によって識別されます。小規模な OSPF ネットワークの場合、バックボーンが唯一の必要なエリアです。複数のエリアをもつ大規模なネットワークの場合、バックボーンはエリアを接続する中核 (コア) になります。他のエリアとは異なり、バックボーンのサブネットは物理的に分離して

いても構いません。その場合、バックボーンの論理的な接続性は、介在する非バックボーン中継エリアを横断するバーチャル・リンク を、バックボーン・ルーター間に構成することによって維持されます。

2 つ以上のエリアに接続するルーターは、ボーダー・ルーター として機能します。エリア・ボーダー・ルーターはすべてバックボーンの一部なので、ボーダー・ルーターはバックボーン IP サブネットに直接接続するか、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ていることが必要です。それに加えて、すべてのバックボーン・ルーターを接続するための、バックボーン・サブネットワークとバーチャル・リンクの集合も存在していることが必要です。

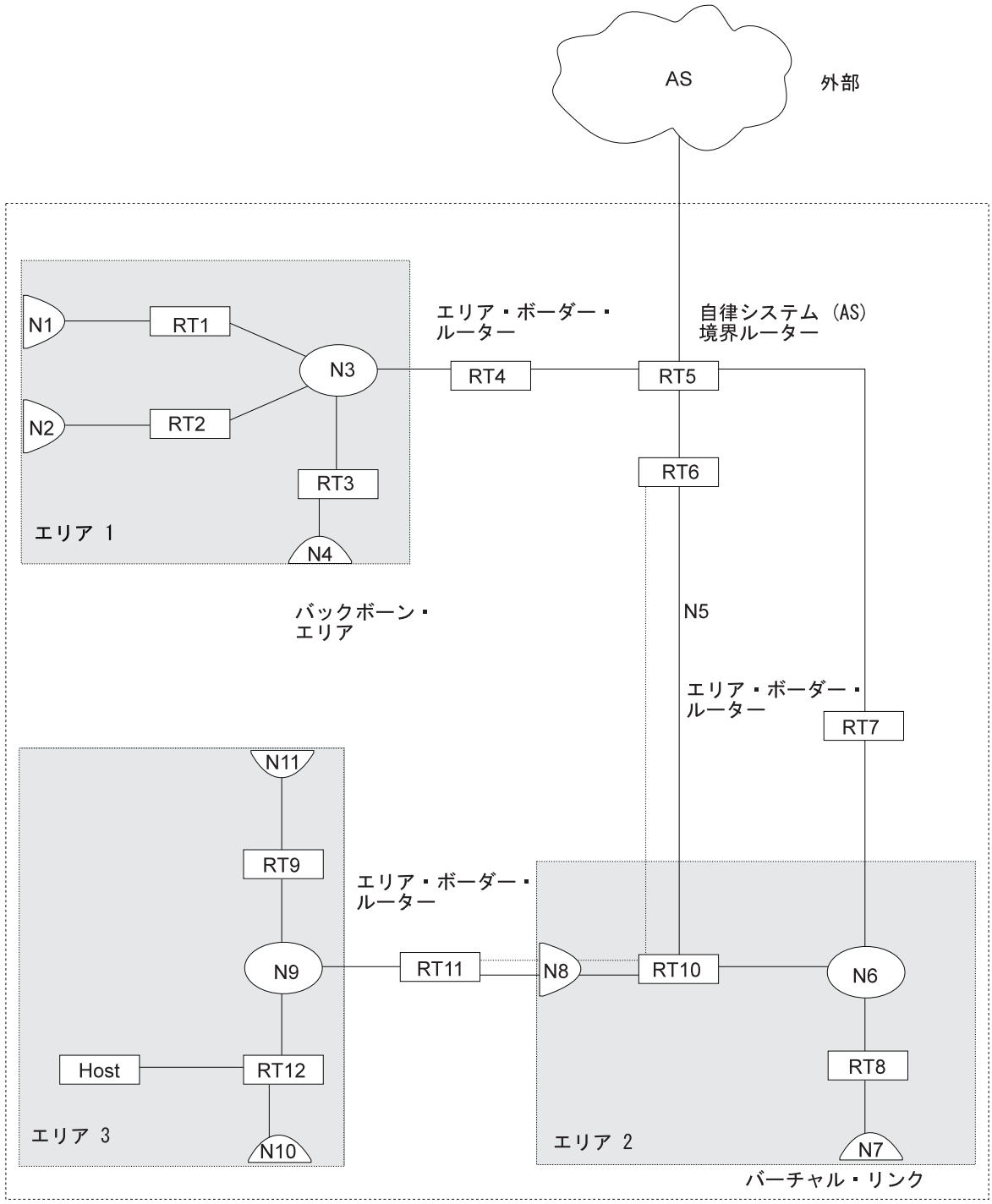


図 32. OSPF エリア

OSPF がルートを計算するのに使用する情報およびアルゴリズムは、あて先 IP サブネットワークが同じエリア内にあるか、同じドメイン内の異なるエリアにあるか、あるいは 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、そのエリア内のすべてのリンクの完全なマップを維持しています。マップには、全ルーター対マルチアクセス・ネットワーク、ネットワーク対マルチアクセス・ルーター、およびルーター対ルーター・リンクがすべて含まれています。エリア内のあて先への最善ルートは、最短パス最優先アルゴリズムを使用して、このマップから計算さ

れます。エリア間のルートは、IP サブネットワーク、IP サブネットワーク範囲、および OSPF ドメインの他のエリアにある自律システム外部 (ASE) 境界ルーターあてに、エリア・ボーダー・ルーターによって発信された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、OSPF ルーティング・ドメイン全体にフラッディングされた ASE 公示から計算されます。

バックボーンは、エリア間ルーティング情報を配布する任務を負っています。バックボーン・エリアは、以下のいずれでも構成できます。

- エリア 0.0.0.0 に属するネットワーク
- これらのネットワークに接続されたルーター
- 複数のエリアに属するルーター
- 構成されたバーチャル・リンク

set area コマンドを使用して、ルーターの接続先のエリアを定義します。**set area** コマンドを使用しない場合、デフォルトでは、バックボーンに接続するルーターのすべてのインターフェースになります。

エリア・ボーダー・ルーターを構成する際に、**set area** および **add range** コマンドのオプションを使用して、エリア境界を超える OSPF ルート情報を制御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、エリアをスタブ として定義することです。スタブ・エリアには、 OSPF ASE 公示は決してフラッディングされません。さらに、**set area** コマンドには、エリア間ルートの要約公示をスタブに発信するのを抑止するオプションもあります。エリア・ボーダー・ルーターは、デフォルト・ルートをスタブ・エリアに公示します。スタブ内の不定の IP サブネットあてのトラフィックは、エリア・ボーダー・ルーターに転送されます。ボーダー・ルーターは、より完全なルーティング情報を使用して、そのトラフィックをあて先への適切なパスに転送します。バーチャル・リンクの中継エリアとして使用されているエリアは、スタブとして構成することはできません。

もう 1 つのオプションは、IP サブネット・アドレス範囲を使用して、エリアのサブネットのエリア間公示に使用される要約公示の数を制限するものです。範囲は IP アドレスとアドレス・マスクによって定義します。範囲マスクを両方のアドレスに適用した後で、サブネット IP アドレスと範囲 IP アドレスが一致している場合、サブネットはその範囲内にあるものと見なされます。

エリア・ボーダー・ルーターのエリアに範囲が追加された場合、ボーダー・ルーターはその範囲に含まれているエリア内のサブネットへの要約公示を抑止します。抑止された公示は、ボーダー・ルーターが接続している他のエリアへ発信されるはずであったものです。代わりに、エリア・ボーダー・ルーターは add range コマンドで選択されたオプションに従ってその範囲に 1 つの要約公示を発信するか、あるいは公示をまったく発信しません。

ある範囲に公示されない場合、その範囲内にあるどのあて先にもエリア間ルートが存在しなくなることに注意してください。また、バーチャル・リンクによって中継エリアとして使用されているエリアに対しては、範囲を使用できないことにも注意してください。

OSPF の使用

OSPF エリア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ます。

```
OSPF Config> set area
Area number [0.0.0.0]? 0.0.0.1
Authentication type [1]? 1
Is this a stub area?  [No]:
```

エリアをスタブ・エリアとして定義するのは、次のような場合です。

1. そのエリアが中継バックボーン・トラフィックを扱う必要がない。
2. エリア・ルーターが、AS の外部へのトラフィックに対して、エリア・ボーダー・ルーターが生成したデフォルトを使用することが許容される。
3. エリア・ルーターが AS 境界ルーター (外部発信元からのルートを AS 公示として公示する OSPF ルーター) である必要はありません。

その場合には、エリア・ボーダー・ルーターおよびバックボーン・ルーターだけが AS 外部ルートを計算し、維持する必要があります。

OSPF インターフェースの設定

OSPF インターフェースは、IP の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 インターフェースに構成されるパラメーターは、OSPF ドメインのトポロジー、そのドメインを通過するのに選択されるルート、および直接接続された OSPF ルーター間の相互動作の特性を決めます。OSPF インターフェースを定義し、その特性の一部のものを指定するのには **set interface** コマンドを使用します。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ています。

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、ある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たルーターの定義、またはこれらの接続がその部分であるエリアによって異なります。基本的には、物理サブネットワークに接続されるルーターはすべて直接接続として定義しますが、1 つの物理サブネットワークを介する複数の IP サブネットワークを定義することも可能です。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た OSPF インターフェースを持っている場合にのみ、直接接続されているものと見なします。また、同じサブネットワークに接続されたルーターが、直接リンク・レイヤー・コネクションをもたないといった構成も可能です。

LAN 媒体の場合、直接接続された OSPF ルーターは、OSPF インターフェースに関連した IP サブネットワークと物理媒体によって判別されます。OSPF インターフェースの IP アドレスは **Interface IP address** に応答して指定します。このアドレスは、IP 構成時に **add address** コマンドで定義した IP インターフェースのアドレスに一致していることが必要です。この IP アドレスと、**add address** コマンドで定義されたサブネットワーク・マスクによって、OSPF インターフェースが接続する先の IP サブネットワークが決まります。また add address コマンドで IP インターフェースに関連付けられた *net index* によって、OSPF インターフェースが接続する物理サブネットワークが決まります。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ているインターフェースを持つ他のルーターを見つけることができます。したがって、OSPF が

LAN を介して直接接続されているルーターを判別するために必要なものは、インターフェース・パラメーターがすべてということになります。

LAN を使用して OSPF ルーターを IP ホストを接続することができます。この場合は、その LAN に定義されている IP サブネットワークに、OSPF インターフェースを定義することも必要になります。そうしないと、OSPF はこれらの IP サブネットワークをあて先とするルートを生成しません。他に接続ルーターがない LAN 上の OSPF ハロー・トラフィックを防止するために、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。その場合は、指定ルーターは必要がないので、ルーターの優先順位をゼロに設定することが必要です。

シリアル・ラインに接続する OSPF インターフェースを構成するための要件は、下位レイヤーの技術によって異なります。

ポイント・ポイント・ラインの場合、インターフェースを介してアクセスできる他のルーターは 1 つだけなので、追加構成しなくても、直接接続されたルーターを判別できます。事実、IP サブネットワークを構成する必要がまったくないので、ポイント・ポイント・ラインでは非番号制 OSPF インターフェースを使用できます。この場合には、IP の add address コマンドで IP アドレスとして使用したのと同じネットワーク・インデックスを、OSPF の set interface コマンドの IP アドレスとして使用します。

1 つのシリアル・ラインを介して複数のルーターに接続することをサポートするフレーム・リレー、および X.25 のようなサブネットワーク技術の場合、OSPF インターフェースの構成は LAN の場合と同様になります。ただし、これらのサブネットワーク技術では、直接接続ルーターは動的に検出されないので、直接接続された近隣を指定するための追加構成が必要です。必要な構成の詳細については、335ページの『広域サブネットワークの構成』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て、ルートを計算します。各パスのコストは、そのパス内の各種のリンクのコストの合計です。直接接続ルーターへのリンクのコストは、**set interface** コマンドの **Type of Service 0 cost** で指定します。

データ・トラフィックに使用するインターフェースのコストを、最適度に応じて正しく構成することは、OSPF ドメインを通過する最適ルートを入手するために非常に重要です。個々のリンクの最適度を決めるファクターは、ネットワークの種類によって異なりますが、最も遅延が少なく、最も容量の大きいルートを選択するのが共通の目的です。一般的には、リンクのコストを、物理サブネットワークに使用される媒体の帯域幅に反比例させることによって、この目的を達成できます。

推奨されるアプローチは、最高の帯域幅をもつ技術のリンク・コストを採用することです。

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
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・ライン	帯域幅に基づくコスト

表 20. OSPF リンクのサンプル・コスト (続き)

インターフェース帯域幅	コスト
エミュレートされたトークンリング (注を参照)	1
エミュレートされたイーサネット (注を参照)	1

注: イーサネットは、インターフェース速度 (たとえば 155 Mbps) で実行するので、コスト 1 で構成する必要があります。

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することができます。この新規コストは、速やかに OSPF ルーティング・ドメイン全体にフラッディングされ、即時にルーティングを変更します。

ルーターをリスタート/再ロードすると、インターフェースのコストは SRAM に構成された値に戻ります。

近隣ルーター間の相互動作

直接接続されたルーターの相互動作を制御するパラメーターを指定するためには、**set interface** コマンドを用いて構成される種々の値が使用されます。これには、次のものが含まれます。

- 再送間隔
- 転送遅延
- ルーター優先順位
- ハロー間隔
- デッド・ルーター間隔
- デマンド・サーキット
- ハロー抑止
- ポーリング間隔
- 認証キー

ほとんどの場合は、デフォルト値を使用できます。

注: ハロー間隔、デッド・ルーター間隔、および認証キーは、同じ IP サブネットワークに接続するすべての OSPF ルーターで同値でなければなりません。これらの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

IP マルチキャスト (クラス D) データグラムのルーティングを使用可能にするには **enable multicast-routing** コマンドを使用します。マルチキャスト・ルーティングを使用可能にする際には、ルーターが OSPF エリア間でマルチキャストを転送するかどうかについても尋ねられます。

```
OSPF Config>enable multicast forwarding
Inter-area multicasting enabled?  [No]: yes
```

enable multicast forwarding コマンドを最初に起動すると、すべての OSPF インターフェース上のマルチキャストがデフォルト・パラメーター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** コマンドを使用します。マルチキャスト・パラメーターについての問い合わせは、マルチキャスト転送を最初に使用可能にしたときだけ出ます。

自律システムの端にあるネットワークは、複数のマルチキャスト・ルーティング・プロトコル (または、1 つのマルチキャスト・ルーティング・プロトコルの複数インスタンス) が存在する可能性があるので、転送をデータ・リンク・ユニキャストとして構成して、データグラムの不必要な複写を回避することが必要になる場合があります。いずれの場合も、共通ネットワークに接続されたすべてのルーターでインターフェース・パラメーターの forward multicast datagrams および forward as data-link unicasts を同一に構成することが必要です。

非同報通信ネットワーク・インターフェース・パラメーターの設定

ルーターが非同報通信、マルチアクセス・ネットワーク (たとえば、 X.25 PDN) に接続されている場合、ルーターが OSPF 近隣を見つけるのを援助するために、ユーザーは次のパラメーターを構成する必要があります。この構成は、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資格がある場合にのみ必要です。

最初に、次のコマンドを使用して OSPF ポーリング間隔を構成します。

```
OSPF Config> set non-broadcast
Interface IP address [0.0.0.0]? 128.185.138.19
Poll Interval [120]?
```

次に、その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。構成した各ルーターについて、指定ルーターになる資格があるかどうかも指定することが必要です。

```
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]?
```

ネットワークを非同報通信として設定することにより、他の OSPF ルーターを持たないネットワークに強制的に公示させることも可能です。その場合には、インターフェースのルーター優先順位をゼロに設定し、近隣を定義してはなりません。

広域サブネットワークの構成

フレーム・リレーおよび X.25 では、1 つのシリアル・ラインを介して複数のルーターを直接接続することができます。この種のネットワークに接続する OSPF インターフェースの場合は、**set interface** コマンドで行ったもの以外に、追加の構成が必要です。これらのネットワークでは OSPF プロトコル・メッセージが特定の近隣に直接送信されるので、動的に発見する代わりに構成を使用して、近隣の関係やルーターの役割が判別されます。

注: この節で説明する構成は、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経由するルーター間の直接接続として 2 つのパターン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)

この 2 つのパターンを区別する主要ファクターは、サブネットワークに接続するすべてのルーターの組み間に直接接続が存在するか (*完全メッシュ接続*)、または一部のルーターが中間ルーターとしてのみ、複数ホップ・パスを介して他のルーターと接続されているのか (*部分メッシュ接続*) ということです。

非同報通信マルチアクセス (NBMA) では *完全メッシュ接続* が必要であるのに対して、ポイント・マルチポイントは *部分メッシュ接続* で構いません。

ポイント・マルチポイントは、完全メッシュ接続と部分メッシュ接続のどちらでも動作するので、これがデフォルト選択になっていますが、完全メッシュ接続が利用可能な場合は、NBMA を選択した方が効率的です。

ポイント・マルチポイント・サブネットワークの構成

ポイント・マルチポイントは、DR がないので NBMA より構成が容易ですが、ポイント・マルチポイント・サブネットを介してデータ・トラフィックを直接交換するすべてのルーターの組みについて、近隣関係を構成する必要があります。各組の直接接続ルーターはハロー・メッセージを交換し、このメッセージを通して、一方の側が相手側を見つけます。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 アドレスを持っていることが必要です。

サブネットワークに接続されたルーターの一部が NBMA として表され、他のルーターがポイント・マルチポイントとして表されている場合、OSPF は正しいコストを計算できないことに注意することが重要です。したがって、ポイント・マルチポイント・ネットワークへのインターフェースには決して **set non-broadcast** コマンドを使用しないようにしてください。

NBMA サブネットワークの構成

NBMA IP サブネットワークでは、接続された OSPF ルーターの一部のサブネットが、指定ルーター (DR) になるのに適格として構成されます。DR に適格の各ルーターは DR に適格の他のすべてのルーターに、定期的にハロー・メッセージを送信します。プロトコルはこれらのメッセージを使用して、DR およびバックアップ DR を選出します。DR とバックアップ DR は両方とも、NBMA IP サブネットワークに接続された他のすべての OSPF ルーターと定期的にハロー・メッセージを交換します。また、NBMA IP サブネットワークを介する OSPF ルート情報の流れは、各接続ルーターと DR またはバックアップ DR 間にのみ流れます。

NBMA サブネットワークに接続するインターフェースに対しては、**set non-broadcast** コマンドを使用して NBMA を選択します。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 になるのに適格であるかどうかによって異なります。

- DR に適格でないルーターの場合は、**set interface** コマンドを使用して、ルーターの優先順位を 0 に設定する必要があります。

- DR に適格のルーターの場合は、**set interface** コマンドを使用して、ルーターの優先順位を非ゼロ値に設定し、さらに **add neighbor** コマンドを使用して、NBMA サブネットワークに接続するインターフェースを持つすべての OSPF ルーターを識別し、そのうちのどのルーターが DR に適格であるかを示す必要があります。

注: スター構成では、ハブで **add neighbor** コマンドを使用します (リモート・サイトの近隣は構成する必要はありません)。**add neighbor** コマンドは、ルーターをリスタートせずに、即時に有効になります。

AS 境界ルーティングの使用可能化

他のプロトコル (RIP および静的に構成された情報) から確認されたルートを OSPF ドメインにインポートするためには、AS 境界ルーティングを使用可能にします。インポートしたい唯一のルートがデフォルト・ルート (あて先が 0.0.0.0) である場合も、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に、インポートしたい外部ルートを尋ねられます。次のカテゴリーに属するルートをインポートする、またはインポートしないことを選択できます。

- BGP ルート
- RIP ルート
- 静的ルート
- 直接ルート

たとえば、BGP ルートと直接ルートは選択するが、RIP ルートと静的ルートは選択しないといったことが可能です。

上記の外部カテゴリーから独立して、サブネット・ルートを OSPF ドメインにインポートするかどうかも構成できます。この構成項目のデフォルトは ENABLED (サブネットがインポートされる) です。

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に対する OSPF ドメインの見方を決めます。2 つのタイプ 2 メトリックを比較する際には、最善ルートの選出には外部コストのみが考慮されます。2 つのタイプ 1 メトリックを比較する際には、比較の前に、ルートの外部コストと内部コストが結合されます。たとえば、10.0.0.0 あてのルートを AS 番号 12 から受信した場合にのみそのデフォルトを発信するようにルーターを設定するといったことが可能です。AS 番号を 0 に設定すると 『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 に設定すると 『受信した任意のルート』 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
```

その他の構成タスク

バーチャル・リンクの設定

バックボーンの接続可能性を維持するためには、すべてのバックボーン・ルーターを、固定リンクまたはバーチャル・リンクのいずれかによって相互接続することが必要です。共通の非バックボーンおよび非スタブ・エリアを共用する任意の 2 つのボーダー・ルーター間にバーチャル・リンクを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・エリアに接続する個別のルーター・インターフェースと見なされます。そのため、バーチャル・リンクを構成する際には、さまざまなインターフェース・パラメーターも指定するように要求されます。

次の例は、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 つのエンド・ポート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ことが必要なので注意してください。

```
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
```

バーチャル・リンクの場合、コストは中継エリアを通るバーチャル・リンク・エンドポイント間の OSPF エリア内コストなので、コストは構成されません。

ルーティング・プロトコル比較の構成

OSPF の他にもルーティング・プロトコルを使用する場合、あるいはルーティング・プロトコルを OSPF に変更する場合は、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 内の OSPF ルーティングは、エリア内、エリア間、および外部の 3 つのレベルで行われます。

エリア内ルーティングは、パケットの発信元とあて先アドレスが同じエリア内に存在する場合に行われます。他のエリアに関する情報は、このタイプのルーティングには影響を与えません。

エリア間ルーティングは、パケットの発信元とあて先アドレスが、同じ AS 内の異なるエリアに存在する場合に行われます。OSPF は、パスを 3 つの隣接する部分に分割することにより、エリア間ルーティングを実行します。すなわち、発信元からエリア・ボーダー・ルーターまでのエリア内パス、発信元エリアとあて先エリア間のバックボーン・パス、およびあて先までの別のエリア内パスです。このハイレベルのルーティングは、バックボーンをハブとし、各エリアをスポークとするスター・トポロジーとして表すことができます。

外部ルートは、AS の外側にあるネットワークへのパスです。これらのルートは、ボーダー・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、またはネットワーク管理者によって入力された静的ルートから導出されます。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る内部ルーティング情報を妨害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することができます。OSPF は、これらのルートを AS 外部リンク公示として表示します。

OSPF は、外部ルートを別々のレベルでインポートします。第 1 のレベルは、タイプ 1 ルートと呼ばれ、外部メトリックが OSPF メトリックと比較可能な場合 (たとえば、両方が遅延をミリ秒で表している場合) に使用されます。第 2 のレベルは、外部タイプ 2 ルートと呼ばれ、外部コストが、どの内部 OSPF (リンク状態) パスのコストよりも大きいものと想定しています。

インポートされた外部ルートには、32 ビットの情報タグが付けられます。ルーターの場合、この 32 ビット・フィールドは、そのルートの送信元の AS 番号を示します。これにより、外部情報を他の自律システムに再公示するかどうかを、より適切に判断できるようになります。

OSPF は 4 つのレベルのルーティング階層を持っています (図33を参照してください)。**set comparison** コマンドは、OSPF 階層内の BGP/RIP/静的ルートが適合するレベルをルーターに知らせます。下位の 2 つのレベルは、OSPF 内部ルートから構成されます。OSPF エリア内ルートおよびエリア間ルートは、他のどのソースから入手した情報よりも優先され、これらはすべて 1 つのレベルに属します。

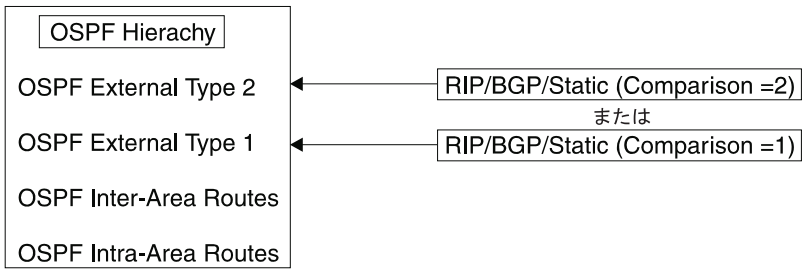


図 33. OSPF ルーティング階層

BGP/RIP/静的ルートを OSPF 外部タイプ 1 ルートと同じレベルに入れる場合は、比較を 1 に設定します。BGP/RIP/静的ルートを OSPF 外部タイプ 2 ルートと同じレベルに入れる場合は、比較を 2 に設定します。デフォルト設定は 2 です。

たとえば、比較が 2 に設定されているとします。この場合、RIP ルートが OSPF ドメインにインポートされるときには、タイプ 2 外部としてインポートされます。メトリックに関係なく、すべての OSPF 外部タイプ 1 ルートは、受信した RIP ルートをオーバーライドします。ただし、RIP ルートの方がコストが小さい場合は、RIP ルートは OSPF 外部タイプ 2 ルートをオーバーライドします。すべての OSPF ルーターの比較値が一致していることが必要です。ルーターに設定されている比較値が矛盾していると、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]?
```

デマンド・サーキット

デマンド・サーキットは、どのインターフェースにでも構成できます。ルート計算のために OSPF によって使用される物理媒体またはモデルには依存しません。デマンド・サーキットが構成され、整合性に問題がない場合は、次のように処理されます。

- 実際の変更を含むリンク状態公示 (LSA) のみが、インターフェースを介して公示されます。通常は、OSPF 高信頼性フラッディング・アルゴリズムにより、トポロジーの変更があっても LSA が 30 分ごとに新規インスタンスを用いてリフレッシュされます。
- インターフェースを介してフラッディングされた LSA に DoNotAge ビットがセットされます。これらはインターフェースを介してリフレッシュされないので、これをセットしておくことが必要です。

ハロー抑止要求

これは、ハロー抑止を要求するようにインターフェースを構成するために使用する追加パラメーターです。このパラメーターは、ポイント・ポイントおよびポイント・マルチポイント・インターフェースに対して有効です。また、インターフェースが接続す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 に通知できることが必要です。現在、ハロー抑止がサポートされているインターフェース・タイプは、ISDN ダイヤル・オンデマンド・インターフェースだけです。

ポーリング間隔

ハロー抑止がアクティブでない場合、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、**set non-broadcast** コマンドを用いて設定されます。このパラメーターは、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、ハロー抑止が要求されていないと構成できません。このパラメーターは、データ転送に障害が起きたためにポイント・ポイント回線がダウンしたが、ネットワークはまだ作動可能であるように見える場合に、OSPF がコネクションの再確立を試みるのに使用されます。

RIP から OSPF への変換

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 を一度に 1 ルーターずつ導入して行きます。徐々に、すべての内部ルートが RIP による確認から OSPF による確認にシフトします (OSPF ルートが RIP ルートより優先されるようになります)。ルートを RIP のもとにあったときと正確に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チェックするために) は、OSPF メトリックとしてホップ・カウントを使用します。これを行うには、各 OSPF インターフェースのコストを 1 に設定します。

プロトコルを使用可能にする場合は、OSPF システムのサイズを見積もる必要があることに注意してください。このサイズの見積値は、OSPF ルーティング・ドメインの最終サイズを反映していることが必要です。

ルーターに OSPF 導入した後で、まだ他のプロトコル (BGP、RIP、および静的に構成されたルート) を介してルートを確認する必要があるすべてのルーターの AS 境界ルーティングをオンにします。これらの AS 境界ルーターの数は、最小限にすることが必要です。

最後に、AS 境界ルーターでないすべてのルーター上の RIP 情報の受信を使用不可にすることができます。

OSPF 構成パラメーターの動的な変更

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、 OSPF コンソールを通じて OSPF プロトコルをリセットすることにより、動的に変更することができます。この技法を使用して、OSPF 近隣、インターフェース、エリア、および AS 境界ルーティング・ポリシーを追加、削除、または変更することができます。ほとんどの場合、これらの変更は完全に非中断的です。たとえば、 OSPF インターフェースを追加することは、他の OSPF インターフェースに (新規の OSPF リンク状態公示を発信すること以外は) 影響を与えません。

ルーターの OSPF 公示がすべて再発信されることを必要とする変更は、 OSPF をリスタートさせます。これには、以下のものが含まれます。

- OSPF マルチキャスト転送 (MOSPF) を使用可能/使用不可にする
- デマンド・サーキットを使用可能/使用不可にする (RFC 1793)
- ルーターの Router-ID の値を変更する

ほとんどの場合、機能が停止するのは OSPF 近隣の隣接が再確立される時間だけであるので、ユーザーはこれに気付きません。

入出力バッファーを割り当てる前にルーター・メモリーが OSPF 用に予約済みであるので、 OSPF は前回のルーターのリスタートの時点で使用可能にされていない限り、動的に使用可能にすることはできません。また、OSPF 用に予約済みのメモリーの量は、システムをリスタートせずに増やすことはできません。予約済みのメモリーの量は、 enable OSPF コマンドで指定されたルーターおよび AS 外部ルートの見積もりによって決定されます。

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

以下の拡張により、既存の IBM 6611 を 2212 に移行できるようになります。

- **最小コスト・エリア範囲**

  OSPF の要約範囲について、6611 は、コンポーネント・ネットワークの最小コストに基づいてコストを計算しますが、2212 は、コンポーネント・ネットワークの最大コストに基づいて要約範囲コストを計算します。**最小コスト・エリア範囲** は、最小コスト範囲を計算するオプションを使用できるようにします。
- **ポイント・マルチポイント近隣コスト**

6611 は、論理ポイント・ポイント・フレーム・リレー・リンクの概念をサポートしますが、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・マルチポイントの方が効率がよいのですが、近隣ごとに異なるコストを指定することはできません。近隣ごとに代替 TOS 0 コストを指定できるように、**ポイント・マルチポイント近隣コスト** が追加されました。

第16章 OSPF の構成および監視

この章では、最短パス最優先オープン (OSPF) プロトコル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・テーブルを作成するために、次の IGP をサポートしています。すなわち、最短パス最優先オープン (OSPF) プロトコルおよび RIP プロトコルです。OSPF は、リンク状態テクノロジー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。 本章には、以下の節が含まれています。

- 『OSPF 構成環境へのアクセス』
- 『OSPF 構成コマンド』
- 362ページの『OSPF 監視環境へのアクセス』
- 362ページの『OSPF 監視コマンド』

OSPF 構成環境へのアクセス

OSPF 構成環境にアクセスするには `Config>` プロンプトで、次のコマンドを入力します。

```
Config> protocol ospf
Open SPF-based Routing Protocol configuration monitoring
OSPF Config>
```

OSPF 構成コマンド

OSPF を使用する前に、OSPF 構成コマンドを使用して構成することが必要です。この節では、OSPF コンソール・コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドは `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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	既存の OSPF 情報に追加します。範囲をエリアに追加し、近隣を非同報通信ネットワークに追加することができます。
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、デマンド・サーキット機能、または IP マルチキャスト・ルーティングを使用不可にします。
Enable	OSPF プロトコル全体、AS 境界ルーティング機能、デマンド・サーキット機能、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	ルーターが 1 つまたは複数のマルチキャスト・グループに所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外します。
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 エリア、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設定または変更します。このコマンドでは、OSPF ルートを他のルーティング・プロトコルから得た情報と比較する方法も設定することができます。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、既存の OSPF 情報にさらに情報を追加するのに使用します。このコマンドを使用して、範囲をエリアに追加したり、近隣を非同報通信ネットワークに追加したりすることができます。

構文:

add range . . .

neighbor . .

range *area# IP-address IP-address-mask*

範囲を OSPF エリアに追加します。OSPF エリアはアドレス範囲で定義できます。エリアの外部では、各アドレス範囲に対して単一ルートが公示されます。たとえば、ある OSPF エリアをクラス B ネットワーク 128.185.0.0 のすべてのサブネットで構成されるようにする場合、それを単一のアドレス範囲として定義することができます。アドレス範囲は、アドレス 128.185.0.0 とマスク 255.255.0.0 というように指定します。エリアの外側では、このサブネット・ネットワーク全体が、ネットワーク 128.185.0.0 への単一ルートとして公示されます。

範囲は、エリアの外部に公示されるルートを制御するために定義することもできます。これには 2 つの選択があります。

- OSPF が範囲を公示するように構成されている場合、エリア内部でその範囲の少なくとも 1 つのコンポーネント・ルートがアクティブの場合は、その範囲に対して 1 つのエリア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ている場合は、その範囲内にあるルートについては、エリア間ルートは公示されません。

バーチャル・リンクによって中継エリアとして使用されるエリアに対しては、範囲を適用することはできません。また、あるエリアに対して範囲が定義されている場合、そのエリアが区分化され、バックボーンによって接続されている場合には、OSPF は正常に機能しません。

例:

```
add range 0.0.0.2 128.185.0.0 255.255.0.0
inhibit advertisement ? [No]
```

1. *area number* の値は、次のとおりです。

   有効値: 任意の有効なエリア番号

   デフォルト値: なし

2. *IP address* の値は、次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

3. *IP address mask* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス・マスク

   デフォルト値: なし

neighbor

このインターフェースを介して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、近隣を構成する必要があるのは、指定ルーターになる資格があるルーターだけです。ポイント・マルチポイント・ネットワークでは、各論理コネクションの少なくとも一方の側に近隣を構成する必要があります。ポイント・マルチポイント・ネットワークの場合、 Alternate TOS 0 cost (代替 TOS 0 コスト) を設定できます。 コストが設定されない場合には、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* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

2. *IP Address of Neighbor* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

3. 質問 `Can that router become designated router on this net?` 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適用されないため、『No』 に設定する必要があります。

   有効値: Yes または No

   デフォルト値: Yes

4. `Alternate TOS 0 cost` は、代替コストを使用できるようにします。

   有効値: 0 〜 65534

   デフォルト値: 0 (インターフェース・コストを使用することを指示します)。

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 エリア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. 範囲の *area number* の値は、次のとおりです。

   有効値: 任意の有効なエリア・アドレス

   デフォルト値: なし

2. *IP Address of Range* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

3. *IP Address Mask of Range* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス・マスク

   デフォルト値: なし

area *area#*

現行の OSPF 構成から OSPF エリアを削除します。

例: delete area 0.0.0.1

area number の値は、次のとおりです。

有効値: 任意の有効なエリア番号

デフォルト値: 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 の値は、次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

neighbor *interface-IP-address neighbor-IP-address*

現行の OSPF 構成から近隣を削除します。

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* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

2. *neighbor IP address* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: 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の情報を削除します。

例: delete non-broadcast 128.185.133.21

1. *interface IP address* の値は、次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: 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)* の値

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

2. *link's transit area* の値は、次のとおりです。

   有効値: 任意の有効なエリア・アドレス

   デフォルト値: 0.0.0.1

Disable

disable コマンドは、OSPF プロトコル全体を使用不可にするか、または AS 境界ルーティング機能のみを使用不可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可にします。使用不可にされると、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可にします。使用不可にされると、ルーターはデマンド・サーキット処理をサポートすることを、そのルーター・リンクのリンク状態公示 (LSA) に示さず、DoNotAge ビットをセットした 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・エリア内の 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・エリア内のどのルーターも DoNotAge LSA を発信しません。

例: disable demand-circuits

least-cost-ranges

最も近い (最小コスト) コンポーネント・ネットワークのコストに基づいた OSPF エリア範囲の計算を使用不可にします。このオプションは、デフォルトでは、使用不可になっています。

multicast forwarding

すべてのインターフェース上の IP マルチキャストを使用不可にします。使用不可にされると、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可にします。

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可にします。複数の OSPF エリアを通じて同じ外部ルートにアクセス可能であり、RFC2178 に記述されたルーティング・ループ問題に類似した問題を経験しているのでない限り、RFC1583 の互換性を使用不可にしないようお勧めします。デフォルトは使用可能です。

例: `disable rfc1583Compatibility`

subnet

ポイント・ポイント・シリアル・ラインへのインターフェースの場合、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・ラインを表すサブネットへのスタブ・ルートの公示を使用不可にします。ユーザーはこのルーターのアドレスを提供して、インターフェースがそれを識別できるようにする必要があります。

例:

```
OSPF Config> disable subnet
Interface IP address [0.0.0.0]? 8.24.3.1
```

interface IP address の値は、次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

Enable

enableコマンドは、OSPF プロトコル全体、サブネットへのスタブ・ルートの公示、または AS 境界ルーティング機能のみ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 (RIP および静的に構成された情報) から確認されたルートを OSPF ドメインにインポートすることができる AS 境界ルーティング機能を使用可能にします。**enable** コマンドの使用についての詳細は、326ページの『OSPF の構成』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 から発信されるデフォルトが AS 外部メトリック・タイプ 1 または 2 をもつかどうかを示します。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と見なされるのに対し、タイプ 2 のメトリックは、OSPF メトリックより高いと見なされます。

   有効値: 1 または 2

   デフォルト値: 2

2. *Default route cost* は、OSPF がそのエリア・ボーダー・ルーターへのデフォルト・ルートに関連付けるコストを指定するパラメーターです。このコストを使用して、エリア・ボーダー・ルーターへのデフォルト・ルートの最短パスが決められます。

   有効値: 0 〜 16777215

   デフォルト値: 1

3. *Default forwarding address* は、インポートされたデフォルト・ルートに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

   デフォルト値: 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、OSPF エリア間で IP マルチキャスト・データグラムを転送するかどうかも尋ねられます。MOSPF (マルチキャスト拡張をもつ OSPF) を実行するには、現在 OSPF を実行しているルーターが、このコマンドを使用するだけです。ユーザーがその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。ルーターはデマンド・サーキット処理をサポートすることを、そのルーター・リンクのリン

ク状態公示 (LSA) に表示します。デフォルトは使用可能なので、OSPF ルーティング・ドメイン内のすべてのルーターを再構成しなくてもデマンド・サーキットを展開することができます。

```
OSPF Config> enable demand-circuits
```

least-cost-ranges

最も近い (最小コスト) コンポーネント・ネットワークのコストに基づいた OSPF エリア範囲の計算を使用可能にします。同じエリアについてエリア・ボーダー・ルーター (ABR) として活動する IBM 6611 と互換であるためには、このパラメーターを使用可能にすることが必要です。このパラメーターは、最小コスト・コンポーネント・ネットワークを使用すると、コストの変更により OSPF LSA が再発信される回数が著しく減少するような状態でも使用できます。このオプションは、デフォルトでは、使用不可になっています。

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場合、ユーザーは OSPF リンク状態データベースのサイズを見積もるための、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 外部ルートの合計数。別々の AS 境界ルーターによってインポートされる場合、1 つのあて先が複数の外部ルートに通じていることがあります。たとえば、OSPF ルーティング・ドメインに 2 つの AS 境界ルーターが存在し、両方が同じ 100 のあて先へのルートをインポートする場合、AS 外部ルートの数は 200 に設定します。

  有効値: 0 ～ 65535

  デフォルト値: 100

- ルーティング・ドメイン内の OSPF ルーターの総数

  有効値: 0 ～ 65535

  デフォルト値: 50

- そのほかに、最大 LSA サイズを指定することもできます。同じ OSPF エリア内に多くの OSPF ダイヤル・リンク (たとえば、ISDN 1 次) をもつ、大規模なルーターがある場合は、この値を大きくする必要がある場合があります。通常、単一の LSA には 2048 は十分なスペースです。

  有効値: 2048 ～ 65535

  デフォルト値: 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 外部ルート選択を使用可能にします。デフォルトは使用可能です。

例: enable rfc1583Compatibility

subnet

ポイント・ポイント・シリアル・ラインへのインターフェースの場合、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・ライン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。ユーザーはこのルーターのアドレスを提供して、インターフェースがそれを識別できるようにする必要があります。

例:

```
OSPF Config> enable subnet
Interface IP address [0.0.0.0]? 8.24.3.1
```

interface IP address の値は、次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: 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の場合、ルーターはグループ・アドレスあてに送信された PING および SNMP 照会に応答します。

グループのメンバーシップの要求を、即時に有効になる方法で (リスタート/再ロードを必要とせずに) 行うには、OSPF 監視から **join** コマンドを発行します。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、ルーターのリスタートおよび再ロード後は保存されません。

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

デフォルト値: なし

Leave

leave コマンドは、ルーターのメンバーシップをマルチキャスト・グループから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・アドレスあてに送信された PING および SNMP 照会に応答しなくなります。

グループのメンバーシップの削除を、即時に有効になる方法で (リスタート/再ロードを必要とせずに) 行うには、OSPF 監視から **leave** コマンドを発行します。OSPF 監視からの場合、実行された leave の回数が、以前に実行された join の回数に等しくなるまでは、グループの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

デフォルト値: 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 すべての OSPF 関連の構成情報をリストします。

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可かを表示します。
# AS ext. routes	自律システム外部ルートの見積数を表示します。ルーターは、この数を超える AS 外部ルートは受け入れることができません。
Estimated # routers	OSPF 構成に示されるルーターの見積数を表示します。
Maximum LSA size	このルーターによって発信される LSA の最大サイズを表示します。
External comparison	外部情報を OSPF ドメインにインポートするとき、および OSPF 外部ルートと RIP/BGP ルートを比較するときに、OSPF によって使用される外部ルート・タイプを表示します。
RFC 1583 compatibility	OSPF AS 外部ルートが RFC 1583 と互換性があるかどうかを示します。

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	インポートされるルートを表示します。
Orig default route	ルーターがデフォルトを OSPF ドメインにインポートするかどうかを表示します。値が 『YES』 のときは、非ゼロのネットワーク番号が括弧内に表示されます。これは、そのネットワークへのルートが使用可能の場合にのみ、デフォルト・ルートが発信されることを示します。
Default route cost	インポートされたデフォルト・ルートに使用されるコストとタイプを表示します。
Default forward addr	発信されたデフォルト・ルートに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るかどうかを表示します。
Least Cost Area Ranges	最小コスト・エリア範囲が計算されるかどうかを表示します。
LSA Max Random Initial Age	自己発信 LSA の最大初期エージを表示します。この値がゼロ (デフォルト) であると、すべての LSA がエージ 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、および OSPF 外部ルートと RIP/BGP ルートを比較するときに、OSPF によって使用される外部ルート・タイプを表示します。
Inter-area multicast	エリア間で 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。
Area-ID	接続されたエリア ID (エリア要約情報) を表示します。
AuType	エリアの認証に使用される方式を表示します。『Simple-pass』 は、エリアの認証に簡易パスワード方式が使用されることを意味します。
Stub area	そのエリアがスタブ・エリアとして要約されるかどうかを表示します。スタブ・エリアは外部ルートを含まないので、ルーティング・データベースが小さくなります。ただし、スタブ・エリアには AS 境界ルーターを含めることができず、構成されたバーチャル・リンクもサポートできません。
OSPF interfaces	各インターフェースについて、その IP アドレスが構成パラメーターと共に印刷されます。『Area』 は、インターフェースが接続する OSPF エリアです。『Cost』 は、インターフェースに関連付けられている TOS 0 コスト (または、メトリック) です。『Rtrns』 は再送間隔で、未確認ルーティング情報の再送間の秒数を表します。『TrnsDly』 は転送遅延で、インターフェースを介してルーティング情報を転送するのに要する秒数の見積値です (これは 0 より大きくなければなりません)。『Pri』 はインターフェースのルーター優先順位で、指定ルーターを選出するときに使用されます。『Hello』 は、インターフェースから送信されるハロー・パケット間隔の秒数です。『Dead』 は、ルーターのダウンを宣言するハローが聞かれなくなった後の秒数です。
Virtual links	このルーターをエンドポイントとして構成したすべてのバーチャル・リンクをリストします。『Virtual endpoint』 は、反対側エンドポイントの OSPF ルーター ID を示します。『Transit area』 は、バーチャル・リンクが中継する非バックボーン・エリアを示します。バーチャル・リンクは、OSPF プロトコルによって、ポイント・ポイント・ネットワークと同様に扱われます。この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維持されます。詳細については、 OSPF list interfaces コマンドを参照してください。

areas 構成された OSPF エリアに関するすべての情報を表示します。

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	接続エリア ID (エリア要約情報) を表示します。
AuType	エリアの認証に使用される方式を表示します。『Simple-pass』 は、エリアの認証に簡易パスワード方式が使用されることを意味します。
Stub area	そのエリアがスタブ・エリアとして要約されるかどうかを表示します。スタブ・エリアは外部ルートを含まないので、ルーティング・データベースが小さくなります。ただし、スタブ・エリアには AS 境界ルーターを含めることができず、構成されたバーチャル・リンクもサポートできません。
Default-cost	スタブ・エリアの場合は、OSPF 要約 (タイプ 3) リンク状態公示 (LSA) として発信されるデフォルトのコスト。通過エリア (たとえば、非スタブ・エリア) の場合、このフィールドは N/A です。
Import-summaries	スタブ・エリアの場合は、OSPF 要約 (タイプ 3) リンク状態公示がスタブ・エリアに発信されるかどうかを示します。この質問はデフォルトの要約には適用されません。通過エリア (たとえば、非スタブ・エリア) 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について、その IP アドレスが構成パラメーターと共に印刷されます。『Area』 は、インターフェースが接続する OSPF エリアです。『Cost』 は、インターフェースに関連付けられている TOS 0 コスト (または、メトリック) です。『Rtrns』 は、再送間隔で、未確認ルーティング情報の再送間の秒数を表します。『TrnsDly』 は転送遅延で、インターフェースを介してルーティング情報を転送するのに要する秒数の見積値です (これは 0 より大きくなければなりません)。『Pri』 はインターフェースのルーター優先順位で、指定ルーターを選出するときに使用されます。『Hello』 は、インターフェースから送信されるハロー・パケット間隔の秒数です。『Dead』 は、ルーターのダウンを宣言するハローが聞かれなくなった後の秒数です。

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可にされている場合には、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ていない場合、デマンド・サーキット・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へ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。その近隣がネット上の 『Designated Router』 およびポイント・マルチポイント・ネットワークの alternate TOS 0 cost (代替 TOS 0 コスト) になるのに適格かどうかも示されます。

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について、ルーターが接続ネットワーク上の指定ルーターとして適格である場合に限り、ポーリング間隔が非同報通信ネットワーク上のルーターの近隣のリストと共に表示されます。

例: `list non-broadcast`

```
        --NBMA configuration--
Interface Addr      Poll Interval
128.185.235.34      120
```

virtual-links

このルーターをエンドポイントとして構成したすべてのバーチャル・リンクをリストします。『Virtual endpoint』 は、反対側エンドポイントの OSPF ルーター ID を示します。『Transit area』 は、バーチャル・リンクが中継する非バックボーン・エリアを示します。バーチャル・リンクは、OSPF プロトコルによって、ポイント・ポイント・ネットワークと同様に扱われます。この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維持されます。詳細については、 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 エリア、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 ルートを他のルーティング・プロトコルから得た情報と比較する方法も設定することができます。

構文:

set area

comparison

interface

non-broadcast

virtual-link

max-random-initial-lsa-age

area OSPF エリアのパラメーターを設定します。エリアが定義されていない場合、ルーターのソフトウェアは、すべてのルーターの直接接続ネットワークがバックボーン・エリア (エリア 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* - OSPF エリア・アドレスです。
- *Stub area designation*で、 『Yes』 を指定すると、次のようになります。
  - このエリアは AS 外部リンク公示を受信せず、データベースのサイズが小さくなり、スタブ・エリア内のルーターによるメモリー所要量が減少する。
  - スタブ・エリアを中継するバーチャル・リンクを構成することができない。
  - スタブ・エリア内のルーターは AS 境界ルーターとして構成することができない。

  External Routing in Stub Areas。 バックボーンはスタブ・エリアとして構成することはできません。スタブ・エリアの外部ルーティングは、デフォルト・ルートに基づいて行われます。スタブ・エリアに接続する各エリア・ボーダー・ルーターが、この目的のためにデフォルト・ルートを提供します。このデフォルト・ルートのコストも **set area** コマンドを用いて構成することができます。

comparison

OSPF 階層内の BGP/RIP/静的ルートが適合するレベルをルーターに知らせます。下位の 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、他のどのソースから入手した情報よりも優先され、これらはすべて 1 つのレベルに属します。

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・インターフェースの 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のアドレスです。
2. *attaches to area* は、インターフェースが接続するエリアです。
3. タイマー値は、共通ネットワーク・セグメントに接続されたすべてのルーターで同値です。
   a. *retransmission interval* は、1 つまたは複数のリンク状態公示のリンク要求が再送されるまでの間隔です。

      有効値: 1 ～ 65535 秒

      デフォルト値: 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転送するのに要する秒数の見積値です。

   各リンク状態公示は、定数 MaxAge (1 時間) に等しい有限の寿命を持っています。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ときに、この構成された転送遅延によってエージングが行われます。最小遅延は 1 秒です。

   有効値: 1 〜 65535 秒

   デフォルト値: 1

c. *Hello Interval* は、インターフェース上でハロー・パケットが送信される間隔です。

   有効値: 1 〜 65535 秒

   デフォルト値: 10

d. *Dead Router Interval*

   デッド・ルーター間隔は、ハローを送信しなくなったルーターがデッドと見なされるまでの間隔です。デッド・ルーター間隔は、デフォルトでは構成されたハロー間隔の 4 倍になります。このパラメーターの値は、ハロー間隔より大きくなければなりません。

   有効値: 2 〜 ≥ 65535 秒

   デフォルト値: 40 (または、構成されたハロー間隔の 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・ネットワークで、指定ルーターを選出するために使用されます。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、このルーターはそのネットワークの指定ルーターに選出してはならないことを意味します。

   有効値: 0 〜 255

   デフォルト値: 1

5. *Type of service 0 cost* は、エリアの最短パス・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

   デフォルト値: 1

6. *Demand Circuit* は、LSA (リンク状態公示) のフラッディングのために、インターフェースがデマンド・サーキットとして扱われるかどうかを示します。デマンド・サーキット上では、LSA は DoNotAge ビットをセットしてこのインターフェースを介してフラッディングされ、LSA の実際の変更がない限り、フラッディングは行われなくなります。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

   デフォルト値: No

7. *Hello Suppression* は、近隣が満ぱいの状態に達した場合、インターフェース上のハロー・パケットを抑止するかどうかを示します。ハロー抑止を要求または許容するためには、インターフェース上のデマンド・サーキットが使用可能になっていることが必要です。現在、ハロー抑止は、ISDN ダイヤル・オンデマンド・リンクでのみサポートされています。詳細については、RFC 1793 を参照してください。

有効値: 許可、要求、または使用不可

デフォルト値: 許可

Allow 近隣がハロー抑止を要求できるようにします。

Request 近隣からハロー抑止を要求します。

Disable ハロー抑止を使用不可にし、ハローを送信し続けます。

8. *Demand Circuit Down Poll Interval* は、ハロー抑止をアクティブにしたデマンド・サーキット上のデータ送信に障害がある場合、ハロー・ポーリングを送信する間隔を示します。現在、ハロー抑止は、 ISDN ダイヤル・オンデマンド・リンクでのみサポートされています。詳細については、RFC 1793 を参照してください。

   有効値: 1 〜 65535

   デフォルト値: 60

9. *Authentication type* は、インターフェース上の OSPF パケットに使用される認証手順を定義します。選択値は 1 (簡易パスワードを示す) または 0 (インターフェース上で OSPF パケットを交換するのに認証の必要がないことを示す) です。1 が指定される場合、認証キーも指定される必要があります。

   有効値: 0、1

   デフォルト値: 0

10. *Authentication key* は、この OSPF エリアで使用されるパスワードを定義するパラメーターです。パスワードの認証が使用されている場合、正しい認証キーを持つパケットのみが受け入れられます。

    有効値: 任意の 1〜8 文字

    デフォルト値: ヌル文字列

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には、ルーター内の各インターフェースの IP アドレスを提供し、それに続く質問に答えます。以下のパラメーターは、共通ネットワークに接続されたすべてのルーターに同じ値を入力する必要があります。

- ハロー間隔
- デッド・ルーター間隔
- 認証キー (認証 1 が使用されている場合)

最初のプロンプトは、インターフェースが接続する OSPF エリアを尋ねます。たとえば、インターフェース・アドレス・マスクが 255.255.255.0 とすると、インターフェースはネットワーク 28.185.0.0 のサブネット (128.185.138.0) に接続します。サブネット 128.185.138.0 に接続する他のすべての OSPF ル

ーターも、*Hello interval* を 10 に設定し、*dead router interval* を 40 に設定し、それぞれのインターフェース *authentication key* を xyz_q に設定する必要があります。

ポイント・ポイント回線への IP インターフェースは非番号制でも構わないことに注意してください。この場合は、IP アドレスの代わりにネットワーク・インデックスが構成されます。この OSPF の実現は、このような非番号制インターフェースを用いて動作しますが、正しく動作するためには、ポイント・ポイント回線の両側で非番号制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されている) では、 OSPF インターフェースの MOSPF パラメーターはデフォルト値に設定されます。これは、以下のことを意味しています。

- マルチキャスト転送が使用可能にされている。
- 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・メンバーシップが、インターフェースを介して 60 秒ごとに送信される。
- ローカル・グループ・データベース・エントリーは、そのグループの 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** コマンドを使用します。マルチキャスト・パラメーター (上記の出力ディスプレイに表示される最後の 5 つのパラメーター) を尋ねられるのは、マルチキャスト転送を最初に使用可能にしたときだけです。

自律システムの端にあるネットワークは、複数のマルチキャスト・ルーティング・プロトコル (または、1 つのマルチキャスト・ルーティング・プロトコルの複数インスタンス) が存在する可能性があるので、転送をデータ・リンク・ユニキャストとして構成して、データグラムの不必要な複写を回避することが必要になる場合があります。いずれの場合も、共通ネットワークに接続されたすべてのルーターで、インターフェース・パラメーター 『forward multicast datagrams』 および 『forward as data-link unicasts』 を同一に構成することが必要です。

non-broadcast

X.25、フレーム・リレー・ネットワークの NBMA を選択するためのポイント・マルチポイント・デフォルトをオーバーライドします。このパラメーターは、非アクティブの近隣にハローを送信する頻度を決める時間間隔を指定します。OSPF を正しく機能させるためには、non-broadcast の設定を、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間で矛盾がないようにする必要があります。

ただし、フレーム・リレー・ネットワークでは、**set non-broadcast** コマンドは、OSPF インターフェースを非同報通信マルチアクセス・ネットワークに接続するように構成するのに使用します。**set non-broadcast** コマンドが使用されていない場合、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 インターフェースは、同じタイプのネットワーク (非

同報通信マルチ・アクセスまたはポイント・マルチポイント) に接続するように構成する必要があるので、 1 つのルーターのインターフェースに **set non-broadcast** コマンドを使用する場合は、その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 の値は、次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

NBMA ポーリング間隔は、ハロー・パケットを非アクティブの近隣に送信するのに使用されます。(非アクティブの近隣とは、デッド・ルーター間隔より長い期間、ルーターがその消息を聞いていない近隣です。) ルーターは、このような近隣に対しても低い頻度でポーリングを続けます。NBMA ポーリング間隔は、ルーターに構成されたハロー間隔よりもはるかに高い値に設定します。

有効値: 1 〜 65535 秒

デフォルト値: 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 つのエリア・ボーダー・ルーター間のバーチャル・リンクを構成します。バックボーンの接続可能性を維持するためには、すべてのバックボーン・ルーターを、固定リンクまたはバーチャル・リンクのいずれかによって相互接続することが必要です。バーチャル・リンクは、バックボーン・エリアに接続する個別のルーター・インターフェースと見なされます。そのため、バーチャル・リンクを構成する際には、さまざまなインターフェース・パラメーターも指定するように要求されます。

バーチャル・リンクは、共通の非バックボーン・エリアへのインターフェースを持っている任意の 2 つのバックボーン・ルーター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の接続可能性を維持するために使用され、両方のエンドポイントで構成する必要があります。

注: この OSPF 実現はバーチャル・リンクの使用をサポートし、その場合、バーチャル・リンクの片側は非番号制ポイント・ポイント回線でも構いません。この構成が機能するためには、バーチャル・リンクを介して送信される OSPF プロトコル・メッセージの発信元アドレスとして、ルーター ID が使用されることが必要です。このルーター ID の使用を確実にするためには、内部 IP アドレスを、ルーター ID として使用するアドレスを用いて構成します。この構成が機能するためのもう 1 つの要件は、バーチャル・リンクの両側の OSPF 実現がそれをサポートしていることです。

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

   デフォルト値: なし

2. *link's transit area* は、バーチャル・リンクが中継する非バックボーン、非スタブ・エリアです。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・エリアへのインターフェースを持つ任意の 2 つのバックボーン・ルーター間に構成することができます。バーチャル・リンクは、リンクの 2 つのエンド・ポートのそれぞれで構成する必要があります。

   有効値: 0.0.0.1 ～ 255.255.255.255

   デフォルト値: 0.0.0.1

3. タイマー値は、共通ネットワーク・セグメントに接続されたすべてのルーターで同値です。

   a. *retransmission interval* は、1 つまたは複数のリンク状態公示のリンク要求が再送されるまでの間隔です。

      有効値: 1 ～ 65535 秒

      デフォルト値: 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転送するのに要する秒数の見積値です。

      各リンク状態公示は、定数 MaxAge (1 時間) に等しい有限の寿命を持っています。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ときに、この構成された転送遅延によってエージングが行われます。最小遅延は 1 秒です。

      有効値: 1 ～ 65535 秒

      デフォルト値: 5

   c. *Hello Interval* は、インターフェース上でハロー・パケットが送信される間隔です。

      有効値: 1 ～ 255 秒

      デフォルト値: 30

   d. *Dead Router Interval* は、ハローを送信しなくなったルーターがデッドと見なされるまでの間隔です。このパラメーターは、デフォルトは構成されたハロー間隔の 6 倍ですが、ハロー間隔より大きい値に設定する必要があります。

      有効値: 2 ～ 65535 秒

      デフォルト値: 180

4. *Authentication type* は、バーチャル・リンク上の OSPF パケットに使用される認証手順を定義します。選択値は 1 (簡易パスワードを示す) または 0 (インターフェース上で OSPF パケットを交換するのに認証の必要がないことを示す) です。1 が指定される場合、認証キーも指定される必要があります。

   有効値: 0、1

   デフォルト値: 0

5. *Authentication key* は、この OSPF エリアで使用されるパスワードを定義します。パスワードの認証が使用されている場合、正しい認証キーを持つパケットのみが受け入れられます。

有効値: 任意の 1～8 文字

デフォルト値: ヌル文字列

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 の最大初期エージを指定します。デフォルトは 0 で、通常、これを変更するのは、LSA 発信同期に問題がある場合だけにしてください。

有効値: 0 ～ 1770

デフォルト値: 0

例:

```
OSPF Config>  set max-random-initial-lsa-age
Maximum initial LSA age [0]?
```

OSPF 監視環境へのアクセス

OSPF 監視コマンドにアクセスするには、次の手順を使用します。このプロセスにより OSPF *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** を入力する。 (このコマンドの詳細については、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*の “OPCON プロセス” の章を参照してください。)たとえば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、端末に GWCON プロンプト (+) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. At the + prompt, enter the **protocol ospf** command to get you to the OSPF> prompt.

   例:

   ```
   + prot ospf
   OSPF>
   ```

OSPF 監視コマンド

この節では、すべての OSPF 監視コマンドの要約を示し、個々のコマンドについて説明します。これらのコマンドを使用して、OSPF ルーティング・プロトコルを監視することができます。363ページの表22 は 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ます。

表 22. OSPF 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix 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 エリアの統計と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 エリア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・テーブルに含まれている OSPF ルートを表示します。
Interface summary	OSPF インターフェースの統計とパラメーターを表示します。
Join	ルーターが 1 つまたは複数のマルチキャスト・グループに所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外します。
Mcache	現在アクティブのマルチキャスト転送キャッシュ・エントリーのリストを表示します。
Mgroups	ルーターの接続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	各種のマルチキャスト・ルーティング統計を表示します。
Neighbor summary	OSPF 近隣の統計とパラメーターを表示します。
Ping	指定のあて先に継続的に ICMP エコー要求 (または PING) を送信し、受信した各レスポンスを 1 行に印刷します。
Reset	OSPF 構成を動的にリセットします。
Routers	到達可能な OSPF エリア・ボーダー・ルーターおよび AS 境界ルーターを表示します。
Size	現在リンク状態データベースに入っている LSA の数を、タイプ別に表示します。
Statistics	メモリーとネットワークの使用状況を詳細に示した OSPF 統計を表示します。
Traceroute	指定のあて先への完全なパスを (ホップごとに) 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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Advertisement Expansion

advertisement expansion コマンドは、OSPF データベースに入っているリンク状態公示のコンテンツを印刷するのに使用します。ルーターの公示の要約を印刷する場合は **database** コマンドを使用します。

リンク状態公示は、そのリンク状態タイプ、リンク状態 ID、および公示ルーターによって定義されます。各 OSPF エリアごとに個別のリンク状態データベースが存在します。コマンド行に area-id を入力して、探索するデータベースをソフトウェアに知らせます。link-state-type に指定する値によって決まる各種の公示は、次のとおりです。

- Router links - 単一ルーターのインターフェースの記述が入っています。
- Network links - 特定インターフェースに接続するルーターのリストが入っています。
- Summary nets - 単一のエリア間ルートの記述が入っています。

- Summary AS boundary routers - 別のエリア内の AS 境界ルーターへのルートの記述が入っています。
- AS external nets - 単一ルートの記述が入っています。
- Multicast group memberships - 公示ルーターの近隣の特定グループのメンバーシップの記述が入っています。

注: リンク状態 ID、公示ルーター (ルーター ID によって指定される)、およびエリア ID は、IP アドレスと同じフォーマットを取ります。たとえば、バックボーン・エリアは 0.0.0.0 として入力できます。

例 1 は、ルーター・リンク公示の拡張を示しています。ルーターの ID は 128.185.184.11 です。これは AS 境界ルーターで、バックボーン・エリアへの 3 つのインターフェース (すべてが、コスト 1) を持っています。マルチキャスト・ルーティングが使用可能にされています。フィールドの詳しい説明は、例と一緒に示してあります。

このコマンドは、2 つの方法で拡張されています。第 1 は、router-LSAs および network-LSAs を表示するときに、それぞれの router-to-router リンクおよび router-to-transit-network リンクの逆方向コストを、従来の順方向コストと共に表示します。このような表示をするのは、発信元が異なるエリア/自律システム内に存在するマルチキャスト・データグラムのルーティングは、順方向コストではなく逆方向コストに基づいて行われるからです。逆方向リンクが存在しない場合 (そのリンクは決して Dijkstra によって使用されることはないことを意味しています) には、逆方向コストは 『1-way』 として表示されます。

さらに、LSA の OSPF オプションが、詳細な OSPF **neighbor** コマンドで表示されるのと同じ形態で表示されます。

新規の group-membership-LSAs も表示されます。各 group-membership-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 1 つまたは複数の接続ネットワーク上にメンバーが存在する各グループの group-membership-LSA を発信します。グループの group-membership-LSA には、グループ・メンバーを持つこれらの接続中継ネットワーク (タイプ 『2』 頂点) をリストし、メンバーが 1 つまたは複数のスタブ・ネットワークに属する場合、あるい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には、タイプ 『1』 頂点 (その ID は、ルーターの OSPF ルーター ID) が組み込まれます。

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	公示のエージ (経過時間) を秒数で示します。
LS options	公示に記述されているルーティング・ドメインによってサポートされるオプションの OSPF 機能を示します。これらの機能は、E (タイプ 5 外部を処理。これが設定されていない場合、公示が属するエリアはスタブとして構成されています)、T (TOS に基づくルーティングが可能)、MC (IP マルチキャスト・データグラムを転送できる)、および DC (デマンド・サーキット処理が可能) です。
LS type	公示を分類し、そのコンテンツを示します。1 (ルーター・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る対象を識別します。これは公示のタイプによって異なります。ルーター・リンクおよび ASBR 要約の場合、これは 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	発信ルーターの OSPF ルーター ID です。
LS sequence number	同じ公示の個別インスタンスを区別するのに使用されます。符号付き 32 ビット整数として表示します。0x80000001 から始めて、公示が更新されるたびに 1 ずつ増分します。
LS checksum	データ汚損を検出するのに使用される公示のコンテンツのチェックサム
LS length	バイト数で表した公示のサイズ
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 はルーターがエリア・ボーダー・ルーターであること意味し、W はルーターがワイルドカード・マルチキャストの受信側であることを意味します。
# Router ifcs	公示に記述されているルーター・インターフェースの番号
Link ID	インターフェースの接続先を識別します。これは、インターフェース・タイプによって異なります。ルーターへ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、リンク ID は近隣のルーター ID です。中継ネットワークへのインターフェースの場合は、そのネットワークの指定ルーターの IP アドレスです。スタブ・ネットワークへのインターフェースの場合は、その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。これは、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中継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	次のいずれかです。1 (別のルーターへのポイント・ポイント・コネクション)、2 (中継ネットワークへのコネクション)、3 (スタブ・ネットワークへのコネクション)、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のメトリックが提供される非ゼロの TOS 値

TOS 0 metric　インターフェースのコスト。括弧の中にリンクの逆方向コスト (別の公示から導出された) が示されます。逆方向リンクが存在しないときは 『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 フィールドは、すべての公示に共通です。Router type および # router ifcs は、ルーター・リンク公示にのみ表示されます。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説明されます。各リンクには、各 IP サービス・タイプ (TOS) の個別のコストを割り当てることもできます。これは No. of metrics および TOS 0 metric フィールドによって記述されます (ルーターは現在 TOS に基づいてルーティングしておらず、TOS 0 コストのみを見ています)。

例 2 は、グループ・メンバーシップ公示の拡張を示しています。グループ/公示ルーターの組み合わせのグループ・メンバーシップ公示は、公示ルーターに直接接続されている、グループ・メンバーを持つネットワークをリストします。また、ルーター自体が指定グループのメンバーであるかどうかも表示します。下の例は、ネットワーク 128.185.184.0 がグループ 224.0.1.1 のメンバーを持ってい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・メンバーを持つオブジェクトを記述しており、次のいずれかです。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 (中継ネットワーク)

Vertex ID　vertex type が 1 のときは、常に公示ルーターの ID です。vertex type が 2 のときは、中継ネットワークの指定ルーターの IP アドレスです。

Area Summary

area summary コマンドは、ルーターに接続されたすべての OSPF エリアの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、ルーターは単一のエリア (バックボーン・エリア) に接続しています。このエリアの認証には、簡易パスワード方式が使用されています。ルーターは、このエリアに接続する 3 つのインターフェースを持っており、バックボーンの SPF ツリーの計算時に、4 つの中継ネットワーク、7 つのルーター、およびエリア・ボーダー・ルーターなしを検出しています。

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	特定エリア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、必ずしも機能するとは限りません。
# nets	このエリアの SPF ツリー計算を行っているときに見つかった中継ネットワークの数を示します。
# rtrs	このエリアの SPF ツリー計算を行っているときに見つかったルーターの数を示します。
# brdrs	このエリアの SPF ツリー計算を行っているときに見つかったボーダー・ルーターの数を示します。
DC-Status	このエリアでデマンド・サーキット処理がアクティブであるかどうかを示します。

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。各公示につき 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。すなわち、そのリンク状態タイプ (AS 外部公示の場合は、常に 5)、リンク状態 ID (LS あて先と呼ばれます)、および公示ルーター (LS 発信元と呼ばれます) です。

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 5 を応答します。
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ます。
LS originator	公示ルーター
Seqno, Age, Xsum	OSPF ルーティング・ドメインには、ある公示の複数のインスタンスが同時に存在することが可能です。ただし、最新のインスタンスのみが OSPF リンク状態データベースに保持されます (そして、このコマンドによって印刷されます)。最新のインスタンスを調べるために、LS シーケンス番号 (Seqno)、LS エージ (Age)、および LS チェックサム・フィールド (Xsum) が比較されます。LS エージ・フィールドは秒数で表されます。その最大値は 3600 です。

ディスプレイの最後に AS 外部公示の合計数が、それぞれのコンテンツのすべてのチェックサムの合計値と共に印刷されます。チェックサム合計値は、個々の公示の LS チェックサム・フィールドを単純に足し算した 32 ビットの和 (切り捨て) です。この情報を使用すれば、 2 つの OSPF ルーターが同期化されたデータベースを持っているかどうかを速やかに判別できます。

Database Summary

database summary コマンドは、特定の OSPF エリアのリンク状態データベースのコンテンツの記述を表示するのに使用します。AS 外部公示は、このディスプレイから省かれています。各公示につき 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。すなわち、そのリンク状態タイプ (Type と呼ばれます)、リンク状態 ID (LS あて先と呼ばれます)、および公示ルーター (LS 発信元と呼ばれます) です。

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
: 個別の LS タイプが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) です。

LS destination
: 公示によって記述される対象を示します。

LS originator
: 公示ルーター

Seqno, Age, Xsum
: OSPF ルーティング・ドメインには、ある公示の複数のインスタンスが同時に存在することが可能です。ただし、最新のインスタンスのみが OSPF リンク状態データベースに保持されます (そして、このコマンドによって印刷されます)。最新のインスタンスを調べるために、LS シーケンス番号 (Seqno)、LS エージ (Age)、および LS チェックサム・フィールド (Xsum) が比較されます。LS エージ・フィールドは秒数で表されます。その最大値は 3600 です。

ディスプレイの最後に、エリア・データベース内の公示の合計数が、それぞれのコンテンツのすべてのチェックサム合計と共に印刷されます。チェックサム合計値は、個々の公示の LS チェックサム・フィールドを単純に足し算した 32 ビットの和 (切り捨て) です。この情報を使用すれば、 2 つの OSPF ルーターが同期化されたデータベースを持っているかどうかを速やかに判別できます。

注: マルチキャスト可能ルーターと非マルチキャスト・ルーターを比較する場合は、上記のデータベース・チェックサム (および # advertisements も) は、必ずしも一致するとは限りません。非マルチキャスト・ルーターは group-membership-LSA を扱わないか、保管しないからです。また、OSPF ルーティング・ドメインまたは OSPF スタブ・エリアでデマンド・サーキット処理がアクティブの場合、データベース・チェックサムは、デマンド・サーキットをもつルーター間で異なっている可能性が高くなります。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・テーブルに存在するすべてのルートを表示します。その出力のフォーマットは、IP 監視の dump routing tables コマンドの出力フォーマットに似ています。

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)	そのルートがどのように導出されたかを示します。 Sbnt - ネットワークがサブネット化されていることを示します。この種のエントリーは、プレースホルダーとしてのみ使用されます。 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 プロトコルを通して確認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 - BGP プロトコルを通して確認されたルートを示します。 BGPR - BGP プロトコルを通して確認され、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 - ルートは OSPF エリア内ルートであることを示します。 SPIA - これは OSPF エリア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 とタイプ 2) を示します。 Rnge - アクティブ OSPF エリア・アドレス範囲を表し、パケット転送には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
コスト	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・エントリーが前回に更新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。パケットを転送するために送信側ルーターによって使用されたインターフェース・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・タイプには静的または直接接続されたバックアップがあることを示します。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/サブネットでは RIP 更新が常に受け入れられることを示します。

欄の最後の括弧内の数字は、そのあて先への等価コスト・ルートの数を示します。これらのルートに属する最初のホップは、IP 監視の **route** コマンドを用いて表示することができます。

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。引き数が与えられていない場合 (例 1 を参照)、各インターフェースを要約した 1 行が表示されます。インターフェースの IP アドレスが与えられている場合 (例 2 を参照)、そのインターフェースの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	接続エリア ID
Type	Brdcst (同報通信、たとえば、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、たとえば、同期シリアル・ライン)、 P-2-MP (ポイント・マルチポイント、たとえば、フレーム・リレー・ネットワーク)、Multi (非同報通信マルチアクセス、たとえば、X.25 コネクション)、または VLink (OSPF バーチャル・リンク) のいずれかです。
State	次のいずれかです。1 (down)、2 (looped back)、4 (waiting)、8 (point-to-point)、16 (DR other)、 32 (backup DR) または 64 (designated router)
#nbrs	近隣の数。これは、ハローを受信したルーターの数に、構成されたルーターの数を加算した値です。
#adjs	隣接の数。これは、状態が Exchange またはそれより大きい値の近隣の数です。これらは、ルーターが同期した、または同期化中の近隣の数です。

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	接続エリア ID
Physical interface	物理インターフェースのタイプと番号を表示します。
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、たとえば、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、たとえば、同期シリアル・ライン)、 P-2-MP (ポイント・マルチポイント、たとえば、フレーム・リレー・ネットワーク)、 Multi (非同報通信マルチアクセス、たとえば、X.25 コネクション)、および VLink (OSPF バーチャル・リンク) のいずれかです。
State	次のいずれかです。1 (Down)、2 (Looped back)、4 (Waiting)、8 (Point-to-Point)、16 (DR other)、 32 (Backup DR)、64 (Designated router)、または 128 (Full)
Authentication Type	インターフェース用にアクティブな認証のタイプを示します。サポートされるタイプは、none (なし) 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た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	現行のデッド間隔値を表示します。
TX delay	現行の転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 パケットの最大サイズを表示します。
Demand circuit	インターフェース上でデマンド・サーキット処理がアクティブになっているかどうかを示します。
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。これは、ハローを受信したルーターの数に、構成されたルーターの数を加算した値です。
# Adjacencies	隣接の数。これは、状態が Exchange またはそれ以上の近隣の数です。
# Full adj	完全隣接の数。完全隣接の数は、その状態が Full (したがって、ルーターはこれと同期化されたデータベースを持っている) の近隣の数です。
# Mcast Floods	インターフェースからフラッディングされたリンク状態更新の数 (再送はカウントしません)。
# Mcast acks	インターフェースからフラッディングされたリンク状態確認の数 (再送はカウントしません)。
MC forwarding	インターフェースのマルチキャスト転送が使用可能にされている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	インターフェース上で IGMP が使用可能にされてい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し、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転送された (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) 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した IGMP ホスト・メンバーシップ照会の数を表示します。
Unexp polls	インターフェースが予期せずに受信した (つまり、ルーター自体が送信したものを受信した) 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した 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上でデータグラムを受信することがサポートされていた場合、アップストリーム・ノードの識別子を表示します。この Type は 1 ～ 3 の数字で、1 はルーターを示し、2 は中継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設定するのに使用します。

このコマンドは OSPF 構成監視の join コマンドと似ていますが、2 つの相違点があります。

- グループ・メンバーシップに関する効果は、OSPF モニターからコマンドが与えられると即時に有効になります (つまり、リスタート/再ロードの必要はありません)。同様に、結合された IP マルチキャスト・グループは、ルーターのリスタートおよび再ロード後は保存されません。
- このコマンドは、特定のグループが 『結合』 された回数を追跡します。

ルーターがマルチキャスト・グループのメンバーの場合、ルーターは、グループ・アドレスあてに送信された 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、ルーターのメンバーシップをマルチキャスト・グループから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・アドレスあてに送信された 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 コマンドと似ていますが、2 つの相違点があります。

- グループ・メンバーシップに関する効果は、OSPF モニターからコマンドが与えられると即時に有効になります (つまり、リスタート/再ロードの必要はありません)。
- 実行された 『leaves』 の回数が、以前に実行された 『joins』 の回数に等しくなるまでは、コマンドはグループのメンバーシップを除去しません。同様に、結合された IP マルチキャスト・グループは、ルーターのリスタートおよび再ロード後は保存されません。

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・エントリーのリストを表示するのに使用します。マルチキャスト・キャッシュ・エントリーは、要求時に (最初の照合マルチキャスト・データグラムを受信するたびに) 作成されます。データグラム発信元ネットワークとあて先グループの組み合わせごとに、個別のキャッシュ・エントリー (したがって、個別のルートも) が作成されます。

キャッシュ・エントリーは、トポロジーが変更されたとき (たとえば、MOSPF システム内のポイント・ポイント回線が起動または切断状態になったとき)、およびグループ・メンバーシップが変更されたときにクリアされます。

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　照合データグラムの発信元ネットワーク/サブネット
Destination　照合データグラムのあて先グループ

Count　キャッシュ・エントリーに一致した受信データグラムの数を表示します。
Upst　転送するデータグラムをそこから受信する必要がある、近隣ネットワーク/サブネットを表示します。これが 『none』 の場合、データグラムは転送されることはありません。
Downstream　データグラムの転送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 0 の場合、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・エントリーには、これ以外にも情報があります。コマンド行で、照合データグラムの発信元とあて先を指定すれば、キャッシュ・エントリーの詳細を表示することができます。照合キャッシュ・エントリーが見つからない場合は、エントリーが作成されます。このコマンドのサンプルを例 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 コマンドで表示される情報の他に、以下のフィールドが表示されます。

Upstream Type　転送するためにはデータグラムをそこから受信する必要がある、ノードのタイプを示します。このフィールドの可能な値は、『none』 (データグラムは転送されないことを示します)、『router』 (データグラムはポイント・ポイント接続を介して受信する必要があることを示します)、『transit network』、『stub network』、および 『external』 (別の自律システムからデータグラムを受信することを想定していることを示します) です。
Downstream　データグラムの送信先の各インターフェースまたは近隣を 1 行ずつに印刷します。TTL 値も示され、このインターフェースから受信する、またはこのインターフェースに転送されるデータグラムには、少なくともその IP ヘッダーに指定された TTL 値が入っていなければならないことを示します。ルーター自体がマルチキャスト・グループのメンバーの場合、『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上のグループ・メンバーシップのみが表示されます。

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報告された (IGMP を介して) グループ・アドレスを表示します。

Interface　グループ・アドレスが報告された (IGMP を介して) 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』 の値で示されます。これらのエントリーの場合、lifetime フィールド (下記を参照) は、特定グループのメンバーシップを要求したアプリケーションの数を示します。

Lifetime　インターフェース上で指定のグループのメンバーシップ報告を受信しなくなった場合に、そのエントリーが存続する期間を秒数で表示します。

Mstats

mstats コマンドは、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のに使用します。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、およびルーターがエリア間または AS 間 (あるいはその両方) のマルチキャスト転送機能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	ルーターがエリア間で 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、この合計には含まれません)。
Datagrams (ext source)	発信元が AS の外側にある受信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 (これにはパケット複写が含まれるので (必要な場合)、このカウントは受信した数よりはるかに大きくなる可能性があります)。
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の非 AS 間マルチキャスト転送機能によって受信されたデータグラムの数を表示します。
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数を表示します。
Unallocated cache entries	資源不足のためにキャッシュ・エントリーを作成できなかったデータグラムの数を表示します。
Off multicast tree	照合キャッシュ・エントリー内にアップストリーム近隣が存在しないか、またはダウンストリーム・インターフェース/近隣が存在しないために転送されなかったデータグラムの数を表示します。
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上で、データ・リンク・マルチキャストとして受信したデータグラムの数を表示します。
Buffer alloc failure	バッファー不足のために複写できなかったデータグラムの数を表示します。
TTL scoping	TTL がグループ・メンバーへの到達が不可能であることを示していた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・エントリーの数を表示します。
DVMRP entries freed	解放された DVMRP エントリーの数を示します。サイズは、ルーティング・エントリー数から解放されたエントリー数を差し引いた値になります。
# fwd cache alloc	割り当てられたキャッシュ・エントリーの数を示します。現行の転送キャッシュ・エントリー・サイズは、割り当てられたエントリーの数 (『# fwd cache alloc』) から、解放されたキャッシュ・エントリーの数 (『# fwd cache freed』) を差し引いた値です。
# fwd cache freed	解放されたキャッシュ・エントリーの数を示します。現行の転送キャッシュ・エントリー・サイズは、割り当てられたエントリーの数 (『# fwd cache alloc』) から、解放されたキャッシュ・エントリーの数 (『# fwd cache freed』) を差し引いた値です。
# fwd cache GC	最近使用されず、キャッシュがオーバーフローしたためにクリアされたキャッシュ・エントリーの数を示します。
# local group DB alloc	割り当てられたローカル・グループ・データベース・エントリーの数を示します。割り当てられた数 (『# local group DB alloc』) から解放された数 (『# local group DB free』) を差し引くと、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・エントリーの数を示します。割り当てられた数 (『# local group DB alloc』) から解放された数 (『# local group DB free』) を差し引くと、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、受信し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』 が原因で廃棄されたデータグラムの合計数を差し引き、さらに 『# local group DB alloc』 を差し引くことによって計算できます。キャッシュ・ミスの数は、単に 『# local group DB alloc』 の値です。

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。引き数が与えられていない場合 (例 1 を参照)、各近隣を要約した 1 行が表示されます。近隣の IP アドレスが与えられている場合 (例 2 を参照)、その近隣の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	近隣の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	次のいずれかです。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	近隣への送信を待っ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新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`

表示されるほとんどのフィールドの意味は、OSPF 仕様 (RFC 2178) の節 10 に示されています。

```
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	近隣の IP アドレス
OSPF router ID	近隣の OSPF ルーター ID
Neighbor State	次のいずれかです。1 (Down)、2 (Attempt)、4 (Init)、8 (2-Way)、16 (ExStart)、32 (Exchange), 64 (Loading) または 128 (Full)
Physical interface	ルーターと近隣の共通ネットワークの物理インターフェースのタイプと番号を表示します。
DR choice, backup choice, DR priority	近隣から受信した最後のハローに示されていた値を示します。
Nbr options	近隣によってサポートされるオプションの OSPF 機能を示します。これらの機能は、E (タイプ 5 外部を処理。これが設定されていない場合、共通ネットワークが属するエリアはスタブとして構成されています)、T (TOS に基づくルーティングが可能)、および MC (IP マルチキャスト・データグラムを転送できる) です。このフィールドは、状態が Exchng またはそれ以上の近隣にのみ有効です。
Alternate TOS 0 cost	ポイント・マルチポイント・インターフェースについて、この近隣の alternate TOS 0 cost (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に要約されるのを待っている公示の数を示します。近隣が状態 Exchange にある場合を除いて、これはゼロでなければなりません。
LS rxmt qlen	近隣にフラッディングされたが、まだ確認されていない公示の数を示します。
LS req qlen	状態が Loading の近隣から要求されている公示の数を示します。
Last hello	近隣からハローを受信してからの秒数を示します。
# LS rxmits	フラッディング中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レスポンスを示します。
# Dup LS rcvd	フラッディング中に発生した重複再送の数を示します。
# Old LS rcvd	フラッディング中に受信した古い公示の数を示します。
# Dup acks rcvd	受信した重複確認の数を示します。
# Nbr losses	近隣が Down 状態に変わった回数を示します。
# Adj. resets	状態 ExStart へのエントリー数

Ping

Ping コマンドの説明は、315ページの『Ping』 を参照してください。

Reset

OSPF **reset** コマンドは、ルーターをリスタートする際に、 OSP ルーティング構成を動的に変更するのに使用します。詳細については、 341ページの『OSPF 構成パラメーターの動的な変更』を参照してください。

注: リスタート時に、IP 転送を維持するため、OSPF ルートはルーティング・テーブル内に保持されます。

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 コマンドの説明は、320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・テーブルに存在するすべてのルートを表示します。**dump routing tables** コマンドを使用した場合、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ています。routers コマンドは、その他のすべてのあて先に適用できます。

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** あて先がエリア・ボーダー・ルーターであることを示します。
- **Fadd** 転送アドレスを示します (外部ルートの場合)。

RType　ルート・タイプとそのルートがどのように導出されたかを示します。

SPF　ルートはエリア内ルートである (Dijkstra 計算から導出された) ことを示します。

SPIA　エリア間ルートである (要約リンク公示から導出された) ことを示します。

Destination　あて先ルーターの OSPF ID。タイプ D ルーターの場合、ルーターの IP アドレスの 1 つ (これは別の AS 内のルーターに一致) が表示されます。

Area　所属する AS エリアを表示します。

コスト　ルート・コストを表示します。

Next hop　あて先ホストへのパス上の次のルーターのアドレス。欄の最後の括弧内の数字は、そのあて先への等価コスト・ルートの数を示します。

Size

size コマンドは、現在リンク状態データベースに入っている LSA の数をタイプ別に表示します。

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る統計を表示するのに使用します。統計は、メモリーおよびネットワークの使用状況を含めて、この実現の性能を示します。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・バージョン・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 外部ルートが RFC 1583 と互換性を持つことになるかどうかを示します。
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のかを表示します。
Orig default route	ルーターが OSPF デフォルト・ルートを公示するかどうかを表示します。この値が 『Yes』 で括弧内に非ゼロ値が表示されている場合、ネットワークへのルートが存在する場合にのみデフォルト・ルートが公示されます。
Default route cost	デフォルト・ルート (公示される場合) のコストとタイプを表示します。
Default forward addr	デフォルト・ルート (公示される場合) に指定されている転送アドレスを表示します。
Attached areas	ルーターがアクティブ・インターフェースを持っているエリアの数を示します。
Estimated heap usage	OSPF リンク状態データベースのサイズの概略値 (バイト数)
Transit nodes	ルーター・リンク公示およびネットワーク・リンク公示を保管するために割り当てられています。
LS adv.	要約リンク公示および AS 外部リンク公示を保管するために割り当てられています。
Queue headers	リンク状態公示のリストを形成します。これらのリストは、フラッディングおよびデータベース交換処理に使用されます。割り当てられた待ち行列ヘッダーの数と解放された数が等しくない場合は、いずれかの近隣とのデータベースの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計算された回数を示します。
Maximum LSA size	このルーターが発信できる最大サイズ LSA。これは、OSPF 構成を通して構成される値の最小値であり、一般構成によって計算または構成される最大パケット・サイズです。
Incremental summ updates, incremental VL updates	新規の要約リンク公示のためにルーティング・テーブルが部分的に作成し直されたことを示します。
Buffer alloc failures.	バッファー割り当て障害を示します。OSPF システムは、パケット・バッファーの一時的な不足から回復します。

Multicast pkts sent	OSPF ハロー・パケット、およびフラッディング手順中に送信されたパケットが含まれます。
Unicast pkts sent	OSPF パケット再送およびデータベース交換手順が含まれます。
LS adv. aged out	60 分間ヒットした公示の数をカウントします。リンク状態公示は、60 分後にエージングによって除去されます。通常は、この時間より前にリフレッシュされます。
LS adv. flushed	リンク状態データベースから除去された (そして、復元しなかった) 公示の数を示します。
Ptrs to Invalid LS adv	形式が間違っているために解釈できなかったデータベース内の公示の数を表示します。
Incremental ext. updates.	ルーティング・テーブルに増分的に導入された外部あて先への変更の数を表示します。
LSA Max Random Initial Age	自己発信 LSA の最大初期ランダム・エージの数値を表示します。
LSA MINARRIVAL Rejects	MINARRIVAL (1 秒) より小さな新しいインスタンスを受け取ったために拒否された 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を提供します。 **Current state** 現行の AS 外部 LSA のデータベースが正常状態であるか、過負荷状態であるか。 **Number of LSA** 現在データベース内にある外部 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コストを変更するのに使用します。この新規コストは、速やかに OSPF ルーティング・ドメイン全体にフラッディングされ、それに応じてルートが変更されます。

インターフェースのコストは、ルーターをリスタートまたは再ロードするたびに、構成されたコストに戻ります。コストの変更を固定させるためには、weight コマンドを起動した後で、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更されない場合を除いて、このコマンドにより新規のルーター・リンク公示が発信されます。

構文:

weight *ip-interface-address new-cost*

例: `weight 128.185.124.22 2`

第17章 BGP4 の使用

この章では、BGP 構成コマンドを使ってボーダー・ゲートウェイ・プロトコル (BGP) を使用する方法について説明します。

本章には、以下の節が含まれています。

- 『ボーダー・ゲートウェイ・プロトコルの概説』
- 『BGP4 の機能』
- 389ページの『BGP4 の設定』
- 390ページの『ポリシー定義のサンプル』

ボーダー・ゲートウェイ・プロトコルの概説

BGP は、自律システム間でネットワーク到達可能性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、基本的には、単一の管理組織の下で動作するルーターおよびエンド・ノードの集合です。各 AS 内で、ルーターおよびエンド・ノードは、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 または OSPF のいずれであっても構いません。

BGP は、自律システム間のルーティング情報をループを生じることなく交換するためにインターネットに導入されました。無クラス・ドメイン間ルーティング (CIDR) に基づき、BGP はそれ以後進化して、ルーティング情報の集約および縮小をサポートするようになりました。

本質的には、CIDR は次の問題を扱うために設計されたストラテジーです。

- クラス B アドレス空間を使い尽くすこと
- ルーティング・テーブルが増大すること

CIDR はアドレス・クラスの概念を取り除き、*n* 通りの異なるルートを単一のルートに要約する方法を提供します。これにより、BGP ルーターが保管および交換する必要のあるルーティング情報の量が著しく削減されます。

注: IBM は BGP の最新バージョンである BGP4 だけをサポートしています。これは RFC 1654 に定義されています。本章および IBM のルーターのインターフェースで BGP に言及する場合はすべて BGP4 を指しており、以前のバージョンの BGP には適用されません。

BGP4 の機能

BGP は自律システム間のルーティング・プロトコルです。本質的には、BGP ルーターは、それ自体の、または他の自律システム内の BGP 近隣との間で到達可能性情報を選択的に収集および公示します。到達可能性情報は、特定の BGP スピーカーへのパスを形成する一連の AS 番号、および公示された各パスを介して到達可能な IP ネットワークのリストから構成されます。AS は、RIP または OSPF など 1 つまたは

BGP4 の使用

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性情報を共用するネットワークおよびルーターの管理グループです。

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、その BGP 近隣 (クライアント) に対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 でパッシブ TCP コネクションをオープンし、この予約済みアドレスで近隣からの着信コネクションを listen します。 ルーターは、使用可能にされた BGP 近隣へのアクティブ TCP コネクションもオープンします。この TCP コネクションは、BGP ルーターに、同じまたは他の自律システム内の近隣と到達可能性情報を共用または更新します。

同じ AS 内の BGP スピーカー間のコネクションは、内部 BGP (IBGP) コネクションと呼ばれるのに対し、異なる自律システム内の BGP スピーカー間のコネクションは外部 BGP (EBGP) コネクションと呼ばれます。

単一の AS は、外部の自律システムへの 1 つまたは複数の BGP コネクションを持つことができます。385ページの図34 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 コネクションを確立しようとします。このコネクションがいったん確立されると、ルーターは到達可能性情報を共用することができるようになります。

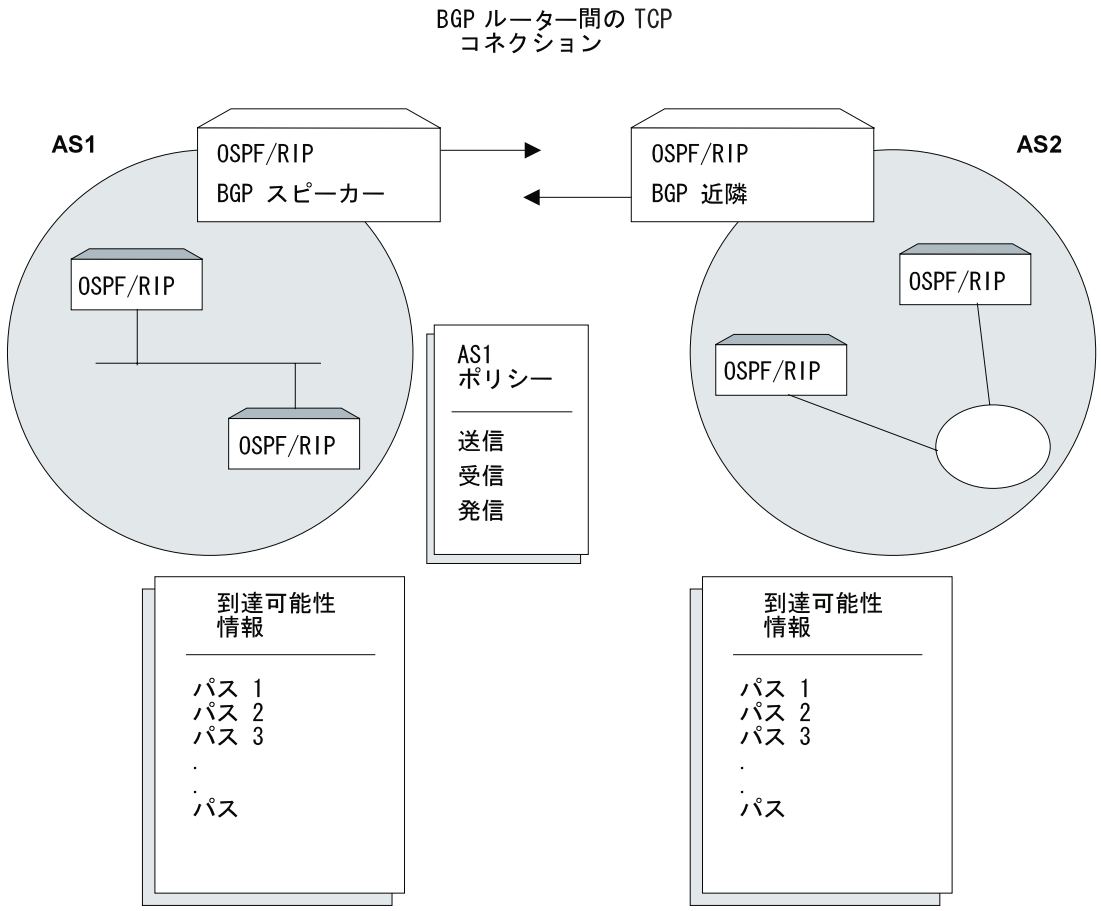


図 34. 2 つの自律システム間の BGP コネクション. AS1 内の BGP スピーカーが AS2 内の BGP 近隣と TCP コネクションを確立すると、 2 つのルーターは到達可能性情報を選択的に交換することができます。各ルーターが送信および受け取る情報は、各ルーターごとに定義されたポリシーによって決まります。

図34 に示された自律システムは 1 つだけの BGP ルーターを持つのに対し、各自律システムは他の自律システムへの複数のコネクションを持つことができました。この例として、386ページの図35 では 3 つの相互接続された自律システムが示されています。AS1 は外部の自律システムへの 3 つの BGP コネクションをもちます。1 つは AS2 へ、1 つは AS3 へ、1 つは ASx へのコネクションです。同様にして、AS3 は AS1、AS2、および ASy へのコネクションを持ちます。

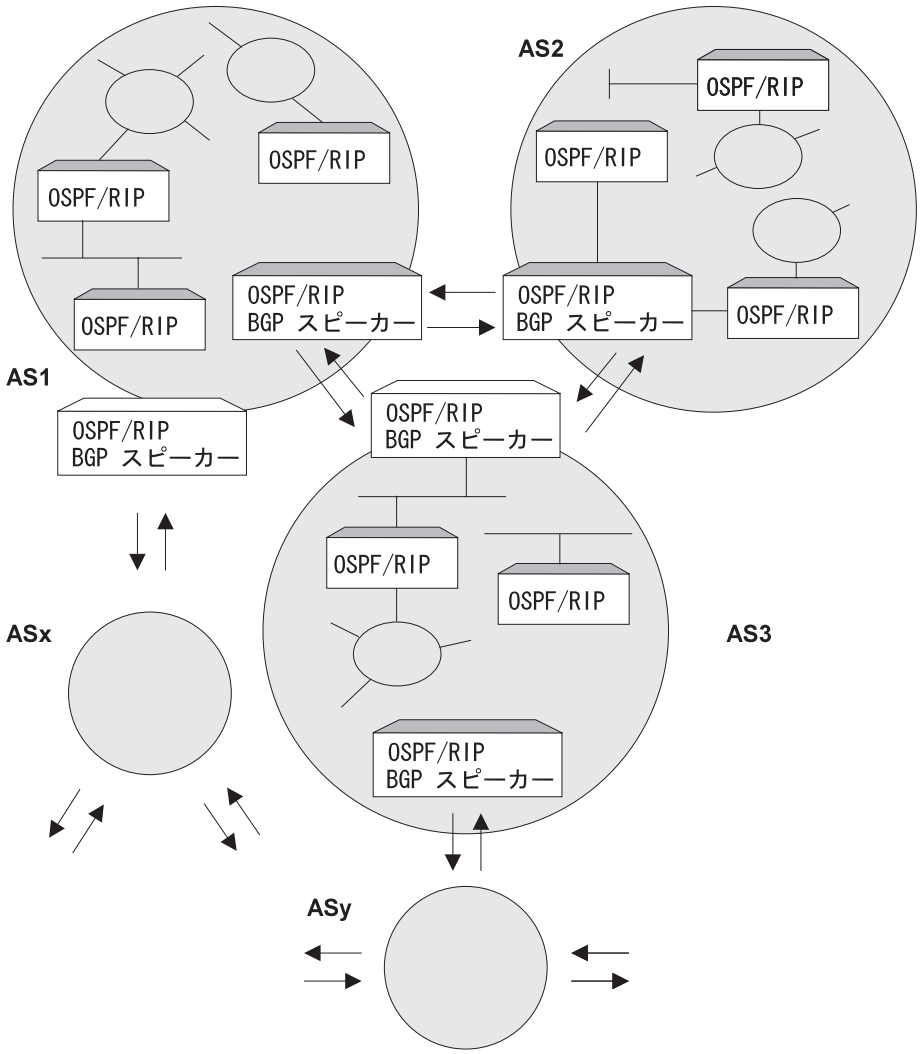


図 35. 3 つの自律システム間の BGP コネクション. AS1 および AS3 は 2 つの BGP スピーカーを持つことに注意してください。

TCP コネクションが確立されると、385ページの図34 に示された 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 BGP 近隣に送信することができます。ただし、セキュリティーまたはその他の理由により、各ネットワーク上の到達可能性情報を AS2 に送信するのは好ましくない場合があります。同様にして、AS2 が AS1 内の各ネットワーク上の到達可能性情報を受信するのは好ましくない場合があります。

ポリシーの発信、送信、および受信

どの到達可能性情報を公示 (送信) し、どれを受け入れる (受信する) かについての判断は、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 による BGP 実現は、次の 3 つのタイプのポリシー・ステートメントをサポートしています。

- Originate Policy
- Send Policy - send ポリシーには次の 2 種類があります。

– AS ベースの send ポリシーは、特定の AS にのみ適用されるか、あるいはすべての AS に適用されます。send ポリシーが設定されないと、あて先アドレスが切り捨てられます。
– 近隣ベースの send ポリシーは、特定の近隣にのみ適用されるか、あるいはすべての近隣に適用されます。特定の近隣について近隣ベースの send ポリシーが設定されない場合には、AS ベースの send ポリシーが適用されます。近隣ベースの send ポリシーが設定された場合、AS ベースの send ポリシーは無視されます。

各 send ポリシーステートメントには、ネットワーク公示分類コードと関連アクションのセットが含まれています。

あて先ネットワーク分類は、次のものに基づいて行われます。

– 正確なあて先ネットワーク
– あて先ネットワークの範囲
– 発信元 AS 番号
– AS パス属性に入っている任意の AS 番号

考えられるアクションは、次のものです。

– あて先ネットワークを公示対象から除外する
– 特定の AS またはすべての AS (AS ベースのポリシーを使用) あるいは特定の近隣 (近隣ベースのポリシーを使用) への公示対象としてあて先ネットワークを組み込む
– MED 値の設定
– ASpath 埋め込み

注: MED および ASpath 埋め込みは、近隣ベースのポリシーにのみ適用されます。

MED 属性値は、そのルートの優先について外部 BGP 近隣にヒントを与えます。最小の MED 属性値をもつルートが優先されます。詳細については、393ページの『ルート優先プロセス』を参照してください。

- ASpath 埋め込みがあると、追加のローカル AS 番号倍数 (1 ～ 10) を BGP ルートの ASpath に追加することができます。最小の ASpath 属性値をもつルートが優先されます。詳細については、393ページの『ルート優先プロセス』を参照してください。

- Receive Policy - receive ポリシーには次の 2 種類があります。
  – AS ベースの receive ポリシーは、特定の AS にのみ適用されるか、あるいはすべての AS に適用されます。receive ポリシーが設定されないと、あて先アドレスが切り捨てられます。
  – 近隣ベースの receive ポリシーは、特定の近隣にのみ適用されるか、あるいはすべての近隣に適用されます。特定の近隣について近隣ベースの receive ポリシーが設定されない場合には、AS ベースの receive ポリシーが適用されます。近隣ベースの receive ポリシーが設定された場合、AS ベースの receive ポリシーは無視されます。

  各 receive ポリシーステートメントには、ネットワーク公示分類コードと関連アクションのセットが含まれています。

  あて先ネットワーク分類は、次のものに基づいて行われます。

- 正確なあて先ネットワーク
- あて先ネットワークの範囲
- 発信元 AS 番号
- AS パス属性に入っている任意の AS 番号

考えられるアクションは、次のものです。

- あて先ネットワークの除外
- 特定の AS またはすべての AS (AS ベースのポリシーを使用) あるいは特定の近隣 (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の組み込み
- MED 値のリセット
- weight (重み) 値の設定
- IGP メトリック値の設定
- ローカル優先値の設定

注: MED 値、 weight (重み) 値、およびローカル優先値は、近隣ベースのポリシーにのみ適用されます。

weight (重み) 値は、最高の weight 値に基づいてルートを選択するようローカル BGP ルーターにヒントを与え、ルート優先アルゴリズムを無視します。

BGP メッセージ

BGP ルーターは、近隣と通信するのに次の 4 種類のメッセージを使用します。OPEN、KEEP ALIVE、UPDATE、および NOTIFICATION メッセージ

OPEN

Open メッセージは、BGP 近隣へのリンクが起動し、コネクションを確立するときに伝送される最初のメッセージです。

KEEP ALIVE

Keep alive メッセージは、BGP ルーターにより、特定のコネクションが起動し、作動していることを相互に通知するために使用されます。

UPDATE

Update メッセージには、内部ルーティング・テーブル情報が入っています。BGP スピーカーが update メッセージを送信するのは、ルーティング・テーブル内に変更がある場合のみです。

NOTIFICATION

Notification メッセージは、BGP スピーカーが、既存のコネクションの終了を強制する条件が検出されるたびに送信されます。これらのメッセージは、コネクションが伝送される前に公示されます。

BGP4 の設定

BGP の設定には、次の 3 つの基本ステップが含まれます。

1. 『BGP の使用可能化』

   BGP を使用可能にするには、BGP ルーターの固有な AS 番号を指定する必要があります。AS 番号は、Stanford 研究所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 近隣の定義』

   BGP 近隣 とは、BGP スピーカーがそれと TCP コネクションを確立する BGP ルーターです。近隣が定義されると、近隣へのコネクションはデフォルトで確立されます。

3. 390ページの『ポリシーの追加』

   ユーザーが設定する *ポリシー* は、どのルートが BGP スピーカーによってインポートまたはエクスポートされるかを決定します。ポリシーは種々の目的で設定することができます。詳細については、 390ページの『ポリシー定義のサンプル』を参照してください。

BGP の使用可能化

BGP を使用可能にするには、以下のように **enable BGP speaker** コマンドを使用します。

```
BGP Config> enable BGP speaker
AS [0]? 167
TCP segment size [1024]?
```

AS number は 1 ～ 65535 の範囲内である必要があります。*TCP segment* size は、1 ～ 65535 の範囲内にある必要があります。*TCP segment* のデフォルト値は 1024 です。この数字は、 BGP がパッシブ TCP コネクションに使用する最大のセグメント・サイズを表しています。

enable bgp コマンドを発行した後で、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 近隣の定義

BGP スピーカーを使用可能にした後、その近隣を定義する必要があります。BGP 近隣は内部または外部になります。内部近隣は同じ AS 内に存在し、相互に直接接続をもつ必要はありません。外部近隣は異なる自律システム内に存在します。これらは、相互に直接接続を持つ必要があります。

内部または外部 BGP 近隣を定義するには、**add neighbor** コマンドを使用します。近隣の IP アドレスを指定し、下記のように近隣に 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 番号をもつ必要があります。

```
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
```

reset neighbor コマンドは、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、指定された BGP 近隣を起動するのに使用します。

ポリシーの追加

IBM による BGP の実現は、次の 3 つのポリシー・コマンドをサポートしています。

- *Originate Policy*。これにより、エクスポートする内部ゲートウェイ・プロトコル (IGP) ネットワークを選択することができます。
- *Receive Policy*。これにより、BGP ピアからインポートするルート情報を選択することができます。
- *Send Policy*。これにより、ピアにエクスポートするルート情報を選択することができます。エクスポート可能なルート情報は、近隣の自律システムから収集した情報、ならびに IGP 内で発信するルートを含むことがあるので注意してください。

近隣ベースのポリシーの追加または変更を行った場合は、**reset neighbor** コマンドを使用して近隣ポリシーを起動してください。AS ベースのポリシーの追加または変更を行った場合には、装置をリブートする必要があります。

ポリシー定義のサンプル

この節では、BGP スピーカー用に設定することができるいくつかの特定のポリシーの例を提供します。すべてのポリシーは、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、396ページの『Add』 を参照してください。

Originate Policy の例

すべてのルートを公示に組み込む

この例では、BGP スピーカーの IGP ルーティング・テーブル内のすべてのルートを公示に組み込みます。この意味では、このコマンドを BGP 用の “デフォルトの” originate ポリシーステートメントとして見ることができます。

このコマンドは単一の (正確な) アドレスではなく、アドレスの範囲を指定することに注意してください。

```
BGP Config> add originate-ポリシーinclusive
Network Prefix [0.0.0.0]?
Network Mask [0.0.0.0]?
Address Match (Exact/Range) [Exact]? range
Tag [0]?
```

ルートの範囲を除外する

この例も範囲を指定しますが、この場合では目的は 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ためです。

この例では、IGP ルーティング・テーブルから 194.10.16.0 ～ 194.10.31.255 の範囲にあるすべてのルートを除外して、それらのルートが公示されないようにします。

```
BGP Config> add originate-ポリシー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]?
```

タグは受信された RIP 情報です。公示のために特定のタグ値に基づきネットワークを選択することができます。タグ値の設定に関する情報については、255ページの『第14章 IP の構成および監視』 の **Set** コマンドの説明を参照してください。

デフォルトでは、BGP スピーカーの IGP ルーティング・テーブルからクラスがあるルートだけが公示対象として選択されます。無クラス・ルートを公示対象として選択するには、bgp-subnets **patch** コマンドを使用します。**patch** についての情報は、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*の “構成プロセス (CONFIG - Talk 6) コマンド” という章を参照してください。

AS ベースの Receive Policy の例

すべての BGP 近隣からすべてのルートをインポートする

この例では、BGP スピーカーがそのすべての近隣からのすべてのルートをその IGP ルーティング・テーブルにインポートすることができるようにします。

```
BGP Config> add receive-ポリシー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 では、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場合のメトリック値を指定します。ルートを組み込むためのポリシーを設定しているときだけ、IGP メトリックの値を入力するよう促されるだけです。

IGP-metric が -1 の場合、これらのルートは IGP にインポートされないので、ルートは再公示可能ではありません。

発信元 AS からの特定ルートをブロックする

この例では、BGP スピーカーが AS 168 で発信されるルートを近隣 AS 165 からインポートできないようにします。セキュリティー上の理由から BGP スピーカーに AS 168 からルートを受信させたくない場合は、このコマンドを使用することができます。

```
BGP Config> add receive-ポリシー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 スピーカーがその ASpath リストに AS 175 をもつルートをインポートしないようにします。

```
BGP Config> add no-receive
Enter AS: [0]? 175
```

近隣ベースの Receive Policy の例

特定の BGP 近隣からすべてのルートをインポートし、weight (重み) を 100 に設定する

この例は、BGP 近隣 192.0.190.178 からすべてのルートをインポートできるようにします。すべてのルートは 100 という重み値と 1 という IGP メトリック値をもちます。

ポリシー・リスト名を receive ポリシーに合わせて定義します。

```
BGP Config> add policy-list
Name[]?S1_100_r
Policy Type(Receive/Send)[Receive]?Receive
```

定義されたポリシー・リスト名を特定の近隣に付加します。

```
BGP Config> attach policy-to-neighbor
Neighbor address [0.0.0.0]?192.0.190.178
First receive ポリシーlist name (none for global AS based policy)[]?S1_100_r
Second receive ポリシーlist name (none for exit)[]?
```

update コマンドと **add** コマンドを使用して近隣の receive poilicy を追加します。

```
BGP Config>update ポリシー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 Send Policy の例

ルート公示を特定の AS に制限する

この例では BGP スピーカーを制限します。このスピーカーは、AS 165 から発信する、アドレス範囲が 143.116.0.0 ～ 143.116.255.255 のルートを、自律システム 168 に公示することはできません。

```
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
```

すべての既知のルートを公示する

この例では、BGP スピーカーはその IGP から発信されたすべてのルート、およびその近隣自律システムから確認されたすべてのルートを公示するようにします。

```
BGP Config> add send ポリシー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 Send Policy の例

すべての既知ルートを、100 という MED 属性値をもつ特定の近隣に公示する

この例は、BGP 近隣 192.0.190.178 に対してすべてのルートを公示できるようにします。すべての公示ルートは、100 という MED 値をもちます。

ポリシー・リスト名を send ポリシーに合わせて定義します。

```
BGP Config> add policy-list
Name[]?S1_100_s
Policy Type(Receive/Send)[Receive]?Send
```

定義された send ポリシーのリスト名 (複数の場合もあります) を特定の近隣に付加します。

```
BGP Config> attach policy-to-neighbor
Neighbor address [0.0.0.0]?192.0.190.178
First send ポリシーlist name (none for global AS based policy)[]?S1_100_s
Second send ポリシーlist name (none for exit)[]?
```

update コマンドと **add** コマンドを使用して近隣についての send ポリシーを追加します。

```
BGP Config>update ポリシー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 スピーカーが特定のあて先のパスをそのピアから受け取ると、BGP は、考えられる最善のパスを選択するために以下のプロセスを行います。

- 構成に基づいて receive ポリシーを適用する。
- ポリシーを受信することによってあて先が許可される場合は、短い方の ASpath 長と Origin タイプに基づいて、受信されたあて先について Degree of Reference (優先度) を計算する。
- 同じあて先までのパスがいくつかある場合は、パス選択プロセスを実行する。新しいパスを既存の選択した最善のパスと比較することにより、考えられる最善のパスを選択する。新しいパスが最善のパスとして選択された場合には、その新しいパスを IP 転送テーブルにインストールする。
- send ポリシーを条件として、選択された最善のパスをその外部/内部 BGP ピアに対して公示する。

パス選択プロセス

最善のパスは、以下の順序で選択します。

- このルーターが発信したパスを優先する。

- その場合、このルーターが発信したパスでなければ、設定済みの最高の Weight 値をもつパスを優先する。
- パスが同じ weight (重み) 値をもつ場合には、設定済みの最高の local-preference (ローカル優先) 値をもつパスを優先する。
- パスが同じ local-preference 値をもつ場合には、最高の Degree of Preference をもつパス優先する。
  - 最も短い ASpath 長をもつパスに、最高の優先度が与えられる。
  - パスが同じ ASpath 長をもっている場合には、EGP および Incomplete よりも Origin タイプ IGP が優先される。
- パスが同じ Degree of Preference をもつ場合には、最小の MED 属性値をもつパスを優先する。
- パスが同じ MED 属性値をもつ場合には、内部 (IBGP) ルートよりも外部 (EBGP) ルートを優先する。
- それでもパスが同じである場合は、最小の BGP ID をもつパスを優先する。

第18章 BGP4 の構成および監視

この章では、BGP 構成コマンドおよび監視コマンドについて説明し、以下の節が含まれています。

- 『BGP4 構成コマンド』
- 『BGP4 構成環境へのアクセス』
- 411ページの『BGP 監視環境へのアクセス』
- 411ページの『BGP4 監視コマンド』

BGP4 構成環境へのアクセス

BGP 構成環境にアクセスするには、`Config>` プロンプトで次のコマンドを入力します。

```
Config> 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、BGP プロトコルの動作をユーザー特有の要件に適合するように変更できます。BGP ルーターが完全に機能するようにするためには、いくらかの構成が必要です。BGP 構成コマンドは `BGP config>` プロンプトで入力します。

表 23. BGP 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	BGP 近隣およびポリシーを追加します。
Attach	receive policy-list と send policy-list を特定の近隣に付加します。
Change	元は **add** コマンドを使用して入力された情報を変更します。
Delete	**add** コマンドを使用して入力された 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た BGP 機能を使用不可にします。
Enable	BGP スピーカー、BGP 近隣、または Classless 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 aggregate (集合体) が定義される順序を変更します。
Set	IP-route-table-scan-timer 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	submenu **add**、**delete**、 **change**、および **move** コマンドを使用して、構成済みの policy-list name 内で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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは BGP 情報を構成に追加するのに使用します。

構文:

add aggregate . . .

neighbor . . .

no-receive asnum . . .

originate-ポリシー. . .

policy-list . . .

receive-ポリシー. . .

send-policy. . .

aggregate *network prefix network mask*

add aggregate コマンドは、BGP スピーカーにアドレスのブロックを集合 (aggregate) させ、その BGP 近隣に単一のルートを公示させます。集合されるすべてのルートに共通のネットワーク・プレフィックスおよびそのマスクを指定する必要があります。次の例では、194.10.16.0 ～ 194.10.31.255 のアドレスのブロックを集合させる方法を示します。

1. *Network Prefix* は影響を受けるアドレスです。プレフィックスは、BGP ポリシーで指定されているアドレスの範囲内の最初のアドレスです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

2. *Network Mask* は、BGP ポリシーで使用されたアドレスを生成するためにネットワーク・プレフィックスで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

   デフォルト値: 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
```

集合体の定義を追加する際、集合されたルートがエクスポートされないようにするためポリシーを定義することを忘れないでください。ポリシーを定義しないと、ルーターは個別のルートおよびユーザーが定義した集合体の両方を公示します。これは、ルーターの IGP ルーティング・テーブルから発信されるルートを集合しているときは、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、外部であっても構いません。近隣を動的に起動するには、BGP 監視から **reset neighbor** コマンドを使用してください。

1. IP アドレスは、ピアにしたい近隣のアドレスです。このアドレスは、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構いません。それが外部の近隣である場合、両方の BGP スピーカーは同じネットワークを共用する必要があります。内部近隣にはそのような制限はありません。アドレスの値は次のとおりです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

2. AS 番号は、ユーザー自身の自律システム番号 (内部近隣の場合) または近隣の自律システム番号です。近隣の AS 番号の値は次のとおりです。

   有効値: 0 ～ 65535 の範囲の整数

   デフォルト値: なし

3. *Init timer* は、資源を初期化し、BGP スピーカーがエラーのために以前に IDLE 状態に変更されていた場合には近隣とのトランスポート・コネクションを再度開始するのに BGP スピーカーが待つ時間の長さを指定します。エラーが続く場合は、タイマーは指数関数的に増加します。

   有効値: 0 ～ 65535 秒

   デフォルト値: 12 秒

4. *Connect timer* は、CONNECT または ACTIVE 状態にある間に TCP コネクションに障害が起きた場合に、BGP スピーカーがその近隣へのトランスポート・コネクションを開始するのに待つ時間の長さを指定します。その間、 BGP スピーカーは、その近隣によって開始されるコネクションがないか listen し続けます。

   有効値: 0 ～ 65535 秒

   デフォルト値: 120 秒

5. 近隣が到達不能であると想定する前に BGP スピーカーが待つ時間の長さを指定するには、*Hold timer* を入力します。両方の近隣は、構成済みの情報を OPEN メッセージで交換し、2 つのタイマーのうち小さい方をネゴシエーションされた Hold Timer 値として選択します。

   近隣が BGP コネクションを確立すると、それらはキープアライブ・メッセージを頻繁に交換し、コネクションがまだ起動しており、近隣が到達可能であることを確認します。キープアライブ・タイマー間隔は、ネゴシエーションされた保留時間値の 1/3 になるように計算されます。したがって、保留タイマー値はゼロまたは少なくとも 3 秒であるかのいずれかである必要があります。

   交換回線では、キープアライブを頻繁に送信しないことによって帯域幅を保管するためにゼロでない Hold Timer 値を持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

デフォルト値: 90 秒

6. *TCP segment size* は、TCP コネクション上で近隣と交換することができる最大データ・サイズを指定します。この値は、近隣とのアクティブ TCP コネクションに使用されます。

   有効値: 0 ～ 65535 バイト

   デフォルト値: 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、特定の AS 番号が AS パス・リスト内のどこかに現れる場合に、AS パスを除外するのに使用します。

AS number の値は次のとおりです。

有効値: 0 ～ 65535

デフォルト値: 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、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・テーブルへと、特定のアドレス、またはアドレスの範囲をインポートすることができるかどうか判別するポリシーを作成するのに使用します。

Exclusive	Exclusive (排他的) 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 (包括的) ポリシーは、特定のルートが 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を受ける、アドレス、またはアドレスの範囲
Tag	特定の AS 用に設定された値。すべてのタグ値は、それらが確認された AS のタグ値に一致します。

Exclusive (排他的) 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* 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

デフォルト値: なし

2. BGP ポリシーで使用されたアドレスを生成するためにネットワーク・プレフィックスで指定されたアドレスに適用される *Network Mask* を入力します。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

3. *Address match* がアドレスの範囲または正確なアドレスのどちらになるのかを選択します。
4. *TAG* は、特定の AS 用に設定された値です。タグ値は、それらが確認された AS のタグ値に一致します。

   有効値: 0 〜 65535

   デフォルト値: なし

次の例には、BGP スピーカーの公示される IGP ルーティング・テーブル内のすべてのルートが含まれます。

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 ポリシーコマンドの詳しい例については、390ページの『Originate Policy の例』を参照してください。

policy-list

add policy-list コマンドは、**attach policy-to-neighbor** コマンドを使用して特定の近隣に付加することのできる ポリシーのグループを構成するのに使用します。

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、392ページの『近隣ベースの Receive Policy の例』 および 393ページの『近隣ベースの Send Policy 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、どのルートが 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か判別するのに使用します。

Exclusive (排他的) 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* 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

   デフォルト値: なし

2. *Network Mask* は、BGP ポリシーで使用されたアドレスを生成するためにネットワーク・プレフィックスで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

   デフォルト値: 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#* の値は次のとおりです。

   有効値: 0 〜 65535

   デフォルト値: なし

5. *Adjacent AS#* は、近隣 AS 番号を指定します。

   有効値: 0 〜 65535

   デフォルト値: 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 ポリシーコマンドの詳しい例については、391ページの『AS ベースの Receive Policy 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、BGP スピーカーの確認されたルートのうちどれを再公示するか判別するポリシーを作成するために使用します。これらのルートは、BGP スピーカーの AS に対して内部でも外部でも構いません。

Exclusive (排他的) 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* は、影響を受けるアドレス用です。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

2. *Network Mask* は、BGP ポリシーで使用されたアドレスを生成するためにネットワーク・プレフィックスで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

   デフォルト値: 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 用に設定された値です。タグ値は、それらが確認された AS のタグ値に一致します。

   有効値: 0 〜 65535

   デフォルト値: なし

5. *Adjacent AS#* は、近隣 AS 番号を指定します。

   有効値: 0 〜 65535

   デフォルト値: 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 ポリシーコマンドの詳しい例については、392ページの『AS ベースの Send Policy の例』を参照してください。

Attach

attach policy-to-neighbor コマンドは、構成済みの policy-list 名を特定の近隣に付加するのに使用します。receive policy-list 名と send policy-list 名は、それぞれ、最大 3 つまで付加することができます。

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、392ページの『近隣ベースの Receive Policy の例』 および 393ページの『近隣ベースの Send Policy の例』 を参照してください。

Change

change コマンドは、以前に add コマンドによって導入された 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、現行の aggregate (aggregate 1) を変更します。変更により、aggregate 1 は、異なるネットワーク・プレフィックスおよびマスクを使用して、アドレス範囲 128.185.0.0 ～ 128.185.255.255 のすべてのルートを集合させます。

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 用に hold timer の値をゼロに変更します。

変更される *neighbor address* の値は次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

近隣を動的に起動するには、BGP 監視から **reset neighbor** コマンドを使用します。

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 originate policy 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 originate policy を更新します。IGP ルーティング・テーブルからプレフィックスが 194.10.16.0 のネットワークを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るようになります。

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

change policy-to-neighbor コマンドは、特定の近隣への policy-list 接続を変更するのに使用します。

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 receive policy 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 receive-policy に制限を追加します。すべての BGP からその IGP ルーティング・テーブルにルート情報をインポートするのではなく、AS 165 からのルートがインポートさせないようになりました。

例: **change receive-policy**

```
Enter index of receive-ポリシー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 send policy をさらに包括的、またはさらに排他的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 send policy に制限を追加します。この制限により、自律システム 165 を公示するとき、アドレス範囲 194.10.16.0 ～ 194.10.31.255 にあるすべてのルートは除外されるようになります。

例: change send-policy

```
Enter index of send-ポリシー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、以前に **add** コマンドによって導入された 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 aggregate 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 番号と同値です。

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。

近隣の削除されるネットワーク・アドレス の値は次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

この近隣を動的に非活性化するには、BGP 監視から **reset neighbor** コマンドを使用します。

例: delete neighbor 192.0.251.165

no-receive *as*

このコマンドは、特定の AS 用に設定された no-receive policy 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 number の値は次のとおりです。

有効値: 0 ～ 65535

デフォルト値: なし

例: delete no-receive 168

originate-policy *index#*

このコマンドは、特定の originate policy を削除するのに使用します。ポリシーに関連するインデックス番号を指定する必要があります。

例: delete originate-policy2

policy-list

delete policy-list コマンドは、policy-list を削除するのに使用します。

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.
```

policy-to-neighbor 接続は、これに応じて調整されます。

policy-to-neighbor

delete policy-to-neighbor コマンドは、特定の近隣への既存の policy-list 名の接続を削除するのに使用します。

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 receive policy を削除するのに使用します。ポリシーに関連する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-ポリシーto be deleted [1]?
```

send-policy *index#*

このコマンドは、特定の send policy を削除するのに使用します。ポリシーに関連するインデックス番号を指定する必要があります。

例: delete send-policy4

Disable

disable コマンドは、以前に使用可能にした BGP 近隣またはスピーカーを使用不可にするのに使用します。近隣は、**add** コマンドを使って追加された場合はいつでも、暗黙的に使用可能にされてい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

disable bgp speaker コマンドは、BGP プロトコルを使用不可にするのに使用します。

例: disable bgp speaker

classless-bgp

このコマンドは、無クラス・ルートを公示に使用できないようにするのに使用します。

例: disable classless-bgp

注: patch bgp-subnets コマンドが使用不可であることを確認してください。

compare-med-from-diff-AS

このコマンドは、異なる AS 間での MED 比較を使用不可にするのに使用します。

例: disable compare-med-from-diff-AS

neighbor *neighbor IP address*

neighbor address の値は次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

例: disable neighbor 192.0.190.178

Enable

enable は、ユーザーの BGP 構成に追加された BGP 機構、機能、および情報を起動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 は BGP の最新バージョンである BGP4 (RFC 1654 に定義されています) だけをサポートしています。

1. *AS number* は、ルーターおよびノードの集合に関係付けられます。

   有効値: 0 〜 65535

   デフォルト値: なし

2. *TCP segment size* は、BGP がパッシブ TCP コネクションに使用する必要のある最大セグメント・サイズを指定するのに入力します。

   有効値: 0 ～ 65535 バイト

   デフォルト値: 1024 バイト

例:

```
enable bgp speaker

AS [0]? 165
TCP segment size [1024]?
```

classless-bgp neighbor

このコマンドは、無クラス・ルートを公示に使用できるようにするのに使用します。

例: enable classless-bgp

compare-med-from-diff-AS

このコマンドは、異なる AS 間での MED 比較を使用可能にするのに使用します。

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。

neighbor address の値は次のとおりです。

有効値: 任意の有効な IP アドレス

デフォルト値: なし

例: enable neighbor 192.0.190.178

List

list コマンドは、起動された特定のサブコマンドに対応する種々の BGP 構成データ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** コマンドを使って定義されたすべての集合されたルートに使用します。

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、集合されたルート、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。提供さ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 構成に追加された no-receive-AS 定義に関する情報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 構成に追加された originate policies 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

list policy-list コマンドは、構成済みの policy-list 名をリストするのに使用します。

例: list policy-list

```
BGP Config>li ポリシーlist
Policy list:
nbr1-rcv  Receive
nbr1-snd  Send
```

policy-to-neighbor

list policy-to-neighbor コマンドは、近隣に付加されたポリシーをリストするのに使用します。

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 構成に追加された receive policies に関する情報を引き出すのに使用します。AS 用に定義されたすべての receive policies を表示するか、policies をインデックスまたはプレフィックス番号別に表示することができます。

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 send policies に関する情報を表示するのに使用します。AS 用に定義されたすべての send policies を表示するか、policies をインデックスまたはプレフィックス番号別に表示することができます。

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、policies および aggregates 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、ルーターが情報を発送するために既存のポリシー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、どのポリシーが定義されているか調べることをお勧めします。

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

set コマンドは、IP-route-table-scan-timer を設定するのに使用します。IP-route-table-scan-timer 値は、IP 転送テーブル・スキャン時間間隔を BGP 更新用に設定するのに使用します。

構文:

set ip-route-table-scan-timer

例:

```
set ip-route-table-scan-timer
```

Update

update コマンドおよびサブコマンドは、ポリシーを操作するのに使用します。

構文:

update *policy-list*

Receive Policy の例:

```
update policy-list
Name[]? nbr1-rcv
```

Add

Add コマンドは、**update** コマンド内に receive policy を追加するのに使用します。

```
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 (排他的) receive policy について MED、Local-pref、Weight、および IGP-metric パラメーターの指定を求めるプロンプトは出されません。MED および Local-pref 値は、'0' と設定されると、受信された公示からは使用されません。weight (重み) パラメーターの値が '0' であると、ルート選択プロセスの weight 値を無視するよう指示されます。

Change

Change コマンドは、**update** コマンド内でポリシーを変更するのに使用します。

例:

```
Enter index of receive-policy to be modified [1]?
```

Delete

delete コマンドは、**update** コマンド内でポリシーを削除するのに使用します。

例:

```
Enter index of receive-policy to be deleted [1]?
```

Move

Move コマンドは、**update** コマンド内でポリシーを移動するのに使用します。

例:

```
Enter index of receive-policy to move [1]?
Move record after record number [0]?
```

List

list コマンドは、**update** コマンド内に receive ポリシーをリストするのに使用します。

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
```

Send Policy の例:

```
update policy-list
Name[]? nbr1-rcv
```

Add

Add コマンドは、**update** コマンド内で send policy を追加するのに使用します。

```
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 (排他的) receive policy について MED および ASpad パラメーターの指定を求めるプロンプトは出されません。MED パラメーターの値が 0 であると、MED 属性を公示に含めないよう指示されます。ASpad パラメーターの値が 0 であると、ASpath に挿入される追加のローカル AS 番号がないことが指示されます。

Change

Change コマンドは、**update** コマンド内でポリシーを変更するのに使用します。

例:

```
Enter index of send-policy to be modified [1]?
```

Delete

delete コマンドは、**update** コマンド内でポリシーを削除するのに使用します。

例:

```
Enter index of send-policy to be deleted [1]?
```

Move

Move コマンドは、**update** コマンド内でポリシーを移動するのに使用します。

例:

```
Enter index of send-policy to move [1]?
Move record after record number [0]?
```

List

list コマンドは、**update** コマンド内に send policy をリストするのに使用します。

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 監視環境へのアクセス

BGP 構成環境にアクセスするには、Config> プロンプトで次のコマンドを入力します。

```
Config> 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、BGP プロトコルの動作をユーザー特有の要件に適合するように変更できます。BGP ルーターが完全に機能するようにするためには、いくらかの構成が必要です。BGP 監視コマンドは BGP> 監視プロンプトで入力します。

表 24. BGP 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。

表 24. BGP 監視コマンドの要約 (続き)

コマンド	機能
Destinations	BGP ルーティング・テーブル内のすべてのエントリーを表示します。
Disable neighbor	特定の近隣またはすべての近隣を使用不可にします。
Dump routing tables	IP ルーティング・テーブルのコンテンツをリストします。
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	現在アクティブ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 グローバル変数を表示します。
Paths	データベース内のすべての利用可能なパスを表示します。
Ping	ICMP エコー要求を 1 秒に 1 度別のホストに送信し、レスポンスを監視します。このコマンドは、インターネットワーク環境の障害を分離するのに使用できます。
Policy-list	特定の近隣の現在のインストール済みポリシーおよび各ポリシーの使用統計値を表示します。
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を (ホップごとに) 表示します。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Destinations

destinations コマンドは、すべての BGP ルーティング・テーブル・エントリーをダンプするか、指定された BGP 近隣アドレス (destinations) に公示されるか、それから受信された情報を表示するのに、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しい情報を表示します。このコマンドは、特定のルートがどのように確認されたか、特定のあて先への最善のパス、ルートに関連するメトリック、およびその他の情報を表示します。

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 パスに沿った自律システムの列挙

-seq: パス内の自律システムの順序

-set: パス内の自律システムの集合

Origin あて先の発信者。これは EGP、IGP、または Incomplete (未知の他の何らかの方法によって発信された) です。

LocalPref あて先への発信側ルーターの優先度

Metric ルートがインポートされるパス・メトリック

Weight パスの重み

MED 同じ AS への複数の入り口/出口点を区別するために使用される multi-exit discriminator 値

NextHop 所定のパスを介して到達可能なあて先への転送アドレスとして使用するルーターのアドレス

AtomicAggr パスを公示するルーターがそのパスを atomic-aggregate に組み込んだかどうかを示します。

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しい情報を表示します。このコマンドは、特定のルートがどのように確認されたか、特定のあて先への最善のパス、ルートに関連するメトリック、およびその他の情報を表示します。

このコマンドは、複数のネットワーク・アドレスが同じプレフィックスと異なるマスクを持つ場合に、便利です。そのような場合、ネットワーク・マスクを指定すると、提示される情報の有効範囲が狭まります。

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 近隣に公示された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、使用可能にされた特定の近隣またはすべての近隣を使用不可にするのに使用します。このコマンドは、 BGP セッションを停止させ、その近隣から確認されたルートを除去します。

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 コマンドの完全な説明については、*プロトコルの構成と監視 解説書 第 1 巻* の 『IP の監視』 という章の 『ダンプ・ルーティング・テーブル』 を参照してください。

Enable Neighbor

enable neighbor コマンドは、使用不可にされた特定の近隣を使用可能にするか、すべての近隣を使用可能にするのに使用します。このコマンドは、近隣との BGP セッションを開始します。

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、すべてのアクティブな 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 コネクションの状態を指定します。可能な状態は、以下のとおりです。

Connect
近隣への TCP コネクションが完了するのを待っています。

Active TCP コネクションに障害が起きるような場合、状態は Active に変更され、近隣を獲得しようとする試行が続きます。

OpenSent
この状態では、OPEN が送信され、BGP が近隣からの OPEN メッセージを待っています。

OpenConfirm
この状態では、近隣の OPEN に応答して KEEPALIVE が送信され、近隣からの KEEPALIVE/NOTIFICATION を待っています。

Established
BGP コネクションが正常に確立され、UPDATE メッセージの交換を開始することができるようになりました。

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# 近隣に送信された最後の UPDATE メッセージのシーケンス番号を指定します。

internet-address

neighbor コマンドは、特定の BGP 近隣に関する詳しい情報を表示するのに使用します。

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 **parameter** コマンドは、BGP システム内のインストール済み BGP グローバル変数を表示するのに使用します。

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

BGP **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 所定のパスを介して到達することができるあて先への転送アドレスとして使用するルーターのアドレス

MED 同じ AS への複数の入り口/出口点を区別するために使用される multi-exit discriminator。

AAG パスが atomic-aggregated されたかどうか、つまりオーバーラップするルートが提示されたときに、所定のパスを公示しているルーターが、特定度の高い方のルートに対して特定度の低い方のルートを選択したかどうかを示します。

AGRAS ルートを集めた BGP スピーカーの AS 番号を示します。

RefCnt 記述子を指すパス・エンティティーの数を示します。

ORG 所定のパス内で公示されたあて先の発信者を指定します。EGP、IGP、または Incomplete (未知の他の何らかの方法によって発信された) のいずれか。

AS Path パスに沿った自律システムの列挙

seq: パス内の自律システムの順序

set: パス内の自律システムの集合

Ping

ping コマンドの完全な説明については、*プロトコルの構成と監視 解説書 第 1 巻* の『IP の監視』 という章の IP Ping コマンド を参照してください。

Policy-List

policy-list コマンドは、特定の近隣の現在のインストール済みポリシーおよび各ポリシーの使用統計値を表示するのに使用します。

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の表示は、次のものです。

```
Receive ポリシー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の表示は、次のものです。

```
Receive ポリシー:
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の表示は、次のものです。

```
send ポリシー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の表示は、次のものです。

```
send ポリシー:
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 ポリシー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、指定された 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、さまざまなデータベースに保管されたエントリー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パスの合計数

Path descriptors
共通の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合計数

Update sequence#
現行の更新シーケンス番号を示します。

Routing tbl entries (allocated)
BGP ルーティング・テーブル内のエントリーの数を示します。

Current tbl entries (not imported)
IGP にインポートされない 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 コマンドの完全な説明については、255ページの『第14章 IP の構成および監視』 を参照してください。

第19章 DVMRP の構成および監視

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・アクティビティーの構成および監視について説明します。本章には、以下の節が含まれています。

- 『DVMRP 構成環境へのアクセス』
- 『DVMRP 構成コマンド』
- 424ページの『DVMRP 監視コマンド』

DVMRP 構成環境へのアクセス

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

```
Config> 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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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または IP 間トンネル・インターフェースを追加することができます。
Change	SRAM 内の DVMRP 情報を変更します。物理インターフェースのコストまたはしきい値、IP 間トンネル、MOSPF インターフェース、あるいは IP 間トンネルのエンドポイントを変更することができます。
Delete	DVMRP 情報を静的構成から削除します。
Disable	DVMRP プロトコル全体または MOSPF インターフェースを使用不可にします。
Enable	DVMRP プロトコル全体または 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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、既存の DVMRP 情報に追加するのに使用します。物理インターフェースまたは IP 間トンネルを追加することができます。

構文:

add interface *ip-address cost threshold*

tunnel *tunnel-source tunnel-destination cost threshold*

interface

DVMRP インターフェースの追加または更新を行います。

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

デフォルト値: なし

cost インターフェースを使用するのにかかる (ホップ・カウントに関する) コストを指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

threshold

インターフェース上の最も近い近隣に到達するのに必要な活動時間を指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

tunnel 非マルチキャスト・ネットワークにまたがる IP 間トンネルの追加または更新を行います。マルチキャスト・トラフィックがマルチキャスト・データグラムをサポートしていないか、あるいはマルチキャスト・ルーティング・プロトコルを実行していないネットワークを通り抜ける必要があるときにはトンネルを構成する必要があります。

source-address

トンネルの元の 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

デフォルト値: なし

destination-address

トンネルの先の 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

デフォルト値: なし

cost トンネルを使用するのにかかる (ホップ・カウントに関する) コストを指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

threshold

インターフェース上の最も近い近隣に到達するのに必要な活動時間を指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

Change

change コマンドは、既存の DVMRP 情報を変更するのに使用します。物理インターフェースのコストまたはしきい値、IP 間トンネル、あるいは MOSPF インターフェースを変更できます。

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

デフォルト値: なし

cost インターフェースを使用するのにかかる (ホップ・カウントに関する) コストを指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

threshold

インターフェース上の最も近い近隣に到達するのに必要な活動時間を指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

tunnel IP 間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

デフォルト値: なし

destination-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

cost インターフェースを使用するのにかかる (ホップ・カウントに関する) コストを指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

threshold

インターフェース上の最も近い近隣に到達するのに必要な活動時間を指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

mospf MOSPF インターフェースを変更します。

cost インターフェースを使用するのにかかる (ホップ・カウントに関する) コストを指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

threshold
インターフェース上の最も近い近隣に到達するのに必要な活動時間を指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

Delete

delete コマンドは、既存の DVMRP 情報を削除するのに使用します。

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

デフォルト値: なし

tunnel IP 間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

デフォルト値: なし

destination-address

有効値: 任意の有効な IP アドレス

デフォルト値: なし

Disable

disable コマンドは、DVMRP プロトコル全体または MOSPF インターフェースを使用不可にするのに使用します。

構文:

disable dvmrp

mospf

dvmrp DVMRP プロトコルを使用不可にします。これが使用不可であると、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・プロトコルへのインターフェースを使用不可にします。これが使用不可であると、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信を行いません。

Enable

enable コマンドは、DVMRP プロトコル全体または MOSPF インターフェースを使用可能にするのに使用します。

構文:

enable dvmrp

mospf *cost threshold*

dvmrp DVMRP プロトコルを使用可能にします。IP 用に構成されているすべてのインターフェースで MOSPF が使用可能になっているわけではありませんが、MOSPF インターフェースは使用可能にされます。

mospf MOSPF ルーティング・プロトコルへ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り、DVMRP はマルチキャスト・データグラムを MOSPF ルーティング・プロトコルに転送することができます。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 インターフェースを使用するのにかかる (ホップ・カウントに関する) コストを指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

threshold
インターフェース上の最も近い近隣に到達するのに必要な活動時間を指定します。

有効値: 0 より大きい、任意の整数

デフォルト値: 1

List

list コマンドは、DVMRP 構成を表示するのに使用します。出力は、現在の DVMRP 状態 (使用不可か使用可能か)、物理インターフェース構成情報、トンネル構成情報、および MOSPF 構成情報を表示します。

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
```

リストされるインターフェースごとに、以下の情報が表示されます。

DVMRP プロトコル
DVMRP が使用可能か使用不可かを表示します

DVMRP 物理インターフェース
各物理インターフェースごとに、その IP アドレスおよびコストとしきい値の値が表示されます。

DVMRP トンネル・インターフェース
各トンネル・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、コストおよびしきい値が表示されます。

DVMRP MOSPF インターフェース
MOSPF インターフェースについて、コストおよび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して、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および統計を表示することができます。

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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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・テーブルに含まれている 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	ルーターが 1 つまたは複数のマルチキャスト・グループに所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外します。
Mcache	現在アクティブのマルチキャスト転送キャッシュ・エントリーのリストを表示します。
Mgroups	ルーターの接続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	各種のマルチキャスト・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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Dump Routing Tables

dump routing tables コマンドは、既知の DVMRP マルチキャスト発信元のセットを表示するのに使用します。各発信元は、確認が行われた DVMRP ルーター、関連コスト、およびルーティング・テーブル・エントリーがリフレッシュされた後の秒数と一緒にリストされます。

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 (すなわち 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
エントリーの元であるゲートウェイの IP アドレスを表示します。

Metric そのルートの関連コストを表示します。

Age ルーティング・テーブル・エントリーのエージを、ルーティング・テーブル・エントリーがリフレッシュされた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のある 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。アスタリスクが付いている VIF は、接続されているネットワーク上にグループ・メンバーがある場合にのみデータグラムが転送されることを示します。

Interface Summary

interface summary コマンドは、DVMRP インターフェース (または VIF) の現在のリストを表示するのに使用します。

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) に割り当てられている番号を表示します。各 VIF には番号が 1 つ割り当てられており、この番号は、他のコマンド内でその VIF を識別するのに使用されます。

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 ルートの関連コスト

Threshold ネットワークの外側でのマルチキャスト・パケットの外部の流れを制御するネットワークの能力を反映します。

Flags VIF が起動していないかどうか、あるい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ことを表示します。

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設定するのに使用します。

このコマンドは OSPF 構成監視の join コマンドと似ていますが、2 つの相違点があります。

- グループ・メンバーシップに関する効果は、モニターからコマンドが与えられると即時に有効になります (つまり、リスタート/再ロードの必要はありません)。
- このコマンドは、特定のグループが 『結合』 された回数を追跡します。

ルーターがマルチキャスト・グループのメンバーの場合、ルーターは、グループ・アドレスあてに送信された 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、ルーターのメンバーシップをマルチキャスト・グループから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・アドレスあてに送信された 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** コマンドと似ていますが、2 つの相違点があります。

- グループ・メンバーシップに関する効果は、モニターからコマンドが与えられると即時に有効になります (つまり、リスタート/再ロードの必要はありません)。
- 実行された 『leaves』 の回数が、以前に実行された 『joins』 の回数に等しくなるまでは、コマンドはグループのメンバーシップを除去しません。

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・エントリーのリストを表示するのに使用します。マルチキャスト・キャッシュ・エントリーは、要求時に (最初の照合マルチキャスト・データグラムを受信するたびに) 作成されます。データグラム発信元ネットワークとあて先グループの組み合わせごとに、個別のキャッシュ・エントリー (したがって、個別のルートも) が作成されます。

キャッシュ・エントリーは、トポロジーの変更時 (たとえば、DVMRP システム内でポイント・ポイント回線が起動または切断状態になったとき)、およびグループ・メンバーシップの変更時にクリアされます。

注: 出力の上部の凡例に表示される数値は、VIF の数を直接参照するのではなく、物理インターフェース (DVMRP または MOSPF のいずれかを実行している可能性があるもの) およびトンネルの数を参照します。

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 照合データグラムの発信元ネットワーク/サブネット

Destination 照合データグラムのあて先グループ

Count そのマルチキャスト・グループについて処理されたエントリーの数を表示します。

Upstream 転送するデータグラムをそこから受信する必要がある、近隣ネットワーク/サブネットを表示します。これが 『none』 の場合、データグラムは転送されることはありません。

Downstream データグラムの転送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* の場合には、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・エントリーには、これ以外にも情報があります。コマンド行で、照合データグラムの発信元とあて先を指定すれば、キャッシュ・エントリーの詳細を表示することができます。照合キャッシュ・エントリーが見つからない場合は、作成されます。このコマンドのサンプルを、以下に示します。

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 コマンドで表示される情報の他に、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するためにそこから受信しなければならないノードのタイプを示します。このフィールドの可能な値は、『none』 (データグラムが転送されないことを示します)、『router』 (データグラムはポイント・ポイント接続を介して受信する必要があることを示します)、『transit network』、『stub network』、および 『external』 (別の自律システムからデータグラムを受信することを想定していることを示します) です。

Downstream

データグラムの送信先の各インターフェースまたは近隣を 1 行ずつに印刷します。TTL 値も示され、このインターフェースから受信する、またはこのインターフェースに転送されるデータグラムには、少なくともその IP ヘッダーに指定された TTL 値が入っていなければならないことを示します。ルーター自体がマルチキャスト・グループのメンバーの場合、*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上のグループ・メンバーシップのみが表示されます。

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報告された (IGMP を介して) グループ・アドレスを表示します。

Interface グループ・アドレスが報告された (IGMP を介して) 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” の値で示されます。これらのエントリーの場合、lifetime フィールド (下記を参照) は、特定グループのメンバーシップを要求したアプリケーションの数を示します。

Lifetime インターフェース上で指定のグループのメンバーシップ報告を受信しなくなった場合に、そのエントリーが存続する期間を秒数で表示します。

Mstat

mstat コマンドは、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のに使用します。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、およびルーターがエリア間または AS 間 (あるいはその両方) のマルチキャスト転送機能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を表示します。

Inter-area forwarding
ルーターがエリア間で 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 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。

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、この合計には含まれません)。

DVMRP 監視コマンド (Talk 5)

Datagrams (ext source)
発信元が AS の外側にある受信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 (これにはパケット複写が含まれるので (必要な場合)、このカウントは受信した数よりはるかに大きくなる可能性があります)。

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の非 AS 間マルチキャスト転送機能によって受信されたデータグラムの数を表示します。

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数を表示します。

Unallocated cache entries
資源不足のためにキャッシュ・エントリーを作成できなかったデータグラムの数を表示します。

Off multicast tree
照合キャッシュ・エントリー内にアップストリーム近隣が存在しないか、またはダウンストリーム・インターフェース/近隣が存在しないために転送されなかったデータグラムの数を表示します。

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上で、データ・リンク・マルチキャストとして受信したデータグラムの数を表示します。

Buffer alloc failure
バッファー不足のために複写できなかったデータグラムの数を表示します。

TTL scoping
TTL がグループ・メンバーへの到達が不可能であることを示していた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・エントリーの数を表示します。

DVMRP entries freed:
解放された DVMRP エントリーの数を示します。サイズは、ルーティング・エントリー数から解放されたエントリー数を差し引いた値になります。

 # fwd cache alloc
割り当てられたキャッシュ・エントリーの数を示します。現行の転送キャッシュ・エントリー・サイズは、割り当てられたエントリーの数 (『# fwd cache alloc』) から、解放されたキャッシュ・エントリーの数 (『# fwd cache freed』) を差し引いた値です。

 # fwd cache freed
解放されたキャッシュ・エントリーの数を示します。現行の転送キャッシュ・エントリー・サイズは、割り当てられたエントリーの数 (『# fwd cache alloc』) から、解放されたキャッシュ・エントリーの数 (『# fwd cache freed』) を差し引いた値です。

 # fwd cache GC
最近使用されず、キャッシュがオーバーフローしたためにクリアされたキャッシュ・エントリーの数を示します。

 # local group DB alloc
割り当てられたローカル・グループ・データベース・エントリーの数を示します。割り当てられた数 (『# local group DB alloc』) から解放された数 (『# local group DB free』) を差し引くと、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・エントリーの数を示します。割り当てられた数 (『# local group DB alloc』) から解放された数 (『# local group DB free』) を差し引くと、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、受信し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』 が原因で廃棄されたデータグラムの合計数を差し引き、さらに 『# local group DB alloc』 を差し引くことによって計算できます。キャッシュ・ミスの数は、単に 『# local group DB alloc』+ の値です。

第20章 RSVP の使用

資源予約プロトコル (Resource ReSerVation Protocol (RSVP)) は、アプリケーションがそれぞれのサービス品質 (QoS) 要件を送信するのに使用する IP シグナル・プロトコルです。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よう設計されています。RSVP がトリガー・トラフィック管理を送信すると、結果として、パケットの送達に必要な QoS を達成するネットワーク資源 (たとえば、帯域幅やバッファー) が動的に予約されます。RSVP は受信側指向です。つまり、QoS の流れ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 送信を開始する役割を担っています。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設定することによって達成されます。予約は、トラフィック・フローの QoS を決定するパラメーター値のセットで構成されます。RSVP に使用可能なホスト・アプリケーションである送信側と受信側は、RSVP メッセージを互いに送信することによって予約を作成します。IBM の拡張機能により、一部の RSVP 使用可能でないアプリケーションでも、代理で最初のホップ・ルーターに RSVP 送信を実行させられるものがあります。RSVP は、IBM ルーターの IPv4 で実行し、ユニキャストとマルチキャスト両方の IP トラフィックをサポートします。RSVP の完全な説明は、RFC 2205 に記載してあります。

予約が設定されている IP トラフィック・フローごとに、RSVP は、2212 上にインプリメントされているとおり、サービス品質の制御付きロードを可能にします。QoS の制御付きロードは、インターネット技術特別調査委員会 (IETF) の統合サービス・モデルに定義されています (RFC 2211)。ネットワークが輻輳 (ふくそう) したときでも、QoS の制御付きロードは、ネットワークが輻輳していないときにトラフィック・フローが受け取るレベルのサービスを提供し続けます。

本章には、以下の節が含まれています。

- 『RSVP の機能』
- 437ページの『RSVP によってサポートされるリンク・タイプ』
- 438ページの『構成のサンプル』

RSVP の機能

図36 に、RSVP が特定のトラフィック・フローに QoS を提供する予約を設定するのに使用するメッセージのシーケンスを示します。この例では、最善的 IP トラフィック・フローがルーター間ですでに確立されているものと想定しています。

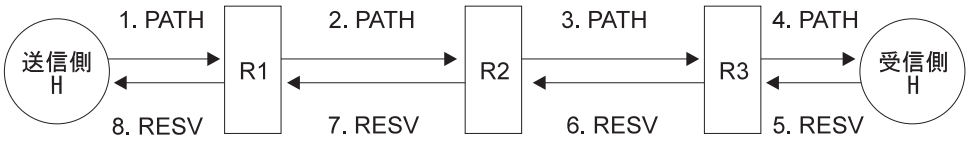


図 36. RSVP 予約 - すべてのルーターが RSVP をサポートする場合

RSVP 予約の設定は、RSVP を使用できる送信側がデータ・トラフィック・フローへ *PATH* メッセージを送信した時点で開始されます。PATH メッセージには、その流れ

を記述するトラフィック情報が含まれています。ルーターは PATH メッセージを受け取る (IP ヘッダーの ALERT オプション・フィールドを見る) と、その PATH メッセージのソフト状態を確立して保持します。RSVP ルーターは、あて先に送信する PATH メッセージに自身の IP アドレスでマークも付けます。これは、直前ホップ、すなわち p ホップと呼ばれます。 RSVP を使用できる受信側は、*RESV* メッセージを送り返すことによって、PATH メッセージの 1 つに応答することができます。RESV メッセージは、ネットワーク資源 (たとえば、帯域幅) をパス内の各リンクで予約するよう要求します。RESV メッセージは、PATH メッセージが通り抜けた逆方向パスで送信されます。RESV メッセージは、逆方向パス上の最初のルーター (ルーター R3) が受信します。このルーターは、アウトバウンド・インターフェース上、つまり、R3 と受信側ホストとの間のリンク上で資源を予約しようとします。要求された資源が使用可能であれば、この流れについて予約され、使用可能な資源の量は、予約された量に相当する分だけ減ります。要求された資源が使用可能でない場合は、そのノードでの予約は異常終了し、RESVERR メッセージが受信側ホストに送り返されます。ここでは、予約は正常に行われるものと想定しています。

ルーター R3 は、送信側の方へ戻るパス上にある次のルーター (R2) に RESV メッセージを送信します。R2 は、自分と R3 との間のリンク上で予約を設定し、R1 に RESV メッセージを送信します。R1 は、自分と R2 との間のリンク上で予約を設定し、送信側ホストに RESV メッセージを送信します。この例では、送信側ホストは RSVP をサポートします。送信側ホストは、自分と R1 との間のリンク上で予約を設定します。ここで、予約されたリンクのパスが、送信側から受信側までに設定された予約を作成します。

今度は、図37 に示されているように、一部のノードしか RSVP をサポートしていないネットワークを考えてみます。

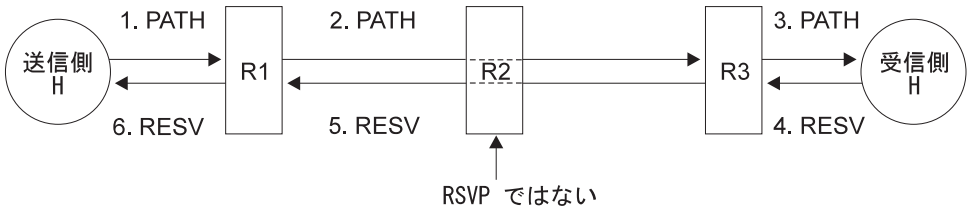


図 37. RSVP 予約 - 一部のルーターだけが RSVP をサポートする場合

詳しくいうと、R2 が RSVP をサポートしていないとします。R2 は PATH メッセージを受信すると、それを通常のパケットとして扱い、それを R3 へ転送します。R2 は、PATH メッセージに含まれている p ホップを変更しません。

以前のように、PATH メッセージは受信側ホストに到着すると、RESV メッセージを R3 へ送信することにより予約プロセスを開始します。R3 が RESV メッセージで認知する直前ホップは R1 のアドレスです。R2 は PATH メッセージにはその直前ホップを与えなかったからです。R3 は、RESV メッセージを R1 に送信し、自分と受信側ホストとの間のリンク上で予約を行います。R1 は R3 から RESV メッセージを受信すると、自身から R3 までに予約を行います。これで、(送信側の方向での) 予約は、送信側、R1、および R3 に存在します。パケットは、通常のベストエフォート・パケットとして R2 を通り抜けます。このようにすると、一部のルーターしか RSVP をサポートしていないネットワークで RSVP が使 用できます。

バーチャル・サーキット資源管理プログラム

バーチャル・サーキット資源管理プログラム (VCRM) は、RSVP が使用可能であれば、いつでも使用できるフィーチャーです。 RSVP からの予約要求に基づいて、VCRM は、物理インターフェースを通るデータ・フローの接続を作成します。これを行うためには、VCRM は、まず最初に、予約に対応できるだけの十分な帯域幅が存在するかどうかを判別する必要があります。

注: WAN インターフェース (たとえば、フレーム・リレーまたは X.25) を使用する場合は、VCRM が使用可能な帯域幅の量を認識できる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手順については、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*のフレーム・リレーおよび X.25 インターフェースの構成の章で説明しています。

VCRM の詳細については、*AIS 機構の使用と構成*の 『VCRM の構成および監視』 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

ルーターのパスおよび予約ソフト状態により、RSVP 予約の存在と、トラフィック・フローがその予約に応じて送信されることが定義されます。RSVP セッションは、予約されたパスを通って同じ IP セッション・アドレス (固有の IP アドレスまたはマルチキャスト IP アドレスのどちらでもよい) までルーティングされている 1 つまたは複数の送信側からのすべてのトラフィック・フローで構成されます。たとえば、436ページの図39 で、セッションには、送信側 S1 から受信側 Rec 1 までのトラフィック・フローと、送信側 S2 から受信側 Rec 1 までのトラフィック・フローの両方が含まれます。このセッションは、受信側 Rec 1 の IP アドレスで識別されます。

送信側と受信側は、予約されたトラフィック・フローの存在を再確認する refresh メッセージを送信することにより、セッション内の各パスと予約の存在を保持します。これらの refresh メッセージは、PATH メッセージと RESV メッセージのコピーにすぎません。構成可能タイマーがタイムアウトになり、ソフト状態を保持しているノードは、一定の時間内に refresh メッセージを受信しないと予約を破壊します。

破壊メッセージには、RSVTEAR と PATHTEAR の 2 種類があります。RSVTEAR メッセージは、受信側が送信するもので、予約を破壊しますが、トラフィック・フローは破壊しないため、ベストエフォート・サービスで継続します。PATHTEAR メッセージは、送信側からセッション・アドレスまでのパスを破壊します。PATHTEAR は、予約とパス・ソフト状態の両方を破壊します。ベストエフォート・トラフィックは、まだ流れています。

予約スタイル

433ページの図36 は、ある特定の送信側から特定の受信側までのトラフィックのストリームのリンクを予約する RSVP 予約の設定を示しています。複数の送信側が同じ受信側に送信すると、複数の IP トラフィック・フロー (つまり、各送信側から受信側まで 1 つずつ) 存在することになります。このような状態では、各種の送信側が受信側 (選択した*予約スタイル* によって異なります) までのリンクのいくつかを介して予約を共用することができます。

図38 は、受信側から固定フィルター (FF) 予約スタイルが要求されている 2 つの送信側 S1 と S2 を示しています。この予約スタイルでは、各送信側に、それぞれの個別予約が与えられます。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。

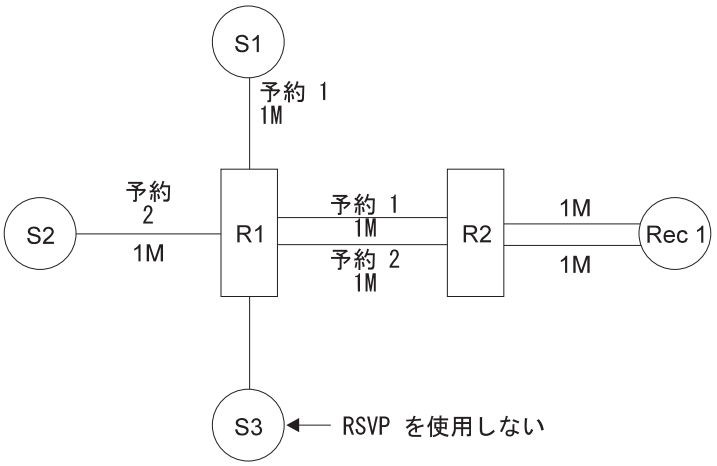


図 38. 固定フィルター予約スタイル

共用明示的 (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た送信側は、予約済みのリンクのいくつかを共用することができます。1 つのグループ内の送信側は、送信側が PATH メッセージで送信する情報 (たとえば、送信側の IP アドレス) に従って、受信側が定義します。図39 で、送信側 S1 および送信側 S2 は、受信側 Rec 1 のあて先アドレスによって識別された RSVP セッションに含まれています。そのグループ内の送信側は、受信側までの送信側のパスが組み合わされるとすぐに予約を共用できます。この場合、共通予約は、ルーター R1 から受信側まで拡張されます。

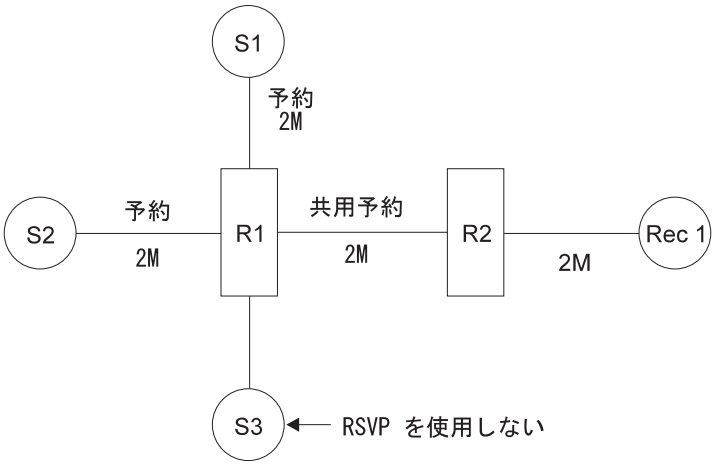


図 39. 共用明示的予約スタイル

3 つ目の予約スタイル、ワイルドカード・フィルター (WF) では、437ページの図40に示されているとおり、*PATH* メッセージをセッション・アドレスに送信するすべての送信側が同じ予約を共用します。

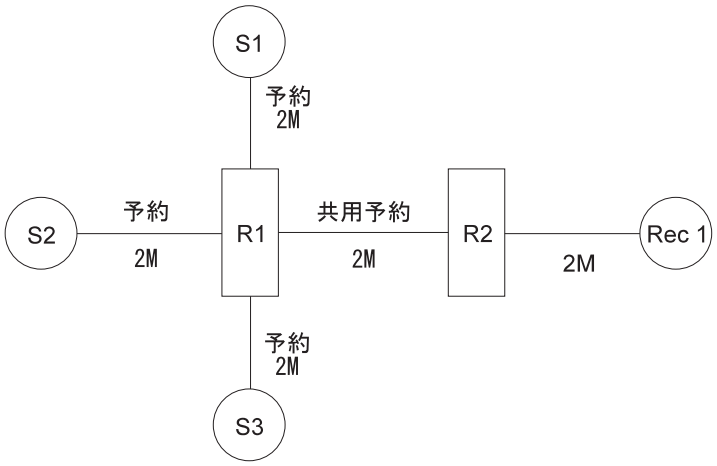


図 40. ワイルドカード・フィルター予約スタイル

OPWA

公示付き 1 パス (OPWA) は、RSVP のオプションの 1 つで、指定は任意です。このフィーチャーは、予約パスで各リンクから使用可能な QoS 値 (たとえば、帯域幅) の記録を受信側が取得できるようにします。たとえば、433ページの図36 に示されているルーター R1 および R3 が OPWA に合うように構成されていると、各リンクの特性に関して情報が与えられます。この情報を使用すると、それらのルーターは、リンクの能力に応じて、最小の資源で PATH メッセージの情報を調整することができます。

たとえば、433ページの図36 のコンテキストで、送信側が、平均速度 1 Mbps、ピーク速度 10 Mbps で PATH メッセージを受信側に送信し始めるとします。また、R2 と R3 との間のリンクが、回線速度 2 Mbps の PPP リンクであるとします。R2 の OPWA は、PATH メッセージ内のピーク速度を変更して 2 Mbps に減速します。いずれのノード・ダウンストリームも 2 Mbps を超えるピーク速度に合わせて予約する理由はないからです。

RSVP によってサポートされるリンク・タイプ

RSVP がサポートするリンク・タイプには、次のものがあります。

- PPP リンク。RSVP は、永続接続を基盤とする、V.35、T1/E1、ISDN といったサポートされているすべてのリンク・タイプについて PPP をサポートします。ダイヤル・オンデマンド、WAN 回復、短時間保留モード、またはロード・バランシング構成で使用されるリンクを、RSVP に使用しないでください。
- フレーム・リレー PVC。PPP の場合と同様、サポートされるすべてのリンク・タイプは RSVP をサポートしていますが、RSVP には、永続接続を基盤とするリンクだけを使用してください。ダイヤル・オンデマンド、WAN 回復、短時間保留モード、またはロード・バランシング構成で使用されるリンクは、RSVP で使用しないでください。

- フレーム・リレー SVC。これは、フレーム・リレー PVC と同様にサポートされます。すなわち、RSVP は QoS トラフィック用に別個の DLCI をセットアップすることはできませんが、デフォルトの DLCI の一部を QoS 帯域幅の割り当てに使用します。
- すべての LAN リンク
  - イーサネット
  - トークンリング
  - 高速イーサネット

  注: LAN などの共用媒体ネットワークの場合、LAN 帯域幅の共用を調整するには、トラフィック・エンジニアリングなど他の手段が必要です。RSVP は、ある特定のルーターの帯域幅を制御しますが、複数のルーターおよびホストによる LAN 帯域幅の使用を調整することはありません。
- X.25。PPP またはフレーム・リレー PVC と同様にサポートされます。RSVP は、QoS トラフィック用に別個の VC をセットアップすることはできません。デフォルトの VC の一部を QoS 帯域幅の割り当てに使用します。

注:

1. 競合を避けるために、RSVP は、帯域幅予約システム (BRS) 用に構成されている PPP や FR リンク上では使用できません。

構成のサンプル

RSVP の構成の手本として、Talk 6 コマンド回線インターフェース構成のサンプルが組み込まれています。RSVP コマンドおよびパラメーターの説明については、443ページの『第21章 RSVP の構成および監視』 を参照してください。以下のステップで、RSVP の構成サンプルについて説明します。

1. `RSVP config>` プロンプトから Talk 6 **enable rsvp** コマンドを使用して、ルーターの RSVP を使用可能にします。RSVP は、IP 用に構成されているインターフェース上でのみ使用可能にすることができます。このコマンドは、インターフェース上のデフォルトの帯域幅としての 0 を含め、RSVP ルーター・パラメーターをデフォルト値に設定します。RSVP が特定のインターフェースで実行できるようにするには、それらのインターフェースを使用可能にし、そこに帯域幅を設定する必要があります。
2. **enable interface** コマンドを使用して、特定のインターフェースごとに RSVP に使用できるようにします。
3. RSVP をこのインターフェース上で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帯域幅を設定するようプロンプトが出されます。特定のインターフェースの帯域幅が 0 (デフォルト値) のままになっていると、そのインターフェースを介して RSVP 予約は行えません。
5. RSVP を使用できるすべてのインターフェース上で OPWA を使用可能にしたい場合は、コマンド **enable opwa-all** 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、コマンド **enable opwa** とインターフェース番号を使用します。OPWA を使用可能にする前に、必ず、インターフェースを介して RSVP を使用可能にしてください。RSVP について使用可能にされていない

インターフェースで OPWA を使用可能にしようとすると、メッセージ Cannot find RSVP i/f rec (RSVP i/f rec が見つからない) が表示されます。

6. その他のパラメーターの指定は任意であるため、RSVP はデフォルト値で実行できます。
7. 必要なら、**add sender** コマンドと **add receiver** コマンドを使用して、ルーターのために静的送信側または受信側を作成することができます。静的送信側および受信側は、RSVP を使用しないホスト・アプリケーション用に RSVP シグナルを生成します。静的送信側および受信側用に構成された IP アドレスおよびポートは、ルーターが RSVP メッセージを送信する IP トラフィック・フローの発信元とあて先を識別します。静的送信側も受信側も構成されない場合、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 メッセージは発信しません。詳細については、440ページの『静的送信側および受信側の構成サンプル』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
```

構成を完了すると、Talk 5 **reset rsvp** コマンドまたは **reset interface** コマンドを使用するか、あるいはルーターを再始動することにより、RSVP を起動することができます。

静的送信側および受信側の構成サンプル

438ページの『構成のサンプル』 に示されているとおりに RSVP を構成すると、そのルーターに接続されているホスト内の RSVP を使用できるアプリケーションによって、RSVP トラフィック・フローとセッションが動的に確立されます。 RSVP に使用できないホスト・アプリケーションで、既知の IP アドレスおよびポートにパケットを送信するものがある場合には、ルーターがその流れのために RSVP シグナルを生成するように静的送信側および受信側を構成することができます。

最初に、RSVP config> プロンプトから **add sender** コマンドを使用して、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る場合、セッション 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の場合は、セッション 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 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。送信側および受信側は、ルーターでない場合は、ルーターに接続されているホストです。ルーターは、この場合、ホストのプロキシーとして行動します。

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後で、受信側として行動する 2 番目のリモート・ルーター内に静的受信側を構成することができます。例では、送信側ルーターは、IP アドレス 5.0.27.27 をもち、受信側ルーターは IP アドレス 5.0.31.1 をもちます。静的受信側を構成するには、**add receiver** コマンドを使用してください。

```
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、およびプロトコルは、送信側の IP セッション・アドレス、ポート、およびプロトコルと一致していることに注意してください。送信側と受信側が、同じトラフィック・フローを識別する必要があります。受信側 (送信側ではない) は、そのパスのルーターが各リンク上にどのような帯域幅を確立しようとするのかを判別します。

2 文字 *wf* は wildcard-filter (ワイルドカード・フィルター) の略語です。これは、RSVP の 3 つの予約スタイルの 1 つです。詳細については、435ページの『予約スタイル』を参照してください。

第21章 RSVP の構成および監視

この章では、資源予約プロトコル (RSVP) の構成および監視方法と、RSVP 監視コマンドの使用法について説明します。本章には、以下の節が含まれています。

- 『RSVP 構成環境へのアクセス』
- 『RSVP 構成コマンド』
- 453ページの『RSVP 監視環境へのアクセス』
- 454ページの『RSVP 監視コマンド』

RSVP 構成環境へのアクセス

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

```
Config> 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。これらのコマンドは 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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	送信側および受信側を追加します。
Delete	送信側および受信側を削除します。
Disable	RSVP または公示付き 1 パス (OPWA) を使用不可にします。
Enable	RSVP または公示付き 1 パス (OPWA) を使用可能にします。
List	RSVP 構成に関する情報をリストします。
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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、静的 RSVP 送信側および受信側をルーターに追加するのに使用します。静的送信側または受信側は、ルーターが RSVP メッセージを送信または受信できるようにします。ほとんどの場合、ルーターが RSVP メッセージの送信および受信するなら、RSVP 用に構成されていないホスト・アプリケーションの代わりにプロキシーとして行動します。そのような場合、送信側 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 IP アドレスは、データ・フローのあて先アドレスです。静的送信側も受信側もルーター用に構成されていない場合には、RSVP メッセージを動的に転送し、予約を確立し、QoS を提供しますが、RSVP メッセージは発信しません。

送信側および受信側の定義は、番号制の SRAM レコードとして構成内に保管されます。Talk 5 **activate** コマンドを使用すると、各レコードを活動化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が RSVP *path* メッセージの送信側に適用されるよう指示するキーワード。

receiver この用語の後に続くパラメーターが受信側に適用され、その結果、RSVP *resv* メッセージが送信側に返されるよう指示するキーワード。

以下のパラメーターのほとんどは、送信側と受信側の両方に対して指定します。送信側または受信側に固有なパラメーターは、その説明で識別してあります。

session-ip-address

これは、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であれば、このアドレスは受信側のアドレスです。トラフィック・フローがマルチキャストであれば、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・アドレスによって識別されるグループのメンバーでなければなりません。送信側および受信側は、セッション・ポート番号とプロトコルをもつセッション IP アドレスを使用して、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 であってはなりません。RSVP を起動するときには、このアドレスが、送信側および受信側でアクセスできるものでなければなりません。

デフォルト値: なし

session-port

RSVP で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 ポート番号または TCP ソケット番号です。

有効値: 0 ～ 65535

デフォルト値: 1

session-protocol

UDP または TCP のいずれか。

有効値: UDP または TCP

デフォルト値: UDP

sender-ip-address

予約されるデータ・フローを発信する送信側アプリケーションである、送信側のアドレス。このパラメーターは、ユニキャスト・アドレスでなければなりません。

有効値: 有効な IPv4 アドレス

デフォルト値: なし

sender-port

QoS 用に予約される IP フローの送信側の IP ポート番号。これは、送信側アプリケーションの UDP ポート番号または TCP ソケット番号です。

有効値: 0 〜 65535

デフォルト値: 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、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・セッションの場合には、このアドレスは、マルチキャスト・セッション・アドレス用に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。これがマルチキャスト・セッションの場合、受信側は、このマルチキャスト・アドレスによって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

デフォルト値: なし

peak-rate

IP セッション上のピーク・データ転送速度を指定します。この速度は、送信側のピーク・トラフィック生成速度 (既知のもので、制御されている場合)、物理インターフェース回線速度 (既知のものである場合)、または無限大 (X'FFFFFFFF'、10 進数 4 294 967 295) (これより良い値が使用できない場合) に設定されます。ピーク・トラフィック速度は、平均トラフィック速度以上の値に設定してください。

受信側が、送信側が提示した速度とは別のピーク・データ転送速度を要求すると、ルーターは、受信側の要求を最優先しようとします。

有効値: 1 〜 4 294 967 295 バイト/秒

デフォルト値: 250 000

average-rate

IP セッション上で送信側が送信したり、受信側が受信する平均データ転送速度を指定します。この速度は、送信側の平均トラフィック生成速度 (既知のもので、制御されている場合)、物理インターフェース回線速度 (既知の場合)、または 200 000 バイト/秒 (デフォルト) に設定されます。

受信側が、送信側が提示したものとは別の平均速度を要求すると、ルーターは、受信側の要求を最優先しようとします。

有効値: 1 〜 4 294 967 295 バイト/秒

デフォルト値: 200 000

data-burst-size

ピーク速度または平均速度に関係なく送信できるバイト数を指定します。たとえば、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、バーストにより、ある特定のインスタンスでピーク速度が 50 000 を超えた場合でもそのインスタンスで 2000 バイトを送信できます。

受信側が、送信側とは別の速度を要求すると、ルーターは、受信側の要求を最優先しようとします。

有効値: 1 ～ 4 294 967 295 bytes

デフォルト値: 2000

max-packet-size

送信側が IP フローで送信する、または受信側が 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。送信側の場合、この値は、送信側アプリケーションが生成する最大パケットのサイズに設定してください。受信側の場合は、最小の パス MTU に設定してください。受信側は、これを、RSVP 公示付き 1 パス (OPWA) パケットに着信する情報から、あるいは他の方法で確認します。

最大パケット・サイズがパス上のリンクの MTU より大きい場合、予約要求はその地点でリジェクトされます。たとえば、予約のパスに沿う 1 つのリンクが 1500 という MTU をもっており、最大パケット・サイズが 2000 であると、予約要求はリジェクトされます。

受信側が、送信側とは別の最大パケット・サイズを要求すると、ルーターは、受信側の要求を最優先しようとします。

最大パケット・サイズは、最小パケット・サイズ以上の値で構成する必要があります。たとえば、最小パケット・サイズが 64 バイトの場合、最大パケット・サイズは 64 バイト以上でなければなりません。

有効値: 1 ～ 4 294 967 295 bytes

デフォルト値: 1500

min-packet-size

送信側が IP フローで送信する、または受信側が 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。送信側の場合、この値は、送信側アプリケーションが生成する最小パケットのサイズに設定してください。

このパケット・サイズは、最大パケット・サイズ以下でなければなりません。たとえば、最大パケット・サイズが 1500 バイトの場合、最小パケット・サイズは 1500 バイト以下でなければなりません。このパケット・サイズには、アプリケーション・データと、IP レベル以上のすべてのプロトコル・ヘッダー (たとえば、IP、TCP、または UDP) が含まれていますが、リンク・レベルのヘッダーは含まれていません。

注: この値は、資源予約のオーバーヘッドを見積もるのに使用されます。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 bytes

デフォルト値: 48

reservation-style

このパラメーターは、受信側用にのみ構成されます。これは、受信側が IP フロー上で受信する予約スタイルを指定します。RSVP 予約があると、IP トラフィック・フロー内でのパケットの特別な処理が保証され、各リンクまたは送信側から受信側へのパスを構築する一連のリンクを介して特定の QoS が提供されます。用意されている 3 つの予約スタイルは、次のものです。

固定フィルター (FF)
受信側が IP フロー上で特定の送信側のデータ・トラフィックを受信するよう指定します。1 つの送信側につき、1 つの予約が設定されます。

共用明示的 (SE)
受信側が、受信側が定義した同じグループ内の送信側のグループからデータ・トラフィックを受信す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は、そのリンクが受信側への共通パスに組み合わされるとすぐに、予約を共用できます。

ワイルドカード・フィルター (WF)
受信側がすべての送信側からデータ・トラフィックを受信するよう指定します。各送信側は、そのリンクが受信側への共通パスに組み合わされるとすぐに、予約を共用できます。

詳細については、435ページの『予約スタイル』を参照してください。

有効値: FF、SE、および WF

デフォルト値: FF

confirm-reservation
受信側が *reservation confirm* メッセージの受信を要求するかどうかを指定します。このメッセージは、要求が既存の大きい方の予約に組み込まれるか、または送信側アプリケーションに送達されると、resv メッセージを送信した受信側に送り返されます。

有効値: Yes または No

デフォルト値: No

Delete

delete コマンドは、送信側または受信側を削除するのに使用します。

構文:

delete sender *sram-record*

receiver *sram-record*

sender or receiver *sram-record*
各送信側または受信側は、**delete** コマンドを使用したときに表示される SRAM レコードによって識別されます。削除される送信側または受信側の SRAM レコード番号を入力すると、その送信側または受信側が構成から削除されます。

Disable

disable コマンドは、RSVP または OPWA を 1 つのインターフェース上またはすべてのインターフェース上で使用不可にするのに使用します。

構文:

disable interface

opwa

opwa-all

rsvp

interface *interface-number*
特定のインターフェース上で RSVP 機能を使用不可にします。RSVP control メッセージは、このインターフェースを流れることができますが、このインターフェース上では RSVP 予約は設定されません。このコマンドは、QoS の設定という、このインターフェースの能力も使用不可にします。

有効値: 任意の有効なインターフェース番号

デフォルト値: 0

OPWA *interface-number*
特定のインターフェース上で OPWA を使用不可にします。

有効値: 任意の有効なインターフェース番号

デフォルト値: 0

OPWA-all
すべてのインターフェース上で 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。デフォルトでは、RSVP は使用不可です。

Enable

enable コマンドは、RSVP または OPWA を 1 つのインターフェース上またはすべてのインターフェース上で使用可能にするのに使用します。

構文:

enable interface

opwa

opwa-all

rsvp

interface *interface-number*
特定のインターフェース上で RSVP 機能を使用可能にします。このコマンドにより、このインターフェースは、RSVP メッセージに応答したり、それらを転送することができますが、メッセージを発信することはできません。静的送信側および受信側を、RSVP メッセージを発信するよう構成する必要があります。

使用可能になったインターフェース上で帯域幅を設定するようプロンプトが出されます。後で **set bandwidth** コマンドを使用して、帯域幅設定値を変更することもできます。このコマンドは、ルーターが RSVP 用に使用可能になっており、しかも、指定されたインターフェースが使用可能で IP 用に構成されている場合に限り機能します。

RSVP をサポートするリンクのリストについては、437ページの『RSVP によってサポートされるリンク・タイプ』 を参照してください。

有効値: 任意の有効なインターフェース番号

デフォルト値: 0

OPWA *interface-number*
特定のインターフェース上で OPWA を使用可能にします。OPWA は、送信側と受信側との間のパスがすべてのホップで予約できるかどうかや、そのパスの各ホップで使用可能な帯域幅の量を受信側に伝えます。この動作は、インターフェースが RSVP 用に使用可能になっている場合に限り許されます。

有効値: 任意の有効なインターフェース番号

デフォルト値: 0

OPWA-all
すべてのインターフェース上で 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 がルーターで使用可能になっている必要があります。

RSVP ルーター内の RSVP 機能を使用可能にします。RSVP が今回初めて使用可能にされた場合には、RSVP のデフォルト・パラメーターのセットも初期化されます。

RSVP を使用可能にしても、RSVP を起動することはできません。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、少なくとも 1 つのインターフェース上で帯域幅を設定する必要があります。その場合、ルーターを RSVP 用に再始動する必要があります。これを行うには、Talk 5 コマンド **reset rsvp** を使用するか、またはルーターをリブートします。詳細については、Talk 5 **reset rsvp** コマンドを参照してください。

List

list コマンドは、RSVP パラメーターをリストするのに使用します。これらのパラメーターのグループは、次のように、別個にリストすることができます。

- 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ついての 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** コマンドは、構成済みの送信側および受信側レコードをリストします。これらのレコードは、アクティブな RSVP トラフィック・フローは識別しません。それらは、送信側のアドレスと受信側のアドレスで定義されます。Talk 5 **show rsvp flows** コマンドを使用して、現在アクティブな RSVP フローを表示してください。

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いくつかの一般値の表示については、Talk 6 **list all** コマンド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*

このパラメーターは、RSVP が RSVP トラフィック・フローについて定義されたパスおよび予約の状態をタイムアウトになる前に失われる可能性のある連続する path and matching resv refresh メッセージの数を定義します。RSVP が特定のトラフィック・フローのパスおよび予約の状態をタイムアウトになると、そのフローは QoS を提供しなくなります。送信側および受信側は、予約を再設定する必要があります。

有効値: 1 ～ 9999

デフォルト値: 3

bandwidth *interface bps*

このパラメーターは、インターフェースの予約可能な帯域幅を定義します。通常、予約可能な帯域幅は、合計リンク帯域幅の小さな部分でなければなりません。目標としては、30% 未満です。予約可能な帯域幅は、RSVP 用に使用可能になっているインターフェース上でのみ設定できます。

この Talk 6 コマンドは、任意により、他のパラメーターの値に影響を与えずに、即時に、しかも動的に有効にすることができます。

interface ネットワーク・インターフェース番号

有効値: 任意の有効なネットワーク・インターフェース番号

デフォルト値: 0

bps このインターフェース上で予約できる帯域幅の 1 秒あたりのビット数 (bps)

有効値: 1 ～ 4 294 967 295 bps (無限大を表します)

デフォルト値: 0

default

このパラメーターは、すべての RSVP パラメーターを、コマンド **enable rsvp** を使用した場合に存在する始めのデフォルトに設定します。**set default** コマンドは、個々のインターフェース上に以前に構成したパラメーター値をすべて上書きします。各インターフェースの帯域幅のデフォルト値は 0 (そのインターフェース上で RSVP 予約が設定されないことを意味します) であるため、RSVP を使用する各インターフェースについて **set bandwidth** コマンドを使用して、RSVP が再実行するよう準備する必要があります。

encapsulation *interface style*

このパラメーターは、インターフェース上で RSVP メッセージのカプセル化スタイルを IP、UDP、または Both (両方) に設定します。通常、RSVP control メッセージ (たとえば、resv メッセージ) は、プロトコル・タイプ 46 の固有の IP フレームで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には、そのホストに接続するインターフェースに対するカプセル化スタイルを

UDP に設定してください。IP を使用するいくつかのホストおよび UDP を使用するいくつかのホストが、同じリンクを介して RSVP メッセージを送信している場合には、カプセル化を Both に設定する必要があります。この動作は、RSVP が指定のインターフェース上で使用可能になっている場合に限り許されます。

この Talk 6 コマンドは、任意により、他のパラメーターの値に影響を与えずに、即時に、しかも動的に有効にすることができます。

interface ネットワーク・インターフェース番号

有効値: 任意の有効なネットワーク・インターフェース番号

デフォルト値: 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

デフォルト値: IP

lifetime

このパラメーターは、存続時間をパスおよび予約状態の秒数で指定します。この状態では、確立された RSVP トラフィック・フローが保持されます。この時間は、allowed-successive-msg-loss パラメーターの値で指定された refresh メッセージ喪失数を RSVP が監視できるだけの長さでなければなりません。この時間を概算するためには、1.5 x refresh-interval x (allowed-successive-msg-loss + 0.5) という公式を使用してください。

予約状態がタイムアウトになったが、パス状態ではない場合、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・サービスで継続します。パス状態がタイムアウトになると、予約と IP トラフィック・フローは両方とも終了します。

この Talk 6 コマンドは、任意により、他のパラメーターの値に影響を与えずに、即時に、しかも動的に有効にすることができます。このパラメーターのデフォルト値は、変更なしで機能するものであると予想されています。

有効値: 1 〜 2 147 483 647 秒

デフォルト値: 158 秒

max-msg-size

このパラメーターは、ルーター内の全体的な最大 RSVP control メッセージ・サイズを定義します。この値は、パスに沿う、RSVP の使用可能なインターフェースによってサポートされる MTU サイズの最小値以下でなければなりません。このパラメーターのデフォルト値は、変更なしで機能するものであると予想されています。

有効値: 64 〜 2 147 483 647 バイト (無限大を表します)

デフォルト値: 1500 バイト

refresh-interval

このパラメーターは、パスおよび予約状態 (RSVP トラフィック・フロー) を受信側と送信側との間で保持する refresh メッセージ間の経過時間間隔を秒数で定義します。

有効値: 10 〜 600 秒

デフォルト値: 30 秒

slew-max

このパラメーターは、リフレッシュ間隔が 1 回のリフレッシュ・サイクル内に変更できる量を制限します。このパラメーターのデフォルト値は、変更なしで機能するものであると予想されています。ただし、このパラメーターの値は、タイミング・エラーを避けるように変更しなければならないことがあります。

たとえば、slew-max が 30% で、リフレッシュ間隔が 30 秒であれば、1 回のリフレッシュ間隔内に最大 9 秒 (30 の 30%) リフレッシュ間隔を変更できます。もっと大きな変更を行うには、リフレッシュ間隔を 2 度変更する必要があります。たとえば、リフレッシュ間隔が 39 であったら、1 回のリフレッシュ間隔内にプラス 11 またはマイナス 11 変更することができます。あるいは、slew-max を増やしてから、変更を行うこともできます。たとえば、リフレッシュ間隔が 30 で、それを 50 に変更したい場合は、最初に slew-max を 70% に増やし (30 をプラス 21 またはマイナス 21 だけ変更することができるようになります)、次いで、リフレッシュ間隔を 50 に増やすことができます。

この Talk 6 コマンドは、任意により、他のパラメーターの値に影響を与えずに、即時に、しかも動的に有効にすることができます。

有効値: 0 ～ 100%

デフォルト値: 30%

total すべてのインターフェースのリンク帯域幅の集合は合計ルーター・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の合計に制限を設定しなければならないことがあります。たとえば、集合リンクの帯域幅の合計が 250 000 000 bps で、ルーター・スループットの合計が 200 000 000 bps になる場合があります。予約可能な帯域幅の合計が 200 000 000 bps に設定されており、200 000 000 bps が現在すべてのインターフェースにわたって予約されている場合、RSVP IP 予約のいくつかが廃棄されるまで、それ以上予約は設定できません。

この Talk 6 コマンドは、任意により、他のパラメーターの値に影響を与えずに、即時に、しかも動的に有効にすることができます。

有効値: 1 ～ 4 294 967 295 bps

デフォルト値: 4 294 967 295 bps (無限大を表します)

RSVP 監視環境へのアクセス

RSVP 監視環境にアクセスするには、OPCON プロンプト (*) で **t 5** と入力します。

```
* t 5
```

次に、以下のコマンドを **+** プロンプトで入力します。

```
+ 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。これらのコマンドは 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
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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または受信側を起動します。
List	RSVP 情報を出力します。
Reset	RSVP および RSVP の特性をリセットします。
Send	各種の RSVP メッセージ (*data-packet*、*ip ping*、*path*、*ptear*、*resv*、および *rtear* を含む) を送信します。
Show	アクティブ RSVP フローに関する情報を表示します。
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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Activate

activate コマンドは、構成済み送信側または受信側を動的にcommand 起動するのに使用します。

構文:

activate *record-number*

このコマンドを使用すると、該当する Talk 6 **enable** コマンドですでに使用可能にされている Talk 6 **add sender** および **add receiver** コマンドを使用して定義した送信側または受信側を動的に起動することができます。

record-number

activate コマンドを使用すると、現在使用可能で構成済みの送信側および受信側が表示され、それぞれがレコード番号で識別されます。レコード番号を指定すると、その受信側または送信側が動的に起動されます。**send ptear**、**send rtear**、または **reset rsvp** コマンドを出すか、ルーターを再始動すると、起動されている送信側または受信側を、Talk 5 で停止することができます。

静的送信側および受信側の構成方法を確認するには、Talk 6 **add sender**、**add receiver**、および **enable** コマンドの説明について 443ページの『RSVP 構成コマンド』 を参照してください。

List

list コマンドは、実行中の RSVP 構成に関する情報を表示するのに使用します。

注: Talk 5 **show rsvp flow** コマンドを使用して、既存の RSVP トラフィック・フローを表示してください。

構文:

list interface

opwa

sender/receiver-records-in-sram

system

interface

このコマンドを使用すると、RSVP インターフェースとそれぞれの現在の状況が表示されます。状態 *bwCtrl* は、RSVP 帯域幅制御を受けているリンクを示します。このインターフェース上で、帯域幅を RSVP QoS に合わせて予約することができます。状態 *notCnf* は、RSVP 用に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 このコマンドを使用すると、RSVP インターフェースとそれぞれの現在の 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

このコマンドを使用すると、静的に構成されている送信側および受信側のリストが表示されます。

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

このコマンドを使用すると、現在実行中の RSVP システム・パラメーターの値が表示されます。このシステム・パラメーター値は、いくつかが Talk 5 コマンドを使用して動的に変更されている場合には、SRAM のそれとは違うものになります。

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

reset コマンドは、RSVP 構成の各種局面をリセットするのに使用します。**reset** コマンドは、Talk 5 を使用して動的に構成されたパラメーターを上書きし、Talk 6 で最後に構成された値を置換します。

構文:

reset interface

queue-stat

rsvp

system-parameters

interface
RSVP インターフェース・パラメーターを、SRAM に保管されている構成データで更新します。このコマンドは、インターフェース番号の入力を求めてきます。

このインターフェースについての予約は消えてしまい、次に path and resv refresh が発生したときに再設定されます。ただし、資源が使用可能であることが必要です。予約を更新する資源 (たとえば、帯域幅) が使用できなくなっている場合には、いくつかの予約が消えてしまって戻らない恐れがあります。

queue-stat
RSVP 用に構成されたすべてのインターフェースにあるフロー制御待ち行列をクリアします。

rsvp ルーター上の RSVP を停止し、それが SRAM で使用可能になっている場合は再始動します。

RSVP が停止された時点で、ルーター上のすべての path and resv メッセージが終結処理されます。RSVP が再始動されると、予約は、資源が使用可能であれば、次に path and rsev refresh が発生した時点で再始動されます。予約を更新する資源 (たとえば、帯域幅) が使用できなくなっている場合には、いくつかの予約が消えてしまって戻らない恐れがあります。

system-parameters
RSVP システム・パラメーターを、Talk 6 で作成され、SRAM に保管されている構成データで更新します。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たものです。

Send

send コマンドは、IP ping および RSVP メッセージを動的に送信するのに使用します。

構文:

send data-packet

ip-ping

path

ptear

resv

rtear

data-packet

これは、定義済みの 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。このコマンドは、ルーターの速度と資源の制限を条件として、1 秒あたり複数のパケットを送信することができます。10 個目のパケットが送信されるたび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 これは、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* の章 『IP の構成および監視』 に記載されている **ping** コマンドを参照してください。

path 自分自身のため、または別のホストのプロキシーとして、RSVP *path* メッセージを送信します。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。必須指定の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。

デフォルトでは、これらのメッセージは、30 秒おきに送信されます。パスは、**send ptear** コマンドを使って削除されるか、あるいは RSVP がリセットされるまで存在します。

このコマンドは、送信側を構成に動的に追加することができます。Talk 2 を使用すると、パスの最新表示の ELS トレースを表示することができます。

ptear 自分自身のため、または別のホストのプロキシーとして、RSVP *ptear* メッセージを送信します。**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・フローと予約の両方が削除されます。このコマンドは、パスを識別するパラメーター (たとえば、IP あて先アドレスおよび IP セッション・アドレス) の入力を求めてきます。要求された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 コマンドに指定されたパスおよび予約の状態は実際に存在しているものでなければなりません。存在しない場合には、ELS エラー・メッセージが生成されます。Talk 2 を使用すると、このコマンドに関連付けられた ELS メッセージを表示することができます。

RSVP 監視コマンド (Talk 5)

resv 自分自身のため、または別のホストのプロキシーとして、RSVP *resv* メッセージを送信します。このコマンドは、パスを識別するパラメーター (たとえば、IP あて先アドレスと IP セッション・アドレス) の入力を求めてきます。要求された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 を使用すると、このコマンドに関連付けられた ELS メッセージを表示することができます。これらの trace メッセージを表示するには、Talk 6 または Talk 5 プロンプトから、次のコマンドを使用して、これらの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
```

このコマンドを、RSVP セッションをセットアップしていない受信側に対して試みると、メッセージ `Inputting session does not exist` (入力セッションは存在しない) が表示されます。既存の RSVP フローを表示するためには、**show rsvp flow** コマンドを使用してください。

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 要求側のアドレスは IP ユニキャスト・アドレスでなければなりません。

2 IP セッション・アドレスは、そのセッションのあて先アドレスですが、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・アドレスでもかまいません。

3 フロー・エントリーの *Rsvd* (Reserved) フィールドは、予約が行われた後で N (No) から Y (Yes) に変化することに注意してください。この値が N であれば、フローは存在しますが、予約はありません。フローは、最善的 QoS を使用して送信中です。

4 Talk 2 ELS トレースは、30 秒おきにデフォルトで送信されている予約最新表示を表示します。

rtear 自分自身のため、または別のホストのプロキシーとして、RSVP *rsvtear* メッセージを送信します。このコマンドは、RSVP トラフィック・フローを切断しますが、送信側からのパスを廃棄しないため、IP トラフィック・フローは最善的 QoS で継続します。このコマンドは、RSVP トラフィック・フローを識別するパラメーター (たとえば、IP 受信側のあて先アドレスおよび IP セッション・アドレス) の入力を求めてきます。要求された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 コマンドに指定された IP トラフィック・フローは実際に存在しているものでなければなりません。存在しない場合には、ELS エラー・メッセージが生成されます。Talk 2 を使用すると、このコマンドに関連付けられた ELS メッセージを表示することができます。

Show

show コマンドは、RSVP の各種局面を表示するのに使用します。

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 の出力です。アクティブ RSVP セッション・パスに沿ったあらゆるリンクで予約された資源に関する情報をリストします。

classifier パケット分類コードの現在のエントリーをすべて表示します。

queue RSVP のソフトウェア待ち行列の現在の統計を表示します。

RSVP 監視コマンド (Talk 5)

rsvp 現在の RSVP 接続状況の局面を表示します。

- **flows** アクティブ RSVP トラフィック・フローを表示します。このコマンドの例については、 Talk 5 **send resv** コマンドに示されている例を参照してください。
- **senders** RSVP 送信側を表示します。送信側は構成済みですが、必ずしも起動されていません。
- **sessions** RSVP セッション (予約済みのフローをもつアクティブ・セッションと、終了しているが、現在のところ予約がない非アクティブ・セッションの両方) を表示します。
- **reservations** RSVP 予約を表示します。
- **requests** RSVP 要求を表示します。

Stop-RSVP

stop-rsvp コマンドは、ルーター内の RSVP 機能を停止するのに使用します。

構文:

stop rsvp

第22章 SNMP の使用

この章では、SNMP について説明します。本章には、以下の節が含まれています。

- 『ネットワーク管理』
- 『SNMP の管理』

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 の管理

サーバーは、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 (IBM NetView for AIX および Nways Campus Manager プロダクトなど) に対してシンプル・ネットワーク管理プロトコル (SNMP) を提供します。

SNMP は IP ネットワーク内の IP ホストの監視および管理のために使用され、SNMP エージェントと呼ばれるソフトウェアを使用して、ネットワークのホストがサーバーの動作パラメーターの一部のものについて、それを読み取ったり、変更したりすることができるようにします。このような方法で、SNMP は IP コミュニティーのためのネットワーク管理を確立します。

サーバーに SNMP を構成する際には、以下の局面を考慮することが必要です。

コミュニティー
コミュニティーには、SNMP エージェントの管理情報ベース (MIB) 内の情報へのアクセスが許可される SNMP 管理ステーションの IP アドレスを定義することができます。MIB へのアクセスに使用するコミュニティー名を定義します。

認証 コミュニティー名は、許可されないユーザーが SNMP エージェントに関する情報を入手したり、その特性を変更したりするのを防止するための認証方式として使用されます。

この方式では、MIB データ (MIB ビューと呼ばれます) とそれに関連するアクセス権 (読み取り専用、読み書き)、IP マスク、および各 MIB ビューのコミュニティー名との組み合わせを 1 つまたは複数定義します。IP マスクは、特定の MIB ビューへ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 要求で一致しなければならないパスワードの役目を果たします。コミュニティー名は各 SNMP メッセージに組み込まれ、IBM 2212 SNMP エージェントによって検証されます。正しいコミュニティー名が提供されていない場合、IP マスクが一致しない場合、または割り当てられたアクセス権に矛盾するアクセスが試みられた場合、SNMP 要求はリジェクトされます。

SNMP パスワード
snmp パスワードは、認証フィーチャーのユーザー・プロファイル部分におけるパスワードまたは暗号化かぎなどのセキュリティーが重要な MIB オブジェ

クトを暗号化し、認証するのに使用されます。snmp パスワードをゼロの長さに設定することは、セキュリティーが重要なデータがアクセス不能であることを意味します。snmp パスワードが *clear* に設定されるとき、データは暗号化なしで SNMP からアクセス可能です。snmp パスワードが他の文字列に設定されるとき、データは、snmp パスワードから引き出されたかぎを使用して暗号化および認証を使って検索可能です。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 は、管理情報へのアクセスを提供するバーチャル情報ストアです。この情報は MIB オブジェクトとして定義されており、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、場合によっては変更もできます。

IBM 2212 は、資源を監視し、管理するための包括的な標準 MIB およびエンタープライズ特定 MIB を提供しています。

IBM 2212 MIB サポートを文書化した readme ファイルを下記の World Wide Web URL で入手できます。

- **ftp://ftp.nways.raleigh.ibm.com/pub/netmgmt/2212/**

特定の MIB のコピーを受信するには、**get** コマンドを入力し、その MIB の名前を指定します。たとえば、**get ibm2212.mib** のように入力します。このコマンドを使用すると、指定された MIB のコピーが、FTP サーバーに接続するときに使用したディレクトリーに入ります。

FTP サイトからは、以下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
- 設定可能値

設定可能値を除いて、サポートされる MIB 属性はすべて読み取り専用モードです。

トラップ・メッセージ

トラップ・メッセージは、ルーターまたはネットワークの状態 (ルーターの再ロードやネットワークのダウン) に応答して、ルーター内の SNMP エージェントから SNMP マネージャーに送信される非送信請求メッセージです。

第23章 SNMP の構成および監視

この章では、SNMP 構成コマンドおよび監視コマンドについて説明します。本章には、以下の節が含まれています。

SNMP 構成環境へのアクセス

SNMP 構成環境にアクセスするには、Config> プロンプトで次のコマンドを入力します。

```
Config> 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 構成コマンドでは、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 2212 のリスタートまたは再ロード後に有効になります。

SNMP 構成コマンドは SNMP Config> プロンプトで入力します。

表 29. SNMP 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix ページの『ヘルプの入手』 を参照してください。
Add	コミュニティーを SNMP コミュニティーのリストに追加するか、IP アドレスをマスクと共にコミュニティーに追加するか、またはサブツリーを MIB ビューに追加します。
Delete	コミュニティーを SNMP コミュニティーのリストから削除するか、IP アドレスをマスクと共にコミュニティーから削除するか、またはサブツリーを MIB ビューから削除します。
Enable/Disable	SNMP プロトコルおよび指定されたコミュニティー名に関連するトラップを使用可能/使用不可にします。
List	現行のコミュニティーを、関連するアクセス・モード、使用可能なトラップ、IP アドレス、およびビューと共に表示します。また、すべてのビューと関連の 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、次のいずれかです。 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 ポートを設定し、セキュリティーが重要なデータを暗号化して認証するために使用されるパスワードを設定するのにも使用します。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

表 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	デフォルト
add	community	<comm_name>			なし
	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>		
		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>		
		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>	
		view	<community>	all	all
				<view_text_name>	
	trap_port	<udpPort#>			

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	デフォルト
	password				
exit					

Add

add コマンドは、コミュニティー名を SNMP コミュニティーのリストに追加するか、アドレスをコミュニティーに追加するか、または MIB の一部 (サブツリー) をビューに追加するのに使用します。

構文:

add community
address
sub_tree

community

add community コマンドを使用して、コミュニティーを作成します。コミュニティーは、デフォルト・アクセスの read_trap、すべてのビュー、全トラップ使用不可、および全 IP アドレス許可で作成されます。

注: add community コマンドでは、アクセス・タイプまたはトラップ制御を選択できなくなりました。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のには set community access コマンドを使用し、トラップ制御には **enable trap** または **disable trap** コマンドを使用してください。

community name パラメーターは、SNMP クライアントによって使用され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、コミュニティー IP アドレス・パラメーターで指定されたホストから装置内の管理情報ベース (MIB) にアクセスするときに使用されます。

有効値: 1 ～ 31 桁の英数字の文字列。スペース、タブ、または <ESC> キー・シーケンスなどの文字はサポートされません。

デフォルト値: public

例: add community <community_name>

```
Community Name []?
```

Community Name — コミュニティーの名前を指定します (最大 32 文字の可視文字)。スペース、タブ、または <Esc> キー・シーケンスなどの文字は受け入れられません。

address

add address コマンドを使用して、このボックスとの通信が許可されるネットワーク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します。コミュニティーの名前とネットワークのアドレスを (標準 a.b.c.d 表記で) 提供する必要があります。個々のホスト (マスク = 255.255.255.255) またはホスト・ネットワークへのアクセスを制限するために

net mask を提供することもできます。1 つのコミュニティーに複数のアドレスを追加することも可能です。その場合は、異なるアドレスを追加するたび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いと、要求は任意のホストによって処理されます。

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ていない場合、トラップは生成されません。

1. *community name* の値は、次のとおりです。

   有効値: 1 〜 32 桁の英数字の文字列。スペース、タブ、または <ESC> キー・シーケンスなどの文字はサポートされません。

   デフォルト値: なし

2. *IP address* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

3. 個々のホスト (マスク = 255.255.255.255) またはホスト・ネットワークへのアクセスを制限するために、*net mask* を提供することもできます。

   有効値: 0.0.0.0 〜 255.255.255.255

   デフォルト値: なし

例: add address <community_name> <ipAddress> <ipMask>

```
Community Name []?
New Address [0.0.0.0]?
```

sub_tree

add sub_tree コマンドを使用して、MIB の一部をビューに追加するか、または新規のビューを作成します。デフォルトは MIB 全体です。**add sub_tree** コマンドは MIB ビューの管理にも使用します。<view_text_name> によって定義されたビューに複数のサブツリーを追加することができます。新規の MIB ビューを作成する場合は **add sub_tree** コマンドを発行し、新規ビュー名を指定します。

注: ビューを有効にするためには、**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割り当てることが必要です。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 および指定の OID よりも語義学的に大きいすべての OID が、MIB ビューの部分と見なされます。

有効値:

- All - すべてのサポートされる MIB ビューを指定のコミュニティー名に割り当てます。
- View - 指定された MIB ビューを指定のコミュニティー名に割り当てます。

デフォルト値: All

MIB OID name は、sub_tree 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、数値で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に含める 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含まれます。

たとえば、MIB-II 内のシステム・グループにアクセスするビューを提供する場合は **1.3.6.1.2.1.1** と指定します。

有効値:

<element1>.<element2>.<element3>... フォーマットのオブジェクト識別子。ただし、

- 最少 3 つの要素が必要です。
- 最大 49 要素まで定義できます。
- element1 は、0、1、または 2 です。
- element2 は、1 と 40 の間の整数です。
- element3 とそれ以降の要素は、1 とサイズ (無符号整数バイト) の間の整数です。

デフォルト値: なし

例: add sub_tree

```
View Name  []?
MIB OID name []?
```

View Name　ビューの名前を指定します (最大 32 文字の可視文字)。スペース、タブ、または <Esc> キー・シーケンスなどはサポートされません。

MIB OID　sub_tree の MIB オブジェクト ID を指定します。これは、記号値ではなくドット表記の数値として入力する必要があります。

Delete

delete コマンドは、以下のものを削除するのに使用します。

- 特定のアドレス
- コミュニティーとそのすべてのアドレス
- ビューのサブツリー

構文:

delete　community
　　address
　　sub_tree

community

コミュニティーとその 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 の値は、次のとおりです。

有効値: 1 ～ 31 桁の英数字の文字列。スペース、タブ、または <ESC> キー・シーケンスなどの文字はサポートされません。

デフォルト値: public

このパラメーターは SNMP クライアントによって使用され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、コミュニティー IP アドレス・パラメーターで指定されたホストから装置内の管理情報ベース (MIB) にアクセスするときに使用されます。

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* の値は、次のとおりです。

   有効値: 1 〜 31 桁の英数字の文字列。スペース、タブ、または <ESC> キー・シーケンスなどの文字はサポートされません。

   デフォルト値: public

   このパラメーターは SNMP クライアントによって使用され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、コミュニティー IP アドレス・パラメーターで指定されたホストから装置内の管理情報ベース (MIB) にアクセスするときに使用されます。

2. *IP address* の値は、次のとおりです。

   有効値: 任意の有効な IP アドレス

   デフォルト値: なし

3. 個々のホスト (マスク = 255.255.255.255) またはホスト・ネットワークへのアクセスを制限するために、*net mask* を提供することもできます。

   有効値: 0.0.0.0 〜 255.255.255.255

   デフォルト値: なし

例: delete address <comm_name> <ipAddress> <ipMask>

sub_tree

ビューから MIB または MIB の一部を除去します。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、関連の SNMP コミュニティーからのそのビューへの参照もすべて除去されます。

1. 除去する*view name* は、Community name パラメーターで定義したコミュニティーが使用するビューを選択するのに使用でき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 オブジェクトを決めます。ビューが指定されていない場合、コミュニティーはルーターの SNMP エージェントが認知しているすべてのオブジェクトにアクセスできます。

   コミュニティーがルーターの SNMP エージェントによって管理される MIB 全体にアクセスするのを制限したい場合は、このパラメーターに応答する必要があります。

   あらかじめ View name パラメーターと MIB Subtree パラメーターが構成されていないと、このパラメーターを構成することはできません。

   有効値:

   – All - すべてのサポートされる MIB ビューを指定のコミュニティー名に割り当てます。

– View - 指定された MIB ビューを指定のコミュニティー名に割り当てます。

デフォルト値: All

2. *MIB OID name* は、sub_tree 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、数値で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に含める 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含まれます。

たとえば、MIB-II 内のシステム・グループにアクセスするビューを提供する場合は **1.3.6.1.2.1.1** と指定します。

有効値:

<element1>.<element2>.<element3>... フォーマットのオブジェクト識別子。ただし、

– 最少 3 つの要素が必要です。
– 最大 49 要素まで定義できます。
– element1 は、0、1、または 2 です。
– element2 は、1 と 40 の間の整数です。
– element3 とそれ以降の要素は、1 とサイズ (無符号整数バイト) の間の整数です。

デフォルト値: なし

例: `delete sub_tree <view_text_name> <oid>`

Disable

disable コマンドは、SNMP SNMP またはルーター上の指定されたトラップを使用不可にするのに使用します。

構文:

disable snmp

trap

snmp SNMP を使用不可にします。

community name の値は、次のとおりです。

有効値: 1 ～ 31 桁の英数字の文字列。スペース、タブ、または <ESC> キー・シーケンスなどの文字はサポートされません。

デフォルト値: 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可にします。次のオプションから、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>

トラップ・タイプ	説明
all	指定されたコミュニティーのすべてのトラップを使用不可にします。コミュニティー名をコマンド行の一部として指定します。
cold_start	指定されたコミュニティーのコールド・スタート・トラップを使用不可にします。コールド・スタート・トラップとは、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・エンティティー実現を変更できることを意味しています。コミュニティー名をコマンド行の一部として指定します。
link_down	指定されたコミュニティーの link_down トラップを使用不可にします。link_down トラップは、エージェントの構成に表示された通信リンクの 1 つの障害を認知します。link_down trap-PDU には、影響を受けたリンクの名前と ifIndex インスタンス値が、その variable-bindings の最初の要素として含まれています。
link_up	指定されたコミュニティーの link_up トラップを使用不可にします。link_up トラップは、ネットワーク内の以前に非アクティブであったリンクがアップになったことを認知します。link_up trap-PDU には、影響を受けたリンクの名前と ifIndex インスタンス値が、その variable-bindings の最初の要素として含まれています。
auth_fail	指定されたコミュニティーの認証障害トラップを使用不可にします。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 エージェントと通信するための正しい許可を持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のエンタープライズ特定トラップを使用不可にします。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たことを示します。specific-trap フィールドは、発生した特定のトラップを識別します。たとえば、ELS イベント・メッセージはエンタープライズ特定トラップで送信されます (そのように構成されている場合)。

Enable

enable コマンドは、SNMP プロトコルまたはルーター上の指定された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。下記のオプションから、トラップ・タイプを指定することができます。

community name の値は、次のとおりです。

有効値: 1 〜 31 桁の英数字の文字列

スペース、タブ、または <ESC> キー・シーケンスなどの文字はサポートされません。

デフォルト値: public

例: enable trap <trap_type> <community_name>

トラップ・タイプ	説明
all	指定されたコミュニティー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ます。
cold_start	指定されたコミュニティーのコールド・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・トラップとは、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・エンティティー実現を変更できることを意味しています。コミュニティー名をコマンド行の一部として指定します。
link_down	指定されたコミュニティーの 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に表示された通信リンクの 1 つの障害を認知します。link_down trap-PDU には、影響を受けたリンクの名前と ifIndex インスタンス値が、その variable-bindings の最初の要素として含まれています。
link_up	指定されたコミュニティーの link_up トラップを使用可能にします。link_up トラップは、ネットワーク内の以前に非アクティブであったリンクがアップになったことを認知します。link_up trap-PDU には、影響を受けたリンクの名前と ifIndex インスタンス値が、その variable-bindings の最初の要素として含まれています。
auth_fail	指定されたコミュニティーの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 エージェントと通信するための正しい許可を持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たことを示します。specific-trap フィールドは、発生した特定のトラップを識別します。たとえば、ELS イベント・メッセージはエンタープライズ特定トラップで送信されます (そのように構成されている場合)。

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・アドレスの現行の構成を表示するのに使用します。

構文:

list all

community

views

list all

SNMP コミュニティーのアクセス、トラップ、アドレス、およびビューについての現行の構成を表示します。オプションの詳細については、**list community** コマンドの説明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の属性を表示します。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	コミュニティーに対して生成された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の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 は、MIB ビューをコミュニティーに割り当てる、SNMP UDP トラップ・ポート番号を設定する、またはコミュニティーのアクセス・モードまたは SNMP パスワ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 コマンドを使用して、3 つのアクセス・タイプのうちの 1 つをコミュニティーに割り当てます。コミュニティーの名前とアクセス・タイプを提供する必要があります。

community name の値は、次のとおりです。

有効値: 1 ～ 31 桁の英数字の文字列

スペース、タブ、または <ESC> キー・シーケンスなどの文字はサポートされません。

デフォルト値: 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への読み取りアクセスと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への読み書きアクセスとトラップ生成を許可します。
trap_only	このコミュニティーは SNMP トラップの送信時にのみ使用されることを示します。

community view

set community view コマンドを使用して MIB ビューをコミュニティーに割り当てます。

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対して、すべての MIB オブジェクトへのアクセスを許可します。All がデフォルトです。
view_text_name	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。

trap_port

set trap_port コマンドを使用して、トラップの送信先の UDP ポート番号 (デフォルトの標準ポート 162 以外) を指定します。デフォルトは、標準ポートです。

例: set trap_port <udpport#>

UDP Port Number　標準 UDP ポート (デフォルト # 162) 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。

password

set password コマンドは、MIB で定義されているセキュリティーが重要な MIB オブジェクトを暗号化し、認証するためのパスワードを指定するのに使用します。パスワードを長さゼロの文字列に設定すると、どのアクセスも不許可にするか、セキュリティーが重要な MIB オブジェクトを設定することにより最大限のセキュリティーが得られます。パスワードを ″clear″ に設定すると、データが認証なしに流れることができるようにすることにより、最小のセキュリティーが与えられます。パスワードを他の文字列に設定すると、このパスワードを使って暗号化して認証されたセキュリティーが重要な MIB オブジェクトへ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には、**+** (GWCON) プロンプトで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。

SNMP 監視コマンド (Talk 5)

表31 は SNMP 監視コマンドをリストしています。SNMP 監視コマンドでは、SNMP 構成のパラメーターを見たり、SNMP エージェントに関するいくつかの統計を表示することができます。

ランタイム SNMP パラメーターの一時的な変更は、監視を通して行うことができます。これらは SNMP エージェントの動作に即時に有効になります。一時的な変更を固定させたい場合は SAVE コマンドを使用します。元の SNMP 構成に復元したい場合は REVERT コマンドを使用します。このフィーチャーにより、構成を固定的に変更せずに、SNMP エージェントの動作を一時的に変更することが可能になります。一時的な変更を有効にするためには、 SNMP 監視プロセスを終了することが必要です。

SNMP 監視コマンドは SNMP> プロンプトで入力します。

表 31. SNMP 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix ページの『ヘルプの入手』 を参照してください。
Add	コミュニティーを SNMP コミュニティーのリストに追加するか、IP アドレスをマスクと共にコミュニティーに追加するか、またはサブツリーを MIB ビューに追加します。
Delete	コミュニティーを SNMP コミュニティーのリストから削除するか、IP アドレスをマスクと共にコミュニティーから削除するか、またはサブツリーを MIB ビューから削除します。
Enable/Disable	SNMP プロトコルおよび指定されたコミュニティー名に関連するトラップを使用可能/使用不可にします。これらのアクションは SNMP 構成環境でのみ許されます。
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・アドレスの現行の構成を表示します。
Revert	指定された変更を削除し、設定値を固定 SNMP 構成の値に戻します。
Save	指定された変更を行った後、SNMP 構成に固定的に保管します。
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、次のいずれかです。 • 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も設定できます。詳細については、 474ページを参照してください。
Statistics	SNMP エージェントに関する統計を表示します。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、コミュニティー名を SNMP コミュニティーのリストに追加するか、アドレスをコミュニティーに追加するか、または MIB の一部 (サブツリー) をビューに追加するのに使用します。

add コマンドの使用については、465ページの『Add』を参照してください。

Delete

delete コマンドは、以下のものを削除するのに使用します。

- 特定のアドレス
- コミュニティーとそのすべてのアドレス
- ビューのサブツリー

delete コマンドの使用については、467ページの『Delete』を参照してください。

Disable

disable コマンドは、SNMP SNMP またはルーター上の指定されたトラップを使用不可にするのに使用します。このコマンドは SNMP 構成環境でのみ利用可能です。

disable コマンドの使用については、469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された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 構成環境でのみ利用可能です。

enable コマンドの使用については、470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・アドレスの現行の構成を表示するのに使用します。

構文:

list all

community

views

list all

SNMP コミュニティーのアクセス、トラップ、アドレス、およびビューについての現行の構成を表示します。オプションの詳細については、**list community** コマンドの説明を参照してください。

list コマンドの例については、 471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の属性を表示します。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	コミュニティーに対して生成された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の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、指定された変更を削除し、設定値を固定 SNMP 構成の値に戻すのに使用します。

Save

save コマンドは、指定された変更を固定的に保存するのに使用します。

Set

set コマンドの使用については、473ページの『Set』を参照してください。

Statistics

statistics コマンドは、SNMP エージェントに関する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24章 DLSw の使用

この章では、データ・リンク交換 (DLSw)、およびデータ・リンク交換 (DLSw) プロトコルの実現について説明します。Config> プロンプトで行われた変更は、即時には有効にならず、その後のルーターのリスタートに使用される SRAM 構成の一部になります。一時的な (ただし、即時に有効になる) 構成変更についての説明は、550 ページを参照してください。

2212 は、システム・ネットワーク体系 (SNA) 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に統合することを可能にする広範な機能を提供しています。

以下の節は、ルーターを DLSw 用に構成する方法を説明しています。

- 『DLSw について』
- 481ページの『DLSw フィーチャーの使用』
- 498ページの『DLSw の設定』
- 505ページの『サンプル DLSw 構成』

DLSw について

DLSw は、 LLC2、SDLC、および QLLC (X.25 経由 SNA) プロトコル用の転送機構です。これは、ルーターのブリッジング機能、スイッチ・ツー・プロトコル (SSP)、および TCP/IP を使用して、インターネットを介して SNA トラフィックを高信頼性でトランスポートします。DLSw は、完全なルーティング機能を提供するのではなく、データ・リンク・レイヤーにおける交換機能を提供します。DLSw は、LLC2 フレームをブリッジングせずに、データを TCP フレームにカプセル化し、得られたメッセージを WAN リンクを介してピア DLSw ルーターに転送し、目的のエンド・ステーション・アドレスに配信します。

DLSw の機能

LLC2、SDLC、および QLLC は、コネクション型のプロトコルです。 DLSw はルート可能プロトコルの動的特性を提供し、***しかも*** エンド・エンド間の信頼性と制御フィーチャーを保持して効率的な通信を行います。

ブリッジング・ソリューションの問題点

480ページの図41 は、WAN リンクを介した LLC2 フレームのブリッジングの従来のアプローチを示しています。 従来のアプローチを使用すると、ネットワークの遅延が LAN よりも WAN で頻繁に発生します。この遅延は、単なるネットワーク輻輳 (ふくそう) や回線速度の遅さなどが原因で起こります。どのような原因であれ、このような遅延は、セッションのタイムアウトやデータが予定のあて先に到達しないといった状態を引き起こす可能性を大きくします。

また、LAN プロトコルは、LLC2 と同様に、再送/レスポンス時間が WAN よりもかなり短くなっています。そのため、WAN リンクを経由するエンド・エンド接続は維持するのが非常に困難で、セッション・タイムアウトの確率がはるかに高くなっています。

セッション・タイムアウトに加えて、WAN を経由する間にデータが遅れると、ある重大な問題が生じます。送信側ステーションは、遅れたデータ (ただし、紛失していない) を再送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、受信側の LLC2 手順の混乱の原因になり、WAN リンクの使用が非効率的になります。

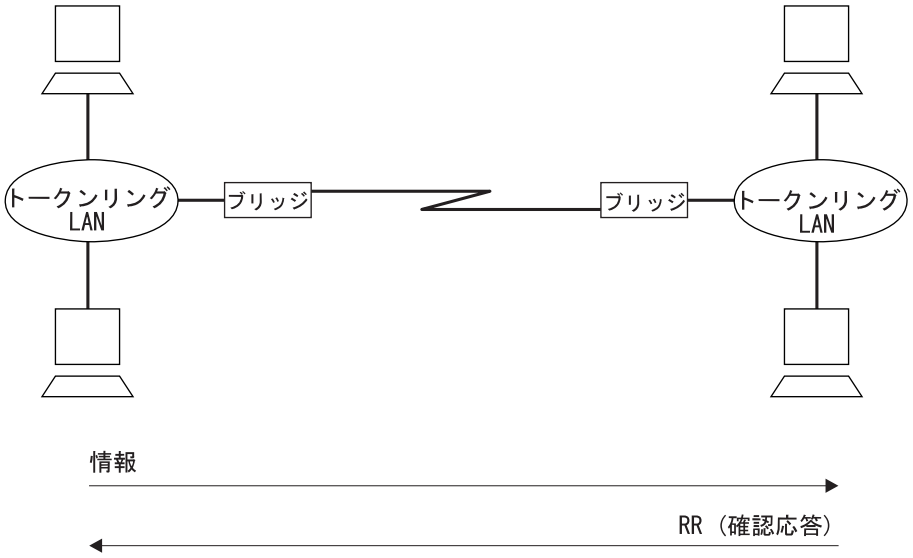


図 41. WAN リンクを介したブリッジングの従来のアプローチ

上の例は、エンド・エンド間データ・リンク制御が含まれている従来のブリッジングを示しています。ブリッジングはコネクションレス型プロトコルなので、WAN 上の LLC トラフィックの保全性を保証するための方策は何も取りません。

プロトコル・スプーフィング

セッション・タイムアウトを減らし、送信側ステーションにエンド・エンド接続が見えるように維持するために、DLSw は LLC2 コネクションをローカル・ルーターの位置で終端する、つまり 『スプーフィング』 します。LLC2 フレームを受信すると、ルーターは確認応答を送信側ステーションに送ります。この確認応答は、前に送信されたデータが受信されたことを送信側に伝えます。

この確認応答により、ステーションの再送が防止されます。この地点から先のデータ転送を保証するのは DLSw ソフトウェアの責任です。ソフトウェアは、データをルート可能 IP フレームにカプセル化し、それを (TCP を介して) DLSw ピアにトランスポートする方法でこれを達成します。ピア DLSw ルーターは、TCP ヘッダーを取り出し、データの予定の受信側のアドレスを調べて、そのエンド・ステーションとの間に新たな LLC2 コネクションを確立します。

図42 は、それぞれトークンリング・ネットワークに接続された 2 つのピア・ルーター間のこの関係を示しています。

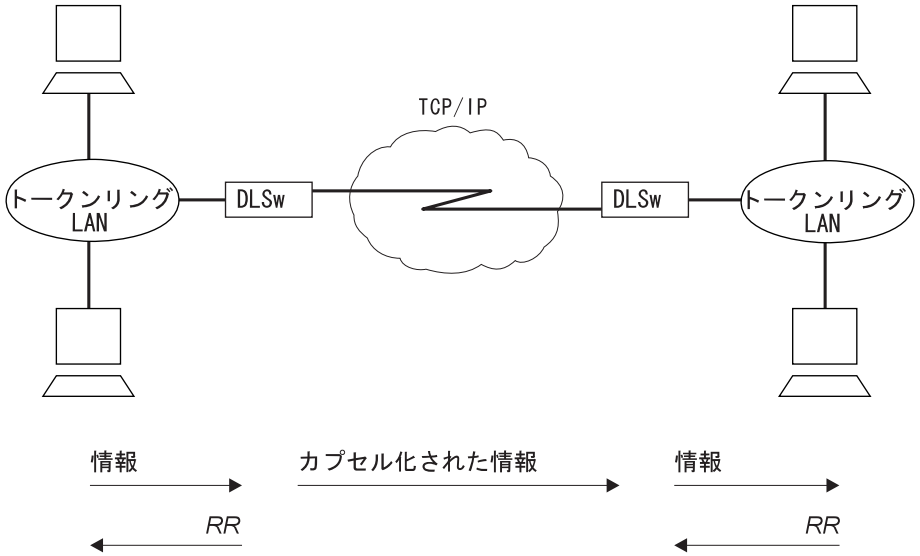


図 42. WAN を介するデータ・リンク交換

DLSw はルーターの位置で LLC2 コネクションを終端します。このことは、LLC2 コネクションは広域ネットワークを経由しないことを意味しています。これにより、セッション・タイムアウトを減らし、本来は広域ネットワークのエリア・リンクを通過するはずの確認応答 (RR) の数を減らすことができます。

DLSw の利点

DLSw は、DLC コネクションをローカル装置の位置で終端するので (図42 を参照)、SNA セッションのタイムアウトを無くし、共用回線上の WAN オーバーヘッドを削減するのに非常に有効です。このプロトコルには、次のような利点があります。

- LLC2、SDLC、および QLLC 制御トラフィックをローカル装置位置で終端させることによって、セッションがタイムアウトになる可能性を減らす。
- 広域ネットワークを介して確認応答 (RR) を転送する必要をなくすことによって、WAN ネットワークのオーバーヘッドを削減する。RR は 各 DLSw ルーターにローカルな LAN までに限定されます。
- DLSw ルーターとそれに接続されたエンド・ステーション間のフロー制御、輻輳 (ふくそう) 制御、および探索パケットの同報通信制御を提供する。
- ソース・ルーティング・ブリッジングのホップ・カウントの限界値を増やす。
- LLC2、SDLC、および QLLC 間のプロトコル変換を可能にする。
- NetBIOS トラフィックをサポートする。

DLSw フィーチャーの使用

以下の節では、各種の DLSw 機能の使用について説明します。

- 『TCP コネクション、近隣ディスカバリー、およびマルチキャスト探索』
- 485ページの『LLC 装置サポート』
- 485ページの『SDLC 装置サポート』
- 489ページの『QLLC 装置サポート』
- 495ページの『APPN インターフェース・サポート』
- 496ページの『近隣優先順位フィーチャーの使用』
- 497ページの『SNA と NetBIOS トラフィックの平衡化』

TCP コネクション、近隣ディスカバリー、およびマルチキャスト探索

DLSw は TCP を使用し IP ネットワークを介して、エンド・ユーザー情報を高信頼性、順序保存で配信します。DLSw メッセージ・フォーマットは、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・コネクションを介して運ぶことができます。DLSw 機能を備えたルーター間に TCP トランスポート・コネクションを構成し、必要なエンド・ステーション接続可能性を実現するには、2 通りの方法があります。

- 各組のルーターの一方または両方で、近隣ルーターの IP アドレスを構成する。これは最も基本的な方法で、すべての DLSw ルーターの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、ルーターが動的に相互の IP アドレスを発見できるようにする。これは、このプロダクトの DLSw の特殊機能で、近隣の IP アドレスを構成する負担を軽くします。

TCP 近隣の構成

ルーターで近隣 IP アドレスを構成するには、そのルーターの近隣のそれぞれに対して 1 回ずつ **add tcp** コマンドを使用します。近隣関係にある 2 つのルーターが、互いに相手の IP アドレスを構成する必要はありません。一方のルーターだけが相手側のアドレスを持っている必要があり、他方のルーターは未構成の近隣からの動的 TCP コネクションを受け入れるように構成できます。**enable dynamic-neighbors** コマンドを使用してこの動作を構成し、**set dynamic-tcp** コマンドを使用して、このような動的コネクションに使用するパラメーターを構成します。動的 TCP コネクションを使用可能にすることは、『ハブ』 ルーターの場合は特に便利です。ハブに接続するリモート支局の新規ルーターを設定するときに、再構成せずに済みます。

IP アドレスの他にも、**add tcp** コマンドでは、近隣および TCP コネクション自体の種々のパラメーターを構成できます。*Keepalive* パラメーターは、ユーザー・データ・トラフィックが途絶えているときに、TCP レイヤーがときどきピア TCP レイヤーにポーリングするするかどうかを制御します。キープアライブ・メッセージを使用可能にすると、TCP コネクションの障害がタイムリーに通知されるようになりますが、WAN のオーバーヘッドが増え、本来なら正常に再ルートできたはずのものが障害として報告されるようになります。

NetBIOS SessionAlive Spoofing パラメーターは、NetBIOS SessionAlive フレームを DLSw ピアに転送するかどうかを制御します。 このパラメーターは、 ISDN リンク

を介して DLSw ピア間に NetBIOS セッションが確立されている場合に特に重要です。 このパラメーターが使用可能にされ、 Keepalive パラメーターが使用不可にされている場合、DLSw ピア間にアイドル NetBIOS セッションが確立されていると DLSw パートナー間で DLSw トラフィックが渡されなくなります。この場合、DLSw 上にアイドル NetBIOS セッションを維持したまま、下位 ISDN コネクションを終了させることが可能になります。

connectivity setup type パラメーターは、DLSw が TCP コネクションを起動および切断する時期を制御します。一方または両方の近隣の CST が *active* に設定されている場合、DLSw はシステムのスタート時にコネクションの起動を試み、起動されるまで一定の間隔で試行します。TCP コネクションが確立された後は、障害が起きたときに再起動を試みることによって、常時起動状態に保つようにします。両方の近隣の CST が *passive* に設定されている場合には、DLSw は実際に DLSw エンド・ステーション・セッションを確立する必要があるときにのみ、TCP コネクションを起動します。最後の DLSw セッションが終了し、構成可能な期間 (*neighbor inactivity timer*) 内に新規セッションがスタートしなかった場合、DLSw は TCP コネクションを切断し、関連の内部資源を解放します。

近隣ディスカバリーのためのグループの構成

近隣ルーターの各組みの一方または両方に近隣 IP アドレスを構成するのを回避するために、DLSw がマルチキャスト IP アドレスを使用して、接続する近隣の IP アドレスを発見するように設定します。**join-group** コマンドを使用して、各ルーターを 1 つまたは複数の DLSw グループのメンバーとし、そのグループ内での役割を割り当てます。役割は、『クライアント』、『サーバー』、または 『ピア』 です。 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のうち、補完的な役割を持っているすべての DLSw ルーターの IP アドレスを見つけます (つまり、クライアントはグループ内のサーバーを (あるいは、その逆) を見つけ、ピアは他のピアを見つけます)。

DLSw は各グループ内の近隣の IP アドレスを確認すると、グループ内のメンバーシップおよび各グループ近隣の 『connectivity setup type』 を使用して、その近隣への TCP コネクションを確立する時期を判別します。個別に構成された近隣を使用する場合と同様に、どちらかの CST が *active* のときは、DLSw はできるだけ速やかに、発見した近隣との TCP コネクションを確立し、そのコネクションを常時アップ状態に保つようにします。両方の CST が *passive* の場合は、DLSw は DLSw セッションを伝送するために必要なときにのみ TCP コネクションを確立し、*neighbor inactivity timer* を使用して、使用されていないときには TCP コネクションを切断するようにします。

マルチキャスト探索とフレーム転送

DLSw は、近隣ルーターの IP アドレスを見つけるため以外にもマルチキャスト IP サービスを使用します。同じサービスを使用して、エンド・ステーションの資源 (たとえば、MAC アドレスや NetBIOS ネーム) を探すための DLSw メッセージの転送、および NetBIOS データグラム・トラフィックの転送を行います。この機能は、探索メッセージやデータグラム・メッセージを伝送するためにすべての近隣に静的 TCP コネクションを構成する必要がないので、DLSw ネットワークのスケーラビリティー (拡張容易性) を劇的に拡大します。また DLSw では、すべての TCP コネクション上で

個々の同報通信メッセージの異なるコピーを送信する必要はなく、マルチキャスト IP インフラストラクチャー内で複写された単一のコピーを送信できます。

探索およびフレーム転送にマルチキャスト IP を使用するためには、**join-group** コマンドを発行し、*connectivity setup type* を *passive* に設定します。DLSw は、マルチキャスト可能な他のグループ・メンバーや、近隣 IP アドレスの発見と静的 TCP コネクションの確立の目的にのみグループ・メンバーシップを利用している他のグループ・メンバーを、自動的に判別します。DLSw は同時に両方のタイプの近隣と協力して、エンド・ステーションの資源の探索、NetBIOS データグラムの転送、および DLSw セッションの確立を実行します。

join-group コマンドを発行する際には、結合するグループを記述するために、2 つのアドレッシング方式のうちの 1 つを選択します。前述のように、グループ ID とクライアント/サーバー/ピアの役割を提供する場合、ルーターは対応するマルチキャスト IP アドレスを作成し、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。あるいは、使用するマルチキャスト IP アドレスと、各アドレスが読み取り、書き込み、またはその両方のいずれであるかを直接指定することもできます。この方式は、RFC 2166 をサポートし、他の DLSw バージョン 2 準拠のプロダクトとのマルチキャスト相互接続を可能にするために導入されたものです。

ルーターは、従来のグループのメンバーとして、DLSw バージョン 2 マルチキャスト・アドレスの読み取りと書き込みを並行して行うことができます。新規のマルチキャスト・アドレスを使用して近隣を見つけることもできますが、TCP コネクションを確立する各組みのルーターについて、書き込み可能アドレス上で一方のルーターが読み取り中のときは、必ず他方のルーターの *connectivity setup type* が *active* になるように設定することが必要です。近隣を見つけ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 とクライアント/サーバー/ピアモデルを使用する場合よりも、より綿密な構成計画を立て、到達可能性を確実なものにする必要があります。

探索トラフィックの削減: DLSw 近隣間で転送される探索トラフィックの量が非常に多い場合は、この探索トラフィックを減らすための機能がいくつかあります。

DLSw オープン SAP
: DLSw 機能交換を介して、各 DLSw は任意のインターフェース上のオープンしているすべての SAP のリストを DLSw 近隣に送信します。DLSw 近隣はこの SAP リストを使用して、この DLSw に送信される探索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・リストを構成することができます。このリストは、排他 (すべての MAC アドレスがこの DLSw を介してアクセス可能であることを表す) または非排他 (1 組の MAC アドレスがこの DLSw を介してアクセス可能であることを表す) として定義されています。リストの各エントリーには MAC アドレス・マスクと MAC アドレス値が入ります。MAC アドレスの全リストと排他タイプが、DLSw 機能交換を介してすべての DLSw 近隣に送信されます。DLSw 近隣はこの MAC アドレス・リストを使用して、この DLSw に送信される探索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 ネーム・リストと同様に動作します。NetBIOS ネーム・リストについては、152ページの『NetBIOS ネーム・リスト』を参照してください。

DLSw MAC キャッシュ・エントリー

DLSw は特定の MAC アドレスを特定の DLSw 近隣にマップする、個別の MAC キャッシュ・エントリーを構成することができます。複数の MAC キャッシュ・エントリーを使用して、特定の MAC アドレスを複数の DLSw 近隣にマップすることも可能です。DLSw はこのリストをローカルで使用して、構成された MAC アドレスあての DLSw 探索パケットの送信先を限定することができます。

MAC アドレス・フィルター

ブリッジ・ネットワーク・インターフェースに構成された MAC アドレス・フィルターを DLSw トラフィックに適用します。ブリッジ・ネットワーク上のあて先 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し、これにより DLSw パートナーに送信する探索トラフィックを制限します。MAC フィルターの詳細については、*アクセス・インテグレーター・サービス 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』 および 『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 エンド・ステーションをサポートします。これらのエンド・ステーションと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、データの順序付けと高信頼性の送達を実現しています。ルーターは現在、以下のインターフェース・タイプを介するブリッジされた LLC トラフィックをサポートしており、DLSw と LLC エンド・ステーション間を流れるトラフィックに対しても、すべてのサポートを使用できます。

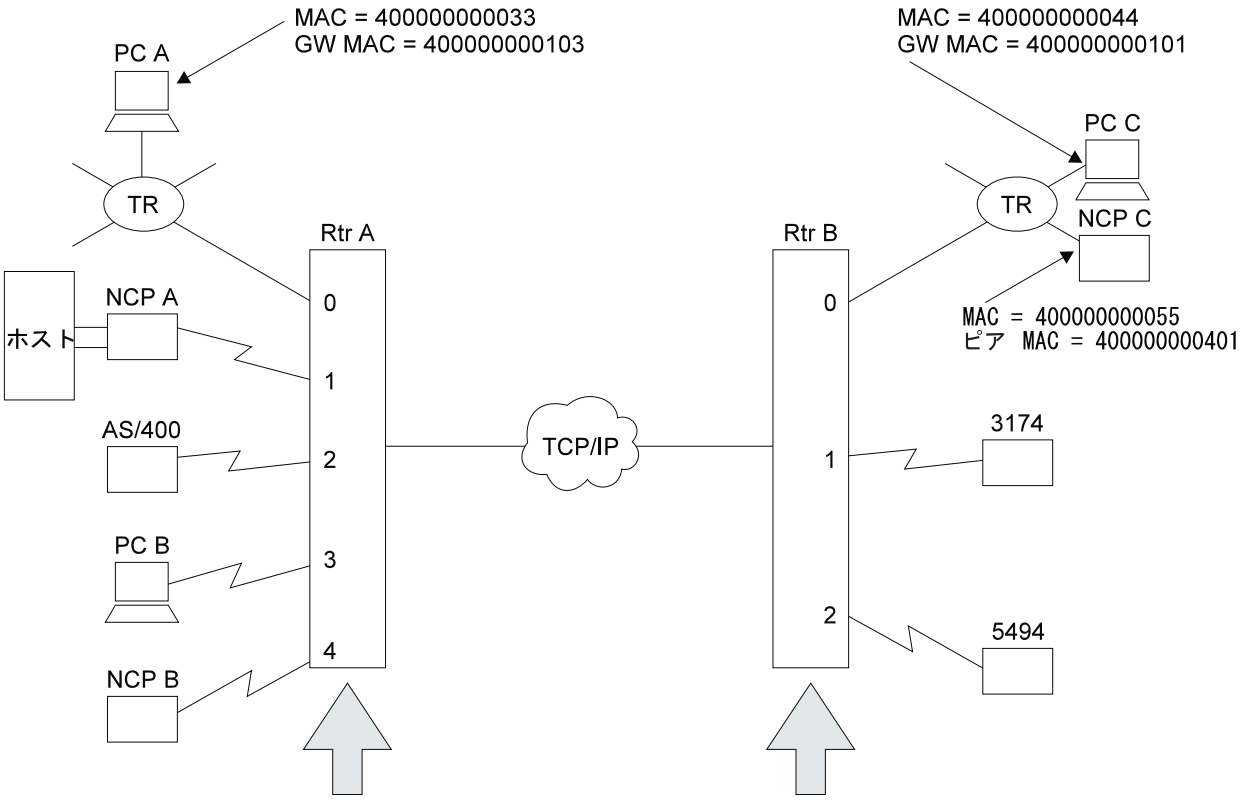
- トークンリング
- イーサネット/802.3
- フレーム・リレー (RFC 1490 のブリッジされたフレーム・フォーマットを使用)
- PPP
- PPP または FR フレームを使用するダイヤル回線 (たとえば、ISDN)

DLSw は、ブリッジされたフレーム内の利用可能な MAC および SAP アドレスを使用するので、DLSw 内で個々の LLC エンド・ステーションに関する情報を構成する必要はありません。DLSw はこれらのエンド・ステーションから送信された同報通信トラフィックを受信し、通常の LAN/ブリッジ同報通信を使用して最初の接続を行います。ただし、DLSw が使用する予定のインターフェースではブリッジング・サポートを構成しておく必要があり、また各インターフェース上で使用する SAP を DLSw 内で構成しておくことも必要です。

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、これは SNA PU タイプ 2.0、2.1、4 (NCP-NCP トラフィックの場合)、または 4/5 (SNA 境界機能を実行するホストまたは NCP) が可能です。ルーターは SDLC インターフェースに構成されて

いる役割に基づいて、または SNA XID ネゴシエーションに基づいて、1 次または 2 次 SDLC リンクの役割を果たすことができます。1 次の役割では、ルーターは同じ物理マルチポイント SDLC 回線上の異なる 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の複数の SDLC 2 次ステーションの役割を果たすことができます。また、2 次の役割では IBM 3174 グループ・ポーリングもサポートします。



Interface	SDLC Addr	PU Type	Source MAC	Dest MAC
1 (sec)	01	2	400000000101	400000000044
	02	5	400000000102	4011111101C1
	03	5	400000000103	400000000033
	04	2	400000000104	400000000301
2 (neg)	01	2	400000000201	4011111102C1
3 (neg)	01	2	400000000301	000000000000
4 (neg)	01	4	400000000401	400000000055

Interface	SDLC Addr	PU Type	Source MAC	Dest MAC
1 (pri)	C1	2	4011111101C1	000000000000
2 (neg)	C1	2	4011111102C1	400000000201

図 43. DLSw SDLC 構成の例

図43 は、DLSw によってサポートされるいくつかの SDLC 構成を図示し、SDLC と DLSw (MAC と SAP) アドレス間のマップに必要な DLSw 構成のサブセットを示しています。図には、*ローカル* (単一ルーター内) とリモート (2 つのルーターと IP ネットワークを経由) の両方の DLSw セッションが示されています。

以下のような DLSw セッションが構成されています。

- NCP A と PC A、B、C および 3174 間

  NCP A がこの 4 つの PU と通信できるようにするためには、ルーター A は各 PU のインターフェース 1 上に 2 次リンク・ステーションが構成されていることが必要です。このインターフェースは SDLC 内に 2 次、全二重、ポイント・ポイントとして構成する必要があります。非生産的なポーリングを減らすために、同じイ

ンターフェース上に複数の 2 次ステーションが存在する場合は、必ずグループ・ポーリングを使用することが推奨されます。

この例では、NCP A は、SDLC ステーション・アドレス 01 を介して PC C と通信し、アドレス 02 を介して 3174 と、アドレス 03 を介して PC A と、そしてアドレス 04 を介して PC B と通信します。PC A および C セッションは、それぞれローカルおよびリモート構成内で、両方とも SDLC-LLC 変換を起動することに注意してください。PC B は、ローカル SDLC-SDLC セッションですが、これはあまり一般的ではないかもしれません。

ルーター A に定義された 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 装置への 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) であることを示しています。ここでの PU タイプ 2 は、SDLC ホスト/FEP が DLSw ネットワーク内の別の T2.1 ノードと通信する T2.1 ノードとして動作していることを示しています。

- AS/400 と 5494 間

  この場合、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 リンクは交渉可能として構成されています (T2.1 ノードは役割が固定されたリンク上でもサポートされ、DLSw はそれに応じて役割の交渉を制限します)。ステーションは役割決定および SDLC アドレス解決 (同じリンク上のルーターとエンド・ステーションがそれぞれ異なる SDLC ステーション・アドレスを持つように構成されている場合) を含めて、完全な XID ネゴシエーションを実行します。リモート SDLC-SDLC 構成の場合は、2 つの異なる SDLC リンク上で使用される SDLC ステーション・アドレスの間には関係がないことに注意してください。リモート SDLC-LLC セッションは T2.1 装置間でもサポートされます。

- NCP B と NCP C 間

  NCP B は PU タイプ 4 として構成されており、これはこの DLSw セッションが NCP 相互間の INN サブエリア・トラフィックを伝送すること (NCP から PU 2 装置への BNN トラフィックを伝送するのではなく) を示しています。例にはリモート SDLC-LLC セッションが示されていますが、これと類似の他のセッションもサポートされます。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ません。

アドレス・マッピング

DLSw 構成は、1 バイト SDLC ステーション・アドレスと (DLSw がエンド・ステーションを識別するのに使用する) MAC アドレスおよび SAP との間のマッピングを提供します。SDLC ステーションの発信元 MAC アドレスは、その SDLC 装置を DLSw ネットワークの残りのものに示します。これは、その装置から着信するフレームの発信元アドレスであり、その装置に送信されるフレームのあて先アドレスになります。SDLC 装置が DLSw を通して通信するためには、発信元 MAC アドレスが必ず必要です。

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する 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になり、決して開始側にはならない SDLC 装置には、ゼロの MAC アドレスを割り当てることが必要です。ルーターが 2 次リンク・ステーションとして構成されている場合は、ホストによるコネクトアウトを正常が行われるようにするために、あて先 MAC アドレスを定義しておくことが重要です。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接続を開始することができず、ポーリングされるのを待たなければならないからです。リモート DLSw エンド・ステーション自体が SDLC であり (たとえば、 486 ページの図43 のルーター B 上の 3174)、ローカル 2 次ステーションと対になっている場合、リモート・ステーションは、このホスト・コネクトアウトへの依存性を反映してゼロのあて先 MAC アドレスを持っていても構わないことに注意してください。

DLSw 構成と SDLC 構成

SDLC インターフェースを介して DLSw を使用するためには、DLSw 構成の一部としてアドレス・マッピングを構成し、さらに SDLC 構成の一部としていくつかの情報を構成します。SDLC では、最小限として、インターフェースを SDLC として設定し、その他のインターフェース・レベルのパラメーター (リンクの役割など) を構成する必要があります。SDLC インターフェース・パラメーターは、そのインターフェース上のすべての SDLC リンク・ステーションのデフォルト値を提供しますが、あるステーションに固有な値を持たせたい場合は、ユーザーが個々の SDLC ステーション情報を構成することも可能です。

インターフェース番号と SDLC ステーション・アドレス のアドレスの組みは、DLSw アドレス・マッピング情報を SDLC のステーション・レベル構成に結び付けるための共通のかぎになります。ルーターのソフトウェアは初期化時に、このアソシエーションを行います。DLSw がインターフェース上の SDLC に構成されていない SDLC ステーション・アドレスを持つリンク・ステーションを初期化しようとした場合、SDLC は動的にリンク・ステーション定義を作成し、そのインターフェースの SDLC に定義されているパラメーターのデフォルト値を使用します。

SDLC リレー機能との関係

SDLC リレーは、SDLC フレーム全体を IP パケットにカプセル化し、それを、SDLC リレーをサポートする別のルーターに転送するルーター機能です。あて先ルーターは、IP ヘッダーを除去し、その SDLC フレームを変更しないままあて先 SDLC リンクに配信します。

この機能は DLSw SDLC サポートとは次の点で異なっています。

- SDLC リレーの場合、ルーター内には稼働している SDLC リンク・ステーションがありません。制御フレーム (たとえば、RR) は IP ネットワークを経由して流れます。DLSw の場合、ルーターの SDLC は SDLC コネクションの終端をサポートします。SDLC フレームからのデータのみが IP ネットワークを経由して流れます。その結果、DLSw は WAN 帯域幅の使用効率が良くなり、WAN の遅延によるリンク・タイムアウトの影響を受けにくくなります。
- SDLC データおよび制御フレームは、SDLC リレーを介して透過的に渡されます。これに対して DLSw はその一部を解釈または変更する必要があります。このことは、DLSw が SDLC コネクションを終端させることと合わせて、特定プロダクトの構成および機能 (たとえば、NCP 間のマルチリンク TG) が DLSw によってサポートされないことを意味しています。
- SDLC リレーでは、両方の通信エンド・ステーションのデータ・タイプが SDLC であることが必要です。DLSw では、プロトコル変換機能が提供されるので、相手側

エンド・ステーションのデータ・タイプは LLC、SDLC、QLLC、あるいは、DLSw プロダクトによってサポートされるその他の任意のデータ・タイプで構いません。

- DLSw は、APPN 実現作業部会によって開発された標準で、IETF RFC に文書化されています。そのため、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によってのみサポートされています。

次の場合は、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
- 制御トラフィック (たとえば、RR フレーム) が IP ネットワークの外側に流れるのを制限したい場合

次の場合は、SDLC リレーを使用する必要があります。

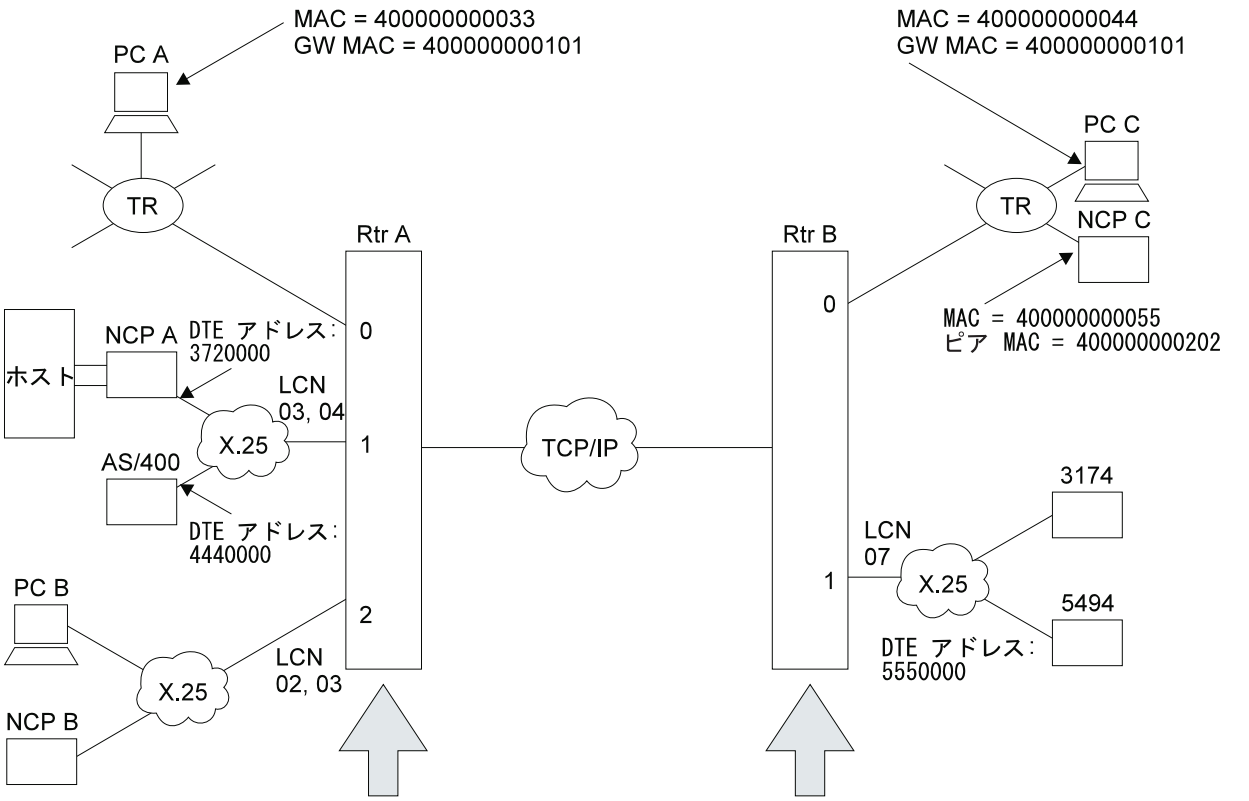
- DLSw では現在サポートされていない SDLC-SDLC 機能または構成の 1 つを使用したい場合

その他の SDLC-SDLC 構成では、構成の容易さ、WAN の使用効率、および現行のエンド・ステーション環境のサポート要件に最も適した機能を選択してください。SDLC リレーの詳細については、*ソフトウェア使用者の手引き*を参照してください。

QLLC 装置サポート

QLLC は X.25 のパケット・レイヤー・プロトコルの上位で動作し、X.25 ネットワーク上の SNA 装置に SDLC に似たステーションを提供するプロトコルです。QLLC は 1 つのバーチャル・サーキット (PVC または SVC) につき 1 つの SNA PU をサポートします。X.25 チャネル多重化は、X.25 ネットワークへの単一の物理インターフェースを介して多数のバーチャル・サーキット または PU を接続する機能を提供します。QLLC アーキテクチャーは 1 次、2 次、およびピア・ステーションの役割を定義していますが、これはエンド・ユーザーのデータ転送には影響しないので、SDLC の場合ほどは重要ではありません。インターフェース上のバーチャル・サーキットのデータはすべて、単一の LAPB レイヤー 2 リンク・コネクション (平衡モードで動作する) を介して流れます。リンクが接続されている間は常時、リンクのどちら側も送信が許されます。

DLSw は QLLC エンド・ステーションをサポートし、これは SNA PU タイプ 2.0、2.1、4 (NCP-NCP トラフィックの場合)、または 4/5 (SNA 境界機能を実行するホストまたは NCP) が可能です。エンド・ステーションは、構成された PVC、構成された SVC、または着信コールから得られた動的 SVC を介して接続することができます。ルーターは、X.25 インターフェースに構成されている役割および SNA XID ネゴシエーションに基づいて、1 次または 2 次 QLLC リンク・ステーションのいずれかの役割を果たすことができます。同じ物理インターフェース内の異なるバーチャル・サーキット上に異なる PU タイプが共存することも可能ですが、各インターフェースでは 1 つのリンク・ステーション役割しかサポートされません。



Interface	VC Type	LCN/DTE Addr	PU Type	Source MAC	Dest MAC
1 (neg)	PVC	03	5	400000000102	401111110101
	PVC	04	5	400000000105	400000000201
	SVC	3720000	5	400000000101	000000000000
	SVC	4440000	2	400000000104	000000000000
2 (neg)	PVC	02	2	400000000201	400000000105
	PVC	03	4	400000000202	400000000055

Interfaces enabled for incoming calls
1

Connection ID	Dest MAC
PCA	400000000033
PCC	400000000044

Interface	VC Type	LCN/DTE Addr	PU Type	Source MAC	Dest MAC
1 (pri)	PVC	07	2	401111110101	400000000102

Interfaces enabled for incoming calls
1

Connection ID	Dest MAC
AS400	400000000104

図 44. DLSw QLLC 構成の例

図44 は、DLSw によってサポートされるいくつかの QLLC 構成を図示し、QLLC と DLSw (MAC と SAP) アドレス間のマップに必要な DLSw 構成のサブセットを示しています。図には、*ローカル* (単一ルーター内) とリモート (2 つのルーターと IP ネットワークを経由) の両方の DLSw セッションが示されています。図には QLLC-SDLC の組み合わせは示されていませんが、この組み合わせはローカルおよびリモート構成の両方でサポートされます。

以下のような DLSw セッションが構成されています。

- NCP A と PC A、B、C および 3174 間

  NCP A は、2 つの PVC と 2 つの SVC を介してルーター A 上のインターフェース 1 に接続されており、各バーチャル・サーキットは 1 つの PU を表しています。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 X.25 装置に接続された DTE アドレス (電話番号) によってアドレス指定

されています。SDLC と同様に、DLSw 構成はこれらの ″ネイティブ″ 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) と通信し、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 のローカルです。NCP は異なる LCN を使用して、対応する PVC を X.25 ネットワークに接続することもできます。ルーター A は、NCP A と PC C (リモート QLLC-LLC) および PC A (ローカル QLLC-LLC) との接続を、NCP A の DTE アドレス 3720000 およびルーター A 上のインターフェース 1 の DTE アドレスとの間 の 2 本の SVC を使用して実現しています。ルーター A は NCP A からのコールを受け入れる必要があるので、インターフェース 1 が DLSw への着信コールに対して使用可能にされています。NCP A はコネクション *ID* (下で説明) を 使用して、PC A および C に接続します。

ルーター B では、PC C は LLC/LAN 接続なので構成されていません。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が、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 番号とは関連がありません。

- AS/400 と 5494 間

  NCP A の他に、AS/400 もインターフェース 1 を介してルーター A に接続されています。SDLC とは異なり、特定インターフェース上のステーション数を制限しても、性能上の利点はありません。リンクの役割に関係なく、1 つのリンク上に複数のステーションを構成することができます。役割が交渉可能であり、ステーションが T2.1 または PU4 ノードの場合、各ステーションが独立して交渉して 1 次または 2 次になることができます。

  AS/400 はルーター A であて先 MAC アドレスが構成されていないので、5494 に接続することはできません。5494 はルーター B で構成されていないので、動的 SVC になります。5494 はコネクション ID を使用して、AS/400 と接続したいことを示します。ルーター B は、インターフェース 1 が DLSw への着信コールに対して使用可能になっているので、5494 からのコールを受信することができます。

- NCP B と NCP C 間

  NCP B は PU タイプ 4 として構成されており、これはこの DLSw セッションが NCP 相互間の INN サブエリア・トラフィックを伝送すること (NCP から PU 2 装置への BNN トラフィックを伝送するのではなく) を示しています。例にはリモート SDLC-LLC セッションが示されていますが、これと類似の他のセッションおよび SDLC を含むセッションもサポートされます。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ません。

アドレス・マッピング

DLSw 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のに使用される MAC/SAP の組みのマッピング、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) の組みのマッピング機能を提供します。このマッピングはコネクションを確立するときに行われますが、アドレッシング情報は、ルーター内およびエンド・ステーション製品内で構成されたものを使用します。

コネクトアウト (QLLC ステーションへ)

DLSw は、特定のターゲット MAC および SAP をアドレス指定した CUR_ex または CUR_cs メッセージを受信します。その場合、QLLC エンド・ステーションの中から SMAC および SSAP (SAP は CUR_cs の場合にのみチェック) がこのターゲット MAC/SAP に一致するものを探索します。SMAC はルーター内で固有であるため、1 つが一致するか、または一致するものが無いかのいずれかになるはずです。

一致が見つかった場合、DLSw は対応するインターフェースと LCN を使用して (PVC の場合) またはインターフェースと電話番号を使用して (SVC の場合)、QLLC ステーションとの接続の確立を開始します。DLSw は 1 つの QLLC ステーション (SVC) 定義を使用して、同じ DTE アドレスに対して複数の発信コールを行うことができます。これにより、最小限の構成作業で、多数の装置を同じあて先に接続することが可能になります。

コネクトイン (QLLC ステーションから)

PVC の場合、QLLC は接続されたエンド・ステーションから回線の確立を開始するフレームを受信します。QLLC および DLSw は、フレームを受信したインターフェースと LCN を、QLLC ステーション・リスト・エントリーと照合します。LCN はインターフェース内で固有なものでなければならないので、1 つの一致または一致なしが検出されます。一致がない場合、またはエントリーに DMAC/DSAP が定義されていない場合には、コネクトインは失敗します。そうでない場合は、定義された DMAC/DSAP への接続が開始されます。この接続の発信元 MAC/SAP は、同じリスト・エントリーからの SMAC/SSAP になります。

SVC の場合、DLSw は X.25 コールする側のアドレス、または受信した Call_Request パケットのコール・ユーザー・データ・フィールド内の *connection id* (バイト 4〜11) を使用して、MAC/SAP アドレスを導出します。コールする側のアドレスが利用可能な場合、 DLSw は最初にそれをコールされる側のインターフェース に構成されているすべての SVC DTE アドレスと照合してチェックします。DTE アドレスはインターフェース内で固有なものでなければならない ので、1 つの一致または一致なしが検出されます。一致が見つかり、QLLC ステーション・リスト・エントリーに非ゼロの DMAC/DSAP がある場合、DLSw はこの DMAC/DSAP をコネクション確立のためのターゲット・アドレスとして使用します。この接続の発信元 MAC/SAP は、同じリスト・エントリーからの SMAC/SSAP になります。

コールする側のアドレスが得られない場合、または得られたが DMAC/DSAP が未定義のエントリーに一致している場合、あるいはコールされる側のインターフェースに定義されている DTE アドレスのどれにも一致しない場合には、DLSw は受信した Call_Request パケット内のコネクション ID (CID) が、DLSw QLLC あて先レコードに定義されているアドレスに一致しないかチェックします。CID は、最高 8 文字の EBCDIC 英数字文字列として解釈されます。

CID が一致した場合、DLSw はあて先レコード内の関連の DMAC/DSAP を、回線確立のためのあて先アドレスとして使用します。コールする側のアドレスも一致した場合 (DMAC/DSAP が未定義の場合)、DLSw は一致した ステーション・リスト・エントリーからの SMAC/SSAP を使用します。そうでない場合、DLSw は動的に SMAC および SSAP を割り当てます。 SMAC の場合、DLSw はグローバル DLSw 構成パラメーター *QLLC base MAC address* と *Max dynamic addresses* で定義された範囲内

の、次の順番の利用可能な MAC アドレスを選択します (ラウンドロビン方式)。動的に選択される SSAP は、常に 0x04 です。

コールする側のアドレスまたはコネクション ID が一致しない場合、DLSw はそのコールを受け取りません。CID は、コールする側の 1 つのアドレスで複数のあて先にコールを設定できる唯一の方法であることに注意してください。

APPN および DLSw は両方とも、コールする側の同じアドレスからの QLLC コールを受け入れることができます。DLSw は受け入れるコールが制約されているので、最初にそのコールにアクセスします。DLSw でコールする側のアドレスまたはコネクション ID の一致が見つからなかった 場合、DLSw はそのコールを切断せずに APPN に提示します。

この場合、着信コールを受け入れるためには、コールする側のアドレスまたはコネクション ID が DLSw に対して定義されていることが必要です。これは主としてアドレス・マッピングを提供するために必要なことですが、不許可パーティーからの着信コールに対するセキュリティー要素の 1 つにもなります。その他の可能なセキュリティー手段としては、DLSw への着信コールに対してインターフェースを使用可能にしないこと、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あります。前者は、そのインターフェース上のすべての着信コールを (DLSw に構成されている DTE アドレスからのものであっても) 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なコールのみを防止します。

X.25 コール側が (DTE アドレスまたは CID にかかわらず) DLSw によって受け入れられ、特定の DMAC および DSAP (ボックスごとに 1 つずつ) に一致することができるようにするため、QLLC あて先レコードを「ANYCALL (任意のコール)」の CID 値および希望する DMAC および DSAP を 使って構成することができます。 DLSw は動的に SMAC および SSAP を割り当てます。このフィーチャーが使用される場合、 DLSw はすべてのコールを受け入れます。APPN にはコールは何も提示されず、アドレス・マッピングに関連するすべてのセキュリティー・フィーチャーはう回されます。

DLSw 構成と X.25 構成

X.25 インターフェースを介した DLSw の QLLC サポートを使用するためには、DLSw 構成の一部としてアドレス・マッピングを構成し、さらに X.25 インターフェース構成の一部として以下の情報を構成する必要があります。以下のステップの例については、503ページの『X.25 インターフェースの構成』 を参照し、追加情報については、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*の “X.25 ネットワーク・インターフェースの使用” を参照してください。

1. インターフェースを X.25 として構成し、基本 X.25 インターフェース・パラメーターを構成する。
2. サポートするプロトコルとして DLS を追加する。
3. DLSw が使用する PVC を構成し、それらを DLSw と関連付ける。
4. DLSw が使用する静的 SVC DTE アドレスを構成し、それらを DLSw と関連付ける。これらは DLSw に構成されたのと同じアドレスです。動的にコールできる QLLC エンド・ステーションの DTE アドレスは、構成する必要はありません。

SDLC とは異なり、X.25 は DLSw に構成された情報に基づいてリンク・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持っていません。

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、XTP をサポートする別のルーターに伝達するルーター機能です。あて先ルーターは、XTP ヘッダー情報を除去し、パケットをあて先の X.25 バーチャル・サーキットに配信します。

この機能を DLSw QLLC サポートと比較すると、次のようになります。

- 両方の機能とも、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 (または、DLSw セッション) からの情報を多重化して、単一の TCP コネクションに送ることができます。
- 両方の機能とも、ルーターは X.25 エンド・ステーションへのレイヤー 2 LAPB およびレイヤー3 パケット・レイヤー・コネクションを終端します。LAPB 制御フレームは TCP/IP を経由して流れません。
- XTP は、2 つの X.25 エンド・ステーション間の通信のみをサポートします。DLSw は、LLC (リモートでブリッジされた、または LAN 上の)、SDLC、QLLC、および DLSw プロダクトによってサポートされる他のデータ・タイプとの間のプロトコル変換を行います。
- XTP は、パケット・レイヤーの上位で動作している LLC タイプ (たとえば、 QLLC または PAD) の影響は受けません。両方の X.25 エンド・ステーションが同一の LLC タイプをサポートしている限り、XTP を介して通信することができます。DLSw QLLC サポートは、QLLC を実行している SNA エンド・ステーションとしか通信できません。
- 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、ピア・ルーター、および別の X.25 ネットワーク上のバーチャル・サーキットの間に、構成されたアソシエーションがあります。SVC の場合のみ、複数のピア・ルーターを定義して、1 次ルーターが利用不能になったときに 2 次ルーターを介して接続の確立を試みることが可能ですが、XTP は並行した探索またはコネクション確立は試行しません。これに対して 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た後、複数のピア間で完全な動的探索を実行し、あて先ステーションを見つけます。DLSw マルチキャスト・サポートを使用すれば、探索する個々のピア IP アドレスを構成する必要もありません。
- XTP は、PVC を別の PVC しかマップできず、また SVC も別の SVC にしかマップできません。DLSw QLLC-QLLC 構成では、PVC を SVC にマップすることが可能です。実際上は、これはあまり価値がないかもしれません。QLLC プロトコルが PVC 上でアクティブのときは、DLSw は必ず SVC の起動を試みるからです。
- 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 アドレスに (または、その逆に) 設定されます。ルーターが複数の DTE アドレスを使用できるようにするためには、 X.25 スイッチまたはネットワーク加入を構成することが必要になる場合があります。 DLSw では、コールはエンド・ステーションからルーターの DTE アドレス に (または、その逆に) 設定されます。

- DLSw は、APPN 実現作業部会によって開発された標準で、IETF RFC に文書化されています。そのため、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によってのみサポートされています。

次の場合は、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 を介して非 QLLC プロトコルを実行している場合

その他の QLLC-QLLC 構成では、ユーザーのネットワークの要件に最も適合してプロトコルを選択してください。XTP の詳細については、*ソフトウェア使用者の手引き*の『XTP の使用、構成、および監視』 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 との内部インターフェースがあり、それを使用して 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がないので、メモリーの所要量を減らすことができます。図45 に示すように、この内部インターフェースは、DLC コネクション (たとえば、LAN 経由の LLC) を圧縮して単一のソフトウェア・インターフェースに代えたのと同等です。

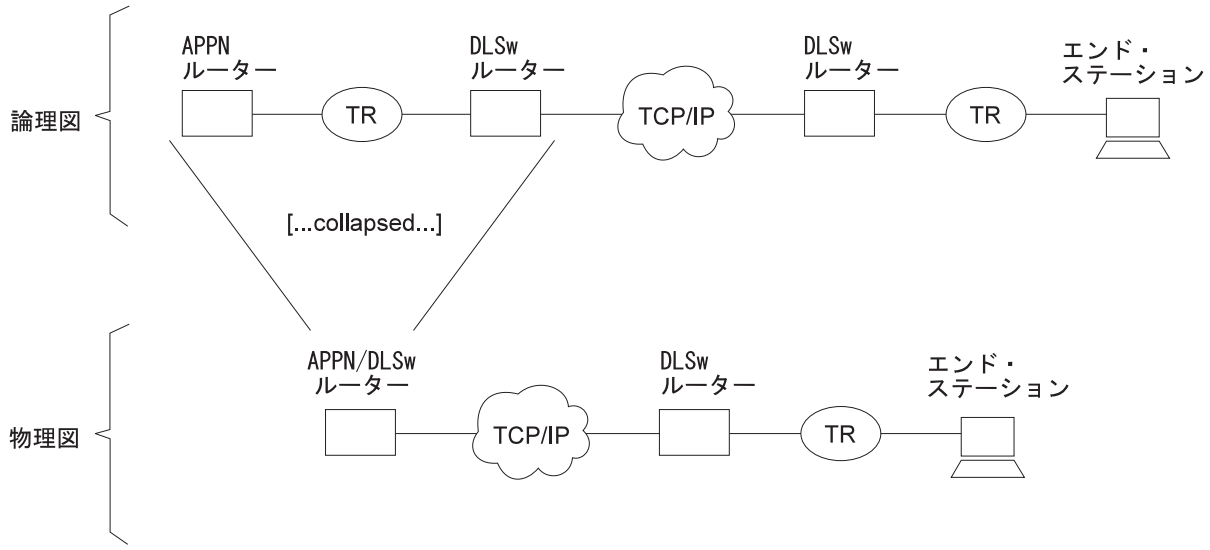


図 45. APPN-DLSw ソフトウェア・インターフェース

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。これらの装置と通信するためには、ネイティブ DLC サポートを使用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 DLSw を追加構成する必要はありません。DLSw リモート・ルーターへの TCP キープアライブ・メッセージを使用可能

にして、DLSw ポート上のリンク・ステーションの損失を検出できるようにします。APPN では、DLSw バーチャル・インターフェースを使用してエンド・ステーションに到達するように構成する必要があります。DLSw を使用する APPN の実現の詳細については、*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の使用

多くの DLSw ネットワーク構成は、エンド・ステーションを複数のあて先 DLSw ルーターのローカルとして構成することによって、あて先 DLSw ルーターからあて先エンド・ステーションへの複数のパスを提供しています。新規回線のために使用されるリモート DLSw ルーターに対して追加制御を提供するために、定義された各近隣に優先順位 (高、中、低) を割り当てることができます。近隣の優先順位は、許容値は似ていますが、497ページの『SNA と NetBIOS トラフィックの平衡化』 で説明している SNA と NetBIOS トラフィックの平衡化のための優先順位と同じでは***ありません***。

近隣の優先順位の場合は、**add tcp** 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、そのグループ内に確立されるすべてのトランスポート・コネクションによって継承されます。

DLSw は、回線を生成するときに、あて先 MAC アドレスまたは NetBIOS ネームに複数のリモート DLSw ルーターを介して到達可能であることが分かった場合、最高の優先順位を持つ近隣の 1 つを介して回線を確立します。この最高優先順位を複数のリモート・ルーターが共有している場合、DLSw は 『ラウンドロビン』 方式を使用して新規回線をこれらのルーター間に割り振ります。

近隣の優先順位を使用して、リモート・ルーター間に 1 次/バックアップ関係を設定することができます。低位の優先順位のルーターは、高位の優先順位のルーターが利用不能にならない限り使用されません。また、ラウンドロビン方式により、同じ優先順位をもつルーター間でロード・バランシングが行われます。

注:

1. SNA フレームを受信したが、そのあて先 MAC アドレスに到達できる近隣に関する情報がキャッシュされていない場合には、SNA 探索メッセージがすべての DLSw 近隣に送信されます。SNA 探索メッセージに対するレスポンスは、『近隣優先順位待機タイマー』 によって指定された期間、収集されます。この期間の後、MAC アドレス・キャッシュ・エントリーは、最高の優先順位をもつ近隣からのレスポンス情報を用いて更新されます。これらの近隣の 1 つが、この SNA 回線を扱うために選択され、受信した元の SNA フレームに対してレスポンスが送信されます。この MAC アドレスあての以降の SNA 回線要求は、キャッシュされた最高優先順位の近隣の 1 つを使用して回線が確立されます。
2. NetBIOS フレームを受信したが、そのあて先 NetBIOS ネームの現行キャッシュ情報エントリーが存在しない場合、NetBIOS 探索メッセージが NetBIOS をサポートするすべての DLSw 近隣に送信されます。SNA の場合とは異なり、指定された期間だけレスポンスが収集された後、元の NetBIOS フレームに対してレスポンスが送信されます。エンド・ステーションのタイマーは、通常はルーターでの待機遅延を許容しません。

   したがって、NetBIOS 探索メッセージへの最初のレスポンスが保管されます。この近隣が、この NetBIOS 回線の確立に使用され、受信した元の NetBIOS フレーム

に対してレスポンスが送信されます。この間に、NetBIOS 探索メッセージへの後続のレスポンスを用いて NetBIOS ネーム・キャッシュが更新されます。

- 現在キャッシュされている情報と同じ優先順位の近隣からレスポンスを受信した場合は、キャッシュに追加されます。
- 現在キャッシュされている情報より高い優先順位の近隣からレスポンスを受信した場合は、現在キャッシュされている情報は除去され、新規の高い優先順位の近隣の情報が追加されます。
- 現在キャッシュされている情報より低い優先順位の近隣からレスポンスを受信した場合は、無視されます。この NetBIOS ネームあての以降の NetBIOS 回線要求は、現在キャッシュされている最高優先順位の近隣の 1 つを使用して回線が確立されます。

すべての MAC アドレスまたは一定の MAC アドレスの集合について近隣優先順位フィーチャーを使用不可にすることができます。すべての MAC アドレスについてこのフィーチャーを使用不能にするには、*wait neighbor priority timer* を 0 に設定してください。MAC アドレスの集合についてこの機能を使用不可にするには、MAC キャッシュ探索機能オーバーライドを作成して、その *wait neighbor priority timer* を 0 に設定してください。

近隣優先順位フィーチャーが使用不可になっていると、MAC アドレスについては、DSLw パートナー情報はキャッシュに入れられません。SNA エクスプローラーおよび NetBIOS エクスプローラーは、必ず、すべての該当する DLSw パートナーに送信され、(その優先順位に関係なく) 最初に応答した DSLw パートナーを使用して DLSw セッションが確立されます。

SNA と NetBIOS トラフィックの平衡化

NetBIOS トラフィックに対する DLSw サポートを導入した場合、DLSw トランスポート・コネクション内の SNA と NetBIOS トラフィックの混合を制御することが必要です。この制御を行わないと、特に TCP コネクションが比較的低速の WAN リンクを介して稼働している場合に、NetBIOS ファイル転送が相互運用されている SNA トラフィックを長時間遮断する傾向が生じます。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、次のことが行えます。

- 輻輳 (ふくそう) の期間中に TCP コネクション上に転送される各プロトコルからのフレーム数の比率を設定する。
- NetBIOS フレームの最大フレーム・サイズを設定して、1 つの大きなフレームが低速 WAN リンクを占有しないようにする。

SNA および NetBIOS フレームの比率を設定するには、各プロトコルに対して 4 つの優先順位値 (クリティカル、高、中、低) の 1 つをグローバルに選択します。回線の設定時に、ルーターは DLSw バージョン 1 (RFC 1795) 回線優先メカニズムを使用して、各新規回線の優先順位を、その回線が使用するプロトコルの値にするように交渉します。回線を開始する DLSw ルーターが、使用する回線優先順位を選択します。ローカル DLSw ルーターが回線を開始する場合は、選択する回線優先順位は、構成された回線優先順位デフォルト値および回線優先順位オーバーライド値に基づきます。リモート DLSw ルーターが回線を開始する場合は、ローカル DLSw ルーターがリモート DLSw ルーターに、構成されたデフォルト値とオーバーライド値に基づく

回線優先順位を使用する必要があることを通知しますが、リモート DLSw ルーターは異なる値を選択することも可能です。いずれにせよ、確立された各回線には、その回線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) の期間中、ルーターはフレーム (転送するデータをもつ回線からの) を 4 つの待ち行列 (各回線優先順位ごとに 1 つの待ち行列) の 1 つに入れます。フレームは、各優先順位内で FIFO で待ち行列化されます。TCP 転送プロセスを進めるために、ルーターは 『優先順位別メッセージ割り当て』 パラメーターの指示に従って、各優先待ち行列からフレームを選択します。このパラメーターのデフォルト値は 4/3/2/1 で、これは、「クリティカル」優先待ち行列からは最大 4 つのメッセージを取り出し、次に「中」優先待ち行列から最大 3 つを取り出すという具合に進められます。待ち行列が空のときには、順番を飛ばされます。

1 つの大きな NetBIOS フレームが低速リンクを長時間占有するのを防止するために、『NetBIOS 最大フレーム・サイズ』 パラメーターを使用して、1 つの NetBIOS フレームのサイズの上限を決めることができます。この値は、回線の確立時に、ソース・ルーティング MAC ヘッダーの最大フレーム (LF) ビットを使用して、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・ステーションは、この LF 値を順守して、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。

構成できるデフォルト回線優先順位が 4 つあります。

- デフォルト SNA 探索トラフィック回線優先順位
- デフォルト SNA セッション・トラフィック回線優先順位
- デフォルト NetBIOS 探索トラフィック回線優先順位
- デフォルト NetBIOS セッション・トラフィック回線優先順位

種々の値を用いて、SNA と NetBIOS の探索トラフィックおよびセッション・トラフィックに異なる比率を割り当てることができます。

場合によっては、特定のトラフィックに特定の回線優先順位を割り当てたいことがあります。たとえば、特定の SNA MAC アドレスあてのトラフィックを、他のどのトラフィックよりも優先させたい場合があります。これは、回線優先順位オーバーライド (**add priority**) コマンドを使用して達成できます。このコマンドは、探索およびセッション回線優先順位を、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 に割り当てることができます。これらの回線優先順位オーバーライドは、構成された順序で評価されます。回線優先順位は、最初に一致が見つかった回線優先順位オーバーライド値に設定されます。回線優先順位オーバーライドの一致が見つからない場合、デフォルトの回線優先順位が使用されます。

DLSw の設定

以下の節では、DLSw の設定手順について説明します。

- 499ページの『DLSw 構成要件』
- 499ページの『グローバル・バッファーの設定』
- 499ページの『DLSw 用の適応ソース・ルート・ブリッジング (ASRT) の構成』

- 501ページの『DLSw 用のインターネット・プロトコル (IP) の構成』
- 501ページの『DLSw 用の OSPF の構成』
- 502ページの『SDLC インターフェースの構成』
- 503ページの『X.25 インターフェースの構成』
- 504ページの『DLSw の構成』

また、サンプル DLSw 構成をその説明も示してあります (505ページの図46を参照してください)。

DLSw 構成要件

DLSw を使用するためには、プロトコル ASRT、IP、および DLSw を構成します。さらに、表32 にリストしたプロトコルも構成することが必要になる場合があります。

表 32. DLSw 任意選択プロトコル

任意選択プロトコル	使用目的
LLC2	非デフォルト 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ため
OSPF	動的ルーティングのため、または DLSw マルチキャスト・グループを使用するため
X.25	QLLC を使用する装置に接続するため

以下の節では、これらの必須および任意選択のプロトコルの構成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

4M DRAM 2212 で DLSw を稼働する場合は、グローバル・パケット・バッファーの数を減らして、DLSw 用のメモリーを増やすことが必要になることがあります。`Config>` プロンプトで **set global** コマンドを入力し、次にグローバル・パケット・バッファーの数. を入力します。

DLSw 用の適応ソース・ルート・ブリッジング (ASRT) の構成

DLSw は、接続されたエンド・ステーションからはブリッジのように見えるので、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、以下のステップで行います。

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** コマンドを使用します。
2. **enable bridge** コマンドを使用して、ルーター上のブリッジングを使用可能にする。各 DLSw 内の各ブリッジは、固有なブリッジ・アドレスを持っていることが必要です。
3. **add port** コマンドを使用して、ブリッジ・ポートを追加する。このディスプレイでは、インターフェース番号とポート番号の入力を求められます。
   - ***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 を介して DLSw を実行する場合は、指定されたブリッジ・ポート上にはソース・ルート・ブリッジングのみが存在するようにする必要があります。つまり、透過ブリッジングを使用不可にすることが必要です。これは **disable transparent** コマンドを使用して行います。その後で **enable source routing** コマンドを発行して、ブリッジ・ポートのソース・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***

  必ず、透過ブリッジングをブリッジ・ポート上で使用可能にします。**enable transparent** コマンドを発行します。

4. ***並行ブリッジングと DLSw*** 用にルーターを構成する場合は、次のようにします。

   DLSw を使用する予定の 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動作、プラス DLSw を介したパケット転送を行う場合、この作業が不可欠です。これが行われていない場合、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ることになります。この概念は、DLSw のルーティングと並行して DLSw パケットが転送される (ブリッジされる) ことを防止することです。

   SAP フィルターを作成するには、Config ASRT> プロンプトで **add protocol-filter dsap 4** コマンドを入力します。

   このコマンドの他に、それを適用するブリッジ・ポートを指定する必要があります。このコマンドは、DLSw 用に指定されているポートを除いて、ルーターは DSAP が 4 のすべてのトラフィックをフィルターに掛けるように指示しています。(ここでは、SAP 4 が DLSw トラフィック用に選択されているものと想定しています。この選択は DLSw の構成時にユーザーが行います。)

5. **enable dls** コマンドを使用して、DLSw を使用可能にする。これは、ユーザーが指定したブリッジ・ポート上の DLSw プロトコルを使用可能にします。

6. ASRT 構成を検証する。これは必須の作業ではありませんが、先に進む前にブリッジ構成をチェックしておくようにします。**list bridge** コマンドを使用して、 ASRT プロトコルの構成を検証します。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) の構成

ローカル DLSw ルーターが他の DLSw ピアへの TCP コネクションを形成できるようにするには、IP を構成することが必要です。これは、次の手順で行います。

1. Config> プロンプトから **protocol ip** コマンドを発行して IP 構成プロセスに入る。
2. IP アドレスをハードウェア・インターフェースに割り当てる。**add address** コマンドを使用して、IP アドレスを他の DLSw ピアに接続するのに使用するハードウェア・インターフェースに割り当てます。
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 はネットワーク・オーバーヘッドが RIP より小さいので、OSPF を使用することお勧めします。
   - OSPF を使用可能にする場合: 『DLSw 用の OSPF の構成』を参照してください。
   - RIP を使用可能にする場合: 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。**set internal-ip-address** コマンドを使用して、特定のインターフェースではなく、ルーター全体に属するアドレスを設定します。内部 IP アドレスは、ルーターが他の DLSw ピアへの TCP コネクションを確立するときに使用します。
   - RIP を使用する場合は、インターフェース・アドレスの 1 つを internal-ip-address として選択します。
   - OSPF を使用する場合は、ユーザーのネットワークで使用する任意のサブネットから、異なるサブネットを持つアドレスを選択します。

DLSw 用の OSPF の構成

OSPF をルーティング・プロトコルとして使用したい場合は、これを次のように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** コマンドを使用します。
2. *OSPF アドレスをハードウェア・インターフェースに割り当てる*。**set interface** コマンドを使用して、 OSPF アドレスを他の DLSw ピアに接続するのに使用するハードウェア・インターフェースに割り当てます。
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 のすべてのデフォルト値で、正常に動作します。add TCP neighbor を使用して TCP コネクションを明示的に定義する必要はなく、**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 インターフェースの構成

SDLC 構成コマンドを使用すると、DLSw 構成プロセスの一部として、SDLC インターフェース構成を作成または変更することができます。

注: SDLC が V.25bis の encapsulator である場合、物理リンク・パラメーターは V.25bis レベルで構成しなければならないので、SDLC レベルで設定することはできません。この場合、以下の SDLC パラメーターは構成する必要がありません。

- Role - これは 1 次である必要があります。
- Group - グループ・ポーリング・アドレスを設定することはできません。
- Type - これはポイント・ポイントである必要があります。
- Duplex
- Idle state
- Clocking
- Speed
- Cable
- Encoding
- Inter-frame delay

DLSw を介する SDLC をサポートしたい場合は、SDLC リンクを構成する必要があります。この節では、SDLC 構成コンソールへのアクセス方法を説明し、SDLC 関連のコマンドについて説明します。

直接接続された SDLC 装置が存在する場合は、次の手順で SDLC プロトコルを構成します。

1. SDLC へのデータ・リンクを設定する。`Config>` プロンプトで **set data-link SDLC** コマンドを使用して、シリアル・インターフェースのデータ・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に求められます。
2. SDLC 構成プロセスに入る。`Config>` プロンプトで **network** コマンドを使用して SDLC 構成プロセスに入ります。インターフェース番号を入力するように求められます。
3. DLSw の構成時にユーザーが SDLC ステーションを追加すると、ソフトウェアはそのステーションに次のデフォルト値を割り当てます。
   - Maximum BTU は、インターフェースによって許容される最大値です。
   - Tx and Rx Windows は、Mod 8 の場合は 7 で、Mod 128 の場合は 127 です。
4. リンクの役割は、デフォルトでは 1 次になります。必要な場合には、**set link role** コマンドを使用して、リンクの役割を 2 次または交渉可能に変更します。
5. リンクの 2 次ステーションに、グループ・ポーリングを設定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・リストに含めます。
6. リンク・クロック・ソースを設定する (任意選択)。モデム・エリミネーターを使用せずに SDLC 装置に直接接続したい場合は、DTE ケーブルとコマンド **set link clocking internal** を使用します。

7. リンク速度を設定する (任意選択)。内部クロックを使用している場合は **set link speed** コマンドを使用して、この伝送路のクロック速度を選択します。

   注: PC からの接続に SDLC を使用する場合は、符号化 (NRZ/NRZI) および二重 (full/half) も、PC の構成に一致するように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。**list link** コマンドを使用して SDLC インターフェース構成を検証します。

X.25 インターフェースの構成

DLSw の QLLC 装置に対するサポートを使用する場合は、X.25 インターフェースを構成します。以下の手順に従ってください。

1. インターフェースを X.25 として設定する。`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に求められます。
2. `Config>` プロンプトで **net** コマンドを使用して X.25 構成プロセスに入る。インターフェース番号を入力するように求められ、それ以降は `X.25 Config>` プロンプトでコマンドを入力することになります。
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の DTE アドレスを定義する。
4. **set pvc** および **set svc** コマンドを使用して、PVC に使用する論理チャネル番号の範囲、および SVC で利用可能な論理チャネル番号の範囲を定義する。DLSw 構成に定義する PVC はすべて、ここで定義された PVC 範囲内のチャネル番号を持っていることが必要です。SVC の場合、コールの着信および発信に利用可能なチャネル数が、DLSw で予想される発信または応答の同時コール数に対応できる十分な数であることを確認する必要があります。
5. **add protocol** コマンドを使用して、このインターフェースの X.25 上で稼働するプロトコルとして ″dls″ を追加する。X.25 はこれが QLLC サポートを意味することを理解し、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 動作パラメーター値を入力するように促されます。
6. **add pvc** コマンドを使用して、指定された PVC 論理チャネル番号と DLSw プロトコルを関連付ける。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 構成で **add qllc station** コマンドを使用した各 PVC) について、この作業を行う必要があります。論理チャネル番号は、このステーションの DLSw 構成をこの X.25 PVC 定義と一致させるためのかぎになります。
7. **add address** コマンドを使用して、DLSw 構成に定義されているすべての PVC および SVC の X.25 DTE アドレスのリストを作成する。DLSw は PVC の DTE アドレスは使用しませんが、これらは X.25 構成内で必須であることに注意してください。動的に DLSw に呼び込むことができる、DLSw に構成されていない QLLC エンド・ステーションの DTE アドレスは、追加する必要はありません。
8. X.25 ネットワークに接続するのに必要な物理レイヤー特性またはナショナル・パーソナリティー特性を設定する。X.25 構成可能パラメーターの説明については、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*の X.25 ネットワーク・インターフェースの構成に関する章を参照してください。

DLSw の構成

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、種々の装置のインターフェース番号をリストします。

DLSw プロトコルを構成するには、次の手順で行います。

1. Config> プロンプトで **protocol dls** コマンドを入力する。これにより、DLSw config> プロンプトが起動します。
2. DLSw config> プロンプトで、**enable dls** コマンドを入力して、ルーターの DLSw を使用可能にする。
3. **set srb** コマンドを入力して、DLS ルーターの 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。

   この SRB セグメント番号は、同じ LAN に接続されたすべての DLSw ルーターで同一であることが必要であり、そのソース・ルート・ブリッジ・ドメイン内でユニークでなければなりません。ブリッジは LAN 上でフレームを送信するときに、ルーティング情報フィールド (RIF) でこの番号を使用します。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 で交換する各 SAP に対して **open-sap** コマンドを入力する。ルーターは、インターフェース番号を入力するように求めます。一般的に使用される SNA SAP (4、8、および C) をオープンする場合は、SNA を指定します。最小限として SAP 0 および 4 をオープンしてください。NetBIOS SAP をオープンする場合は、 NB または F0 を指定します。LNM SAP をオープンする場合は、LNM を指定するか、または最小限として 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 アドレスを追加する。構成されていないピアからのコネクションをルーターが受け入れるようにしたい場合は、**enable-dynamic neighbor** コマンドを 使用します。TCP コネクションも、マルチキャスト OSPF と **join-group** コマンド を使用して確立することができます。

   注: ルーターは、そのピア・ルーターが DLSw を稼働する MAS ベースのプラットフォームである場合に**のみ**、グループに参加することができます。あるグループに対して 1 つの DLSw ルーターを構成した場合、そのグループ内のすべての DLSw ルーター上の 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 をサポートする場合は、 **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 をサポートする場合は、**add qllc station** コマンドを使用して QLLC リンクを追加します。

   あるいは、動的 SVC をサポートしたい場合は、**enable qllc callin** コマンドを使用して X.25 インターフェースのコールインを使用可能にし、**add qllc destination** コマンドを使用して DLSw あて先を定義します。

サンプル DLSw 構成

以下のサンプル DLSw 構成では、装置は他のプロトコルまたはデータ・リンク用には構成されていないものと想定しています。そのため、 Config> ではなく Config (only)> プロンプトで開始しています。

サンプル図

この例は、図46 に示されている情報に基づいています。

構成される DLSw ルーター (図の R1) は、その DLSw ピア (R2) への 1 つの LLC コネクションと、1 つの SDLC コネクションをサポートしています。2 つのルーター間の TCP コネクションは、シリアル・ラインを介しています。

R1 を DLSw 用に構成するためには、図に示されているすべての情報が必要です。この情報は、次のとおりです。

- R1 および R2 の内部 IP アドレス
- ルーター間の TCP コネクション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たインターフェース番号、および TCP コネクションに使用す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

例には、構成手順の中でこの情報を提供する個所が示されています。

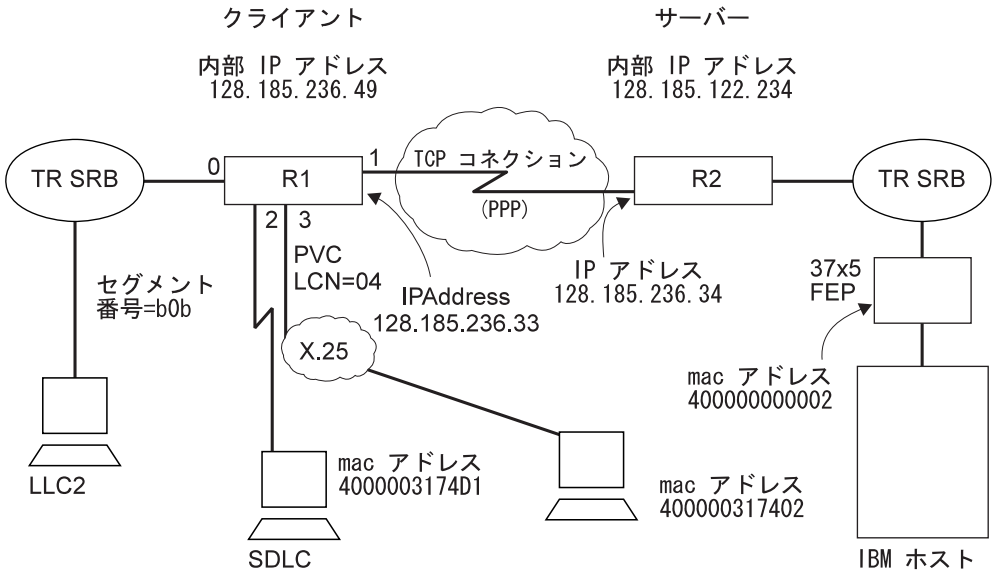


図 46. DLSw 構成のサンプル図

サンプル構成コマンド

この節では、以下の例を示します。

- 『ステップ 1: 装置の追加』
- 510ページの『ステップ 2: プロトコルの構成』
- 513ページの『ステップ 3: プロトコル・フィルターの実現』
- 514ページの『ステップ 4: DLSw の構成』

ステップ 1: 装置の追加

追加する装置は、トークンリング、SDLC、または QLLC です。イーサネットを透過型ブリッジ・ポートとして追加することもできます。例として示すために、このサンプル DLSw 構成では SDLC、LLC、および QLLC をサポートします。実際の構成では、これらのデータ・リンクの 1 つをサポートするだけで済みます。

SDLC および QLLC の場合、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) もサポートするので、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、それらが適切なルーター・インターフェースに割り当てられたことを確認することができます。

config> プロンプトで **list device** コマンドを入力すると、構成済みの装置およびそれらのインターフェース番号のリストが表示されます。

```
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
```

この例の **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 に割り当てられたことを示しています。

1. ***トークンリング装置の追加***

   トークンリングの設定を構成します。通常は UTP ケーブルでは 16 Mbps が使用されるので、ここでもそれを使用します。以下の手順に示されている **list** コマンドは、この手順で (あるいは、ルーターの構成時の他の時点でも) 必ず使う必要があるというわけではありません。

   ```
   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 インターフェースの構成。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 用に選択されたデータ・リンクは PPP です。これがデータ・リンクのデフォルト選択です。その他の可能な選択として、フレーム・リレーと X.25 があります。

```
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、シリアル・インターフェースの回線速度とクロック・タイプを設定します (必要な場合)。

```
PPP Config>set hdlc clock internal
Must also the line speed to a valid value
Line speed (2400 to 2048000) [0]? 56000
```

回線速度とクロック・タイプを設定した後で、次のように **list hdlc** コマンドを使用して構成をチェック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 装置の追加***

SDLC をサポートするように DLSw を構成している場合、次のステップは SDLC を構成するためのものです。ほとんどの構成項目は、変更する必要がありません。

SDLC 構成にアクセスするには、**network** コマンドと 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ほとんどは、ハードウェアに関連するものです。

この例は **list link** コマンドから始まっています。**list** コマンドは、構成を変更するものではなく、現在 SDLC リンクに関連付けられている値をユーザーに示すためのものです。

IBM 2212 Access Utility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
Modulo        8                Frame Size   2048

Timers:    XID/TEST response:  2.0 sec
           SNRM response:      2.0 sec
           Poll response:      0.5 sec
           Inter-poll delay:   0.2 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ときと同様に、クロック・タイプと回線速度をSDLC 装置用に変更する必要があります。外部モデム・エリミネーターを使用している場合は、その必要はありません。

```
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 装置の追加***

505ページの図46 に示されている QLLC ステーションをサポートするためには、インターフェース 3 を X.25 として構成し、指定の PVC 上の DLSw に対して QLLC サポートを構成する必要があります。次の例は、非 X.25 シリアル・インターフェースを使用するスクラッチから始まっています。以下のサンプル構成は、PVC 上の DLSw の QLLC サポートを示しています。ここでは、次のことを行う必要があります。

   a. list device コマンドを使用して、構成されたインターフェースのリストを入手する。
   b. X.25 を構成したいシリアル・インターフェースを選択する。
   c. インターフェース番号を記録し、set data-link コマンドでそれを指定して、インターフェース上の X.25 を構成する。

   例では、X.25 はインターフェース 1 に構成されています。

```
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』 の PVC に使用されている DTE アドレス 『4444』 は、DLSw では使用されず、X.25 のみが構成情報を相関させるために使用します。同様に、DLSw プロトコル・アドレス (この例では 『Chicago』) も DLSw には何も意味を持たず、単に DLSw が使用できる種々の DTE アドレスへの参照を容易にするためだけのものです。X.25 上で実行されている他のプロトコルとは異なり、DLSw アドレス変換は X.25 の構成ではなく、DLSw の構成の一部として定義されます。

ステップ 2: プロトコルの構成

装置の構成が完了したら、必要なプロトコルを構成することが必要です。DLSw 上で実行するために、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 の構成***

   この例は、IP の構成から始まっています。

```
Config>protocol ip
Internet protocol user configuration
```

   list all コマンドは、デフォルト IP 構成を表示します。

```
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]
```

   この例は、最小限の IP 構成の作成を示しています。この重要なプロトコルの詳細については、227ページの『第13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、それを IP トラフィックを伝送するインターフェースに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、いま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。IP 用に選択された

ルーティング・プロトコルが RIP の場合、内部 IP アドレスがインターフェースに構成された IP アドレスと一致していることが必要です。

```
IP config>set internal-ip-address 128.185.236.49
```

- この後 **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の構成***

この構成では RIP ではなく OSPF が使用されています。これらのルーティング・プロトコルはどちらを使用しても構いませんが、 RIP を選択した場合は DLSw グループ機能は使用できません。

最初に **list** コマンドを入力します。このコマンドは、デフォルト OSPF 構成を表示します。DLSw を実行するためには、この構成を変更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 グループ機能を実現しているので、次のようにマルチキャスト OSPF を使用可能にすることが必要です。

```
OSPF Config>enable multicast
Inter-area multicasting enabled? [No]:
```

- OSPF を使用するすべての物理 IP インターフェースに対して **set interface** コマンドを発行します。この例では、バックボーンが OSPF エリア (0.0.0.0) であるものと想定しています。この時点では、IP インターフェースは 1 つしか定義されていません。

```
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>
```

- 次の例は、構成後の OSPF ディスプレイを示しています。構成の中の何が変更されたかを見るために、このディスプレイを、前に示したデフォルト OSPF 構成のディスプレイと比較してみてください。

```
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 の構成***

   ルーターをソース・ルート・ブリッジング用に構成し、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** コマンドを使用すると、ポートはデフォルトの透過ブリッジングになっていることが示されます。透過ブリッジングは、接続装置がイーサネットの場合に必要なものですが、装置がトークンリングの場合は機能しません。ポート番号 1 はインターフェース 0 上のポート 1 であることに注意してください。言い換えれば、ポート 1 は トークンリング用に設定された物理インターフェース (505ページの図46 を参照) の論理ブリッジ・ポートです。

```
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) を介して稼働するためには、 DLSw には SRB (ソース・ルート・ブリッジング) が必要です。この場合、最初に行うことは、このポートの透過ブリッジングを使用不可にすることです。

```
ASRT config>disable transparent
Port Number [1]?

ASRT config>enable source-routing
```

- ここで、ポートにセグメント番号を割り当てます。セグメント番号を割り当てる必要があるのは、トークンリングのような ソース・ルート・ブリッジ装置を構成する場合だけです。この例では (505ページの図46 を参照) **b0b** が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・ポート上の DLSw を使用可能にします。

```
ASRT config>enable dls
```

ここまでのステップが完了したら、次のように DLSw を使用可能にします。ブリッジ構成を表示してみると、ASRT が正しく構成されたかどうかを確認できます。

```
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・フィルターの実現

これは重要なステップですが、DLSw の構成時におろそかされることがしばしばあります。

SAP (サービス・アクセス・ポイント) 04、08、0C 上のトラフィックの転送には、ブリッジングではなく DLSw が使用されるので、ブリッジング設定に特別なプロトコル・フィルターを追加する必要があります。

注: ここで説明するフィルターを実現する必要があるのは、DLSw に加えて WAN リンク経由のブリッジングが構成されている場合だけです。この例の場合は、これには該当しません。この例では、参考のために、SAP フィルターを作成する手順を示してあります。

フィルターの目的は、DLSw のみが扱う必要のあるパケットを、他のポート上のブリッジが転送するのを防止することです。DLSw とブリッジング機能が同じパケットを転送するのは、適切とは言えません。このようになると、競争状態が起こり、ネットワークの性能低下の原因になります。

次のコマンドは、あて先 SAP が 4 のすべてのパケットに適用されるフィルターを作成します。後で **list** コマンドを発行すると、フィルターの特性が表示されます。

```
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設定されたら、ASRT 構成を終了します。

```
ASRT config>exit
```

ステップ 4: DLSw の構成

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、デフォルトを表示します。

```
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。セグメント番号は、505 ページの図46 に示されるようにトークンリング装置を参照します。

```
DLSw config>enable dls
DLSw config>set srb 020
```

DLSw グループと静的セッションの構成: この例は、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 の構成では、これは必須の要件ではありませんが、近隣 DLSw ルーターにコネクトアウトするために、いずれか一方 (DLSw グループまたは構成された TCP セッション) を定義する必要があります。未構成ルーターがコネクトインするようにしたい場合は **enable dynamic-neighbors** コマンドを発行します。

Join-Group コマンド: **join-group** コマンドは、DLSw グループを作成するのに使用します。各グループ・メンバーを、クライアント/サーバーまたはピアとして指定することができます。ピアがデフォルトです。

ここでは、R1 (505ページの図46 を参照) のために **join-group** コマンドが実行され、この DLSw ルーターをグループ 1 のクライアントとして指定しています。このグループに結合するためには、R2 をサーバーとして追加することが必要なので、R2 上で **join-group** コマンドを発行します。

```
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** コマンドは、構成された DLSw 近隣を明示的に定義するのに使用します。ここで追加されている近隣 DLSw IP アドレスは、ピア DLSw ルーター (505ページの図46 における R2) の内部 IP アドレスです。R2 が R1 の近隣 IP アドレスを持つように構成したり、 R2 が動的近隣を受け入れるように構成したりすることもできます。

```
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・ステーションの定義: 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・ステーションの定義: 各 PVC および構成された SVC のアドレス・マッピングを定義します。この構成例では、 1 つの QLLC 装置が PVC に接続されています。

```
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) のオープン: 次に行うことは、各ブリッジング・インターフェース上のサービス・アクセス・ポイント (SAP) をオープンすることです。

SAP 番号 0、4、8、および C は、一般的に使用される SNA SAP です。これらの SAP をすべてオープンする場合は、次のように **open-sap** コマンドで SNA オプションを使用します。NetBIOS 用の SAP をオープンする場合は、NB オプションを選択します。また、希望であれば、16 進数を入力して SAP を個別に入力することも可能です。

```
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、構成後の DLSw ディスプレイです。

```
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 の構成が完了したら、DLSw 構成を終了し、ルーターをリスタートします。

```
DLSw config>exit
Config (only)>restart
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

第25章 DLSw の構成および監視

この章では、データ・リンク交換プロトコルを構成し、監視する方法について説明します。本章には、以下の節が含まれています。

- 『DLSw 構成環境へのアクセス』
- 『構成前の要件』
- 『DLSw 構成コマンド』
- 550ページの『DLSw 監視環境へのアクセス』
- 550ページの『DLSw 監視コマンド』

DLSw 構成環境へのアクセス

CONFIG プロセスを使用して、ルーターの構成を変更します。新規の構成は、装置をリスタートすると有効になります。

構成プロセスに入るには、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、次の例に示されているような CONFIG> プロンプトが表示されます。

```
MOS Operator Control

     * talk 6
     Gateway user configuration

     CONFIG>
```

CONFIG> プロンプトがすぐに表示されない場合は、**Enter** キーをもう一度押してください。

DLSw 構成コマンドはすべて DLS 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 **protocol DLSw** コマンドを、次のように入力します。

```
     Config>protocol dls
     DLSw protocol user configuration
     DLSw config>
```

構成前の要件

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、各種の装置のインターフェース番号のリストを表示します。構成コマンドの詳しい説明が必要な場合は、本章の構成コマンドの説明個所を参照してください。

DLSw 構成コマンド

この節では、DLSw 構成コマンドの要約を示し、個々のコマンドについて説明します。DLSw 構成コマンドを使用すると、DLSw 構成を作成または変更することができます。520ページの表33 は、各コマンドの簡単な要約を示しています。DLSw 構成コマンドはすべて DLSw Config> プロンプトに従って入力します。コマンドとそのパラメーターのデフォルト値は、プロンプトの直後に大括弧に入れて表示されています。

DLSw 構成コマンド (Talk 6)

ルーターの構成に加えた変更は、即時には有効にはならず、ルーターがリスタートされたときに、ルーターの SRAM 構成の一部になります。

表 33. DLSw 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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 ステーションまたはあて先、キャッシュ・エントリー、MAC アドレス・リスト・エントリー、回線優先順位オーバーライド、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、BAN 構成コマンドを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 SAP を使用して、LLC をサポートするインターフェース上の通信に使用します。
Delete	構成済みの SDLC リンク・ステーション、TCP 接続、QLLC ステーションまたはあて先、キャッシュ・エントリー、MAC アドレス・リスト・エントリー、回線優先順位オーバーライド、または MAC キャッシュ・エクスプローラー・オーバーライドを削除します。
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 ステーションまたはインターフェース、あるい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可にします。
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 ステーションまた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 優先順位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ることができるようにします。
Leave-Group	指定された DLSw グループからルーターを除去します。
List	SDLC リンク・ステーション、SAP、回線優先順位、 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・エントリー、または MAC アドレス・リスト・エントリーの情報を表示します。このコマンドは TCP コネクションに関する詳細情報も提供します。
NetBIOS	NetBIOS 構成プロンプトへのアクセスを提供します。
Open-SAP	DLSw が指定の SAP を介してデータを転送できるようにします。DLSw は SAP を使用して、LLC をサポートするインターフェース上で通信を行います。
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、メモリー割り当て、プロトコル・タイマー、回線優先順位、動的近隣用パラメーター、QLLC 動作用のパラメーター、および MAC アドレス・リストに関連する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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、SDLC リンク・ステーション、 TCP 近隣 IP アドレス、QLLC ステーションまたはあて先、キャッシュ・エントリー、MAC アドレス・リスト・エントリー、回線優先順位オーバーライド、または MAC キャッシュ・エクスプローラー・オーバーライドを構成するのに使用します。

構文:

add cache-entry

explorer-override

mac-list

priority

qllc...

sdlc

tcp

cache-entry

構成された MAC キャッシュ・エントリーを追加します。このキャッシュ・エントリーは、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・エントリーを追加することによって、1 つの MAC アドレス を複数の DLSw ピアにマップできます。

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・エントリーを追加します。このオーバーライドにより、MAC アドレスの集合は、異なる MAC キャッシュ特性およびエクスプローラー・フロー特性をもつことができます。MAC キャッシュ・エントリーが作成されるときに、エクスプローラー・オーバーライドのリストが、構成された順に探索されます。一致するものが見つかると、最初の一致エクスプローラー・オーバーライドからの MAC キャッシュおよびエクスプローラー関連パラメーターが使用されます。一致するものが見つからなかった場合には、DLSw グローバル MAC キャッシュおよびエクスプローラー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 and MAC address mask

これら 2 つのフィールドが結合されると、MAC アドレスの集合を表します。指定された値とマスクをもつ構成済みの 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 アドレスに使用するかどうかを判別するために、以下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

未使用の DLSw エントリーを保持する期間を指定します。データベース・エントリーは、あて先 MAC アドレスを、それらに到達可能な DLSw ピアの集合にマップします。

ゼロの値は、このデータベース内のエントリーはエージング (経時処理) されないことを示します。これはダイヤル・インターフェースを介して近隣 TCP コネクションを稼働している場合には便利ですが、さまざまな他の DLSw 機能を使用不可にするので、一般的には推奨できません。

Max wait timer ICANREACH

前に送信した CANUREACH に対する ICANREACH レスポンスを待つ時間を指定します。

Neighbor priority wait timer

探索時に、近隣を選択する前に待つ時間の長さを指定します。これにより、ICANREACH メッセージに最初に応答しなくても高い優先順位の近隣が選択されるようにすることができます。

値ゼロは、近隣優先順位機能を使用しないことを指示します。MAC アドレスについての、キャッシュに入れられた DLSw ピア情報はありません。CANREACH は常に送信され、(優先順位に関係なく) 最初に ICANREACH を送信した DLSw ピアが使用されます。

Delay sending TEST response

MAC アドレスの探索から TEST レスポンスを送信するまでに待つ時間の長さ。これは、DLSw ピアを介して同じ MAC アドレスに到着できる、同じブリッジ LAN 上に DLSw 2212 が 2 つある場合に役立ちます。一方の DLSw 2212 を優先する場合、優先しない DLSw 2212 でTEST レスポンスを遅らせることができます。

Forwarding explorers

エクスプローラーをすべての該当する DLSw ピアに転送するか、ローカル TCP 接続上のものだけに転送する、またはまったく転送しないかを指定します。

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・オーバーライド照合が使用されるので、MAC キャッシュ・エクスプローラー・オーバーライド・エントリーを構成する順序は重要です。このフィールドは、現行のオーバーライド・リストの中の、この新規エントリーを挿入する位置を指定します。**list explorer-override** コマンドを使用すれば、現行のエクスプローラー・オーバーライド・リストを見ることができます。このフィールドがゼロの値の場合は、新規エントリーを現行リストの末尾に追加することを指定します。

mac-list

ローカル MAC アドレス・リスト・エントリーを追加します。追加されたすべてのローカル MAC アドレス・リスト・エントリーが、ローカル MAC アドレス・リストを構成します。このローカル MAC アドレス・リストが各 DLSw ピアに送信され、この DLSw を使用して到達可能な 1 組の MAC アドレスが示されます。

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

この 2 つのフィールドを組み合わせて、この DLSw を使用して到達可能な 1 組の MAC アドレスを表します。フレームがピア DLSw で受信されると、この 2 つのフィールドは、 次のような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

回線優先順位エントリーを追加します。DLSw セッションを確立するときに、回線優先順位オーバーライドのリストが、構成された順序で検索されます。発信元 SAP 範囲と発信元 MAC アドレス範囲、およびあて先 SAP 範囲とあて先 MAC アドレス範囲に一致が見つかった場合、一致している回線優先順位オーバーライド・エントリーのセッションと探索優先順位が使用されます。どの回線優先順位オーバーライド・エントリーにも一致しなかった場合には、回線優先順位のデフォルト値が使用されます。

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

この 2 つのフィールドを組み合わせて、この回線優先順位オーバーライドに割り当てられた発信元 SAP の範囲を表します。発信元 SAP の値は重要でない場合は、全範囲の発信元 SAP 値 (下限発信元値 = 0、上限発信元値 = fe) を指定します。

Lower source MAC address

Upper source MAC address

この 2 つのフィールドを組み合わせて、この回線優先順位オーバーライド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 アドレスの値は重要でない場合は、全範囲の発信元 MAC

アドレス値 (下限発信元 MAC アドレス = 000000000000、上限発信元 MAC アドレス = ffffffffffff) を指定します。

Lower destination sap value

Upper destination sap value
この 2 つのフィールドを組み合わせて、この回線優先順位オーバーライドに割り当てられたあて先 SAP の範囲を表します。あて先 SAP の値は重要でない場合は、全範囲のあて先 SAP 値 (下限あて先 SAP 値 = 0、上限あて先 SAP 値 = fe) を指定します。

Lower destination MAC address

Upper destination MAC address
この 2 つのフィールドを組み合わせて、この回線優先順位オーバーライドに割り当てられたあて先 MAC アドレスの範囲を表します。あて先 MAC アドレスの値は重要でない場合は、全範囲のあて先 MAC アドレス値 (下限あて先 MAC アドレス = 000000000000、上限あて先 MAC アドレス = ffffffffffff) を指定します。

Priority for session traffic
この回線優先順位オーバーライド・エントリーの発信元 SAP、発信元 MAC アドレス、あて先 SAP、およびあて先 MAC アドレスの範囲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回線優先順位

Priority for explorer traffic
この回線優先順位オーバーライド・エントリーの発信元 SAP、発信元 MAC アドレス、あて先 SAP、およびあて先 MAC アドレスの範囲に一致するすべての探索トラフィックに割り当てる回線優先順位。

Position in circuit priority override list to insert new entry
最初に一致した回線優先順位オーバーライド照合が使用されるので、回線優先順位オーバーライド・エントリーを構成する順序は重要です。このフィールドは、現行の回線優先順位オーバーライド・リストの中の、この新規エントリーを挿入する位置を指定します。**list priority** コマンドを使用すれば、現行の回線優先順位オーバーライド・リストを見ることができます。このフィールドがゼロの値の場合は、新規エントリーを現行リストの末尾に追加することを指定します。

qllc X.25 ネットワーク上の QLLC ステーションに対するサポート、または QLLC ステーションの DLSw あて先のサポートを追加します。QLLC ステーションは、X.25 インターフェースを介してルーターに接続する QLLC 装置を表します。QLLC あて先は、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、任意のサポートされる DLC タイプを介して近隣 DLSw ルーターに接続され、QLLC 装置自体ではない場合もしばしばあります。

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 Call_Request パケット内のコール・ユーザー・データ・フィールドのバイト 4〜11 によって照合される英数字文字列。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ます。

重要: QLLC あて先レコードが ″ANYCALL″ を使って構成される場合、すべてのコールが DLSw によって受け入れられます (DTE アドレスまたはコネクション ID とは無関係に)。すべての着信コールを受け入れるときは、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たセッションのターゲットとして使用される MAC アドレス (Call_Request パケットが上記のコネクション ID に一致した場合)。

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 #

QLLC 装置をルーターに接続する X.25 インターフェースの数

PVC or SVC

QLLC 装置が接続されるバーチャル・サーキット (パーマネントまたはスイッチド) のタイプ

Logical channel number

PVC の場合、QLLC ステーションが加入している X.25 チャネル番号。動的に割り当てられるチャネル番号を使用する SVC には、このフィールドは適用されません。

DTE address

SVC の場合、QLLC ステーションを X.25 ネットワークに識別する ″電話番号″。これは、ルーターによって発信されたコールのコールされた相手側のアドレスであり、QLLC ステーションからのコールのコールする側のアドレスです。固定された論理チャネル番号によってユニークに識別できる PVC には、 このフィールドは適用されません。

Source MAC address

この QLLC ステーションを DLSw ネットワークの残りに識別する媒

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た DLSw セッションの発信元アドレスであり、DLSw ネットワーク内の他の装置によって開始されたセッションのターゲット・アドレスです。

このアドレスは、各ステーションごとに必要であり、ルーターに構成された QLLC および SDLC 装置のすべての発信元 MAC アドレス間でユニークでなければなりません。高信頼性で動作するためには、DLSw ネットワーク内のすべてのエンド・ステーション MAC アドレス間でもユニークであることが必要です。デフォルト値は、ネットワーク内でユニークである確率の高い値に設定されています。これを含めたすべての DLSw MAC アドレスは、非標準 (トークンリング) ビット順序フォーマットです。

Source SAP

発信元 MAC アドレスと対になるサービス・アクセス・ポイント・アドレス。これは同じ方法で使用されます。

Destination MAC address

QLLC 装置を接続する 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 装置が正常に接続されると、速やかにこのターゲット・アドレスへのセッションの開始を試みます。 SVC の場合、DLSw は QLLC 装置が着信コールを受信すると、速やかにこのターゲット・アドレスへのセッションの開始を試みます。

このアドレスは必須ではありません。これを構成しなかった場合、QLLC ステーションは DLSw セッションのターゲットにのみなることができ、開始側になることはできません。

Destination SAP

あて先 MAC アドレスと対になるサービス・アクセス・ポイント・アドレス。これは同じ方法で使用されます。 DLSw が DLSw セッションのターゲットとして使用するためには、あて先 MAC アドレスとあて先 SAP の両方とも非ゼロであることが必要です。

PU type

QLLC ステーションの SNA 物理装置タイプ。これは次の値のいずれかです。

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あります。

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。これらは通常、別の NCP への中間ネットワーク・ノード (INN) モードで IBM のNCP ソフトウェアを稼働し、PU 2 装置への NCP 境界機能接続には使用されません。

5 DLSw ネットワーク内の PU 2.0 への境界機能接続を行う、ホストまたはフロントエンド・プロセッサー搭載ホスト (たとえば、NCP 搭載 37xx)。ホストが DLSw ネットワーク内の T2.1 装置への接続を行う場合は、ホスト自体も T2.1 装置 (つ

まり、PU タイプ=2、XID0 block/id num=0) として構成することが望まれます (ただし、これは必須条件ではありません)。

XID0 block num

ルーターが QLLC ステーションの代わりに 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 の場合にのみ適用され、入力を促されます。T2.1 装置および XID_null ポーリングに対して自分で応答できる PU 2.0 装置の場合は、このフィールドは任意選択であり、ゼロのままにしておくべきです。確信がない場合は、PU2.0 QLLC 装置はすべてこのフィールドに記入し、T2.1 装置はすべてゼロのままにするのが最も安全です。非ゼロの場合、その値はリンク・ステーションの IBM NCP 交換回線大ノード構成内の対応する PU アドレス・フィールドに一致していることが必要です。

XID0 id num

XID0 ブロック番号フィールドと一緒に使用される XID 識別子番号。これは、同じ目的に使用され、同じ状況で必要とされます。

sdlc 指定の SDLC シリアル・インターフェースの構成に SDLC リンク・ステーションを追加するために、特別に 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 1 回使用します。

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 #

SDLC 装置をルーターに接続する SDLC インターフェースの番号

SDLC Address

接続するリンク・ステーションの SDLC アドレスで、 01 ～ FE または 『sw』。『Sw』 は、これがスイッチド SDLC コールイン・サーキットであることを意味します。

Source MAC address

この SDLC PU 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た SDLC および QLLC ステーション間でユニークでなければならず、またすべての LAN、SDLC、および QLLC間でユニークであることが必要です。

Source SAP in hex

発信元 MAC アドレスと合わせて、DLSw ドメイン内の SDLC エンド・ステーションを識別します。

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、非標準ビット順序 (トークンリング) フォーマットです。これは、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も同じです。その場合は、ASRT 監視 **flip** コマンドを使用して MAC アドレスを反転させてください。

注: これがスイッチド SDLC コールイン・サーキットである場合、あて先アドレスは 0 の値をもつことができません (『sw』 によって SDLC アドレスとして示されます)。

Destination SAP in hex

リンク・ステーションが起動されたときに自動的に接続を試みる場合に使用される SAP を定義します。この SAP が 0 のときは、そのリンク・ステーションは受動 (passive) モードにあり、回線の確立を開始しません。この場合は、あて先 MAC アドレスは無視されます。

注: これがスイッチド SDLC コールイン・サーキットである場合、あて先 SAP は 0 の値をもつことができません (『sw』 によって SDLC アドレスとして示されます)。

PU type

SDLC ステーションの SNA 物理装置タイプ。これは次の値のいずれかです。

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。通常、これらは別の NCP への中間ネットワーク・ノード (INN) モードで IBM のNCP ソフトウェアを稼働し、PU 2 装置への NCP 境界機能接続には使用されません。

5 DLSw ネットワーク内の PU 2.0 への境界機能接続を行う、フロントエンド・プロセッサー搭載または非搭載のホスト (たとえば、NCP 搭載 37xx)。ホストが DLSw ネットワーク内の T2.1 装置への接続を行う場合は、ホスト自体も T2.1 装置 (つまり、PU タイプ=2、XID0 block/id num=0) として構成する必要があります。

注: スイッチド SDLC コールイン・サーキットの場合は、このパラメーターを設定できません。PU タイプは 2.0 と想定します。

XID0 block num

ルーターが SDLC ステーションの代わりに 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 のときにのみ適用され、入力を促されます。これは任意選択であり、T2.1 装置および XID_null ポーリングに対して自分で応答できる PU 2.0 装置の場合はゼロのままにしておくべきです。確信がない場合は、PU2.0 SDLC はすべてこのフィールドに記入し、T2.1 装置はすべてゼロのままにするのが最も安全です。非ゼロの場合、その値はリンク・ステーションの IBM NCP 交換回線大ノード構成内の対応する PU アドレス・フィールドに一致していることが必要です。

注: スイッチド 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に設定すると、構成された情報は XID_0 に入り

ます。スイッチド SDLC コールイン・サーキットの場合、構成された XID_0 ブロック番号は異なった方法で使用されます。ソフトウェアは、コールイン・ステーションが常にそれ自体の XID_0 を作成すると想定します。このパラメーターが非ゼロに設定される場合、ステーションの XID_0 は、構成された値を用いて変更されます。このパラメーターがゼロ値に設定される場合、ステーションの XID_0 は変更されません。

XID0 id num
XID0 ブロック番号フィールドと一緒に使用される XID 識別子番号。これは、同じ目的に使用され、同じ状況で必要とされます。

Poll type
SDLC 装置にポーリングする方法と時期を定義します。

TEST インターフェースがアクティブになったときに TEST フレームで 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ときに SNRM フレームで 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ており、インターフェースがアクティブであるときに SNRM フレームで SDLC 装置をポーリングします。

tcp この DLSw が接続できる 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
接続したい 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 コネクションを、ルーターのスタート時に確立するのか (Active)、必要に応じて確立するのか (Passive) を示します。これらのオプションの概説は、482ページの『TCP コネクション、近隣ディスカバリー、およびマルチキャスト探索』を参照してください。

Transmit Buffer Size
1024 ～ 32768 の範囲のパケット転送バッファーのサイズ。デフォルトは 5120 です。

Receive Buffer Size
1024 ～ 32768 の範囲のパケット受信バッファーのサイズ。デフォルト・サイズは 5120 です。

Maximum Segment Size
64 ～ 16384 の範囲の TCP セグメントの最大サイズ。デフォルトは 1024 です。

Enable/Disable Keepalive (E/D)
DLSw が TCP コネクションのキープアライブ・メッセージを送信するかどうかを指示します。デフォルトは D (使用不可) です。

Enable/Disable NetBIOS SessionAlive Spoofing (E/D)
NetBIOS SessionAlive I フレームを廃棄する (DLSw パートナーに送信しない) かどうかを指示します。デフォルトは D (使用不可) で、これはフレームを廃棄しないことを意味します。

Neighbor Priority
近隣の優先順位を「高」、「中」、または「低」として指定できるようにします。あて先ステーションに異なる優先順位を持つ複数の近隣ルーターを介して到達可能の場合、DLSw は最高の優先順位を持つ近隣を介してそのステーションへの回線の確立を試みます。

BAN

ban コマンドは、境界アクセス・ノード (BAN) 構成プロンプトに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。各コマンドについての説明は、89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) の DLSw 交換を使用不可にするのに使用します。これらの SAP は、ネットワークの構成のために LLC によって使用されます。

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 #
オープンされた SAP によって使用されるインターフェース番号

Enter SAP
個々の SAP を 16 進数で入力することも、SNA、NB (NetBIOS)、または LNM (LAN ネットワーク・マネージャー) 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、0 ～ FE の範囲とし、SAP は偶数の番号でなければなりません。

SNA を入力した場合は、SAP 0、4、8、および C はクローズされます。

NB を入力した場合は、SAP F0 はクローズされます。

LNM を入力した場合は、SAP 0、2、D4、F2、F4、F8、および FC はクローズされます。

Delete

delete コマンドは、SDLC リンク・ステーション、 TCP 近隣 IP アドレス、QLLC ステーションまたはあて先、キャッシュ・エントリー、MAC アドレス・エントリー、回線優先順位オーバーライド、および MAC アドレス・エクスプローラー・オーバーライドを DLSw から削除するのに使用します。

構文:

delete cache-entry
explorer-override
mac-list
priority
qllc...
sdlc
tcp

cache-entry

構成された MAC キャッシュ・エントリーを除去します。

例: delete cache-entry

```
Enter mac cache record number [1]? 1
MAC cache entry has been deleted
```

mac cache record number

削除する MAC キャッシュ・エントリーのレコード番号。レコード番号は **list cache all** 構成コマンドを使用して調べることができます。

explorer-override

MAC キャッシュ・エクスプローラー・オーバーライド・エントリーを削除します。

例: delete explorer-override

```
Enter explorer override record number [1]?
Explorer override record has been deleted.
```

Explorer override record number

削除する MAC キャッシュ・エクスプローラー・オーバーライド・エントリーのレコード番号。このレコード番号は、*talk 6* からの **list explorer-override** コマンドを使用して調べることができます。

mac-list

ローカル MAC アドレス・リスト・エントリーを除去します。

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
削除する MAC リスト・エントリーのレコード番号。レコード番号は **list mac-list all** 構成コマンドを使用して調べることができます。

priority
回線優先順位エントリーを除去します。

例: delete priority

```
Enter circuit priority override record number [1]? 1
Circuit priority override record has been deleted.
```

Circuit priority override record number
削除する回線優先順位オーバーライド・エントリーのレコード番号。レコード番号は **list priority** 構成コマンドを使用して調べることができます。

qllc X.25 ネットワーク上の QLLC ステーションに対するサポート、または QLLC ステーションの DLSw あて先に対する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 ルーターをリスタートしたときに DLSw がサービスを提供できるようにな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 の範囲にあるか、スイッチド SDLC コールイン・サーキットの場合は 『sw』 です。

tcp TCP コネクションを確立できる 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・リストの使用を使用不可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、DLSw の構成されたすべてのインターフェースを介して DLSw 機能を実行するのを防止します。

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*以外* の IP アドレスからの着信 DLSw TCP コネクションを受け入れるのを防止します。

例: disable dy

llc ルーターが DISC LLC フレームを発行することによって能動的に LLC コネクションを終了させるのを防止します。代わりに、ルーターは受動的に LLC コネクションを終了します。これにより、エンド・ステーションの LLC コネクションは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対して異なった応答をします。

このコマンドは DLSw 内の LLC の交換機能には影響を与えません。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可にします。

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 が指定の X.25 インターフェース上の着信 QLLC コールを受け入れるのを防止します。これがデフォルト状態です。DLSw への着信コールを許すためには、インターフェースを特別に使用可能にする必要があります。

『station』 を指定すると、構成された QLLC ステーションが DLSw セッションの開始側またはターゲットになるのを防止します。

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 コネクションを防止します。

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・リストの使用を使用可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 ルーター上の DLSw の動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*以外* の IP アドレスからの着信 DLSw TCP コネクションを受け入れるように設定します。これがデフォルト状態です。

ipv4 dlsw precedence
ルーターを IP バージョン 4 用の IP 優先順位ビットを設定するように設定します。これらの優先順位ビットは、ルーターの BRS フィーチャーによって読み取られ、 DLSw トラフィックに優先順位を付けます。

例:

```
enable IPv4 DLSw Precedence
IPv4 Precedence is now enabled.
```

llc ルーターが TCP コネクション損失時に LLC コネクション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可にします。

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 が指定の X.25 インターフェース上の着信 QLLC コールを受け入れます。

『station』 を指定すると、構成された QLLC ステーションが DLSw セッションの開始側またはターゲットになることができます。これが構成された各 QLLC ステーションのデフォルト状態です。

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 コネクション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 隣接が動的に相互を発見し、相互間に TCP セッションを作成して、マルチキャスト探索およびフレーム転送を行えるようにするのに使用します。これらの機能の概説は、482ページの『TCP コネクション、近隣ディスカバリー、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、使用している 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することが必要であり、ユーザーは OSPF Config> プロンプトから 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、グループ識別のグループ ID モデルを使用するのか (この場合は、ルーターが対応するマルチキャスト・アドレスを作成します)、あるいはユーザー自身がマルチキャスト・アドレスを指定するのかを選択します。グループ ID モデルを使用すると構成が簡単ですが、IBM 以外の DLSw バージョン 2 プロダクトとのマルチキャスト接続性を持ちたい場合は、ユーザー自身がマルチキャスト・アドレスを指定する必要があります。ルーターは、同時に両方の形態のグループのメンバーになることができます。

グループ ID モデルを使用して、最大 64 のグループを結合することができます。DLSw ルーターをグループに割り当てると、DLSw プロトコルは自動的に 2 つのアドレスのうちの 1 つをグループ番号に付加して、マルチキャスト・アドレスを生成します。ルーターは、自身を他のグループ・メンバーに識別し、これらのメンバーにパケットを転送するために、このマルチキャスト・アドレスを転送します。グループ番号に付加される 2 つのアドレスは、DLSw クライアントとピアの 225.0.1.0 および DLSw サーバーの 225.0.1.64 です。 たとえば、グループ 2 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、デフォルト [G] についてのものです。例の後の説明には、 (G) と (M) の両方について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
ルーターがユーザーの代わりにマルチキャスト・アドレスを構成するのか、ユーザー自身がマルチキャスト・アドレスを供給するのかを選択します。

Multicast IP address
マルチキャスト IP アドレスは、DLSw バージョン 2 に準拠するマルチキャスト IP アドレスで、224.0.10.0 ～ 224.0.10.191 の範囲にあり、 DLSw 探索トラフィックを送信または受信あるいはその両方を行うのに使用されます。

Read Only , Write Only or Read Write
このパラメーターは、構成済みのマルチキャスト IP アドレスを、探索トラフィックの受信専用 (Read Only)、探索トラフィックの送信専用 (Send Only)、または探索トラフィックの送信と受信の両方 (Read Write) に使用するかどうかを示します。

Group ID
このルーターを結合するグループの番号

Client/Server or Peer Group Member
グループ内でこのルーターが果たす役割。クライアントの場合は C、サーバーの場合は S、ピアの場合は P

Connectivity setup type
ルーターが Active (能動) または Passive (受動) メンバーのいずれとしてグループに参加するのかを指定します。 482ページの『TCP コネクション、近隣ディスカバリー、およびマルチキャスト探索』で説明したように、他のグループ・メンバーと TCP コネクションを確立する時期を制御します。

Transmit Buffer Size
1024 ～ 32768 の範囲のパケット転送バッファーのサイズ。デフォルトは 5120 です。

Receive Buffer Size
1024 ～ 32768 の範囲のパケット受信バッファーのサイズ。デフォルト・サイズは 5120 です。

Maximum Segment Size
64 ～ 16384 の範囲の TCP セグメントの最大サイズ。デフォルトは 1024 です。

Enable/Disable Keepalive
DLSw が TCP キープアライブ・メッセージを送信するかどうかを指示します。デフォルトは D (使用不可) です。

Enable/Disable NetBIOS SessionAlive Spoofing (E/D)
NetBIOS SessionAlive I フレームを廃棄する (このグループに関連した DLSw パートナーに送信しない) かどうかを指示します。デフォルトは D (使用不可) で、これはフレームを廃棄しないことを意味します。

Neighbor Priority (H/M/L) [M]?
近隣の優先順位を「高」、「中」、または「低」として指定できるようにします。あて先エンド・ステーションに異なる優先順位を持つ複数の近隣ルー

ターを介して到達可能の場合、DLSw は最高の優先順位を持つ近隣を介してそのエンド・ステーションへの回線の確立を試みます。

Leave-Group

leave-group コマンドは、**join-group** コマンドを使用して構成したグループからルーターを除去するか、または構成されたマルチキャスト・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 コネクションには影響を与えません。

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・ステーション上の DLSw 情報、回線優先順位、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・エントリー、MAC アドレス・リスト・エントリー、回線優先順位オーバーライド、および MAC キャッシュ・エクスプローラー・オーバーライドを表示するのに使用します。

構文:

list
- cache
- dls
- explorer-override
- groups
- llc2
- mac-list
- open
- priority
- qllc...
- sdlc
- tcp
- timers

cache 構成された MAC アドレス・キャッシュ・エントリーをリストします。

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** コマンドを使用し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 dls global** コマンドからの出力と同じです。)

explorer-override

構成済みの 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
```

llc2 **set llc2** コマンドを使用して構成された LLC2 パラメーターを表示します。(これらのパラメーターについての詳しい説明は、545 ページの **set llc2** コマンドの項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します。**set llc2** コマンドを使用して LLC2 パラメーターを変更しなかった場合は、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 受信確認タイマー

ti 非活動タイマー

n2 最大再試行値

n3 ACK の送信前に受信した 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 の数

acc 現行の LLC2 実現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デフォルトの 0 になります。

mac-list

構成された MAC アドレス・リスト・エントリーをリストします。

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 と関連の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 および NetBIOS 回線用に選択された回線優先順位、種々の回線優先順位間の転送比率、および NetBIOS 用に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
```

回線優先順位は、クリティカル (Critical)、高 (High)、中 (Medium)、または低 (Low) です。ルーターは、ユーザーが割り当てた優先順位値を使用して、特定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。たとえば、SNA トラフィックに「クリティカル」の優先順位、NetBIOS セッション・トラフィックに「中」の優先順位を割り当て、メッセージの割り振りが 4/3/2/1 の場合、ルーターは 4 つの SNA セッション・フレームを処理した後で、2 つの NetBIOS フレームを処理します。この例では、利用可能な帯域幅の 2/3 が SNA トラフィックに割り当てられています。ユーザーが指定した優先順位を使用してルーターが帯域幅を割り振る際には、*バイト数ではなくフレーム数を使用します。*

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は、525 ページの **add qllc destination** コマンドの項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
```

ここにリストされているパラメーターについては、525 ページで説明しています。『E/D』 は、ステーションが **disable qllc station** コマンドによって使用不可にされているるかどうかを示します。

sdlc **add sdlc link station** コマンドを使用して構成した SDLC リンク・ステーション情報を表示します。

注: スイッチド SDLC コールイン・サーキットは、アドレス・フィールドの『FF(sw)』 によって示されています。

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 リンク・ステーションを接続する SDLC アドレス (01 ～ FE またはスイッチド SDLC コールイン・サーキットの場合は 『FF(sw)』 の範囲)。

Status
リンク・ステーションの状態 (使用可能か使用不可か)

Source SAP/MAC
接続された SDLC ステーションを DLSw ドメインに識別する LLC SAP アドレスと MAC アドレス

Dest SAP/MAC
SDLC ステーションがアクティブになったときに、接続された SDLC ステーションが回線の確立を開始するリモート・エンド・ステーションの LLC SAP アドレスと MAC アドレス

PU 接続された SNA 装置の SNA PU タイプ。次のとおりです。

2 PU 2.0 または T2.1 ノード

4 別の PU への INN サブエリア・ルーティング (つまり、NCP-NCP) を行う PU 4

5 DLSw ネットワーク内の PU 2.0 への境界機能接続を行う、ホストまたはフロントエンド・プロセッサー搭載ホスト (たとえば、NCP 搭載 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 ブロック番号と ID 番号。このフィールドは、PU タイプ 2 装置の場合にのみ表示されます。

PollType
ルーターが SDLC ステーションと最初に接続するのに使用する SDLC フレームのタイプで、TEST フレーム、SNRM フレーム、または遅延された SNRM フレーム (DLSw セッションが確立された後でのみ送信される SNRM フレーム) です。このフィールドは、PU タイプ 2 装置の場合にのみ表示されます。

tcp 構成された DLSw TCP 近隣を表示します。近隣は **add tcp** コマンドを使用して構成されています。

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 接続性設定タイプで、Active (能動) または Passive (受動) です。

Xmit Bufsize
1024 ～ 32768 の範囲のパケット転送バッファーのサイズ。デフォルトは 5120 です。

Rcv Bufsize
1024 ～ 32768 の範囲のパケット受信バッファーのサイズ。デフォルトは 5120 です。

Max Segsize
64 ～ 16384 の範囲の TCP セグメントの最大サイズ。デフォルトは 1024 です。

Keepalive
キープアライブ機能の状態で、使用可能または使用不可です。

SesAlive Spoofing
NetBIOS SesAlive スプーフィング機能の状態で、使用可能または使用不可です。

Priority
選択プロセスにおける近隣ルーターの優先順位。近隣優先順位は、高 (High)、中 (Medium)、または低 (Low) です。

timers 各種のアクティビティーに対するユーザー指定の待ち時間

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
```

詳細については、**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 コマンドの説明は、168ページの『NetBIOS コマンド』を参照してください。

構文:

netbios

Open-Sap

open-sap コマンドは、DLSw が DLSw 回線の開始側またはターゲットとして使用するすべての SAP に対して発行します。一般的に使用される SNA SAP 値は、00、04、08、および 0C です。これらのすべての SAP を、ニーモニックの 『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、『NB』 として表すことができます。LAN ネットワーク・マネージャー機能に関連する SAP は、集合的に 『LNM』 として参照されます。DLSw が SNA または NetBIOS エンド・ステーション、LNM、あるいは LNM が管理しているブリッジに到達するのに使用するインターフェース上で、ユーザーが選択したプロトコルの 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 をオープンするのに使用するインターフェースの番号

Enter SAP in hex
個々の SAP を 16 進数で入力することも、SNA、NB (NetBIOS の場合)、または LNM (LAN ネットワーク・マネージャーの場合) 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、0 ～ FE の範囲とし、SAP は偶数の番号でなければなりません。前に同じインターフェース上の SAP 0 をオープンせずに、SAP 4、8、または C を入力した場合、SAP 0 が自動的にオープンします。

SNA を入力した場合、SAP 0、4、8、および C がオープンします。

NB を入力した場合、SAP F0 がオープンします。

LNM を入力した場合、SAP 0、2、D4、F2、F4、F8、および FC がオープンします。

Set

set コマンドは、MAC アドレス/IP アドレス・マッピング・キャッシュのサイズ、LLC2 パラメーター、DLSw セッションの最大数、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 動作用のパラメーター、 MAC アドレス・リストに関連するパラメーター、および回線優先順位オーバーライド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** コマンドを使用すると、MAC アドレス/IP アドレス・マッピング・キャッシュのサイズを指定することができます。

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見つけます。キャッシュが大きいほど、DLSw がすべての既知の TCP/IP 近隣に CANUREACH フレームを送信せずに、希望するリモート・ステーションを見つける確率が高くなります。

ただし、このキャッシュ・サイズは大きく設定し過ぎないようにすることが必要です。大きく設定し過ぎると、ルーター上のメモリーを使い尽くし、実際の DLSw セッションに必要なメモリーにまで食い込みます。その結果、ルーターが扱える DLSw セッションの数が減ります。

例: set cache

```
MAC  IP cache size (4 - 65535) [128]?
```

dynamic-tcp 動的近隣 TCP コネクション (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のコネクトイン) の種々の TCP パラメーターを指定できるようにします。DLSw は動的近隣が使用可能にされている場合にのみ、これらの値を使用します。

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]?
```

ここにリストされているパラメーターの説明は、529 ページの **add tcp** コマンドの項を参照してください。

llc2 特定の SAP の特定の LLC2 属性を構成できるようにします。

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 ピアが相手側の LLC2 ピアから確認または応答を受信できないと満了します。

Receive Ack timer (T2)
受信した I フォーマット・フレームの確認応答を送信するのにかかる遅延 (ミリ秒)

Inactivity Timer (Ti)
このタイマーは、LLC が指定された期間にフレームを受信しないと満了します。このタイマーが満了すると、LLC2 ピアは LLC2 ピアが応答するまで、または N2 再試行カウントを超過するまで、RR を送信します。デフォルトは 30 秒です。

Transmit Window (Tw)
RR を受信する前に送信できる I フレームの最大数。値は 1 ～ 127 の範囲です。0 は Tw をデフォルトに設定します。デフォルトは 2 です。

Receive Window (Rw)
LLC2 ピアがリモート・ホストから受信できる未確認のシーケンス番号制 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の動作方法に影響を与えます。エラー状態の後の確認応答の数を指定します。デフォルトは 1 です。動作ウィンドウ (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 エラーが検出された後、動作ウィンドウ (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け取る必要がある確認応答の数を指定します。Ww はこの方式で Ww = Tw に達するまで増分を続けます。

Max Retry value (N2)
非活動タイマー (Ti) が満了したときに、LLC2 ピアが確認応答を受信せずに RR を送信する最大回数

Number I-frames received before sending ACK (N3)
この値は、T2 タイマーと合わせて、受信 I フレームの確認応答トラフィックを削減するのに使用されます。このカウンターは指定された値にセットされ、I フレームを受信するたびに減分されます。このカウンターが 0 に達するか、T2 タイマーが満了すると、確認応答が送信されます。

高性能を確保するために、N3 はリモート LLC の Tw より小さい値に設定してください。デフォルトは 1 です。

mac-list ローカル MAC アドレス・リストの排他性を変更します。

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 アドレスが排他 (すべての MAC アドレスがこの DLSw を介してアクセス可能であることを表す) か、非排他 (1 組の MAC アドレスがこの DLSw を介してアクセス可能であることを表す) かを示します。

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 および NetBIOS セッション (回線) の両方が含まれます。

例: set maximum

```
Maximum number of DLSw sessions (1-60000) [1000]?
```

memory DLSw に利用可能なメモリーの総量、ならびに各 DLSw セッションおよび NetBIOS UI フレームに利用可能なメモリーの量を指定できるようにします。ルーターは per-session 値および UI-frame 値を使用して、フロー制御アルゴリズムによるデータ送信側への逆方向圧力の適用の開始/停止、および UI フレーム・トラフィック廃棄の開始/停止の限界を設定します。

ルーターは現在 overall DLSw allocation value は使用していないので、この値はデフォルトのままにすることができます。グローバル送信および受信プール (NetBIOS UI フレーム・プールではなく) に関する DLS.161 メッセージはすべて無視して構いません。これらの論理プールを使用する代わりに、DLSw ペーシング・アルゴリズムは物理記憶域の状態を使用して、公示するウィンドウ・サイズを決めます。

LLC、SDLC、および QLLC セッション割り当て値は、それぞれ、LLC、SDLC、および QLLC に接続された装置から TCP へと流れるデータのバッファリングに関する回線当たり (エンド・ステーションの組み) の限界を指定します。ルーターは、この限界に達すると、RNR/RR を該当するエンド・ステーションに送ります。per-session pools の状態は、DLSw 監視コマンド **list dlsw memory** を使用して、アクティブ・セッションのリストの一部として表示することができます。

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 フレーム割り当て値は、DLSw が一度にバッファーできる UI フレームの数 (NetBIOS DATAGRAM、NAME_QUERY、ADD_NAME_QUERY などを含む) 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、発信元エンド・ステーションはそれらを再送しなければなりません。したがって、この限界値を低く設定し過ぎると、NetBIOS 回線確立の試行時に断続的に障害が生じる原因になります。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、フレームの廃棄状態を報告します。

priority

SNA 回線および NetBIOS 回線に使用する回線優先順位と、これらの優先順位の*相互間* のトラフィック比率を指定できるようにします。**set priority** コマンドを使用して、回線優先順位を Critical、High、Medium、または Low に (Critical から Low に降順で) 指定できます。ルーターは、ユーザーが割り当てた優先順位値を使用して、近隣に送信する特定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。

この機能が動作するのは輻輳 (ふくそう) の期間中 (この間、DLSw メッセージは TCP に送信される前に待ち行列に入れられます) だけです。たとえば、SNA トラフィックにセッションおよび探索優先順位 Critical (これは、デフォルトではメッセージ割り当て値 4 に相当します) を指定し、次に NetBIOS セッションおよび探索トラフィックに優先順位 Medium (これはメッセージ割り当て値 2 に相当します) を指定した場合、ルーターは 4 つの SNA フレームを送信した後、2 つの 2 NetBIOS フレームを送信します。2 つの NetBIOS フレームを処理した後、ルーターは再び 4 つの SNA フレームを処理するという具合で進められます。ルーターは、ユーザーが指定した優先順位を使用して帯域幅を割り振る際に、バイト数ではなくフレーム数をカウントします。また、特定の回線の優先順位は、回線の起動時に近隣ルーターと交渉されます。したがって、近隣ルーターは、ユーザーがこのルーターに指定した構成値に基づくポリシー以外の別のポリシーを使用して新規回線の優先順位を設定する可能性があります。ユーザーは SNA と NetBIOS のセッションおよび探索トラフィックに異なる優先順位を割り当てることも可能です。

また、**set priority** コマンドを使用して、このルーターを経由するすべての NetBIOS フレームの最大フレーム・サイズを設定することもできます。NetBIOS エンド・ステーションは許容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リンクを占有し、相互運用されている SNA トラフィックに悪影響を与えることがあります。この影響を減らすために、標準ソース・ルート・ブリッジング・メカニズムを使用して、ルーターが NetBIOS エンド・ステーションに通知する最大フレーム・サイズを小さく設定することができます。NetBIOS を稼働するネットワーク上に透過的にブリッジされる (TB) セグメントが存在する場合は、最大 NetBIOS フレーム・サイズを少なくとも 1470 に設定してください。

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

着信した動的 QLLC コールの発信元 MAC アドレスとして使用される、動的割り当て MAC アドレスの範囲を指定できるようにします。

範囲の指定は、範囲の基本 MAC アドレス 『X』 と動的アドレスの最大数 『N』 によって行います。DLSw は X ～ X+(N-1) の範囲の 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・ネットワーク上の DLSw を識別するソース・ルーティング・ブリッジ (SRB) 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

未使用の DLSw エントリーを保持する期間を指定します。データベース・エントリーは、あて先 MAC アドレスを、それらに到達可能な DLSw ピアの集合にマップします。

ゼロの値は、このデータベース内のエントリーはエージング (経時処理) されないことを示します。これはダイヤル・インターフェースを介して近隣 TCP コネクションを稼働している

場合には便利ですが、さまざまな他の DLSw 機能を使用不可にするので、一般的には推奨できません。

Max wait timer
前に送信した CANUREACH に対する ICANREACH レスポンスを待つ時間を指定します。

Wait timer LLC test response
断念する前に LLC テストのレスポンスを待つ時間を指定します。

Wait timer SDLC test response
断念する前に SDLC テストのレスポンスを待つ時間を指定します。

QLLC session retry timer
ルーターが DLSw セッションを開始するために QLLC ステーションに再度接続を試みる前に待つ時間。

Group join timer interval
ルーターが一連のグループ公示メッセージを同報通信する前に待つ時間。これは、グループ・ベースの DLSw 機能が中間ルーターの障害から回復するのにかかる時間、およびマルチキャスト機能が動作するために必要なオーバーヘッドの量に影響を与える可能性があります。DLSw のマルチキャスト機能を使用する代わりに TCP コネクションを構成した場合には、この値は使用されません。

Neighbor priority wait timer
探索時に、近隣を選択する前に待つ時間。これにより、ICANREACH メッセージに最初に応答しなくても高い優先順位の近隣が選択されるようにすることができます。

値ゼロは、近隣優先順位フィーチャーを使用しないことを指示します。各 MAC アドレスについての、キャッシュに入れられた DLSw ピア情報はありません。CANUREACH は常に送信され、(優先順位に関係なく) 最初に ICANREACH を送信した DLSw ピアが使用されます。

Inactive neighbor termination timer
DLSw が、非アクティブの (セッション数がゼロの) 受動 TCP コネクションを切断する前に待つ時間

Delay sending TEST response
MAC アドレスの探索から TEST レスポンスを送信するまでに待つ時間の長さを指定します。これは、DLSw ピアを介して同じ MAC アドレスに到着できる、同じブリッジ LAN 上に DLSw 2212 が 2 つある場合に役立ちます。一方の DLSw 2212 を優先する場合、優先しない 2212 でTEST レスポンス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 構成の一部にはなりません。すなわち、監視コマンドはルーターの構成をリアルタイムで変更することができますが、これらの変更はルーターをリスタートしたときに SRAM 構成によってオーバーライドされます。監視は、以下のアクションから構成されます。

- 現在ルーターによって使用されているプロトコルおよびネットワーク・インターフェースを監視する。
- ルーターのアクティビティーに関連する ELS (イベント・ログ・システム) メッセージを表示する。
- DLSw 構成に固定的な影響を与えずに、DLSw 構成をリアルタイムで変更する。

DLSw 監視環境へのアクセス

DLSw 監視環境 (GWCON プロセス) にアクセスするには、次の例に示すように、OPCON (*) プロンプトで **talk 5** (または **t 5**) を入力し、GWCON (+) プロンプトで **protocol dls** を入力します。

```
MOS Operator Control

* talk 5
+ protocol dls
DLS>
```

DLSw 監視コマンド

この節では、表34 にリストされる 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、データベースから情報を収集するのに使用します。

表 34. DLSw 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	現行の構成に、SDLC リンク・ステーション、 TCP 近隣 IP アドレス、QLLC ステーションまたはあて先、キャッシュ・エントリー、 MAC アドレス・リスト・エントリー、回線優先順位オーバーライド、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の境界アクセス・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るようにします。詳しい説明については、61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の通信のために 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 ステーションまたはあて先、キャッシュ・エントリー、MAC アドレス・リスト・エントリー、回線優先順位オーバーライド、および 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可にします。

表 34. DLSw 監視コマンドの要約 (続き)

コマンド	機能
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	指定された 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、回線優先順位、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のセッション、キャッシュ・エントリー、MAC アドレス・リスト・エントリーの情報を表示します。このコマンドは、 TCP 機能、コネクション、および統計に関する詳細情報も提供します。
NetBIOS	NetBIOS サポート・プロンプトへのアクセスを提供します。
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、メモリー割り当て、プロトコル・タイマー、回線優先順位、動的近隣用のパラメーター、QLLC 動作用のパラメーター、または MAC アドレス・リストに関連するパラメーターを動的に変更します。
Test	特定の MAC アドレスを、現行の 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します。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、SRAM 構成に影響を与えずに、SDLC リンク・ステーション、TCP 近隣 IP アドレス、QLLC ステーションまたはあて先、キャッシュ・エントリー、MAC アドレス・リスト・エントリー、回線優先順位オーバーライド、および 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のに使用します。

構文:

add
- cache-entry
- explorer-override
- mac-list
- priority
- qllc...
- sdlc
- tcp

例とフィールドの説明は、520ページの『Add』 の章の **add** コマンドの項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ます。

構文:

ban

DLSw 監視コマンド (Talk 5)

BAN 監視プロンプトにアクセスしたら、特定の監視コマンドの入力を開始できます。BAN 監視コマンドの説明は、61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。

exit コマンドを入力すれば、いつでも DLSw> プロンプトに戻れます。

Close-SAP

close-sap コマンドは、DLSw SRAM 構成に影響を与えずに、DLSw が指定の SAP を使用するのを動的に使用不可にするのに使用します。

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]? 04
SAP(s) 4 closed on interface 1
```

(**close-sap** パラメーターの説明は、530 ページにあります。)

Delete

delete コマンドは、DLSw SRAM 構成に影響を与えずに、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 ステーションまたはあて先、キャッシュ・エントリー、MAC アドレス・リスト・エントリー、回線優先順位オーバーライド、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除去するのに使用します。このコマンドは、既存のセッションを終了するのにも使用できます。

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・エントリーを削除します。

例: delete cache-entry

```
Enter MAC Address [400000000000]?
10005a123456
MAC 10005A123456 / IP address 128.185.122.234 configured cache entry deleted.
```

dls 現在アクティブの 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・エントリーを削除します。

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・エントリーを削除します。

例: delete mac-list

```
Enter mac list record number [1]?

Local MAC list entry 10005A000000 / FFFFFF000000 has been deleted.
```

priority

指定された回線優先順位エントリーを削除します。

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対するサポートを除去します。ユーザーが現在アクティブのステーションを削除すると、DLSw はコネクションを切断する前にユーザーの意志を確認します。あて先を削除しても、既存のコネクションには影響を与えません。

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 現在アクティブの SDLC リンクを、SDLC リンク・ステーション構成情報に影響を与えずにクローズします。

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 (01 ～ FE の範囲、またはスイッチド SDLC コールイン・サーキットの場合は 『sw』)

tcp TCP コネクションを確立する相手の TCP ピアの IP アドレス (*ip_address*) を除去します。TCP コネクションはクローズされます。

例: delete tcp

```
IP Address [0.0.0.0]? 128.185.14.1
```

Disable

disable コマンドは、 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、DLSw SRAM 構成に影響を与えずに動的に使用不可にするのに使用します。監視から DLSw 機能**全体**を使用不可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の使用例は、533 ページ以降に示されています。)

Enable

enable コマンドは、DLSw SRAM 構成に影響を与えずに、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のに使用します。

構文:

enable dynamic-neighbors
llc
mac-list
qllc...
sdlc

(**enable** コマンドのパラメーターの使用例は、535 ページ以降に示されています。)

Join-Group

join-group コマンドは、DLSw に対して、近隣ディスカバリー、マルチキャスト探索、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。

追加情報と例については、479ページの『第24章 DLSw 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 に対して、指定されたグループ内の、または指定されたマルチキャスト・アドレスを使用する、近隣ディスカバリー、マルチキャスト探索、およびマルチキャスト・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・アドレスのもとで起動された既存の TCP コネクションを終了させます。追加情報と例については、479ページの『第24章 DLSw 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・ステーション上の DLSw 情報、回線優先順位、SAP、TCP 近隣、グループ、動的近隣、QLLC ステーション、あて先およびインターフェース、構成済みキャッシュ・エントリー、MAC アドレス・リスト・エントリー、および MAC キャッシュ・エクスプローラー・オーバーライドを表示するのに使用します。

構文:

list
- dls...
- explorer-override
- groups...
- llc2...
- mac-list
- priority...
- qllc...
- sdlc...
- tcp...

timers

dls DLSw プロトコルに関する情報を表示します。DLSw パラメーターのオプション (global、memory、sessions、および cache) について、以下に説明します。

Global
構成された一般 DLSw パラメーターの動作値を表示します。

Memory
構成された DLS メモリー情報および現在のメモリーの使用状況を表示します。

Sessions
発信元、あて先、状態、フラグ、着信 IP アドレス、およびセッション ID を含めて、現在の DLS 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 プロトコルの状態、使用可能または使用不可

LLC2 send disconnect is
TCP コネクション損失時にルーターが LLC2 コネクションを終了するのを防止する状態。値は、使用可能または使用不可です。

Dynamic Neighbors
DLSw が、構成されていない (つまり、**add tcp** コマンドを使用して) DLSw ルーターからの着信 TCP コネクション試行を受け入れるかどうかを指示します。

SRB Segment number
RIF 内の 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 セッションの最大数 (SNA および NetBIOS セッションの両方)

DLSw global memory allotment
DLSw が使用できるメモリーの最大量

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 フレームに許されるメモリーの最大量

Dynamic Neighbor Transmit Buffer Size
動的 TCP コネクションのための TCP 転送バッファーのサイズ

Dynamic Neighbor Receive Buffer Size
動的 TCP コネクションのための TCP 受信バッファーのサイズ

Dynamic Neighbor Maximum Segment Size
動的 TCP コネクションの最大 TCP セグメント・サイズ

Dynamic Neighbor Keep Alive
新規の動的 TCP コネクション時にキープアライブ・メッセージを送信するかどうか。

Dynamic Neighbor NetBIOS SessionAlive Spoofing
新規の動的 TCP コネクションで確立された DLSw ピアに NetBIOS SessionAlive I フレームを転送するかどうか。

Dynamic Neighbor Priority
すべての新規の動的 TCP コネクションに使用する近隣優先順位

QLLC base source MAC address
動的着信 QLLC コール (SVC) の発信元 MAC アドレスとして使用される範囲の最低 MAC アドレス

QLLC maximum dynamic addresses
動的着信 QLLC コールで一度に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。
SDLC、QLLC、または APPN 発信元とのセッションの場合、MAC アドレスは以下の文字列に置き換えられるので、これらのセッションは容易に識別できます。

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。以下の状態が表示されます。

DISCONECT

回線またはコネクションが確立されていない初期状態を示しています。

RSLV_PEND

ターゲット DLSw が、SSP_STARTED 表示を待っているか、SSP_START 要求を出した後かのいずれかであることを示しています。

CIRC_PEND

ターゲット DLSw が SSP_ICANREACH メッセージに対する SSP_REACHACK レスポンスを待っていることを示しています。

CIRC_EST

エンド・エンド回線が確立されたことを示しています。

CIR_RSTRT

リセットを発信した DLSw が、データ・リンクがリスタートされて SSP_RESTART メッセージに対する SSP_RESTARTED レスポンスを受け取るのを待っていることを示しています。

CONN_PEND

開始側 DLSw が SSP_CONTACT メッセージに対する SSP_CONTACTED レスポンスを待っていることを示しています。

CONT_PEND

ターゲット DLSw が SSP_CONTACT メッセージに対する SSP_CONTACTED 確認を待っていることを示しています。

CONNECTED

回線はコネクション指向のデータ転送のために完全にアクティブになっていることを示しています。

DISC_PEND

切断を発信した DLSw が SSP_HALT メッセージに対する SSP_HALTED レスポンスを待っていることを示しています。

HALT_PEND
リモート DLSw が SSP_HALT 要求の後で SSP_HALTED 表示を待っていることを示しています。

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ています。

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ています。

HLT_NOACK
ローカル DLSw が HALT_DL_NOACK を受信したが、まだリンク・ステーションのクローズを完了していないことを示しています。

Flags フラグは以下のいずれかです。

A - CONTACT MSG PENDING

B - SAP RESOLVE PENDING

C - EXIT BUSY EXPECTED

D - TCP BUSY

E - DELETE PENDING

F - CIRCUIT INACTIVE

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のに使用される番号。この番号は、セッション ID を必要とするすべてのコマンドで使用します。

dls sessions appn

このルーター内の APPN をエンドポイントとするセッションの 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 セッションに関する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

DLS 情報を、あて先 MAC アドレス別に表示します。

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
```

DLSw 監視コマンド (Talk 5)

dls sessions detail

詳細 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
コネクションの 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 ピアとの間で送受信した XID の合計数

Datagrams sent Datagrams rcvd
この DLSw ピアがリモート DLSw ピアとの間で送受信したデータグラムの合計数

Info frames sent Info frames rcvd
この DLSw ピアがリモート DLSw ピアとの間で送受信した I フレームの合計数

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 回線 ID

Remote CID
近隣ルーターによって割り当てられた DLSw 回線 ID

Priority
開始時にこの回線に設定された DLSw 回線優先順位

dls sessions ip

指定の TCP 接続された近隣への 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 をサポートする現在アクティブの回線に関する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。この数値は発信元 MAC アドレスの左側に表示されます。

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

すべての DLS セッションを発信元 MAC アドレス別に表示します。

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 『SDLC 04』 ネームにマップされます。このコマンドのパラメーターとして必要な発信元 MAC アドレスが分からない場合は、**list SDLC config all** コマンドを使用して、この情報を入手してください。

dls sessions state

指定された状態のすべての 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 コマンドは、DLSw MAC アドレス・キャッシュのエントリーをリストします。このキャッシュには、最新の MAC アドレスから IP 近隣への変換データベースが入っています。これは、MAC アドレス、キャッシュ内に存在した時間 (秒数)、および近隣の IP アドレスを提供します。

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 が構成した MAC キャッシュ・エントリーを表示します。

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

指定された範囲のキャッシュ・エントリー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 このコマンドは、既存のすべての DLSw セッションと、各セッションによって使用されているメモリー量をリストします。

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合計量を示します。これには、すべてのセッションへの割り当てと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関する情報を提供し、以下のいずれかです。

Ready セッションが輻輳 (ふくそう) していないことを示しています。

Session セッションがそのセッション割り当てのほとんどを使い尽くしており、おそらくデータ・リンクがフロー制御されていることを示しています。

Global ルーター内のメモリー不足のために、セッションが輻輳 (ふくそう) していることを示しています。

Ses/gbl セッション・メモリー不足とグローバル・メモリー不足が組み合わさって、セッションが輻輳 (ふくそう) していることを示しています。

『DLC Xmits Queued』 フィールドは、LLC または SDLC に転送するために DLS 内で待ち行列化されているフレーム数、プラス、接続されたエンド・ステーションからの確認を待っている DLS 内の待ち行列化されたフレーム数の合計数を示します。

explorer-override

構成済みの MAC キャッシュ・エクスプローラー・オーバーライドをリストします。

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・エントリーを表示します。

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

すべてのローカルに構成された MAC アドレス・リスト・エントリーを表示します。

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 すべてのアクティブなローカル MAC アドレス・リスト・エントリーを表示します。

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 ピアの、すべてのアクティブなリモート MAC アドレス・リスト・エントリーを表示します。

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 コマンドを使用して構成されたこの DLSw ピア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 グループの場合は、読み取りまたは書き込み用の マルチキャスト・アドレスが構成されています。

Role クライアント/サーバー/ピア・グループの場合は、このルーターに構成されたグループ内での役割。DLSw バージョン 2

グループの場合は、構成されたマルチキャスト・アドレスの読み取り/書き込みの役割 (読み取り専用、書き込み専用、または読み書き)。

CST このルーターがグループ内で使用するように構成されている接続性設定タイプ、Active (a) または Passive (p) のいずれか。

Xmit Bufsize
1024 ～ 32768 の範囲のパケット転送バッファーのサイズ。デフォルトは 5120 です。

Rcv Bufsize
1024 ～ 32768 の範囲のパケット受信バッファーのサイズ。デフォルトは 5120 です。

Max Segsize
64 ～ 16384 の範囲の TCP セグメントの最大サイズ。デフォルトは 1024 です。

Keepalive
キープアライブ機能の状態 (使用可能または使用不可) を表示します。

SesAlive Spoofing
NetBIOS SessionAlive スプーフィング機能の状態 (使用可能または使用不可) を示します。

Priority
選択プロセスにおける近隣ルーターの優先順位を表示します。近隣優先順位は、高 (High)、中 (Medium)、または低 (Low) です。

groups config

join-group コマンドを使用して構成されたこの DLSw ピアのグループ情報を表示します。

例:`list groups config`

```
   Group# /                        Xmit     Rcv      Max
Mcast IP Addr    Role        CST  Bufsize  Bufsize  Segsize  Keepalive
Priority

224.0.10.0       READ/WRITE   p    5120     5120     1024    DISABLED   MEDIUM
   1             CLIENT       p    5120     5120     1024    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 グループの場合は、読み取りまたは書き込み用の マルチキャスト・アドレスが構成されています。

Role クライアント/サーバー/ピア・グループの場合は、このルーターに構成されたグループ内での役割。DLSw バージョン 2 グループの場合は、構成されたマルチキャスト・アドレスの読み取り/書き込みの役割 (読み取り専用、書き込み専用、または読み書き)。

CST このルーターがグループ内で使用するように構成されている接続性設定タイプ、Active (a) または Passive (p) のいずれか。

Xmit Bufsize
1024 ～ 32768 の範囲のパケット転送バッファーのサイズ。デフォルトは 5120 です。

Rcv Bufsize
1024 ～ 32768 の範囲のパケット受信バッファーのサイズ。デフォルトは 5120 です。

Max Segsize
64 ～ 16384 の範囲の TCP セグメントの最大サイズ。デフォルトは 1024 です。

Keepalive
キープアライブ機能の状態 (使用可能または使用不可) を表示します。

Priority
選択プロセスにおける近隣ルーターの優先順位を表示します。近隣優先順位は、高 (High)、中 (Medium)、または低 (Low) です。

groups statistics

前回のルーターのリスタートまたはグループの作成以降の、探索トラフィックのための DLSw グループの使用に関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 ピア間の現在オープンされているすべての SAP 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。変更された構成のみが表示されます。**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。以下の状態が表示されます。

DISCONNECTED
データ・リンク制御構造は存在するが、データ・リンクが確立されていないことを示しています。

CONNECT_PEND
NULL SAP へのテスト・コマンド・フレームを受信したとき、または DLS から DLC_START_DL コマンドを受信したときに、接続中状態に入ります。

RESOLVE_PEND
DLC_RESOLVE_C コマンドを DLS に送信すると、解決中状態に入ります。

CONNECTED
これは、LLC タイプ 1 レベルのサービスが DLS ネットワークを介して利用可能であるときの定常状態です。DLS から DLC_RESOLVE_R コマンドを受信したとき、またはネットワークから TEST レスポンス・フレームを受信したときに、この状態に入ります。

CONTACT_PEND
送信または受信した SABME に対するレスポンスをまだ受け取っていないときは、必ずこの状態に入ります。

CONTACTED
これは、送信した SABME に対する UA レスポンスを受信したとき、または受信した SABME に対する UA をすでに送信したときに必ず入る定常状態です。この状態のときに、DLS ネットワークを介して LLC2 情報フレームが交換されます。

DISCONNECT_PENDING
DISC コマンドを送信または受信したとき、または DLS から DLC_HALT を受信したときには、必ずこの状態に入ります。

llc2 sessions ban
BAN 機能も含めて、LLC2 セッションの現行の情報を表示します。

llc2 sessions nb
NetBIOS プロトコル・トラフィックを伝送する LLC2 セッションの現行の情報を表示します。

llc2 sessions range
選択された範囲の LLC2 セッションの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 回線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
```

このディスプレイの構成可能フィールドについての説明は、479ページの『第24章 DLSw の使用』 の **add qllc** コマンドの項を参照してください。*Hits* フィールドは、 DLSw が着信 QLLC Call_Request パケット内のコネクション ID とこのコネクション ID 間の一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
```

このディスプレイの構成可能フィールドについての説明は、479ページの『第24章 DLSw の使用』 の **add qllc** コマンドの項を参照してください。

Type フィールドは、次の値を取ります。

PERM (Permanent)
このステーション定義は、前回にルーターがスタートした時点でルーター構成の一部になりました。

STAT (Static)
このステーション定義は、前回にルーターがスタートした後で、DLSw 監視機能を使用してユーザーによって追加されました。

DYNM (Dynamic)
DLSw は、着信コールの結果として、または 1 つのリモート

DTE アドレスに複数の発信コールを行う必要があるために、このステーション定義を動的に作成しました。

セッション・リストの最下部の要約行に、現在存在する各タイプのセッション数が表示されます。

State フィールドは、QLLC 側から見た DLSw コネクションの状態を示しています。これらの状態は、**list dls sess** コマンドによって表示されるメイン DLS 状態とは異なっており、QLLC インターフェースの状態に関する追加情報を提供します。可能な値は、次のとおりです。

NET_DOWN
X.25 インターフェースが現在ダウンしています。

PLC_DOWN
X.25 パケット・レイヤーが現在ダウンしています。

DISCONNECTED
この状態および以降のすべての状態では、X.25 インターフェースおよびパケットはアップです。この状態では、DLSw はエンド・ステーションが接続を確立するのを待っています。

XID_POLL
DLSw は、最初に装置に接続するため、または損失した接続を回復するために、QXID (XID_null) を使用して 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、最初に装置に接続するため、または損失した接続を回復するために、QSM を使用して 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・ステーションから応答を受信し、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 の探索が成功し、回線開始要求が開始されました (CUR_cs を送信)。

CALL_REQ_PEND
DLSw は QLLC エンド・ステーションにコール・リクエストを送信し、そのコールが正常に応答されるかどうかを待っています。

ESTABLISHED
DLSw 回線は 『circuit established』 状態にあります。SNA XID の送受信に使用できます。

CONTACT_PEND
DLSw は QSM を QLLC エンド・ステーションに送信し、QUA を待っています。

CONNECTED

DLSw 回線は完全にアップになり、I フレーム・エンド・ユーザー・データを伝送することができます。

DISC_PEND

DLSw は回線切断を QLLC ステーションに要求し、確認を待っています。

RESET_PEND

DLSw は PVC リセットまたは SVC 切断要求を QLLC ステーションに要求し、確認を待っています。

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
```

このディスプレイの構成可能フィールドについての説明は、479ページの『第24章 DLSw の使用』 の **add qllc** コマンドの項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、使用可能であるかどうかを示しています。『Type』 フィールドは、上記の **list qllc sessions** コマンドの項で説明したのと同じ値を取ります。

sdlc config SDLC 接続 PU の構成された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 セッションに関する情報を表示します。

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 ネゴシエーションを行う能力を備えているので、接続された SDLC リンク・ステーションはリンクを、ルーターで構成された値とは異なる SDLC ステーション・アドレスに設定することが可能です。その場合には、2 つの SDLC ステーション・アドレスが、このディスプレイの 『Addr』 欄の下に xx(yy) のフォーマットで表示されます。このフォーマットでは、xx は、このルーターで構成されたステーション・アドレスを示し、引き続きすべての構成コマンドおよび監視コマンドで、このリンク・ステーションを参照するために使用されます。接続 SDLC 装置によって設定された現行の動作アドレスは、右側に括弧に入れて表示されている値 yy です。

tcp capabilities

パートナー DLSw ルーターからの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 2212 AIS 2212-AIS
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 組織ユニーク識別子 (OUI)。IBM の OUI は X'10005A' です。

Vendor version

近隣 DLSw が自身を説明するために送信するテキスト文字列。『(not available)』 は、近隣の実現がそのような文字列を送信しなかったことを示しています。

Initial pacing window

各新規回線に対して許可されている初期ペーシングを受信したときに、この DLSw が近隣 DLSw に送信できるペーシング SSP メッセージの数

Preferred TCP connections

この近隣が希望する TCP コネクションの数 (1 または 2)。IBM 2212 は要求された数に合わせて調整し、これを要求した近隣への全二重 TCP コネクションを 1 つだけ持つことになります。

Supported SAPs

近隣 DLSw がその LAN インターフェース上にオープンした (または、自動的にオープンする) SAP、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・リストを、その近隣にローカルな MAC アドレスの全リストまたは部分リストとして見なすかどうかを示します。『(not supplied)』 のレスポンスは、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示します。

MAC List

この近隣が MAC アドレス・リストに入れて送信した、すべての MAC リスト値およびマスクを表示します。『(none supplied)』 のレスポンスは、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示します。

NetBIOS Exclusivity

この近隣によって送信された NetBIOS ネーム・リストを、その近隣にローカルな NetBIOS ネームの全リストまたは部分リストとしてみなすかどうかを示します。『(not supplied)』 の

レスポンスは、この近隣が NetBIOS ネーム・リストを、その機能の一部として送信しなかったことを示します。

NetBIOS Name List
この近隣がその NetBIOS ネーム・リストに入れて送信した、すべての NetBIOS ネーム修飾子を表示します。『(none supplied)』 のレスポンスは、この近隣が NetBIOS ネーム・リストを、その機能の一部として送信しなかったことを示します。

Multicast Version
この近隣がどのバージョンのマルチキャストを、AIW 標準によって定義されるようにサポートしているかを示します。*not supplied* のレスポンスは、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示します。

IBM CST
どの IBM コネクティビティー・セットアップ・タイプ (CST) をこの近隣が構成したかを示します。*not supplied* のレスポンスは、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示します。

IBM Multicast
特定の IBM マルチキャスト機能がこの近隣で利用可能かどうかを示します。*not supplied* のレスポンスは、この近隣が IBM マルチキャスト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
この近隣から受信された最後の IBM Capex Correlator の値を示します。*not supplied* のレスポンスは、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された TCP コネクション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 セッションの状態を表示します。

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 その近隣が発見されたグループ (該当する場合)

IP Address
DLSw に使用された近隣 IP アドレス

Conn State

この近隣へのトランスポート・コネクション (1 つまたは 2 つの TCP コネクションから構成される) の状態。有効な状態は、次のとおりです。

DOWN
TCP セッションが確立されていません。機能の交換は行われません (受動パートナーのみ)。

CAPEX FAILED
機能交換の試みが失敗しました。TCP セッションはダウンしました。

Unicasting
TCP セッションは確立されていません。機能は正常に交換されました (受動パートナーのみ) (DLSw 探索トラフィックに対してレディー状態)。

PENDING R/W
この 2212 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 2212 間の TCP セッションはアクティブですが、この 2212 と近隣間の TCP セッションはアクティブでありません。

RD EST/WR PEND
この 2212 と近隣間の TCP セッションはアクティブですが、近隣とこの 2212 間の TCP セッションはアクティブでありません。

CAPEX PENDING
TCP セッションが確立されました。機能の交換が進行中です。

ESTABLISHED
TCP セッションが確立されました。機能が交換されました (DLSw セッションへの使用準備完了)。

CLOSING
TCP セッションをダウンにしているところです。

RECONNECT WAIT
TCP 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っています。

CST 現行の接続性設定タイプ。次のとおりです。

```
a - Locally configured as active
p - Locally configured as passive
A - Locally configured as passive, but operating in active mode
    due to neighbor requirements
D - Not locally configured, but a dynamic neighbor TCP connection
```

Version
近隣の DLSw プロトコル・レベル。AIW VnRm (AIW 標準準拠のルーター)、RFC1434+ (AIW V1R0 以前の実現)、または UNKNOWN のいずれか。

Active Sess
このトランスポート・コネクション上のアクティブの (任意の状態) DLSw セッション (回線) の現在数

Sess Creates
前回のルーターのリスタートまたはこのトランスポート・コネクションの 『add tcp』 以降に CIRC_EST 状態に入った DLSw セッション (回線) の合計数

tcp statistics 前回のルーターのリスタートまたはこのトランスポート・コネクションの 『add tcp』 以降の、TCP トランスポート・コネクション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 各種のアクティビティーに対するユーザー指定の待ち時間。

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/IP アドレス・データベース・エントリーを保持する時間。ゼロは、このデータベース内のエントリーは経時処理されないことを示します。

Max wait timer for ICANREACH
ルーターが、そのセッションは起動しないものと判定する前に CANUREACH メッセージに対するレスポンスを待つ時間

Wait timer for LLC test response
ルーターが LLC テスト・フレームを再送する前に LLC テスト・レスポンスを待つ時間

Wait timer for SDLC test response
ルーターが DLSw セッションをスタートするために SDLC ステーションへの接続を再試行する前に待つ時間

QLLC session retry timer
ルーターが DLSw セッションをスタートするために QLLC ステーションへの接続を再試行する前に待つ時間

Join Group Interval
DLSw グループ公示の同報通信間の時間

Neighbor priority wait timer
指定のセッション確立の試行時に DLSw が近隣を選択する前に待つ時間

Neighbor Inactivity Timer
DLSw が、非アクティブの (セッション数がゼロの) 受動 TCP コネクションを切断する前に待つ時間。

Delay sending TEST response
MAC アドレスの探索から TEST レスポンスを送信するまでに待つ時間の長さ。

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 コマンドの説明は、165ページの『第8章 NetBIOS の構成および監視』を参照してください。

Open-Sap

open-sap コマンドは、DLSw SRAM 構成に影響を与えずに、指定されたサービス・アクセス・ポイント (SAP) の DLSw 交換を動的に使用可能にするのに使用します。

構文:

open-sap

例: **`open-sap`**

open-sap パラメーターの追加情報および説明については、543ページの『Open-Sap』を参照してください。

Set

set コマンドは、 LLC2 パラメーター、最大数 DLSw セッション、プロトコル・タイマー、 TCP 動的近隣、 QLLC 動作のパラメーター、mac アドレス・リスト関連パラメーター、および回線優先順位パラメーターを、DLSw SRAM 構成に影響を与えずに動的に変更するのに使用します。

構文:

set dynamic-tcp

llc2

mac-list

memory

priority

qllc

timers

dynamic-tcp 動的近隣 TCP コネクション (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のコネクトイン) の種々の TCP パラメーターを指定できるようにします。DLSw は動的近隣が使用可能にされている場合にのみ、これらの値を使用します。

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は、479ページの『第24章 DLSw の使用』の **add tcp** コマンドの項を参照してください。

llc2 特定の SAP の特定の LLC2 属性を構成できるようにします。

例: set llc2

(**set llc2** コマンドの例が 545 ページにあります。)

mac-list ローカル MAC アドレスの排他性を設定できるようにします。このコマンドは、以下の監視コマンドを使用して以前に行ったすべての変更を認定するのにも使用できます。

- 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、新しい情報を通信するために、新規のランタイム機能がすべての 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 このコマンドは、DLSw に割り振られるメモリーの総量、および各 DLSw セッションに配分されるメモリーの総量を動的に指定することができます。

例: set memory

set memory コマンドの使用例が 546 ページに示されています。

priority SNA 回線および NetBIOS 回線に使用する回線優先順位を指定できるようにします。回線優先順位を Critical、High、Medium、または Low に (Critical から Low に降順で) 指定できます。

また、このコマンドを使用して、各回線優先順位のトランスポート転送数の比率を構成したり、NetBIOS に使用する最大フレーム・サイズを設定することもできます。ユーザーのネットワークに透過的にブリッジされる (TB) セグメントが含まれている場合は、最大 NetBIOS フレーム・サイズは少なくとも 1470 を使用してください。

例: set priority

set priority コマンドの詳細については、547 ページを参照してください。

qllc 着信した動的 QLLC コールによって確立される DLSw セッションの開始側 MAC アドレスとして使用される動的割り当て MAC アドレスの範囲を指定できるようにします。

範囲の指定は、範囲を示す基本 MAC アドレス 『X』 と、動的アドレスの最大数 『N』 とによって行います。DLSw は X ～ X+(N-1) の範囲の 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 コマンドの例が 548 ページに示されています。

Test

test コマンドは、現在アクティブの MAC アドレス・キャッシュおよび MAC アドレス・リストと照合してテストするのに使用します。

構文:

test cache

mac-list

cache 特定の MAC アドレスあてのフレームを、現行のキャッシュおよび DLSw ピアの情報に基づいて転送する方法を決めることができます。

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 指定された MAC アドレスを、現在アクティブのすべての MAC アドレス・リスト・エントリー (ローカルおよびリモート) と照合できるようにします。これは MAC アドレス・リストの競合問題を解決するのに役立ちます。

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26章 ARP の使用

この章では、ルーター上でのアドレス解決プロトコル (ARP) および逆アドレス解決プロトコル (逆 ARP) 使用法について説明します。本章には、以下の節が含まれています。

ARP の概説

ARP プロトコルは、ネットワーク・レイヤー・アドレスを物理媒体アクセス制御 (MAC) アドレスに動的にマップする低位プロトコルです。あて先システムのネットワーク・レイヤー・アドレスのみが与えられている場合、ARP は同じネットワーク・セグメント内のあて先ホストの MAC アドレスを見つけます。

たとえば、ルーターがその LAN の 1 つに接続されたホストあての IP パケットを受信したとします。このパケットには、32 ビットの IP あて先アドレスのみが入っています。データ・リンク・レイヤー・ヘッダーを作成するために、ルーターはあて先ホスト の物理 MAC アドレスを獲得します。次に、ルーターはこのアドレスを 32 ビット IP アドレスにマップします。この機能を*アドレス解決* と呼んでいます。 580ページの図47 は、ARP がどのように働くかを示しています。

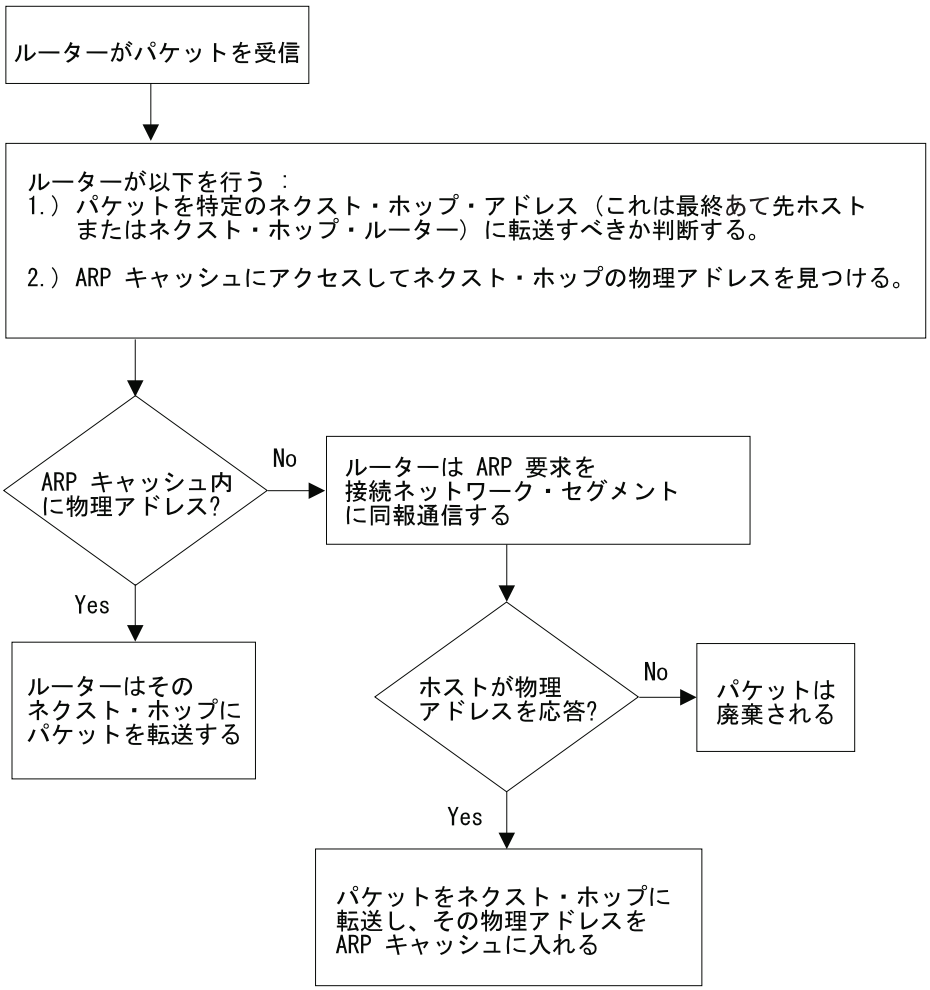


図 47. ARP アドレス解決同報通信

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ときに、ルーターは ARP (変換) キャッシュにアクセスします。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、ルーターは接続されたネットワーク・セグメント上のすべてのホストに ARP 要求を同報通信し、正しい 物理 MAC アドレスを見つけます。正しい物理 MAC アドレスを持つノードは、ルーターに応答します。ルーターはそのノードにパケットを送信し、将来に使用するために、その物理 MAC アドレスを変換キャッシュに入れます。

逆 ARP の概説

逆 ARP (RFC 1293 で説明) は、フレーム・リレー・ネットワークのために作成されたものです。このプロトコルは、フレーム・リレー・ネットワーク上のルーターが、他のルーターのプロトコル・アドレスを確認する方法を定義しています。この方式は、アドレス解決のために同報通信 ARP パケットを使用する必要性を排除することによって、トラフィックを非常に効率的に削減します。逆 ARP は、回線がアクティブになるとただちに、逆 ARP 要求パケットをハードウェア・アドレスに送信してプロトコル・アドレスを見つけます (フレーム・リレー回線の場合、回線識別子が

フレーム・リレーにおけるハードウェア・アドレスに相当します)。リモート・ルーターはそのプロトコル・アドレスを用いて応答し、得られたマッピングが ARP キャッシュに保管されます。

逆 ARP によって確認されたプロトコル・アドレス/ハードウェア・アドレス・エントリーは、ARP リフレッシュ・タイマーが満了してもタイムアウトになりません。マッピングは、フレーム・リレー回線がダウンした場合を除いて、エージングされることはありません。このことは、ルーターは ARP キャッシュを更新するために ARP 同報通信を送信する必要がないことを意味しています。ただし、ルーターは、他の (リモート) ルーターがそのプロトコル・アドレスを変更したときには、エントリーの更新を許します。

ARP および逆 ARP に対するサポートはどちらも、プロトコルおよびハードウェア・アドレスの動的マッピングのために、ルーターがフレーム・リレーを介して他のベンダーのルーターと相互運用する可能性を大きく拡大します。フレーム・リレーで接続された他のルーターが逆 ARP をサポートしている場合は、上述のように、マッピングが動的に確認されます。接続ルーターが、逆 ARP はサポートしないがフレーム・リレー上で 『従来の』 ARP はサポートしている場合も、ARP を使用してマッピングを動的に確認することが可能です (580ページの図47を参照してください)。

必要な場合には、フレーム・リレー構成コマンド **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、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*のフレーム・リレー・インターフェースの構成および監視の章を参照してください。

第27章 ARP の構成および監視

この章では、ARP プロトコルのアクティビティーを構成および監視する方法、および ARP 監視コマンドを使用する方法について説明します。本章には、以下の節が含まれています。

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は、*アクセス・インテグレーター・サービス 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。

ARP *構成* プロセスにアクセスするには、次の手順を使用します。

1. OPCON プロンプトで、**talk 6** を入力する。 (このコマンドの詳細については、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*の “OPCON プロセス” の章を参照してください。)たとえば、次のように入力します。

   ```
    * talk 6
   Config>
   ```

   talk 6 コマンドを入力すると、端末に CONFIG プロンプト (`Config>`) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。
2. CONFIG プロンプトで **prot arp** コマンドを入力して、`ARP Config>` プロンプトに進む。

ARP および逆 ARP 構成コマンド

この節では、非 ATM ネットの ARP 監視コマンドについて説明します。 表35 は、ARP 構成コマンドをリストしています。ARP 構成コマンドへは `ARP config>` プロンプトからアクセスします。

表 35. ARP 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add Entry	MAC アドレス変換エントリーを追加します。
Change Entry	MAC アドレス変換エントリーを変更します。
Delete Entry	MAC アドレス変換エントリーを削除します。
Disable Auto-refresh	ARP 自動リフレッシュを使用不可にします。
Enable Auto-refresh	ARP 自動リフレッシュ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、タイムアウト値をリフレッシュします。

表 35. ARP 構成コマンドの要約 (続き)

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

Add Entry

add entry コマンドは、『static protocol-to-hardware address mapping』 エントリーを追加するのに使用します。このコマンドは、現在は IP アドレスに対して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

デフォルト値: 0

prot-type **有効値**: ARP がサポートする任意のプロトコル

デフォルト値: IP

prot-addr **有効値**: 任意の有効な IP アドレス

デフォルト値: 0

MAC-addr **有効値**: 任意の有効な MAC アドレス

デフォルト値: 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、『static protocol-to-hardware address mapping』 エントリーを変更するのに使用します。このコマンドは、現在は IP アドレスに対して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、変更す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

デフォルト値: 0

prot-type **有効値**: ARP がサポートする任意のプロトコル

デフォルト値: IP

prot-addr **有効値**: 任意の有効な IP マスク

デフォルト値: なし

MAC-addr **有効値**: 任意の有効な MAC アドレス

デフォルト値: 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、『static protocol-to-hardware address mapping』 エントリーを削除するのに使用します。このコマンドは、現在は IP アドレスに対して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

デフォルト値: 0

prot-type **有効値**: *IP* または *IPX*

デフォルト値: IP

prot-addr **有効値**: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

例: delete entry

```
Interface Number [0]?
Protocol [IP]?
IP Address [0.0.0.0]?
```

Disable Auto-Refresh

disable auto-refresh コマンドは、自動リフレッシュ機能を使用不可にするのに使用します。自動リフレッシュ機能は、リフレッシュ・タイマーが満了する前に、変換キャッシュ内のエントリーに基づいて ARP 要求を送信するルーターの機能です。要求は、同報通信されるのではなく、現行の変換内のハードウェア・アドレスに直接送信されます。自動リフレッシュが使用不可の場合、 'プリエンプティブ (優先権)' ARP 要求は行われず、リフレッシュ・タイマーは満了が許され、ARP 変換はテーブルから除去されます。着信プロトコル・アドレスあての次のプロトコル・パケットによって、新しい ARP 要求がネットワークに同報通信されます。

構文:

disable auto-refresh

例: disable auto-refresh

Enable Auto-Refresh

enable auto-refresh コマンドは、自動リフレッシュ機能を使用可能にするのに使用します。自動リフレッシュ機能は、リフレッシュ・タイマーが満了する前に、変換

キャッシュ内のエントリーに基づいて ARP 要求を送信するルーターの機能です。要求は、同報通信されるのではなく、現行の変換内のハードウェア・アドレスに直接送信されます。

自動リフレッシュを使用可能にすると、エントリーは、その使用状況に関係なくキャッシュ内に保存されます。多数のノードが存在するネットワークでは、過度のエントリーがキャッシュに保存されることになり、ルーターの性能に悪影響を与えることがあります。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役立ちます。

構文:

enable auto-refresh

例: `enable auto-refresh`

List

list コマンドは、SRAM に保管されているルーターの ARP 構成のコンテンツを表示するのに使用します。list コマンドは、リフレッシュおよび使用タイマーの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 構成の後に、すべての ARP エントリーを表示します。

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 各種の ARP パラメーター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 エントリーをリストします。

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*

リフレッシュ・タイマーのタイムアウト値を変更します。 リフレッシュ・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数で入力します。ゼロ (0) の設定値は、リフレッシュ・タイマーをオフ (使用不可) にします。

このタイマーは、ARP 変換キャッシュ・エントリーをリフレッシュする時期 (自動リフレッシュが使用可能の場合)、または除去する時期 (自動リフレッシュが使用不可の場合) を決めます。タイマーを使用不可にすると、新たに確認されたアドレス変換によってエントリーが除去されるまで、ARP **clear** 監視コマンドによってエントリーが手動でクリアされるまで、あるいはルーターがリスタートされるまで、エントリーは保存されます。

有効値: 0 ～ 65535 の範囲の整数 (分)

デフォルト値: 5 分

例: set refresh-timer 3

ARP 監視環境へのアクセス

ARP 監視コマンドにアクセスするには、次の手順を使用します。このプロセスにより 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** を入力する。 (このコマンドの詳細については、*アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*の “OPCON プロセス” の章を参照してください。)たとえば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、端末に GWCON プロンプト (+) が表示されます。最初に構成に入ったときにプロンプトが表示されない場合は、**Return** をもう一度押してください。

2. + プロンプトで **protocol arp** コマンドを入力して、ARP> プロンプトを表示する。

   例:

   ```
   + prot arp
   ARP>
   ```

ARP 監視コマンド

この節では、ARP 監視コマンドについて説明します。 ARP 監視コマンドには ARP> プロンプトからアクセスできます。 表36 は、コマンドを示しています。

表 36. ARP 監視コマンド

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Clear	指定されたインターフェースのキャッシュをクリアします。
Dump	指定されたインターフェースのキャッシュを表示します。
Hardware	各 ARP が構成されたネットワークをリストします。
Ping	装置と指定のエンド・ステーション間の接続可能性を検証します。
Protocol	各 ARP が構成された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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Clear

clear コマンドは、指定されたネットワーク・インターフェースの ARP キャッシュをフラッシュするのに使用します。 不正なトランザクションを強制的に削除するのにも **clear** コマンドを使用できます。

特定のインターフェースをクリアする場合は、インターフェースまたはネットワーク番号を、コマンドの一部として入力します。インターフェース番号を入手するには 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、指定されたネットワーク/プロトコルの組み合わせの 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を表示する場合は、インターフェースまたはネットワーク番号を、コマンドの一部として入力します。インターフェース番号を入手するには CONFIG **list devices** コマンドを使用します。

そのネットワークに複数のプロトコルがある場合は、プロトコル番号も指定する必要があります。これにより、監視は、そのデータベースに保管されているハードウェア・アドレスとプロトコルのマッピングを表示します。ARP が、指定のインターフェースで 1 つだけのプロトコルに使用されている場合は、プロトコル番号は任意選択です。プロトコル番号を入手するには CONFIG **protocol** コマンドを使用します。

dump コマンドのディスプレイには、各マッピングのハードウェア・アドレス、プロトコル・アドレス、およびリフレッシュ・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
```

有効なリフレッシュ・タイマー・パラメーターは、次のとおりです。

Permanent
静的に構成されたハードウェア・アドレスとプロトコル・アドレス間のマッピング (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)。これらのエントリーはエージングが行われず、動的に確認された (learned) マッピングによって上書きされることもありません。

minutes to expire
このマッピングがエージングによって満了するまで、またはこのマッピングがリフレッシュされるまで (自動リフレッシュが使用可能の場合) の分数。このパラメーターは数値で表します。

Not Aging
逆 ARP を通して確認された固定 SVC または PVC マッピング。これは、回線がダウンしたときにのみエージングが開始されます。このマッピングは、新規に確認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 で登録されたネットワークを表示するのに使用します。**hardware** コマンドは、ARP によって登録された各ネットワークをリストし、各ネットワークのハードウェア・アドレス・スペース (Hardware AS) とローカル・ハードウェア・アドレスを表示します。

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 エントリーは IP トンネル伝送を表しており、ハードウェア・アドレス・フィールドは、IP トンネルの IP アドレスを示しています。

Ping

ping コマンドは、ルーターに ICMP エコー要求を指定のあて先に送信させるのに使用します。**ping** コマンドの詳細については、315ページの『Ping』を参照してください。

Protocol

protocol コマンドは、ARP によって登録されたアドレスをもつプロトコルを表示 (ネットワーク別に) 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・スペース (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 エントリーはソース・ルーティングを表しています - MAC アドレスを示すのにプロトコル・アドレスが使用されます。トークンリング **dump** コマンドを使用すると、実際の RIF エントリーを見ることができます。

Statistics

statistics コマンドは、ARP モジュールの動作に関する各種の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 レイヤーがビジーのため入力で廃棄された ARP パケットの数を表すカウンターを表示します。表示されるカウントは、ネットワーク・インターフェース当たりの数値です。

ARP cache meters	ARP キャッシュの動作に関する各種の計量値から構成されます。表示されるカウントはすべて各インターフェースのプロトコル当たりの数値です。
Net	インターフェースの数を表示します。
Prot	プロトコルの数を表示します。
Max	通常の最大長ハッシュ・チェーンを表示します。
Cur	現行の最大長ハッシュ・チェーンを表示します。
Cnt	現在アクティブのエントリーのカウントを表示します。
Alloc	作成されたエントリーのカウントを表示します。
Rfrsh:Tot	このネットワーク・インターフェースとプロトコルあてに送信されたリフレッシュ要求の数を表示します。
Fail	内部資源が利用不能であったために失敗した自動リフレッシュの試行回数を表示します。このカウントは、エントリーがリフレッシュされたか否かには関係ありません。
TMOs:Rfrsh	リフレッシュ・タイマーのタイムアウトのために削除されたエントリーのカウントを表示します。

第28章 IPX の使用

この章では、2212 上での IPX プロトコルの使用方法について説明します。本章には、以下の節が含まれています。

- 『IPX の概説』
- 598ページの『IPX の構成』
- 599ページの『オプションの構成タスク』

IPX の概説

IBM の IPX 実現方式では、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。これは、次のような特性を持っています。

- すべての以前の Novell NetWare バージョン環境との整合性
- NetWare ファイル・サーバーのブリッジング機能、および独立型 NetWare ブリッジとの整合性
- Novell NetBIOS エミュレーターに対するサポート

IPX アドレッシング

以下の節で IPX アドレッシング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。郵便の住所の都市 - 町村 - 番地のように、複数の部分から構成されるアドレスを使用することができます。たとえば、IPX はネットワーク番号 (都市)、ホスト番号 (町村)、およびソケット番号 (番地) のように指定します。これらのアドレスにより、異なるネットワーク上にある 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 回線には 6 バイトのホスト (ノード) 番号が必要です。

トークンリングおよびイーサネット・インターフェースは、それぞれの MAC アドレスをホスト番号として使用しており、これらは変更できません。

シリアル・ラインは、ハードウェア MAC アドレスを持っていないので、ユーザーが固有なホスト番号を指定する必要があります。IPXWAN は、後ろに x'0000' を付いた構成済みノード ID を使用します。

IPX 回線

IPX ルーティング・ソフトウェア・モデル・ネットワークは、単一の IPX 同報通信回線として、1 つまたは複数の IPXWAN ポイント・ポイント回線として、あるいは両方の回線タイプを組み合わせたものとしてインターフェースをとります。回線上

で使用されるカプセル化、IPX アドレッシング、およびルーティング・プロトコルのタイプは、基礎となる DLC のほか、IPX 回線が同報通信または IPXWAN ポイント・ポイントとして構成されているかどうかによって異なります。

IPX 同報通信回線には、次の特性があります。

- LAN インターフェース上で使用される
- IPXWAN が構成されていない場合は WAN インターフェース上で使用される
- 1 つのインターフェースにつき単一の IPX 同報通信に制限される
- 非ゼロ IPX ネットワーク番号を割り当てる必要がある
- LAN の場合、ネットワーク・インターフェースの MAC アドレスを回線の IPX ノード番号として使用する
- WAN の場合、構成済みの IPX ホスト番号を回線の 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同時使用を可能にする

IPXWAN ポイント・ポイント回線には、次の特性があります。

- WAN インターフェース上でのみ使用できる
- 1 つのインターフェースにつき単一の IPXWAN ポイント・ポイント回線に制限されない
- IPXWAN を使用してパラメーターをネゴシエーションする
- IPX ネットワーク番号を必要としない
- 回線の IPX ノード番号として IPXWAN ノード ID の後に 0000 を使用する
- 単一のネゴシエーションされたルーティング・タイプに制限される

以下の節では、サポートされているネットワーク・インターフェースの各タイプ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)

IPX ルーティング・ソフトウェアは、LAN インターフェースを単一の IPX 同報通信回線としてモデル化します。

回線には、固有の非ゼロ IPX ネットワーク番号を割り当てる必要があります。

ネットワーク・インターフェースの MAC アドレスは、回線の IPX ノード番号として役立ちます。

LAN 全ステーション・アドレス (x'FFFFFFFFFFFF') は、RIP や SAP 更新といった同報通信パケットの受信や送信に使用されます。

該当するタイプの LAN インターフェースについては、通常のカプセル化タイプがサポートされています。

IPX 最大パケット・サイズは、インターフェース用に構成された MTU から割り出されます。

トークンリング・インターフェースの場合、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ると、IPX 転送機能は、ソース・ルート・ブリッジを介してエンド・ステーション (およびその他のルーター) まで到達します。

以下のルーティング・タイプのどちらも、あるいはそれらすべてを回線上で使用できます。

- 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・ソフトウェアは、PPP インターフェースを単一の IPX 同報通信回線として、あるいは単一の IPXWAN ポイント・ポイント回線としてモデル化します。

IPX 最大パケット・サイズは、基礎となる PPP DLC によってネゴシエーションされた MTU から割り出されます。

IPX 同報通信回線: 同報通信回線として構成する場合には、回線にゼロ以外の固有のネットワーク番号を割り当てる必要があります。

PPP インターフェースと関連付けられている MAC アドレスはないため、回線の IPX ノード番号として、構成済みのホスト番号が使用されます。

以下のルーティング・タイプのどちらも、あるいはそれらすべてを回線上で使用できます。

- 静的ルート/サービス
- RIP/SAP (番号制)

IPXWAN ポイント・ポイント回線: IPXWAN ポイント・ポイント回線として構成されている場合は、IPXWAN を使用して、ルーティング・パラメーターをネゴシエーションします。

IPXWAN 番号制 RIP ルーティング・タイプには、回線に割り当てられるゼロ以外の固有のネットワーク番号が必要です。その他の IPXWAN ルーティング・タイプ (無番号 RIP、静的ルーティング) には、ネットワーク番号 (値 0) は必要ありません。

PPP インターフェースと関連付けられている MAC アドレスはないため、回線の IPX ノード番号として、後ろに 0000 が付いている IPXWAN ノード ID が使用されます。

回線上でネゴシエーション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であれば、その他のルーティング・タイプはネゴシエーションされません。以下に示す残りのタイプのどちらも、またそのすべてを使用可能にすることができ、優先順位の高いものから低い方へ単一のルーティング・タイプに対してネゴシエーションされます。

- 無番号 RIP/SAP
- 番号制 RIP/SAP

フレーム・リレー

IPX ルーティング・ソフトウェアは、フレーム・リレー・インターフェースを、以下のものとしてモデル化します。

- 単一の IPX 同報通信回線として
- 1 つまたは複数の IPXWAN ポイント・ポイント回線の集合として

- これら両方を組み合わせたものとして

IPX 最大パケット・サイズは、インターフェース用に構成された MTU から割り出されます。

基礎となるフレーム・リレー DLC は、InARP を使用して、あて先 IPX ノード・アドレスを適切なフレーム・リレーにマップします。任意により、あて先 IPX ノード・アドレスを、InArp をサポートしていないルーターに接続されているVC に合わせて静的に構成することができます。

IPX 同報通信回線: IPXWAN ポイント・ポイント回線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すべてのバーチャル・サーキットは、ゼロ以外の固有のネットワーク番号を割り当てる必要のある単一の IPX 同報通信回線としてグループにまとめられ、モデル化されます。そのため、フレーム・リレー・ネットワーク上のルーターを相互接続するためにユーザーが定義した、基礎となるバーチャル・サーキットは、IPX ルーティング・ソフトウェアには影響を与えません。

フレーム・リレー・インターフェースと関連付けられている MAC アドレスはないため、回線の IPX ノード番号として、構成済みのホスト番号が使用されます。

LAN 全ステーション・アドレス (x'FFFFFFFFFFFF') は、回線上で IPX 同報通信アドレスとして役立ちます。同報通信アドレスにアドレス指定されたパケットは、基礎となるフレーム・リレー DLC により、IPX 同報通信回線内のすべての VC で送信されます。このフレーム・リレー・プロトコル同報通信機能は、以下のフレーム・リレー構成オプションを使用可能にすると起動されます。

- プロトコル同報通信
- マルチキャスト・エミュレーション

非完全メッシュ・フレーム・リレー・トポロジーをサポートするために、IPX 同報通信回線上で水平分割を使用不可にすることができます。こうすると、RIP および SAP は IPX 同報通信回線内のすべてのバーチャル・サーキットに情報を伝達することができるため、同じ IPX 同報通信回線内のバーチャル・サーキット間での中間ルーティングが発生します。

完全メッシュ・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。

以下のルーティング・タイプのどちらも、あるいはそれらすべてを回線上で使用できます。

- 静的ルート/サービス
- RIP/SAP (番号制)

IPXWAN ポイント・ポイント回線: 個別のフレーム・リレー PVC (SVC はサポートされていません) を介した IPXWAN ポイント・ポイント回線として動作するよう、IPX を構成することができます。IPXWAN は、ルーティング・パラメーターをネゴシエーションするのに使用されます。

IPXWAN 番号制 RIP ルーティング・タイプには、回線に割り当てられるゼロ以外の固有のネットワーク番号が必要です。その他の IPXWAN ルーティング・タイプ (無番号 RIP、静的ルーティング) には、ネットワーク番号 (値 0) は必要ありません。

フレーム・リレー・インターフェースと関連付けられている MAC アドレスはないため、回線の IPX ノード番号として、後ろに 0000 が付いている IPXWAN ノード ID が使用されます。

回線上でネゴシエーション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であれば、その他のルーティング・タイプはネゴシエーションされません。以下に示す残りのタイプのどちらも、またそのすべてを使用可能にすることができ、優先順位の高いものから低い方へ単一のルーティング・タイプに対してネゴシエーションされます。

- 無番号 RIP/SAP
- 番号制 RIP/SAP

X.25

IPX ルーティング・ソフトウェアは、X.25 インターフェースを単一の IPX 同報通信回線としてモデル化します。そのため、フレーム・リレー・ネットワーク上のルーターを相互接続するためにユーザーが定義した、基礎となる VC は、IPX ルーティング・ソフトウェアに影響を与えません。

回線には、ゼロ以外の固有の IPX ネットワーク番号を割り当てる必要があります。

X.25 インターフェースと関連付けられている MAC アドレスはないため、回線の IPX ノード番号として、構成済みのホスト番号が使用されます。

LAN 全ステーション・アドレス (x'FFFFFFFFFFFF') は、回線上で IPX 同報通信アドレスとして役立ちます。同報通信アドレスにアドレス指定されたパケットは、基礎となる X.25 DLC により、IPX 同報通信回線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に構成された MTU から割り出されます。

非完全メッシュ X.25 トポロジーをサポートするために、IPX 同報通信回線上で水平分割を使用不可にすることができます。こうすると、SAP は IPX 同報通信回線内のすべてのあて先 X.25 アドレスに情報を伝達することができるため、同じ IPX 同報通信回線内の VC 間での中間ルーティングが発生します。

完全メッシュ 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。

以下のルーティング・タイプのどちらも、あるいはそれらすべてを回線上で使用できます。

- 静的ルート/サービス
- RIP/SAP (番号制)

あて先 IPX ノード・アドレスは、すべてのあて先 X.25 アドレス用に静的に構成する必要があります。X.25 DLC は InArp をサポートしていないからです。

IPX の構成

この節では、最初に IPX の構成方法について説明します。その後の各節で、ユーザーが設定できるオプション・パラメーターについて説明します。

1. 次のような IPX 構成プロンプトを表示する。

```
* 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. WAN または LAN 上に同報通信回線、あるいは WAN 上に IPXWAN 回線を追加します。

```
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 は、IPXWAN 番号なし RIP または静的ルーティング・インターフェースにのみ有効です。IPX ネットワーク番号 FFFFFFFF は、有効な IPX ネットワーク番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX デフォルト・ルート用に予約されているため、IPX ネットワーク番号として使用してはなりません。

4. シリアル・サーキットを介して実行するよう IPX を使用可能にしてある場合には、ルーターに固有のホスト番号を割り当てます。

```
IPX config>set host-number
Host number for serial lines (in hex) []? 2
```

5. 任意により、イーサネットまたはトークンリングのフレーム・タイプを変更します。イーサネットまたはトークンリング以外の回線のフレーム・タイプを設定する必要はありません。利用可能なフレーム・タイプについての説明は、629ページの『Frame』を参照してください。

   デフォルトのカプセル化フォーマットは、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

   次のような **frame** コマンドを使用します。

```
IPX config> frame ethernet_8023
IPX circuit number [1]? 2
```

6. 任意により、デフォルト値を使用したくない IPXWAN パラメーターをどれでも変更します。

```
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
```

オプションの構成タスク

ユーザーが調整できるオプション設定について、以下の節で説明しています。

- 『IPX RIP ネットワーク・テーブル・サイズの指定』
- 『RIP 更新間隔の指定』
- 600ページの『IPX SAP サービス・テーブル・サイズの指定』
- 600ページの『SAP 更新間隔の指定』
- 601ページの『IPX キープアライブおよびシリアル化パケット・フィルター』
- 601ページの『複数ルートの構成』
- 602ページの『静的ルートの構成』
- 603ページの『静的サービスの構成』
- 603ページの『RIP デフォルト・ルートの構成』
- 604ページの『グローバル IPX フィルター (IPX アクセス制御) の構成』
- 606ページの『グローバル SAP フィルター』
- 608ページの『IPX 回線フィルター - 概説』
- 611ページの『IPX 性能の調整』
- 613ページの『水平分割ルーティング』

IPX RIP ネットワーク・テーブル・サイズの指定

IPX RIP ネットワーク・テーブルには、各 IPX ネットワークに関する情報が入っています。デフォルトのテーブル・サイズは 32 です。テーブル・サイズは 1 ～ 2048 の範囲に構成できますが、ルーターのメモリーの限界から、最大テーブル・サイズは使用できない場合があります。

```
IPX config>set maximum networks
New Network table size [32]? 32
```

RIP 更新間隔の指定

IPX 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、パケットが通るパスを示します。RIP 更新間隔は、ルーターがその回線にルーティング情報テーブルを同報通信する頻度を決めます。また、RIP エントリーが除去される前に残存する時間の長さも決めます。

有効なエントリーは RIP 更新間隔の 3 倍の期間ルーティング・テーブルに残存し、ルーターはその RIP テーブルを更新間隔ごとに 1 回同報通信します。

たとえば、デフォルト間隔は 1 分ですが、この場合、有効なエントリーは 3 分間テーブルに残存することができます。この時間の後、エントリーが RIP 更新によってリフレッシュされない場合、そのルートに無限大 (16) のホップ・カウントがマークされ、エントリーは削除されます。60 秒ごとに、ルーターは RIP テーブルを対応する回線に同報通信します。

RIP 間隔は 1 ～ 1440 分 (24 時間) に構成できます。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、ダイヤル・オンデマンド回線が頻繁にダイヤルアウトするのも防止します。

注: RIP 公示全体がこの間隔によって制御されている間も、ルーターはネットワーク・トポロジー変更を確認すると、速やかにそれを伝送します。

RIP 間隔は Novell ファイル・サーバー上では構成できません。

```
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・サイズの指定

IPX サービス公示プロトコル (SAP) サービス・テーブルは、 NetWare サービス (たとえば、ファイル・サーバー) を見つけるのに使用される分散データベースです。サービスは、2 バイトの数字のタイプと 47 文字の名前によって、ユニークに識別されます。各サービス提供者は、サービス・タイプ、名前、およびアドレスを指定して、そのサービスを公示します。ルーターはこの情報をテーブル内に蓄積し、それを他のルーターに送信します。デフォルトのテーブル・サイズは 32 です。

テーブル・サイズは 1 ～ 2048 の範囲に構成できますが、ルーターのメモリーの制約によって、最大テーブル・サイズは使用できない場合があります。

```
IPX config>set maximum services
New Service table size [32]? 32
```

SAP 更新間隔の指定

IPX サービス公示プロトコル (SAP) 間隔は、IPX SAP 更新の時間間隔を回線単位で構成することができます。同じネットワーク上のすべてのルーター・サーキットは、同一の SAP 間隔を使用することが必要です。この間隔は、テーブル情報が時間切れになる時間、およびルーター・サーキットへの同報通信の間隔を決めます。

有効なエントリーは SAP 更新間隔の 3 倍の期間 SAP サービス・テーブルに残存し、ルーターは SAP サービス・テーブル情報を、更新間隔ごとに 1 回同報通信します。

SAP 間隔は 1 ～ 1440 分 (24 時間) に構成できます。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、ダイヤル・オンデマンド回線が頻繁にダイヤルアウトするのも防止します。

注: SAP 公示全体がこの間隔によって制御されている間も、ルーターはネットワーク・トポロジー変更を確認すると、速やかにそれを伝達します。

SAP 間隔は Novell ファイル・サーバー上では構成できません。

```
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シリアル化パケット・フィルター

IPX は、キープアライブ・パケットおよびシリアル化パケットが継続的にダイヤル・オンデマンド・リンクを起動するのを防止するように、あるいはダイヤル・オンデマンド・リンク上の通信量を最小化するように構成することができます。

たとえば、図48 では、Novell クライアントが Novell サーバーにログインし、アイドル状態のままでいる場合、サーバーは定期的にキープアライブ要求をクライアントに送信し、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・フィルターを使用すると、ルーターは最初のキープアライブ応答をそれぞれのキープアライブ・テーブルに入力した後、応答を転送します。それ以降、ルーターは、このクライアント/サーバー・コネクションに対するキープアライブ・トラフィックを WAN リンクを介して転送しません。代わりに、ルーター A がサーバーから受信したキープアライブ要求に応答し、ルーター B はキープアライブ要求を Novell クライアントに送信します。

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 シリアル化パケットを転送するのも防止します。

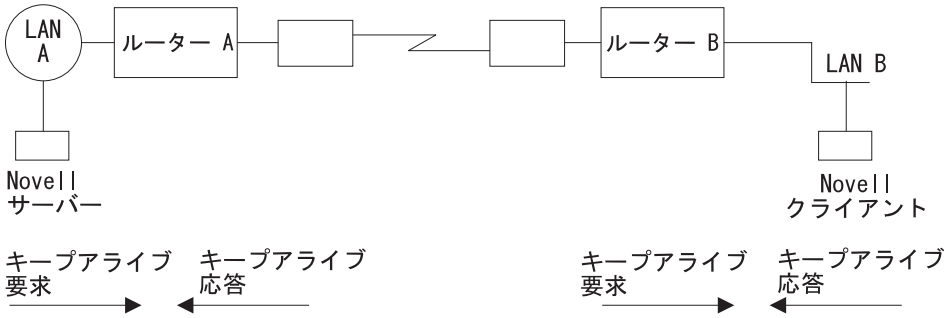


図 48. キープアライブ・フィルター

キープアライブ・フィルターを設定するためには、ダイヤル回線上のこの機能を使用可能にします。

```
IPX Config> enable keepalive-filtering
IPX circuit number [1]? 5
```

複数ルートの構成

IPX は、同一のあて先ネットワークに対して複数のルーティング・テーブル・エントリーを維持するように構成できます。この機能の利点は、あるルートに障害が起きたときに、代替ルートを即時に使用できることです。ルーターは、新規ルートを確認するために RIP 同報通信 (これには、数秒から 1 分かかります) を待つ必要はありません。ルーターは、等価コスト・パスのみをルーティング・テーブルに保管します。

各あて先のルーティング・テーブルに保管され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。デフォルトは 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・テーブルに保存されるエントリー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。デフォルトは 32 です。エントリーの数は、少なくとも RIP ネットワーク・テーブルと同じサイズに設定します。(RIP ネットワーク・テーブルのサイズは、本章で説明する **set maximum networks** コマンドを使用して構成します。)

```
IPX config> set maximum total-route-entries
New route table size [32]? 40
```

静的ルートの構成

静的ルートは、あて先ネットワーク番号ごとに構成することができます。各静的ルートは回線に関連付けられており、回線で IPX が起動されたときに、ルーティング・テーブルに挿入されます。静的ルートは、回線上の IPX が停止されたとき、回線自体がダウンしたとき、またはその着信ネットワークへの動的確認ルートが確認されたときに、ルーティング・テーブルから除去されます。動的に確認されたルート (RIP を介して) は、常に静的ルートをオーバーライドします。静的ルートは、回線上の IPX が再起動されたとき、回線自体がアップ状態に戻ったとき、またはその着信ネットワークへのすべての RIP ルートが失われたときに、ルーティング・テーブルに再挿入されます。

静的ルートは、RIP が使用不可にされ、あて先ネットワークへのルートがダイヤル・オンデマンド回線上で静的に構成される場合、ダイヤル・オンデマンド回線では特に便利です。

静的ルーティングは、回線上で単独で使用することも、RIP と組み合わせて使用することもできます。ただし、唯一の例外は、IPXWAN 回線上で静的ルーティングが使用可能にされている場合です。この場合は、静的ルーティングだけが IPXWAN によって交渉される唯一のルーティング・タイプになります。

静的ルートは、水平分割および適用可能なフィルターに応じて、 RIP によって公示されます。

1 つのあて先ネットワークに対して複数の静的ルートが構成されている場合、RIP ルートを選択するのに使用されるのと同じ規則を使用して、どの静的ルートをルーティング・テーブルに挿入するのかが決められます。それらが等価コストの場合、同じあて先ネットワークへの複数の静的ルートがルーティング・テーブルに挿入されます。ルーティング・テーブルには、構成された「あて先当たりのルート数」まで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
```

静的サービスの構成

静的サービスは、サービス・タイプまたは名前の組みに対して構成することができます。各静的サービスは回線に関連付けられており、回線で IPX が起動されたときに、およびそのサービス・ネットワークへのルートが判明したとき (静的ルートまたは RIP 公示によって) に、SAP サービス・テーブルに挿入されます。静的サービスは、回線上の IPX が停止されたとき、回線自体がダウンしたとき、サーバー・ネットワークへのルートが失われたとき、あるいは同じサービスが動的に確認されたときに、SAP テーブルから除去されます。サーバー・ネットワークへのルートが分かっている限り、静的サービスは、回線上の IPX が再起動されたとき、回線自体がアップ状態に戻ったとき、または SAP によって確認されたサービスが失われたときに、サービス・テーブルに再挿入されます。動的に確認されたサービス (SAP を使用して) は、常に静的サービスをオーバーライドします。

静的サービスは、SAP が使用不可にされ、サービスがダイヤル・オンデマンド回線上で静的に構成される場合に、ダイヤル・オンデマンド回線では特に便利です。

静的サービスは、回線上で単独で使用することも、RIP/SAP と組み合わせて使用することもできます。ただし、唯一の例外は、IPXWAN 回線上で静的ルーティングが使用可能にされている場合です。この場合は、静的ルーティングだけが IPXWAN によって交渉される唯一のルーティング・タイプになります。

静的ルートは、水平分割および適用可能なフィルターに応じて、 SAP によって公示されます。

1 つの名前またはタイプに対して複数の静的サービスが構成されている場合、SAP サービスを選択するのに使用されるのと同じ規則を使用して、どの静的サービスをルーティング・テーブルに挿入するのかが決められます。等価コストの静的サービスが構成されている場合、同じ回線上でサーバー・ネットワークへの現行ルートとして定義されたサービスが、サービス・テーブルに挿入されます。

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 デフォルト・ルートの構成

デフォルト・ルートは、静的ルートの特殊なケースです。これは、最後の手段として、不定のあて先ネットワークのネクスト・ホップとして使用されます。

デフォルト・ルートは、RIP が使用不可にされている場合、ダイヤル・オンデマンド回線では特に便利です。ダイヤル・オンデマンド回線でデフォルト・ルートを構成

すると、各あて先への静的ルートを構成する必要なしに、クライアントはルートを要求し、回線の相手側のあて先ネットワークにパケットを送信することが可能になります。

RIP の扱い

RIP を使用するルーターの場合、デフォルト・ルートはネットワーク番号 FFFFFFFE によって指定されます。

RIP ルートを公示する際には、デフォルト・ルートは (他の静的ルートと同様に) RIP フィルターおよび水平分割を適用した後で公示されます。

不定のあて先ネットワークへの RIP 要求に応答する際には、ルーターはデフォルト・ルートがルーティング・テーブルに存在する場合にのみ、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へのルートが不定の場合、転送機能はデフォルト・ルートを公示しているネクスト・ホップ・ルーター (静的ルーティングの場合は、ローカル静的デフォルト・ルート定義によって指示されているネクスト・ホップ・ルーター) にパケットを転送します。

次の例は、RIP デフォルト・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]? fffffffe
IPX circuit number [1]? 2
Next-hop address, in hex: []? 400000003030
Ticks: (0-30000) [0§? 4
Hops: (0-14) [0]? 4
```

SAP との相互動作

一般に、SAP 公示は、サーバー・ネットワークへのルートが判明している場合にのみ受け入れられます。サーバー・ネットワークへのルートは不明であるが、デフォルト・ルートは分かっている場合にも、公示は受け入れられます (SAP フィルターに掛けた後で)。

デフォルト・ルートが存在したお陰で受け入れられた SAP 公示は、その SAP 公示の発信元以外のすべての IPX 回線に公示されます (水平分割)。当然のことながら、公示の前に SAP フィルターに掛けられます。これと同じ規則が、SAP 要求への応答にも適用されます。

グローバル IPX フィルター (IPX アクセス制御) の構成

グローバル IPX フィルターは、すべての IPX 回線に適用されます。これは、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するのを防止するのに使用できます。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したり、“ノイズを多発する” アプリケーションからパケットが対象エリアより先に転送されるのを防止することもできます。

グローバル IPX フィルターは、発信側の IPX の発信元アドレスと最終あて先 IPX アドレスに基づきます。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 (発信元またはあて先) 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範囲の IPX ソケット番号から構成されます。ネットワーク番号およびホスト番号は 0 として指定できます。これはワイルドカードで、それぞれ、すべてのネットワーク番号およびホスト番号に一致します。0 ～ FFFF は、ソケットのワイルドカードです。

グローバル・フィルターは、順序付けられたエントリーのリストです。各グローバル・フィルター・エントリーは、包含 (inclusive) または排他 (exclusive) として構成できます。ルーターは、受信したパケットをグローバル・フィルター・リストに照らして比較します。

- パケットが「包含」エントリーに一致した場合、ルーターはパケットを転送します。
- パケットが「排他」エントリーに一致した場合、ルーターはパケットを廃棄します。
- パケットがどのエントリーにも一致せずにリストの終わりに達した場合、ルーターはパケットを廃棄します。(これは、リストの終わりにワイルドカード「排他」エントリーを持つ場合と同じです。)

グローバル・フィルター・リストを作成するときには、IPX について以下のことを考慮してください。

- 第 1 に、RIP および SAP ソケット (X'0453' および X'0452') は決してブロックしないでください。RIP と SAP は、IPX パケットを正しく転送するために必要です。
- グローバル・フィルター・リストは、すべての回線に適用されることに注意してください。方向制御を有効にするためには、グローバル・フィルター内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指定する必要があります。
- 保護しようとしているサービスの場所を確認してください。サービスのアドレスを調べるには、`IPX>` プロンプトで **slist** コマンドを入力します。

  注: Novell ファイル・サーバーのサービス (バージョン 3.0 以上) はすべて、サーバーの内部ネットワーク (通常は、ホスト 000000000001) 上にあります。内部ネットワーク番号は IPX ネットワーク全体で固有なので、内部ネットワーク・ソケット範囲 0 ～ FFFF へのすべてのパケットを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。ファイル・サーバーのみをブロックする場合は、ソケット範囲 0451～0451 を使用します。
- グローバル・フィルター・リストを作成するために、**slist** からソケット番号を抽出する際には、一部のサービスは固定ソケット番号を持ち、一部のサービスは動的 (一時) ソケット番号を持っていることに注意してください。範囲 4000～7FFF のソケットは動的なので、次回にファイル・サーバーをリブートしたときも、そのサービスが同じソケット番号を持つことは保証されません。ただし、範囲 8000～FFFF は Novell によって割り当てられており、通常は一定に保たれています。

注: グローバル・フィルターと回線フィルターは相互に排他的です。グローバル SAP フィルターが使用可能のときは、回線 SAP フィルターを使用可能にすることはできません (その逆も同じです)。グローバル IPX フィルターが使用可能のときは (*access-controls*)、回線 IPX フィルターを使用可能にすることはできません (その逆も同じです)。

IPX の使用

ルーターは、各 IPX フレームがグローバル・フィルター・リスト内のエントリーに一致するかどうかを調べます。最初に一致したものを適用するので、グローバル・フィルターの順序は非常に重要です。ルーターは、以下の基準に従って IPX パケットを調べます。

1. グローバル・フィルターのタイプ (2 つのタイプ)
   a. Inclusive (包含)。パケットが以下の基準に一致する場合、パケットを転送することを示します。
   b. Exclusive (排他)。パケットが以下の基準に一致する場合、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・フィールドではなく) 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・サービスに結合する、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 発信元ホスト・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、ネットワーク 18730 の Novell ファイル・サーバー 0000 C93A 0912 上の NCP アプリケーションにあてた、IPX net 1871 上の任意のクライアントからの IPX パケットのみ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廃棄されます。

```
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、すべての回線に適用されます。これは、サービス公示情報がルーターを通して伝送されるのを防止するのに使用できます。グローバル SAP フィルターを使用する主な理由は 4 つあります。

- バインダリー・サイズが小さいサーバー (たとえば、NetWare バージョン 2.15 以下) を使用しており、SAP データベース内の情報量を制限する必要がある場合
- リモートからアクセスされるのは不都合なので、特定のサービスをローカル・エリアの外に公示したくない場合
- SAP テーブルからクラッターを除去したい場合
- SAP 公示はかなりの WAN 帯域幅を消費する可能性があるので、WAN リンク上の不要な SAP 公示を減らしたい場合

注: これらの理由のいずれも、セキュリティーについては明示的に言及していません。グローバル SAP フィルターは、サービスを保護することはできません。SAP が行うのは、サービスの名前をアドレスに変換することだけです。潜在的な侵入者がサービスのアドレスを知っている場合、グローバル SAP フィルターによってその公示をブロックしても、サービスは保護されません。セキュリティーを提供できるのは、アクセス制御だけです。

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・グループの最大ホップ・カウントを設定することが基本になっています。指定のホップ・カウント (または、それ以下) を持つ照合サービス公示を受信した場合、それを受け入れて SAP テーブルに入れます。それ以外は無視されます。SAP データベース内のサービスのみが、再公示または照会への応答に使用されます。

注: ルーターは、サービス・ネームを 7 ビットの ASCII でのみ入力することを許します。一部のサービス・ネームは 2 進データを使用しており、Novell SAP 仕様に違反しています。このようなサービスは、名前でフィルターに掛け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 は、各タイプのサービスに対して 4 桁の 16 進数のタイプ番号を割り当てています。あるいは、グローバル SAP フィルターを、あるタイプの 1 つの特定のサービスに適用することも可能です。これは、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・タイプの複数のサーバー (それぞれ固有なサービス・ネームを持つ) が存在することも可能です。この場合は、同じサービス・タイプを持つ複数のグローバル SAP フィルターを構成して、固有なサービス・ネームをフィルターに掛けたり、あるいは単一の SAP フィルターを構成して、そのサービス・タイプのすべてのサービス・ネームをフィルターに掛けたり (ワイルドカード・フィルター) することができます。

グローバル SAP フィルターの作成

グローバル SAP フィルターを構成するには、次の手順で行います。

1. IPX Config> プロンプトで **add filter** を入力します。通常の SAP 同報通信に使用される、いくつかの主要なエントリーを指定する必要があります。
   a. ホップ数 (Number of hops.)。このエントリーは、SAP エントリーに許容されるホップ・カウントを示します (これより高いと、廃棄されます)。
   b. サービス・タイプ (Service type)
   c. サービス・ネーム (Service name)
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。

次の例は、特定のプリント・サーバーに適用されるグローバル SAP フィルターを作成する方法を示しています。

```
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 ホップ以上離れている **rem-ptr1** という名前のプリント・サーバーからの SAP 公示を無視します。フィルターは、ルーターがこの基準に一致する公示を伝送するのを防止します。

グローバル SAP フィルターのサービス・タイプの決定

設定するフィルターの SAP タイプを決めるには、以下のステップに従います。

1. * プロンプトで **talk 5** を入力する。次に、+ プロンプトで **protocol ipx** を入力します。

   IPX> プロンプトで **slist** を入力する。フィルターに掛けたいサービスのエントリーをメモします。
2. * プロンプトで **talk 6** を入力する。次に Config> プロンプトで **protocol ipx** を入力します。該当するグローバル SAP フィルター、およびフィルターに掛けたいサービスの適切なホップ・カウントを追加します。
3. フィルターを作成した後で、ルーターをリスタートする。
4. サービスが正常にフィルターに掛けられると、そのサービスはリストされなくなるはずです。IPX> プロンプトで **slist** を入力して、そのサービスがリストされなくなったことを確認してください。

IPX 回線フィルター - 概説

IPX ルーティング機能は、ROUTER、RIP、SAP、および IPX の 4 つのタイプの回線ベースのフィルターをサポートします。1 つの回線につき、1 つの *入力フィルター* と 1 つの *出力フィルター* を定義することができます。フィルター基準 (*項目* と呼ばれる) を組み立てて *フィルター・リスト* が作成され、これが入力フィルター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、複数のフィルターに付加することができます。これにより、複数の回線で同じフィルター基準を構成しなくても済みます。

注: グローバル・フィルターと回線フィルターは相互に排他的です。グローバル SAP フィルターが使用可能のときは、回線 SAP フィルターを使用可能にすることはできません (その逆も同じです)。グローバル IPX フィルターが使用可能のときは (*access-controls*)、回線 IPX フィルターを使用可能にすることはできません (その逆も同じです)。

IPX 回線フィルターの構成

IPX 回線フィルターを構成するには、次のようにします。

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・リストを変更し、フィルター基準と、そのフィルター・リストが「inclusive (包含)」か「exclusive (排他)」かを指定します。
3. **create filter** コマンドを使用して、必要な回線上にフィルターを作成し、それが入力フィルターであるか出力フィルターであるかを指定します。
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、フィルターのデフォルト・アクションを設定します。付加されたフィルター・リストのいずれにも一致しない場合に、デフォルト・アクションが取られます。

IPX 回線上のフィルターを削除するコマンド、特定の IPX 回線 (または、すべての IPX 回線) 上のフィルターを使用不可にするコマンド、フィルターからフィルター・リストを切り離すコマンド、フィルター内でフィルター・リストを移動するコマンド (フィルター・リストは順序付きであるため)、フィルターをリストするコマンド、およびフィルター・キャッシュのサイズを設定するコマンド (IPX フィルターのみ) もあります。

ROUTER フィルター

ROUTER フィルターは、すべての受信 RIP レスポンス・パケットの IPX ヘッダーに適用されます。出力 ROUTER フィルターはサポートされません。ROUTER フィルターを使用して、ルーティング情報を交換するルーターを制御することにより、個々の IPX ネットワークを複数の異なる IPX インターネットにグループ化することができます。

RIP ROUTER フィルターは、回線別に、順序付き項目リストとして保持されます。項目は、受信した各 RIP レスポンス・パケットに順次に適用されます。一致が見つかると、一致したフィルター・リストに指定されている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)。Excluded パケットは廃棄されるので、そのネットワーク・エントリーに含まれていた情報は RIP ルーティング・テーブルに入れられません。一致するものが見つからなかった場合、指定されたデフォルト・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 レスポンス・パケットのネットワーク・エントリーに適用されます。これは、選択されたネットワークに関するルーティング情報を公示する範囲を制御するのに使用できます。*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のルーティング情報が保管 されるのを防止することができます。これは、他の***すべて*** のネットワークが選択されたネットワークを確認する (learn) こと (少なくとも、このルーターを介して) を防止します。

RIP フィルター (入力) は、回線別に、順序付き項目リストとして保持されます。項目は、受信した各 RIP レスポンス・パケット内の各ネットワーク・エントリーに順次に適用されます。一致が見つかると、一致したフィルター・リストに指定されているアクションが実行されます (Exclude = ネットワーク・エントリーを無視する、Include = ネットワーク・エントリーを処理する)。Excluded ネットワーク・エントリーは無視されるので、RIP ルーティング・テーブルには入れられません。一致するものが見つからなかった場合、指定されたデフォルト・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関するルーティング情報が公示 (保管ではなく) されるのを防止することができます。これは、一部 (全部ではなく) のネットワークが選択されたネットワークを確認する (learn) こと (少なくとも、このルーターを介して) を防止します。

RIP フィルター (出力) は、回線別に、順序付き項目リストとして保持されます。項目は、RIP レスポンス・パケットで転送される各ネットワーク・エントリーに順次に適用されます。一致が見つかると、一致したフィルター・リストに指定されているアクションが実行されます (Exclude = ネットワーク・エントリーをパケットから除外する、Include = ネットワーク・エントリーをパケットに含める)。このフィルターは、RIP ルーティング・テーブルのコンテンツには影響を与えません。一致するものが見つからなかった場合、指定されたデフォルト・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 レスポンス・パケットのサーバー・エントリーに適用されます。これは、サービスに関する情報を公示する範囲を制御するのに使用し、低速 WAN 上の 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ネットワークのルーティング情報が保管 されるのを防止することができます。これは、他の**すべて** のネットワークが選択されたサーバーを確認すること (少なくとも、このルーターを介して) を防止します。

SAP フィルター (入力) は、回線別に、順序付き項目リストとして保持されます。項目は、受信した各 SAP レスポンス・パケット内の各ネットワーク・エントリーに順次に適用されます。一致が見つかると、一致したフィルター・リストに指定されているアクションが実行されます (Exclude = サーバー・エントリーを無視する、Include = サーバー・エントリーを処理する)。Excluded サーバー・エントリーは無視されるので、SAP サービス・テーブルには入れられません。一致するものが見つからなかった場合、指定されたデフォルト・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関するサービス情報が公示 (保管ではなく) されるのを防止することができます。これは、*一部* (全部ではなく) のネットワークが選択されたサーバーを確認すること (少なくとも、このルーターを介して) を防止します。

SAP フィルター (出力) は、回線別に、順序付き項目リストとして保持されます。項目は、各 SAP レスポンス・パケット内の各サーバー・エントリーに順次に適用されます。一致が見つかると、一致したフィルター・リストに指定されているアクションが実行されます (Exclude = サーバー・エントリーをパケットから除外する、Include = サーバー・エントリーをパケットに含める)。このフィルターは、SAP サービス・テーブルのコンテンツには影響を与えません。一致するものが見つからなかった場合、指定されたデフォルト・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 ヘッダーに適用されます。これは、発信元およびあて先ネットワーク、ノード、およびソケット・フィールド、プロトコル・タイプ、およびホップ・カウントに基づいて、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する範囲を制御するのに使用できます。

入力 フィルターとして、一致した場合はパケットを廃棄することを指示することにより、パケットが**すべて** の回線に転送されるのを防止できます。

IPX フィルター (入力) は、回線別に、順序付き項目リストとして保持されます。項目は、受信した各 IPX パケットに順次に適用されます。一致が見つかると、一致したフィルター・リストに指定されている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)。一致するものが見つからなかった場合、指定されたデフォルト・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、出力回線に基づいて、パケットを転送するかどうかを決定します。これにより、ある回線では受信パケットの転送を許し、他の回線では転送を許さないようにすることができます。

IPX フィルター (出力) は、回線別に、順序付き項目リストとして保持されます。項目は、転送される各 IPX パケットに順次に適用されます。一致が見つかると、一致したフィルター・リストに指定されているアクションが実行されます (Exclude = パケットを廃棄する、Include = パケットを転送する)。一致するものが見つからなかった場合、指定されたデフォルト・フィルター・アクションが実行されます。

IPX フィルターは、受信した各パケットごとに起動されるので、必需性が高い場合 (つまり、ROUTER、RIP および SAP フィルターを使用できない場合) にのみ使用することをお勧めします。一般に、RIP フィルターは特定の 1 組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 フィルターはインターネットワーク全体におけるワークステーションが到達可能なサーバーを制御し、IPX フィルターは ***個々の*** ワークステーション (または、個々のワークステーション上の個々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。

642ページの『IPX 回線回線フィルター構成コマンド』 で、IPX 回線フィルターを構成するのに使用されるコマンドについて詳しく説明しています。

IPX 性能の調整

IPX ルーターは、トラフィックを効率的にルーティングするために、二重のパケット転送パス (速いパスと遅いパス) を実現しています。

速いパスは、データ・パケットのみを転送し、遅いパスは、RIP および SAP パケットのような管理パケットを扱います。速いパスは、アドレス・キャッシュを使用して、ルーターがパケットを速やかに転送できるようにします。

低速でのルーティング・テーブルの検索は、キャッシュ・エントリーを作成するときしか行われません。キャッシュはエージング・メカニズムを使用して、オーバーフローを巧みに処理します。キャッシュ・サイズの構成は、IPX 構成メニューを通して行うことができます。

IPX ファースト・パス・キャッシュには 2 つのエントリー (ローカルとリモート) があります。各エントリーは、それに該当するタイプのアドレッシング要件を処理することができます。

キャッシュに許されるエントリー・タイプの最大数は、キャッシュ・コマンドを使用して設定します。

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・ネットワークまたはクライアント・ネットワーク上のクライアントの合計数に、過度のパージ要求を防止するための 10% のバッファーを加算した値に等しく設定することが必要です。613ページの図49 の例を使用すると、ルーター 5 (RTR R5) は、9 つのクライアント (C) と 1 つのサーバー (S) を持っているので、合計数は 10 になります。この合計数に基づいて、次のように計算します。

1. 10% を掛ける (例では 10)。
2. その合計 (1) をクライアントの合計に加算する (安全マージンのために)。
3. 新しい合計 (11) をローカル・キャッシュ・エントリーの数として使用する。

たとえば、次のように指定します。

```
IPX config>set local-cache size
New IPX local node cache size [32]? 11
```

すべてのキャッシュ・エントリーが使用されている場合、最も使用頻度の低いエントリーが除去されます。

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、過度のパージ要求を防止するための 10% のバッファーを加算した値に等しく設定することが必要です。613ページの図49 では、RTR R5 が IPX ネットワーク 5 を介し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 は合計 10 のクライアントを持っています。この合計数に基づいて、次のように計算します。

1. 10% を掛ける (例では 10)。
2. その合計 (1) をリモート・ネットワークの合計 (10) に加算する (安全マージンのために)。
3. 新しい合計 (11) をリモート・キャッシュ・エントリーの数として使用する。

たとえば、次のように指定します。

```
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・エントリーを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
```

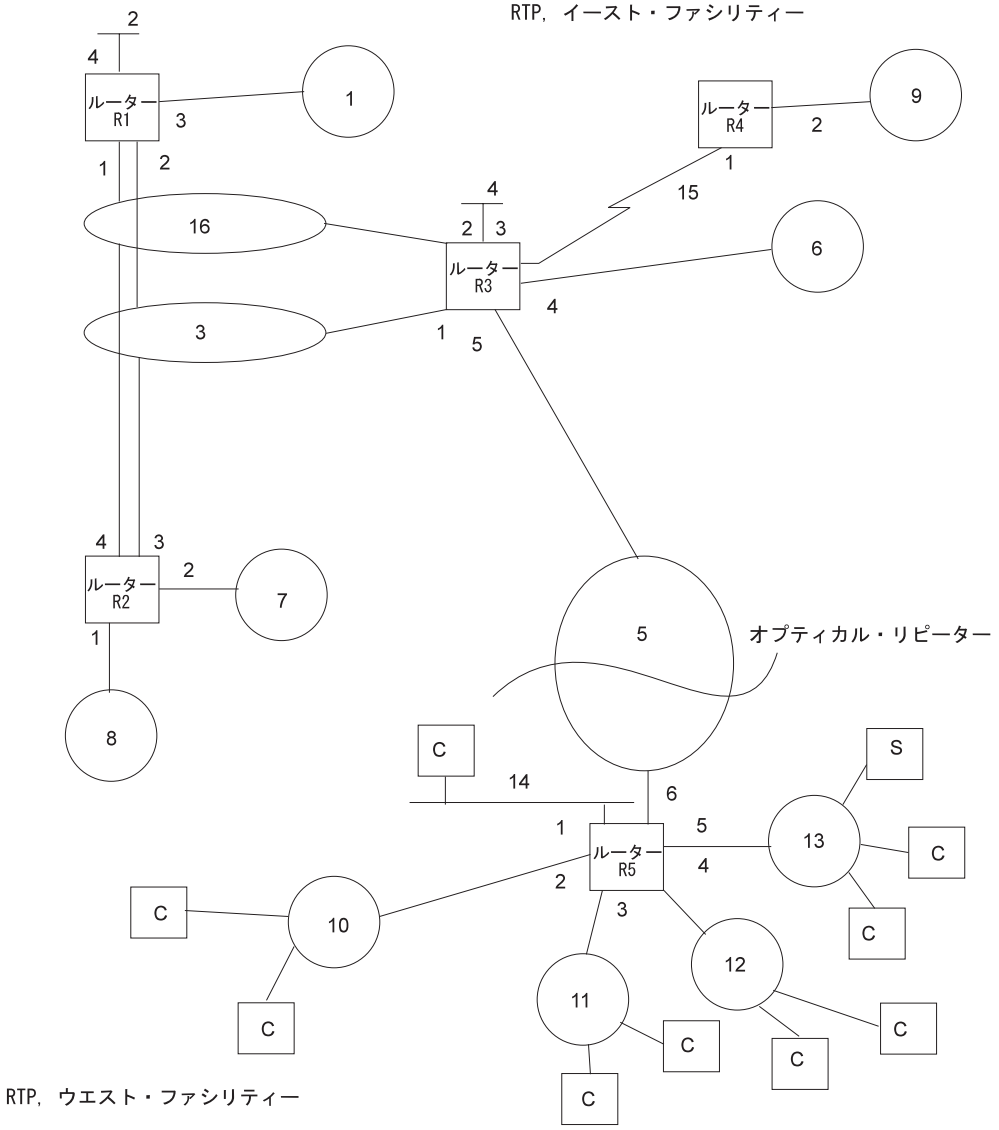


図 49. IPX ネットワークの例

水平分割ルーティング

水平分割というのは、RIP および SAP 更新を、それを入手したルーターに同報通信するのを回避するルーティング方式です。

一般的には、すべての回線で水平分割を使用可能にし、パケットが無限大までカウントされるのを防止して、不要な RIP および SAP 公示を回避する必要があります。ただし、部分メッシュ・フレーム・リレー、および X.25 構成など、水平分割を使用不可することが必要な場合もあります。

部分メッシュの RFC 1483 をサポートする IPX ルーティング構成も、水平分割を使用不可することが必要な一例です。

IPX の使用

図50 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、本局のルーターがすべてのルーティング情報をすべての他のルーターに同報通信しない限り、支局のルーターは相互に通信することができません。この場合、本局のフレーム・リレー・サーキットでは水平分割を使用不可にし、支局の各回線では使用可能にして、不要なトラフィックが生成されるのを防止することが必要です。

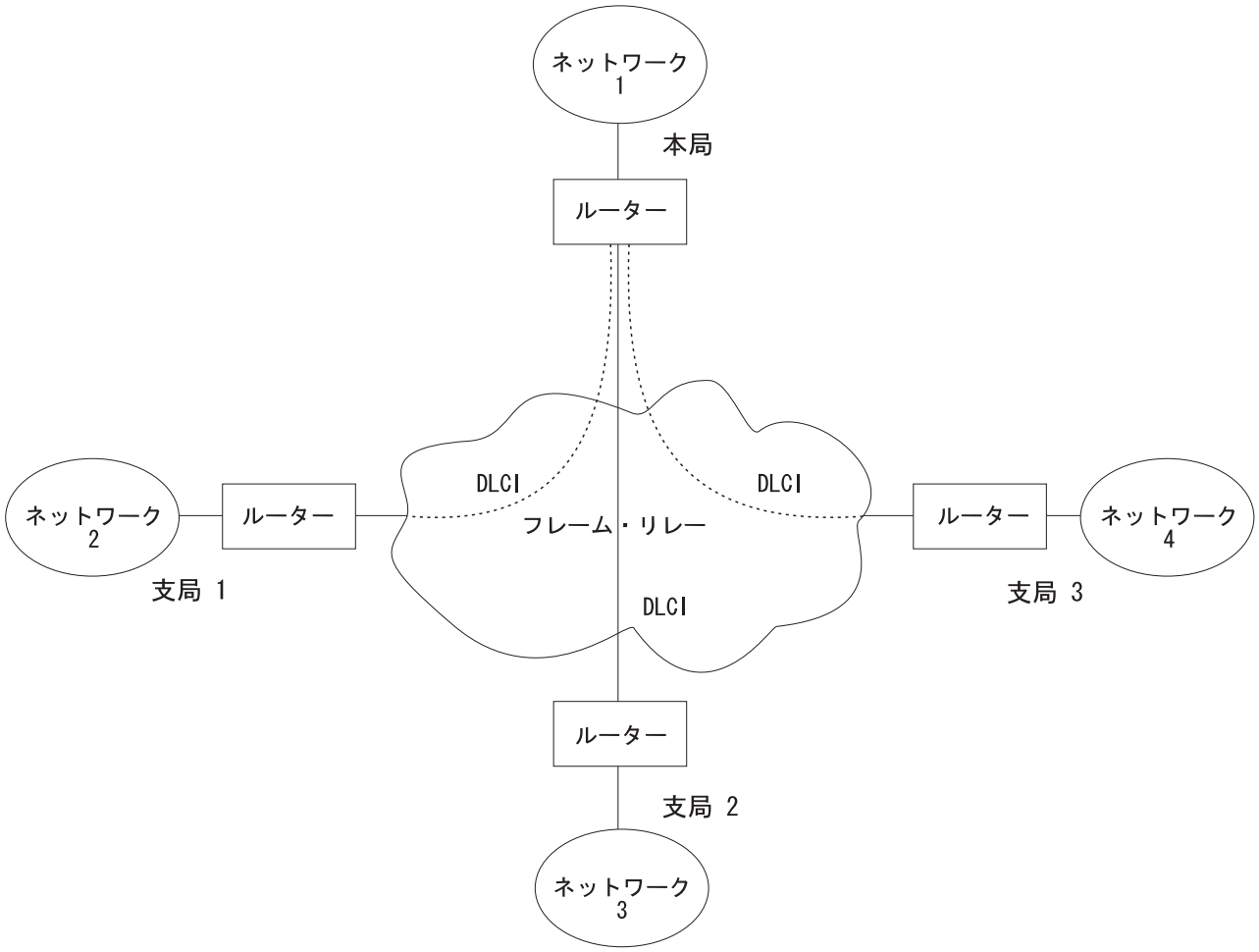


図 50. 部分メッシュ・フレーム・リレー・ネットワーク

水平分割の設定を変更する必要がある場合は、**set split-horizon** コマンドを次のように使用します。

```
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29章 IPX の構成および監視

この章では、IPX プロトコルを構成する方法、および IPX 監視コマンドを使用する方法について説明します。本章には、以下の節が含まれています。

- 『IPX 構成環境へのアクセス』
- 『IPX 構成コマンド』
- 654ページの『IPX 監視環境へのアクセス』
- 654ページの『IPX 監視コマンド』

IPX 構成環境へのアクセス

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

```
Config> 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37 は、IPX 構成コマンドをリストしています。これらのコマンドは、IPX パケットを転送するルーターのネットワーク・パラメーターを指定します。コマンドは IPX config> プロンプトで入力します。構成変更を起動するために、ルーターをリスタートします。

表 37. IPX 構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Add	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、またはサービスを追加します。
Delete	IPX ブロードキャストまたは 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、または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 静的ルートまたは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 同報通信ペーシング、最も近いサーバーを取得するための SAP 応答、NetBIOS 同報通信を使用不可または使用可能にし、特定の回線上で RIP または SAP を使用不可または使用可能にします。
Filter-lists	IPX 回線フィルター構成にアクセスします。この環境では、IPX 回線に基づく ROUTER、RIP、SAP、および IPX フィルターが構成されます。
Frame	
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) の順序を再編成したり、あるインターフェースから別のインターフェースへ IPX 回線を移動します。

表 37. IPX 構成コマンドの要約 (続き)

コマンド	機能
Set	ホスト番号、IPXWAN ルーター・ネームとノード ID、IPXWAN ルーティング・タイプ、コネクション・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、および水平分割の使用を設定します。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Add

add コマンドは、グローバル IPX フィルター (アクセス制御)、IPX 同報通信回線、グローバル SAP フィルター、IPX ポイント・ポイント回線、あるいは静的ルートまたはサービスを IPX 構成に追加するのに使用します。

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のかどうかを決めます。IPX アクセス制御は、IPX プロトコルのために 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、ルーターがパケットをフィルターに掛けるのに使用する、順序付きエントリーの集合です。各エントリーは Inclusive (包含) または Exclusive (排他) のいずれかです。各エントリーには、発信元およびあて先ネットワーク番号、ホスト・アドレス、およびソケット範囲が入っています。

IPX プロトコルのネットワークからパケットを受信し、アクセス制御が使用可能になっている場合、パケットはアクセス制御リストと照合して検査されます。一致するものが見つかるまで、ネットワーク/アドレス/ソケットの組み合わせと比較されます。一致するものが見つかり、そのエントリーが Inclusive タイプの場合、パケットの受信 (そして、転送される可能性があります) が進められます。一致したエントリーが Exclusive タイプである場合、パケットは廃棄されます。一致するものが何もない場合も、パケットは廃棄されます。

add access-control コマンドを使用してアクセス制御リストを作成した後で、**set access-control on** コマンドを使用してエントリーを使用可能にします。アクセス制御リストの順序を変更するときは **move** コマンドを使用します。

注: アクセス制御はすべての受信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と、IPX 転送機能は機能しません。

```
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集合へのパケットが、送信されるのか廃棄されるのかを識別します。包含 (include) の場合は I を入力します。これにより、ルーターはパケットを受信し、残りの引き数の基準に一致した場合は、それを転送します。排他 (exclude) の場合は E を入力します。これにより、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。ネットワーク番号を 16 進数で入力します。

有効値: X'00000000' ～ X'FFFFFFFF'

ゼロ (0) は、全ネットワークを指定します。

デフォルト値: 0

Dest-host

あて先ネットワークのホスト番号。ホスト番号を 16 進数で入力します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

ゼロ (0) はネットワーク上の全ホストを示します。

デフォルト値: なし

Dest-socket-range

あて先ソケットの範囲 (両端を含む) を指定する 2 桁の数字。あて先ソケット値は、IPX パケットのフィルターに使用されます。

有効値: X'0000' ～ X'FFFF'

デフォルト値: 0

Src-net

発信元のネットワーク番号。ネットワーク番号を 16 進数で入力します。

このパラメーターは、このルーターによってフィルターに掛けられるパケットの発信元 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のみ をフィルターに掛けることを選択した場合、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、およびホップ数に適用されます。

有効値: X'00000000' ～ X'FFFFFFFF'

ゼロ (0) は、全ネットワークを指定します。

デフォルト値: 0

Src-host
発信ネットワークのホスト番号。ホスト番号を 16 進数で入力します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

ゼロ (0) はネットワーク上の全ホストを示します。

デフォルト値: なし

Src-socket-range
発信元ソケットの範囲 (両端を含む) を指定する 2 バイトの数字

有効値: X'0000' ～ X'FFFF'

デフォルト値: 0

注: NetWare 環境で動作する場合は、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。必要な場合に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 を持つファイル・サーバーにアクセスするのを防止します。

broadcast-circuit *interface# ipx-circuit# network#*
IPX 同報通信回線を追加します。

interface#
IPX 回線番号が構成されているネットワーク・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

デフォルト値: 0

ipx-circuit#
IPX 回線番号を指定します。この番号は、ルーター内のすべての構成済み IPX 回線で固有なものでなければならず、多くの構成コマンドで IPX 回線を参照するのに使用されます。

有効値: 1 ～ 65535

デフォルト値: 次に使用可能な IPX 回線番号

network#
回線上で使用する 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 は、IPXWAN 番号なし RIP または静的ルーティング・インターフェースにのみ有効です。IPX ネットワーク番号 FFFFFFFF は、有効な IPX ネットワーク番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX デフォルト・ルート用に予約されているため、IPX ネットワーク番号として使用してはなりません。

有効値: 1 ～ FFFFFFFD

デフォルト値: 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*

指定のサービスに適切なホップ数を決めることによって、大規模ネットワークのユーザーの NetWare バインダリー・オーバーフローを防止します。IPX SAP フィルターを使用して、SAP 公示の特定のエントリーを無視するようにプロトコルを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ことによって行います。古いバージョンの NetWare ファイル・サーバーはサイズに限界があるので、これが必要になる場合があります。また、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必要になることもあります。

SAP フィルターは、グローバルな順序付きフィルター・エントリーのリストです。各フィルター・エントリーには、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・ネームが入っています。SAP レスポンス・パケットを受信すると、各 SAP エントリーがフィルター・リストと照合して比較されます。SAP エントリーがフィルター・リスト内のエントリーに一致し、指定されたホップ数より大きい場合、パケットは無視されて、ローカル SAP データベースには入力されません。SAP エントリーがフィルター・リスト内のエントリーに一致し、指定されたホップ数以下の場合、パケットは受け入れられ、ローカル SAP データベースに入力されます。一致するものが何もない場合も、SAP エントリーは受け入れられます。このコマンドの引き数は、次のとおりです。

Hops

そのサービスに許容されるホップの最大数

有効値: 0 〜 16 の範囲の整数

デフォルト値: 1

Service-type

数値で示すサービス・クラス

有効値: X'0000' 〜 X'FFFF' の範囲の 16 進値

値 X'0000' は、全サービス・タイプをフィルターに掛ける場合に使用します。

デフォルト値: 4

IPX> プロンプトで **slist** コマンドを入力すると、サービス・タイプのリストを見ることができます。

Service-name

サーバーの名前を識別します。通常は、このフィールドには入力しません。

有効値: 1 〜 47 字の ASCII 文字 (X'20' 〜 X'7E')

デフォルト値: なし

例: `add filter 2 039B NOTES-CHICAGO`

この例は、2 ホップを超える Lotus Notes サーバー 『NOTES-CHICAGO』 あてのすべての SAP 公示を無視します。

ipxwan-circuit *interface# ipx-circuit# network# [FR-circ#]*

IPXWAN ポイント・ポイント回線を追加します。

interface#
IPX 回線を構成する必要のある既存の PPP またはフレーム・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

デフォルト値: 0

ipx-circuit#
IPX 回線番号を指定します。この番号は、ルーター内のすべての構成済み IPX 回線で固有なものでなければならず、多くの構成コマンドで IPX 回線を参照するのに使用されます。

有効値: 1 ～ 65535

デフォルト値: 次に使用可能な IPX 回線番号

network#
回線上で使用する 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 は、IPXWAN 番号なし RIP または静的ルーティング・インターフェースにのみ有効です。IPX ネットワーク番号 FFFFFFFF は、有効な IPX ネットワーク番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX デフォルト・ルート用に予約されているため、IPX ネットワーク番号として使用してはなりません。

有効値: 0 ～ FFFFFFFD

デフォルト値: 1

FR-circ#
フレーム・リレー PVC 回線番号を指定します。このパラメーターの指定は、IPX 回線が、フレーム・リレー・インターフェースに追加される IPXWAN 回線である場合に限り必須です。

有効値: 有効なフレーム・リレー PVC 回線番号

デフォルト値: 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'

デフォルト値: 1

ipx-circuit#
静的ルートを構成する必要のある既存の IPX 回線を指定します。

有効値: 既存の IPX 回線番号

デフォルト値: 1

nextHop
あて先ネットワークに到達するために経由するネクスト・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'

デフォルト値: なし

ticks
あて先ネットワークとこのルーター間のティック数を指定します。ティック数は、576 バイトの IPX パケットをこのルーターからあて先ネットワークに転送するのに 要する時間を表します。1 ティックは 55 ミリ秒です。

有効値: 0 ～ 30000

デフォルト値: 0

hops
あて先ネットワークとこのルーター間のホップ数を指定します。

有効値: 0 ～ 14

デフォルト値: 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'

デフォルト値: 4

serviceName
サービスの ASCII ネームを指定します。

有効値: 最大 47 字までの次の ASCII 文字: 'A'～'Z'、'a'～'z'、'0'～'9'、'_'、'-'、'@'

デフォルト値: なし

ipx-circuit#
SAP 静的サービスを構成する必要がある既存の IPX 回線を指定します。

有効値: 既存の IPX 回線番号

デフォルト値: 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'

デフォルト値: 1

serverNode
サーバーの IPX ノードを指定します。

有効値: X'1' 〜 X'FFFFFFFFFFFE'

デフォルト値: 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'

デフォルト値: 451

hops
サーバーとこのルーター間のホップ数を指定します。

有効値: 0 〜 14

デフォルト値: 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 同報通信または IPXWAN ポイント・ポイント回線、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、またはサービスを削除するのに使用します。

構文:

delete access-control . . .
circuit . . .
filter . . .
route-static . . .
sap-static . . .

access-control *line#*
入力された行番号に一致するアクセス制御を削除します。現行の行番号を表示したい場合は **list** コマンドを入力します。

例: delete access-control 2

circuit *ipx-circuit#*
IPX 同報通信または IPXWAN ポイント・ポイント回線を削除します。指定された *ipx-circuit#* と関連付けられているすべての静的ルート、静的サービス、および回線フィルターも削除します。

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*

指定された SAP フィルターを削除します。list コマンドを実行するときには、SAP フィルターを表示通りに正確に入力することが必要です。引き数は、次のとおりです。

Hops

そのサービスに許容されるホップの最大数

有効値: 0 ～ 16

デフォルト値: 16

Service-type

数値で示すサービス・クラス。2 バイトの 16 進数を入力します。

有効値: X'0000' ～ X'FFFF'

デフォルト値: なし

Service-name

削除するエントリーに名前がある場合は、名前を指定します。

有効値: 1 ～ 47 字の ASCII 文字 (X'20' ～ X'7E')

デフォルト値: 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'

デフォルト値: 1

ipx-circuit#

静的ルートが構成される IPX 回線を指定します。

有効値: 既存の IPX 回線番号

デフォルト値: 1

nextHop

あて先ネットワークに到達するために経由するネクスト・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'

デフォルト値: 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'

デフォルト値: 4

serviceName

サービスの ASCII ネームを指定します。

有効値: 最大 47 字までの次の ASCII 文字: 'A'～'Z'、'a'～'z'、'0'～'9'、'_'、'-'、'@'

デフォルト値: なし

ipx-circuit#

SAP 静的サービスが構成される IPX 回線を指定します。

有効値: 既存の IPX 回線番号

デフォルト値: 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、グローバルまたは特定の IPX サーキット上で使用不可にし、IPX 静的ルートまたはサービスの使用をグローバルに使用不可にするのに使用します。また、**disable** コマンドは、特定の回線上の SAP get-nearest-server 要求に対する応答、RIP-SAP 同報通信ペーシング、RIP、または SAP を使用不可にするのにも使用します。

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 同報通信または IPXWAN ポイント・ポイント回線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# によって指定された IPX 同報通信回線または IPXWAN ポイント・ポイント回線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# によって指定された IPX 回線上での Novell NetBIOS 同報通信 (パケット・タイプ 20) の受信および送信を使用不可にします。デフォルト値は、enabled (使用可能) です。Novell NetBIOS 同報通信の受信および送信は、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・サーキット城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# によって指定された IPX 同報通信回線または IPXWAN ポイント・ポイント回線上でルーターが SAP get-nearest-server 要求に応答しないようにします。

注: このフィーチャーを使用不可にするときは、十分な注意が必要です。このコマンドは、IPX ネットワーク上に複数のルーター (または、サーバー) が存在し、 このルーターの背後には 『最善』 サーバーが存在しないことが明らかな場合にのみ使用するようにします。

例: disable reply-to-get-nearest

```
IPX circuit number [1]? 2
```

rip *ipx-circuit#*

ipx-circuit# によって指定された IPX 同報通信回線または IPXWAN ポイント・ポイント回線上で RIP を使用不可にします。デフォルトでは、すべての回線上の RIP が使用可能になります。IPXWAN 静的ルーティングを使用している回線では、たとえ使用可能に構成されていても、RIP は自動的に使用不可になります。

例:disable rip 1

rip-sap-pacing *ipx-circuit#*

ipx-circuit# によって指定された IPX 同報通信回線または IPXWAN ポイント・ポイント回線上で RIP/SAP 同報通信ペーシングを阻止します。ペーシングが使用不可にされている場合、回線上の RIP および SAP 定期同報通信は、55 ミリ秒のパケット間間隔 (デフォルト設定) で転送されます。RIP および

SAP 同報通信が輻輳 (ふくそう) の原因になる可能性がある回線についてのみ、ペーシングを使用可能にしてください (たとえば、多数のバーチャル・サーキットを持つフレーム・リレーまたは X.25 回線では、ペーシングを使用可能にすることができます)。

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可にします。

例:disable route-static

sap *ipx-circuit#*
ipx-circuit で指定された IPX 同報通信または IPXWAN ポイント・ポイント回線上で SAP を使用不可にします。デフォルトでは、すべての回線上の SAP が使用可能になります。SAP は、RLAN 回線および IPXWAN 静的ルーティング上では、たとえ使用可能として構成されていても、自動的に使用不可になります。

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可にします。

例: disable sap-static

Enable

enable コマンドは、IPX をグローバルに、または特定の回線上で使用可能にするのに使用します。enable コマンドを使用して、IPX 静的ルートまたはサービスの使用をグローバルに使用可能にしたり、キープアライブ・フィルター、RIPS-SAP 同報通信ペーシング、get-nearest-server に対する SAP 応答、特定の回線上での RIP または SAP を使用可能にすることもできます。

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 同報通信または IPXWAN ポイント・ポイント

回線を使用可能にし、IPX 回線の IPX ネットワーク番号を指定します。IPX 回線は、有効な IPX ネットワーク番号が構成されていれば使用可能になります。

例: enable circuit

```
IPX circuit number [1]?
IPX network number in hex
(0 is allowed only on IPXWAN unnumbered circuits) [1]?
```

ipx-circuit#
使用可能にする IPX 同報通信または IPXWAN ポイント・ポイント 回線を指定します。

有効値: 任意の有効な IPX 回線番号

デフォルト値: 0

network#
回線上で使用する IPX ネットワークを指定します。IPX ネットワーク番号 0 は、IPXWAN 番号なし RIP または静的ルーティング・インターフェースにのみ有効です。IPX ネットワーク番号 FFFFFFFF は、有効な IPX ネットワーク番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX デフォルト・ルート用に予約されているため、IPX ネットワーク番号として使用してはなりません。

有効値: X'0' ～ X'FFFFFFFD'

デフォルト値: 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 同報通信または IPXWAN ポイント・ポイント回線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# によって指定された IPX 回線上での Novell NetBIOS 同報通信 (パケット・タイプ 20) の受信および送信を使用可能にします。デフォルト値は、enabled (使用可能) です。Novell NetBIOS 同報通信の受信および送信は、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・サーキット城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 同報通信または IPXWAN ポイント・ポイント回線上でルーターが SAP get-nearest-server 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# によって指定された IPX 同報通信回線または IPXWAN ポイント・ポイント回線上で RIP を使用可能にします。デフォルトでは、すべての IPX 回線上の RIP が使用可能になります。RIP は、RLAN 回線および IPXWAN 静的ルーティング・サーキット上では、たとえ構成で使用可能になっていても、自動的に使用不可になります。

例: enable rip

```
IPX circuit number [1]? 2
```

rip-sap-pacing *ipx-circuit#*

ipx-circuit# によって指定された IPX 同報通信回線または IPXWAN ポイント・ポイント回線上で RIP/SAP 同報通信ペーシング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 更新間隔内に同報通信が完了することを保証できるパケット間の間隔を計算します。ルーターが十分な大きさのパケット間隔を算出するようにするために、これらの更新間隔をより大きな値に構成することが必要になる場合があります。

ペーシングは、RIP および SAP 同報通信が輻輳 (ふくそう) の原因になる可能性がある回線 (たとえば、多数のバーチャル・サーキットを持つフレーム・リレーまたは X.25 回線) についてのみ使用可能にすることが必要です。

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# によって指定された IPX 同報通信回線または IPXWAN ポイント・ポイント回線上で 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。有効なフィルター・リスト・タイプは、rip、sap、および ipx です。

IPX *filter-type*.-List Config> プロンプトで利用可能なコマンドについての情報は、642ページの『IPX 回線回線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 回線のパケット・フォーマットを指定するのに使用します。(カプセル化も CONFIG **network** コマンドを使用して設定できます。)

注: 誤った、または無効の構成レコードがあった場合は、デフォルト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# によって指定された IPX 同報通信回線上でフレーム・タイプを ethernet_II に設定します。ethernet_II カプセル化は、プロトコル・タイプ 8137 でイーサネット・バージョン 2.0 を使用します。これは、NetWare 4.0 以上のデフォルトです。

例: frame ethernet_II

```
IPX circuit number [1]?
```

ethernet_8022 *ipx-circuit#*

ipx-circuit# によって指定された IPX 同報通信回線上でフレーム・タイプを ethernet_8022 に設定します。ethernet_8022 カプセル化は、SAP E0 で 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# によって指定された IPX 同報通信回線上でフレーム・タイプを ethernet_8023 に設定します。ethernet_8023 カプセル化は、LLC ヘッダーなしでイーサネット 802.3 カプセル化を使用します。これは、NetWare 4.0 以前のデフォルトです。これは、ルーターのデフォルトでもあります。

例: frame ethernet_8023

```
IPX circuit number [1]?
```

ethernet_SNAP *ipx-circuit#*

ipx-circuit# によって指定された IPX 同報通信回線上でフレーム・タイプを

ethernet_SNAP に設定します。ethernet_SNAP カプセル化は、0000008137 という PID で 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# によって指定された IPX 同報通信回線上でフレーム・タイプを token-ring MSB に設定します。token-ring MSB カプセル化は、SAP E0 で LLC カプセル化を使用し、非標準 MAC アドレスを使用します。これは、NetWare のデフォルトです。これは、ルーターのデフォルトでもあります。

例: frame token-ring MSB

```
IPX circuit number [1]?
```

token-ring LSB *ipx-circuit#*

ipx-circuit# によって指定された IPX 同報通信回線上でフレーム・タイプを token-ring LSB に設定します。token-ring LSB カプセル化は、SAP E0 で LLC カプセル化を使用し、非標準 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# によって指定された IPX 同報通信回線上でフレーム・タイプを token-ring_SNAP MSB に設定します。token-ring_SNAP MSB カプセル化は、PID 0000008137 で SNAP カプセル化を使用し、標準 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# によって指定された IPX 同報通信回線上でフレーム・タイプを token-ring LSB に設定します。token-ring LSB カプセル化は、PID 0000008137 で SNAP カプセル化を使用し、非標準 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。このコマンドは、**list all** の 『Access Control Configuration』 のセクションに示されている情報を表示します。

all 全 IPX 構成をリストします。

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
```

IPX 構成コマンド (Talk 6)

circuit *ipx-circuit#*

ipx-circuit# によって指定された IPX 同報通信または IPXWAN ポイント・ポイント 回線をリストします。このコマンドは、**list all** コマンドの例の 『IPX Configuration』、『RIP Configuration』、『SAP Configuration』 、および 『IPXWAN Configuration』 のセクションに示されている情報を表示します。

filters グローバル SAP フィルターをリストします。このコマンドは、**list all** コマンドの例の 『SAP Filter Configuration』 のセクションに示されている情報を表示します。

route-static

静的ルートをリストします。このコマンドは、**list all** コマンドの例の 『静的ルート構成』 の節に示されている情報を表示します。

sap-static

静的サービスをリストします。このコマンドは、**list all** コマンドの例の 『Static Services Configuration』 のセクションに示されている情報を表示します。

summary

IPX が使用可能なすべての回線の IPX、RIP、SAP、IPXWAN、およびキープアライブ・フィルター構成の要約をリストします。このコマンドは、**list all** コマンドの例の 『IPX Globals』、『IPX Configuration』、『RIP Configuration』、『SAP Configuration』、および 『IPXWAN Configuration』 の各セクションに示されている情報を表示します。

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または使用不可にされているか
- 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
- あて先当たりのルートの最大数
- ローカル・キャッシュ・エントリーの最大数
- リモート・キャッシュ・エントリーの最大数
- キープアライブ・フィルター・テーブル・サイズ

IPX Configuration

IPX が使用可能になっている各回線について、以下の情報が表示されます。

- IPX 回線番号
- 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)
- IPX が回線上で使用可能であるか、使用不可であるか
- 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 が使用可能になっている各回線について、以下の情報が表示されます。

- IPX 回線番号
- 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可か
- RIP 更新間隔タイマー
- 水平分割が使用可能か使用不可か
- RIP 同報通信ペーシングが使用可能か使用不可か

SAP Configuration

IPX が使用可能になっている各回線について、以下の情報が表示されます。

- IPX 回線番号
- 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可か
- SAP 更新間隔タイマー
- 水平分割が使用可能か使用不可か
- SAP 同報通信ペーシングが使用可能か使用不可か
- SAP get-nearest-server 要求への応答が使用可能か

IPXWAN Configuration

以下のグローバル情報が表示されます。

- ルーター・ネーム
- ノード ID

各 IPXWAN エントリーについて、以下の情報が表示されます。

- IPX 回線番号
- 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または使用不可にされているかどうかを表示します。また、構成された各静的ルートについて、以下の情報も表示されます。

- IPX あて先ネットワーク番号
- ホップ数
- ティック数
- ネクスト・ホップ・ノード・アドレス
- IPX 回線番号
- 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または使用不可にされているかどうかを表示します。また、構成された各静的サービスについて、以下の情報も表示されます。

- サービス・タイプ
- サービス・ネーム
- 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)
- ソケット
- ホップ数
- IPX 回線番号
- 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であるか使用不可であるかを表示します。また、構成された各グローバル SAP フィルターについて、以下の情報も表示されます。

- Index
- 最大ホップ数
- サービス・タイプ
- サービス・ネーム

Access Control Configuration

グローバル IPX フィルター (アクセス制御) が使用可能であるか使用不可であるかを表示します。また、構成された各グローバル IPX フィルター (アクセス制御) について、以下の情報も表示されます。

- アクセス制御指標 (#)
- フィルター・タイプ (include または exclude)
- あて先 IPX ネットワーク番号
- あて先 IPX ノード番号 (ホスト)
- あて先 IPX ソケット範囲
- 発信元 IPX ネットワーク番号
- 発信元 IPX ノード番号 (ホスト)
- 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) の順序を再編成したり、IPX 回線をあるインターフェースから別のインターフェースに移動するのに使用します。

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# scrLine の移動先となる行の直前の行番号を指定します。

アクセス制御を受けている行を移動すると、行の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#]*

あるネットワーク・インターフェースから別のネットワーク・インターフェースへ IPX 回線を移動します。このコマンドは、与えられた *ipx-circuit#* と関連付けられている静的ルート、静的サービス、および IPX 回線フィルターも同じ *interface#* に移動します。IPXWAN 回線をフレーム・リレー・インターフェースに移動している場合は、新しいフレーム・リレー回線番号の入力も求められます。

ipx-circuit#

移動する既存の IPX 回線を指定します。

有効値:有効な IPX 回線番号

デフォルト値: 1

interface#

IPX 回線が移動先にす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

デフォルト値: 0

FR-circ#

フレーム・リレー PVC 回線番号を指定します。このパラメーターの指定は、IPX 回線が、フレーム・リレー・インターフェースに移動される IPXWAN 回線である場合に限り必須です。

有効値:有効なフレーム・リレー PVC 回線番号

デフォルト値: 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・ネームとノード ID、IPXWAN ルーティング・タイプ、コネクション・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、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、および水平分割の使用を設定します。

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 を実行するシリアル・サーキットに使用されるホスト番号を指定します。シリアル・サーキットを介して動作する IPX ルーターはすべて、固有なホスト番号をもっている必要があります。シリアル・サーキットには、ホスト番

号を作成するもとになるハードウェア・ノード・アドレスがないので、これが必要になります。これは、マルチキャスト・アドレスであってはなりません。

注: IPX 同報通信と IPXWAN 回線を同じインターフェース上に組み合わせて構成する場合は、必ず、host-number が、後ろに X'0000' が付いた IPXWAN ノード ID であるように構成してください。

有効値: X'000000000001' ～ X'FEFFFFFFFFFF' の範囲の 12 桁の 16 進数

デフォルト値: なし

この番号は、各ルーターでユニークであることが必要です。

例: `set host-number 0000000000F4`

注: IPXWAN では、ルーター・ノード ID とネームを構成することが必要です。これらのパラメーターは **set node-ID** および **set name** コマンドを使用して構成します。

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、および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 回線を追加しておく必要があります。

ipx-circuit#

パラメーターを設定する既存の IPXWAN ポイント・ポイント回線を指定します。

有効値: 任意の既存 IPXWAN ポイント・ポイント回線番号

デフォルト値: 1

routingType

交渉する必要がある IPXWAN ルーティング・タイプを指定します。

- 無番号 RIP の場合は **u**
- 番号制 RIP の場合は **r**
- 無番号および番号制両方の RIP の場合は **b**
- 静的ルーティングの場合は **s**

有効値: 'u'、'U'、'r'、'R'、'b'、'B'、's'、'S'

デフォルト値: 'u'

timeout

この値は、その時間内に IPXWAN ネゴシエーションを正常に完了させることが必要な時間制限を秒数で指定します。コネクション・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スタートさせます。装置は再試行タイマーが満了するまでは、ネゴシエーションを再試行しません。

有効値: 5 ～ 300 の範囲の整数の秒数

デフォルト値: 60 秒

retryTimer

このパラメーターは、コネクションがタイムアウトになった後、コネクションの再確立を試みる前に待つ時間の長さを指定します。

有効値: 5 ～ 600 の範囲の整数の秒数

デフォルト値: 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*

キープアライブ・テーブルが保持するエントリーの数を設定します。これらのエントリーには、WAN リンクを介して接続された現行のすべてのクライアント/サーバーおよびサーバー/サーバーの組みが含まれます。

有効値: 1 ～ 250

デフォルト値: 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・ネットワークまたはクライアント・ネットワーク上のクライアントの合計数に、過度のパージ要求を防止するための 10% のバッファーを加算した値に等しく設定することが必要です。

有効値: 範囲は 1 ～ 10000 です。

デフォルト値: 64。詳細については、612ページの『ローカル・キャッシュ』および 612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たりのルートの最大数を指定します。

有効値: 1 ～ 64 の範囲の整数

デフォルト値: 1。複数ルートについての詳細は、601ページの『複数ルートの構成』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 が動作しているインターネット内のネットワークの数を反映します。

有効値: 1 ～ 2048

ルーターのメモリーの制約によって、最大テーブル・サイズは使用できない場合があります。

デフォルト値: 32。この値は、最大 total-route-entries *size* より大きくすることはできません。

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 が動作しているインターネットワーク内の SAP サービスの数を反映します。

有効値: 1 ～ 2048

ルーターのメモリーの制約によって、最大テーブル・サイズは使用できない場合があります。

デフォルト値: 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。これは IPX が動作しているインターネットワーク内のルートの合計数 (代替ルートを含む) を反映します。

有効値: 1 ～ 4096

デフォルト値: 32

この値は少なくとも *maximum networks size* と同じ大きさにする必要があります。複数ルートについての詳細は、601ページの『複数ルートの構成』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、ルーターがノード ID とネームをもつことが必要です。

有効値: 1 ～ 47 文字の可変長文字列

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。

デフォルト値: なし

例: set name newyork_accounting

net-number *ipx-circuit# network#*

IPX 同報通信または IPXWAN ポイント・ポイント回線についての IPX ネットワーク番号を指定します。

ipx-circuit#

既存 IPX 同報通信または IPXWAN ポイント・ポイント回線を指定します。

有効値: 既存の回線番号

デフォルト値: 1

network#

IPX 回線上で使用する 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 は、IPXWAN 番号なし RIP または静的ルーティング・インターフェースにのみ有効です。IPX ネットワーク番号 FFFFFFFF は、

有効な IPX ネットワーク番号ではありません。IPX ネットワーク番号 FFFFFFFE は、IPX デフォルト・ルート用に予約されているため、IPX ネットワーク番号として使用してはなりません。有効なネットワーク番号が構成されていない場合には、set コマンドは無視されます。

有効値: X'0' ～ X'FFFFFFFD'

デフォルト値: 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。値 0、FFFFFFFF または FFFFFFFE は、内部ネットワーク番号には無効です。有効なノード ID が構成されていない限り、IPXWAN は使用可能になりません。

デフォルト値: 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、過度のパージ要求を防止するための 10% のバッファーを加算した値に等しく設定することが必要です。

有効値: 範囲は 1 ～ 10000 です。

デフォルト値: 64。

例: set remote-cache size

```
New IPX remote network cache size [64]? 80
```

rip-update-interval *ipx-circuit# interval*

定期的な RIP 同報通信が特定の IPX 回線上で発生する間隔を指定します (分単位)。

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・オンデマンド回線が頻繁にダイヤルアウトするのも防止します。

注: RIP 公示全体がこの間隔によって制御されている間も、ルーターはネットワーク・トポロジー変更を確認すると、速やかにそれを伝達します。

ipx-circuit#

IPXWAN ポイント・ポイント回線への既存 IPX 同報通信を指定します。

有効値: 任意の有効な IPX 回線番号

デフォルト値: 1

interval

間隔を指定します (分単位)。

有効値: 範囲は 1 ～ 1440 分です。

デフォルト値: 1 分。RIP 間隔についての詳細は、 599ページの『RIP 更新間隔の指定』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*

定期的な SAP 同報通信が特定の IPX 回線上で発生する時間遅延を指定します (分単位)。

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・オンデマンド回線が頻繁にダイヤルアウトするのも防止します。

注: SAP 公示全体がこの間隔によって制御されている間も、ルーターはサービス変更を確認すると、速やかにそれを伝達します。

ipx-circuit#

既存 IPX 同報通信または IPXWAN ポイント・ポイント回線を指定します。

有効値: 任意の有効な IPX 番号

デフォルト値: 1

interval

間隔を指定します (分単位)。

有効値: 範囲は 1 ～ 1440 分です。

デフォルト値: 1 分。

例: set sap-update-interval

```
IPX circuit number [1]? 2
SAP Timer Value (minutes) [1]? 2
```

split-horizon *heuristic enabled disabled*

IPX 回線上で使用される水平分割のタイプを指定します。

回線上にフレーム・リレー VC が 1 つしかない場合には、水平分割は使用可能になります。そうでない場合、水平分割は使用不可です。

一般的には、水平分割は *enabled* に設定してください。ただし、部分メッシュ・フレーム・リレー、および X.25 構成では、ときには水平分割を使用不可にすることが必要になります。水平分割についての詳細は、613ページの『水平分割ルーティング』を参照してください。

heuristic

IPX 回線上で水平分割を使用可能にします。ただし、フレーム・リレー IPX 同報通信回線の場合は除きます。

有効値: 任意の有効な IPX 回線番号

デフォルト値: 1

enabled

IPX 回線上で水平分割を使用可能にします。

有効値: 1 ～ 1440

デフォルト値: 1

disabled
水平分割 IPX 回線を使用不可にします。

有効値: 1 ～ 1440

デフォルト値: 1

例: set split-horizon enabled 0

```
IPX circuit number [1]? 2
```

IPX 回線フィルター構成環境へのアクセス

IPX 回線フィルター構成環境にアクセスするには IPX config> プロンプトで、次のコマンドを入力します。

```
IPX Config> filter-lists type
IPX type-List Config>
```

ただし *type* は、構成する 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場合、IPX 回線番号の指定は必須です。

IPX 回線回線フィルター構成コマンド

この節では、IPX 回線をベースとしたフィルター、つまり、ROUTER、RIP、SAP、および IPX の構成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、次に IPX *type*-List Config> プロンプトで構成コマンドを入力します。

表 38. IPX フィルター構成コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxixページの『ヘルプの入手』 を参照してください。
Attach	指定のフィルター・リストを指定のフィルターに付加します。
Create	フィルターまたはフィルター・リストを作成します。
Default	フィルターのデフォルト・アクションを *include* または *exclude* 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・リストをフィルターから切り離します。
Disable	フィルターを使用不可にします。
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・リストを再順序付けします。
Set-cache	指定のフィルターのキャッシュ・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。xxixページの『下位レベル操作環境の終了』 を参照してください。

Attach

attach コマンドは、フィルター・リストをフィルターに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** コマンドを使用すると、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 文字の英数字文字列

デフォルト値: 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、構成済みフィルターの番号付きリストを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*
指定された名前を持つリストを作成します。

有効値: 最大 16 文字の英数字文字列

デフォルト値: なし

リスト名を指定せずに **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に求められます。

例: `create list example_list`

filter *direction ipx-circuit#*
指定された回線上で指定方向のフィルターを作成します。指定の回線で受信したパケットをフィルターに掛ける場合は *input* を指定します。指定の回線によって送信されるパケットをフィルターに掛ける場合は *output* を指定します。

フィルターが作成された時点で、番号が自動的に割り当てられ、その時点からそのフィルターを識別するために使用されるようになるので、それ以降のすべてのコマンドでは、回線および方向 (入力または出力) を指定する必要はありません。

例: `create filter input 1`

Default

default コマンドは、フィルターのデフォルト・アクションを設定するのに使用します。デフォルト・アクションは、フィルター項目のどれにも一致しない場合に取られます。

構文:

default *action filter#*

例: `default exclude 1`

action
デフォルト・アクションを指定します。**Include** は、フィルター項目のどれにも一致しない場合、パケットが処理されることを指定します。**Exclude** は、一致が見つからない場合、パケットは廃棄されることを指定します。

filter#
フィルターの番号を指定します。**list** コマンドを使用すると、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。

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#*
指定され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・リストをフィルターから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 文字の英数字文字列

デフォルト値: 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、フィルターをグローバルに使用不可にするため、または指定されたフィルターを使用不可にするために使用します。

構文:

disable 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を使用不可にします。

例: disable all

filter *filter#*
指定されたフィルターを使用不可にします。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、フィルターをグローバルに使用可能にするため、または指定されたフィルターを使用可能にするために使用します。

構文:

enable 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を使用可能にします。

例: enable all

filter *filter#*
指定されたフィルター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、現行のフィルター・タイプの状態をグローバルに表示するため、または特定のフィルターに関する情報を表示するために使用します。

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関する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#*

指定されたフィルターに関する情報をリストします。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 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・リストの順序を変更するのに使用します。パケットは、リストに表示された順序でフィルター・リストに照らして評価されます。最初の一致で、フィルター・プロセスは停止します。

構文:

move *src-list-name dst-list-name filter#*

src-list-name
フィルター内で移動する必要があるリストを指定します。

dst-list-name
移動先のリスト (それの前に src-list-name を移動する) を指定します。

filter#
リストが所属するフィルターを指定します。list コマンドを使用すると、構成済みのフィルターとそれぞれに付加されたフィルター・リストのリストを表示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・キャッシュは、IPX 回線フィルターでのみサポートされます。ROUTER、RIP、および SAP 回線フィルター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を (エントリー数で) 指定します。

有効値: 4 〜 64 キャッシュ・エントリー

デフォルト値: 10 エントリー

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、更新する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は、更新するフィルター・リスト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 コマンドを使用すると、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、構成する回線・フィルターのタイプ (ROUTER、RIP、SAP、または IPX) によって異なります。どのタイプの回線フィルターも、パラメーターを指定せずに **add** コマンドを入力することが可能です。その場合は、必要なパラメーターを入力するように求められます。

Add (ROUTER)

構文:

add *node-number mask*

node-number
RIP レスポンス・パケットを送信したルーターの発信元ノード番号 (マスクと AND した後で) と比較される値を指定します。単一のノードと照合したい場合は、node-number パラメーターをそのアドレスに設定し、mask を FFFFFFFFFFFF

に設定します。すべてのノードと照合したい場合は、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'

デフォルト値: なし

mask

RIP レスポンス・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 される (アドレス・パラメーターと比較する前に) 値を指定します。

単一のアドレスと照合したい場合は、address パラメーターをそのアドレスに設定し、mask を FFFFFFFFFFFF に設定します。すべてのアドレスと照合したい場合は、 address パラメーターおよび mask パラメーターを 000000000000 に設定します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

デフォルト値: X'FFFFFFFFFFFF'

例: add 400000001000 ffffffff0000

Add (RIP)

構文:

add *net-range-start net-range-end*

net-range-start

フィルターに掛ける IPX ネットワーク番号の範囲 (両端を含む) の開始番号を指定します。単一のネットワーク番号と照合したい場合は、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ます。すべてのアドレスと照合したい場合は、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'

デフォルト値: X'1'

net-range-end

フィルターに掛ける IPX ネットワーク番号の範囲 (両端を含む) の終了番号を指定します。

有効値: X'1' ～ X'FFFFFFFE'

デフォルト値: X'1'

例: add 00000001 FFFFFFFE

Add (SAP)

構文:

add *comparitor hops sap-type name*

comparitor

このリスト項目のホップ・カウントの比較演算子を指定します。

有効値:

<

<=

=

>=

>

デフォルト値: <= 出力フィルターでは comparitor および hops パラメーターは無視されます。

hops

このリスト項目のホップ・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に掛けたくない場合は、比較演算子とホップ・カウントに <= 16 を入力します。出力フィルターでは comparitor および hops パラメーターは無視されます。

有効値: 0 ～ 16

デフォルト値: 16

sap-type

フィルターに掛けるサービス・タイプを指定します。サービス・タイプを入力するか、あるいは全サービス・タイプの場合は X'0000' を入力します。

有効値: X'0' ～ X'FFFF'

デフォルト値: 4

name

フィルターに掛けるサービス・ネームを指定します。

有効値:

1 ～ 47 字の ASCII 文字 (X'20' ～ X'7E')。

疑問符 (?) とアスタリスク (*) 文字を、ワイルドカード文字として使用できます。疑問符は、サーバー名の任意の 1 文字を表すために複数回使用できます。アスタリスクは、サーバー名の任意の部分を表すために複数回使用できます。疑問符とアスタリスクを合わせて使用することも可能です。

デフォルト値: 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

このリスト項目のホップ・カウントの比較演算子を指定します。出力フィルターでは comparitor および hops パラメーターは無視されます。

有効値:

- <
- <=

- =
- >=
- >

デフォルト値: <=

hops
このリスト項目のホップ・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に掛けたくない場合は、比較演算子とホップ・カウントに <= 16 を入力します。出力フィルターでは comparitor および hops パラメーターは無視されます。

ipx-type
フィルターに掛ける 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、あるいは全パケット・タイプの場合は 00 を入力します。

有効値: X'0' ～ X'FF'

デフォルト値: X'0'

dst-net-range-start
フィルターに掛けるあて先 IPX ネットワーク番号の範囲 (両端を含む) の開始番号を指定します。単一のネットワーク番号と照合したい場合は、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ます。すべてのアドレスと照合したい場合は、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'

デフォルト値: X'00000000'

dst-net-range-end
フィルターに掛けるあて先 IPX ネットワーク番号の範囲 (両端を含む) の終了番号を指定します。単一のネットワーク番号と照合したい場合は、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ます。すべてのアドレスと照合したい場合は、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'

デフォルト値: X'00000000'

dst-node
あて先ノード番号 (dst-mask と AND した後で) と比較される値を指定します。単一のノードと照合したい場合は、dst-node パラメーターをそのノード番号に設定し、dst-mask を X'FFFFFFFFFFFF' に設定します。すべてのノードと照合したい場合は、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'

デフォルト値: X'000000000000'

dst-mask
あて先ノード・アドレスと AND される (dst-address パラメーターと比較する前に) 値を指定します。単一のアドレスと照合したい場合は、dst-address パラメーターをそのアドレスに設定し、dst-mask を X'FFFFFFFFFFFF' に設定します。すべ

てのアドレスと照合したい場合は、dst-address パラメーターおよび dst-mask パラメーターを X'000000000000' に設定します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

デフォルト値: X'000000000000'

dst-sck-range-start
フィルターに掛けるあて先 IPX ソケットの範囲 (両端を含む) の開始番号を指定します。単一のソケットと照合したい場合は、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ます。すべてのソケットと照合したい場合は、dst-sck-range-start を X'0000' に設定し、dst-sck-range-end を X'FFFF' に設定します。

有効値: X'0000' ～ X'FFFF'

デフォルト値: 0

dst-sck-range-end
フィルターに掛けるあて先 IPX ソケットの範囲 (両端を含む) の終了番号を指定します。単一のソケットと照合したい場合は、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ます。すべてのソケットと照合したい場合は、dst-sck-range-start を X'0000' に設定し、dst-sck-range-end を X'FFFF' に設定します。

有効値: X'0000' ～ X'FFFF'

デフォルト値: 0

src-net-range-start
フィルターに掛ける発信元 IPX ネットワーク番号の範囲 (両端を含む) の開始番号を指定します。単一のネットワーク番号と照合したい場合は、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ます。すべてのアドレスと照合したい場合は、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'

デフォルト値: X'00000000'

src-net-range-end
フィルターに掛ける発信元 IPX ネットワーク番号の範囲 (両端を含む) の終了番号を指定します。単一のネットワーク番号と照合したい場合は、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ます。すべてのアドレスと照合したい場合は、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'

デフォルト値: X'00000000'

src-node
発信元ノード番号 (src-mask と AND した後で) と比較される値を指定します。単一のノードと照合したい場合は、src-node パラメーターをそのノード番号に設定し、src-mask を X'FFFFFFFFFFFF' に設定します。すべてのノードと照合したい場合は、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'

デフォルト値: X'00000000'

src-mask
発信元ノード・アドレスと AND される (src-address パラメーターと比較する前に) 値を指定します。単一のアドレスと照合したい場合は、src-address パラメーターをそのアドレスに設定し、src-mask を X'FFFFFFFFFFFF' に設定します。すべてのアドレスと照合したい場合は、src-address パラメーターおよび src-mask パラメーターを X'000000000000' に設定します。

有効値: X'000000000000' ～ X'FFFFFFFFFFFF'

デフォルト値: X'000000000000'

src-sck-range-start
フィルターに掛ける発信元 IPX ソケットの範囲 (両端を含む) の開始番号を指定します。単一のソケットと照合したい場合は、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ます。すべてのソケットと照合したい場合は、src-sck-range-start を X'0000' に設定し、src-sck-range-end を X'FFFF' に設定します。

有効値: X'0000' ～ X'FFFF'

デフォルト値: X'0000'

src-sck-range-end
フィルターに掛ける発信元 IPX ソケットの範囲 (両端を含む) の終了番号を指定します。単一のソケットと照合したい場合は、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ます。すべてのソケットと照合したい場合は、src-sck-range-start を0000 に設定し、src-sck-range-end を FFFF に設定します。

有効値: X'0000' ～ X'FFFF'

デフォルト値: 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～6A から IPX ネットワーク 4 へのすべてのパケットをフィルターに掛けます。

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#
リスト内の項目の番号を指定します。この番号は、list コマンドを使用してフィルター・リスト内の項目を表示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 コマンドは、フィルター・リスト・アクションおよびフィルター・リスト項目を表示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 (Update サブコマンド)

move サブコマンドは、フィルター項目の順序を変更するのに使用します。フィルター項目の順序を変更すると、新しい順序を反映するように番号が付け直されます。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、移動する行を示します。この行は、*dest-line#* パラメーターで指定された項目の直前に移動します。

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・リストが一致したときに取るべきアクションを指示します。

構文:

set-action include

exclude

include

現行フィルターで一致が見つかった場合、ROUTER および IPX フィルターでは、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 フィルターでは、**include** は RIP または SAP エントリーが処理されることを指定します。

例: set-action include

exclude

現行フィルターで一致が見つかった場合、ROUTER および IPX フィルター

では、パケットが廃棄される (除外される) ことを指定します。RIP および SAP フィルターでは、**exclude** は、一致が見つかった場合、RIP または SAP エントリーが無視されることを指定します。

例: `set-action exclude`

IPX 監視環境へのアクセス

IPX 監視環境にアクセスする方法については、 *アクセス・インテグレーター・サービス ソフトウェア使用者の手引き*の 『Getting Started (Introduction to the User circuit)』を参照してください。

IPX 監視コマンド

表39 は、IPX 監視コマンドをリストしています。IPX 監視コマンドを使用して、IPX パケットを転送する回線およびネットワークのパラメーターおよび統計を表示することができます。監視コマンドは、物理レベル、フレーム・レベル、およびパケット・レベルの構成値を表示します。この 3 つのプロトコル・レベルのすべての値を同時に表示するオプションもあります。

IPX 監視コマンドは `IPX>` プロンプトで入力します。表39 は、IPX 監視コマンドを要約しています。

表 39. IPX 監視コマンドの要約

コマンド	機能
? (Help)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、特定のコマンドについてのオプション (ある場合) をリストします。 xxix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・キャッシュの現在のコンテンツをリストします。
Counters	ルーティング・エラーとパケット・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・エントリーを削除します。
Disable	IPX をグローバルに、または特定の回線上で使用不可にします。
Dump routing tables	ルーティング・テーブルのコンテンツを表示します。
Enable	IPX をグローバルに、または特定の回線上で使用可能にします。
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、およびフィルターに掛けられた SAP 公示のカウントを表示します。
Filter-Lists	IPX 回線フィルター・コンソールにアクセスします。ここで、RIP ルーター、RIP SAP、および IPX 回線ベースのフィルターを監視することができます。
IPXWAN	IPXWAN ポイント・ポイント回線の IPXWAN 情報をリストします。
Keepalive	キープアライブ・フィルター・テーブル内のアクティブな各クライアント/サーバー・コネクションの状況を表示します。
List	現行構成または使用可能な各回線の IPX アドレスをリストします。

表 39. IPX 監視コマンドの要約 (続き)

コマンド	機能
Ping	IPXPING パケットを別のホストに送信し、レスポンスを監視します。このコマンドは、インターネットワーク環境の障害を分離するのに使用できます。
Recordroute	IPXPING レコード・ルート・パケットを別のホストに送信し、レスポンスを監視します。このコマンドは、この装置と別のホスト間の往復ルートを記録および監視するのに使用します。この情報をインターネットワーク環境の障害を分離するのに利用してください。
Reset	特定の IPX 回線、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、あるいはルーター、RIP、SAP、または IPX 回線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	構成されたローカル・ノードおよびリモート・ネットワーク・キャッシュのサイズ、および現在使用されているキャッシュ・エントリーの数を表示します。
Slist	IPX SAP サーバー・テーブルのコンテンツを表示します。
Traceroute	IPXPING トレース・ルート・パケットを別のホストに送信し、レスポンスを監視します。このコマンドは、この装置からあて先ホストまでの途中にパケットが通過する各ホップを追跡し、表示するのに使用します。この情報をインターネットワーク環境の障害を分離するのに利用してください。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

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)、 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が適用された回数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
```

アクセス制御インデックス番号

Type 特定のアドレスまたはアドレスの集合へのパケットが、送信されるのか廃棄されるのかを識別します。I は include (包含) を意味します。これはパケットを送信することを許可します。E は exclude (排他) を意味します。これにより、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、全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、そのネットワーク上の全ホストを意味します。

Dest-sck あて先ソケットの範囲 (両端を含む) を指定する 2 桁の数字

Src-net 発信元のネットワーク番号。ゼロ (0) は、全ネットワークを意味します。

Src-host あて先ネットワークのホスト番号。ゼロは、そのネットワーク上の全ホストを意味します。

Src-sck 発信元ソケットの範囲 (両端を含む) を指定する 2 バイトの数字

Count 各アクセス制御ステートメントに一致し、関連のタイプ (Include または Exclude) が実行された、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・キャッシュのコンテンツ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
```

最初のエントリーは、リモート・ネットワーク 420 には、IPX ネットワーク番号 412 を持つシリアル・サーキットを介して到達できることを示しています。2 番目のエントリーは、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。このエントリーは、一般ローカル・ネットワーク・エントリーです。直接接続されたネットワークは、IPX パケットの送信を開始すると、それぞれ 1 つの一般ローカル・ネットワーク・エントリーが作成されます。最後のエントリーは、イーサネット上のローカル・エントリーです。この IPX キャッシュ・エントリーを使用して、1 個のパケットがネットワーク番号 412 上の IPX ノード番号 0000 0420 0000 に送信されています。

Counters

counters コマンドは、発生したルーティング・エラーの数およびパケット・オーバーフローの数を表示するのに使用します。例では、counters 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定のエラーが発生しました。

Checksum チェックサムが誤りであるか、またはあて先に到達する前に、パケットに何か他の重大な不整合がありました。

Destination unreachable
ここからはあて先ホストに到達できません。

Hop count expired
パケットは 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。

circuit size exceeded
パケットが大きすぎて、ある中間ネットワークを通して転送できません。

Destination errors

Unknown あて先で不定のエラーが検出されました。

Checksum チェックサムが誤りであるか、またはあて先でパケットに何か他の重大な不整合が検出されました。

Nonexistent socket
指定されたソケットが、指定のあて先ホストに存在しません。

Congestion 資源の限界のために、あて先がパケットを受け取ることができません。

IPX Input Packet Overflows

Net 回線ネームを指定します。

Count 資源の限界のために受信できなかったパケット数を指定します。

Delete

delete コマンドは、キープアライブ・フィルター・テーブル・エントリーを削除するのに使用します。

構文:

delete *entry#*

entry# 削除するテーブル・エントリーを指定します。**Keepalive** コマンドを使用して、キープアライブ・フィルター・テーブルのコンテンツをリストすることができます。

例: `delete 1`

Disable

disable コマンドは、IPX をグローバルに、または特定の回線上で使用不可にするのに使用します。

構文:

disable circuit ...

ipx

circuit *ipx-circuit#*

ipx-circuit# で指定された IPX 回線を使用不可にします。 IPX は、**enable** コマンドを使用して再び使用可能にすることができます。

例: disable circuit 2

ipx すべての回線上の IPX をグローバルに使用不可にします。IPX は、**enable** コマンドを使用して再び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、ルーター・テーブルのコンテンツを表示するのに使用します。

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 - このネットワークはルーターに直接接続されていることを指定します。
- RIP - このルートは IPX ルーティング・プロトコルの RIP によって提供されたことを指定します。
- Old - このルートはタイムアウトになり、もう使用されていないことを指定します。そのルートはもはや有効でないことを他のルーターに通知するために、ルートは短時間テーブルに残っています。この短い時間が過ぎると、もう表示されなくなります。
- Stat - これは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 このあて先のホップ数を指定します。

Delay ルーターが転送し、パケットがあて先に到着するまでにかかる時間の見積も

りを指定します。遅延の単位は、576 バイトのパケットを送信するための IBM PC クロック・ティック数で、これは 18.21 クロック・ティック/秒に相当します。最小遅延は 1 単位です。

Age ルーティング情報のエージ (経過時間) を分と秒で指定します。ルーティング・テーブル内のエントリーが更新されない場合、ルーターは次のアクションを取ります。

- 3 回の RIP 更新間隔が経過した後、そのルートは Old として指定され、ルーターはそのルートがもはや有効でないことを公示します。RIP 更新間隔は **config** コマンドを使用して表示することができます。RIP 間隔についての詳細は、599ページの『RIP 更新間隔の指定』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、ダンプのディスプレイ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行くパケットのネクスト・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、そのパケットを転送するルーター・サーキットのアドレスになります。

Circ IPX 回線番号

Ifc ネットワーク・インターフェース番号

ディスプレイの最上部に、使用されているルートとネットワーク・エントリーの数、および利用可能な総数が表示されます。すべてのネットワーク・エントリーが使用されている場合は、ルーティング・テーブルの大きさが不十分である可能性があります。サイズを大きくするには、IPX 構成 **set maximum networks** コマンドを使用します。

ルート・エントリーがすべて使用されている場合は、新規の着信ネットワークを含めて、保管できない IPX ネットワークへのルートが存在する可能性があります。利用可能なルート数を増やしたくない場合は、ネットワーク当たりの最大ルート数を減らしてください。

Enable

enable コマンドは、IPX をグローバルに、または特定の回線上で使用可能にするのに使用します。

構文:

enable circuit ...

ipx

circuit *ipx-circuit#*
ipx-circuit# で指定された回線上で IPX を使用可能にします。 IPX を使用可能にする前に、IPX ネットワーク番号をその回線用に構成しておく必要があります。

例: `enable circuit 2`

ipx 使用可能なすべての IPX 回線上で IPX をグローバルに使用可能にします。

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、およびフィルターに掛けられた 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 フィルターに掛けられた (廃棄された) SAP 公示の数を示します。

Max Hops そのサービスに許容されるホップの最大数を示します。

Type 数値で表したサービス・クラスです。

Service name
サービスの名前です (名前を持っている場合)。

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 ipx-lists です。

このプロンプトから利用可能なコマンドについては、671ページの『IPX 回線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・ポイント回線の IPXWAN 情報をリストするのに使用します。

構文:

ipxwan detailed . . .
summary

detailed *ipx-circuit#*
指定された IPX 回線の IPXWAN 情報をリストします。

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し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も呼ばれます)。これはインターネットワーク全体で固有な IPX ネットワーク番号です。長さは 32 ビットです。

Negotiated Routing Type

ネゴシエーション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、無番号 RIP、および静的ルーティングです。無番号 RIP または静的ルーティングがネゴシエーションされたルーティング・タイプの場合、そのリンクの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 秒単位のティック数で表されたリンク遅延。16 ビットの長さです。これは常に計算されるので、デフォルトはありません。

Common Net#

リンクの両側で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でユニークでなければなりません。長さは 32 ビットです。ネゴシエーションされたルーティング・タイプが無番号 RIP または静的ルーティングのどちらかである場合には、**IPXWAN detailed** コマンドおよび **IPXWAN summary** コマンドの両方について Common Net# には値 0 が表示されます。デフォルトはなく、ネゴシエーションする必要があります。

Connection Timeouts

コネクション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と、コネクションは定期的にタイムアウトになります。タイムアウト期間は **set ipxwan** コマンドを使用して構成することができます。タイムアウト期間のデフォルト値は 60 秒です。

Connection Retries

タイムアウト後にコネクションが再試行される回数。待ち時間 (再試行前の) は **set ipxwan** コマンドを使用して構成することができます。デフォルトは 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
受信した 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・レスポンス・パケットの数

Timer Responses Received
受信した IPXWAN タイマー・レスポンス・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
受信した IPXWAN 情報要求パケットの数

Info Responses Sent
送信された IPXWAN 情報レスポンス・パケットの数

Info Responses Received
受信した IPXWAN 情報レスポンス・パケットの数

summary
すべての IPXWAN ポイント・ポイント回線の IPXWAN 要約情報をリストします。

例: ipxwan summary

```
Circ   Ifc    Name        Common Net#  NodeID   Neighbor Name
3      2       PPP/1      412          420      ipxwan-420
```

Circ IPX 回線番号

Ifc ネットワーク・インターフェース番号

Common Net#
リンクの両側で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でユニークでなければなりません。ネゴシエーションされたルーティング・タイプが無番号 RIP または静的ルーティングのどちらかである場合、common net# は 0 になります。

NodeID
近隣のノード ID (内部ネットワーク番号とも呼ばれます)。

Neighbor Name
RIP/SAP 情報要求パケットで受信した近隣のルーター名

Keepalive

キープアライブ・フィルター・テーブル内のアクティブな各クライアント/サーバー・コネクションの状況を表示します。

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、現行構成または使用可能な各 IPX 回線の IPX アドレスをリストするのに使用します。

構文:

list *addresses*

configuration

addresses
使用可能な各 IPX 回線のアドレスをリストします。

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
現行の IPX 構成を表示します。このコマンドは、**list summary** 構成コマンドと同じ情報を表示します。表示の例および出力の説明については、630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 IPXPING パケットを指定のあて先に送信し (つまり、『PING』 して) レスポンスを監視するのに使用します。このコマンドは、インターネットワーク環境内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。対応する受信レスポンスが、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) と共に表示されます。

PING プロセスを停止するときは、監視で任意の文字を入力します。このとき、パケット紛失、往復時間、および到達不能あて先の数の要約が表示されます。

マルチキャスト・アドレスをあて先として指定した場合は、送信されたパケットに対して複数のレスポンス (各グループ・メンバーにつき 1 つ) が存在する場合があります。戻された各レスポンスが、応答側の発信元アドレスと共に表示されます。

注:

1. 同報通信アドレス (FFFFFFFFFFFF) を指定するときは、これによって多数の IPXPING レスポンス・パケットが生成され、ネットワークおよびルーティング・ソフトウェアの性能を低下させる可能性があるので、注意が必要です。
2. **ping** コマンドをパラメーターを付けずに入力した場合、すべてのパラメーターを入力するように促されます。***destination network*** および ***destination node*** のみを入力した場合、残りのパラメーターはデフォルト値が使用されます。

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。このパラメーターは必須です。

有効値: X'1' ～ X'FFFFFFFD'

デフォルト値: 1

dest-node
あて先 IPX ノード・アドレスを指定します。このパラメーターは必須です。

有効値: X'1' ～ X'FFFFFFFFFFFF'

デフォルト値: なし

src-net
発信元 IPX ネットワーク番号を指定します。これはオプション・パラメーターです。この値は、直接接続された IPX 回線と関連付けられている既知のネットワーク番号でなければなりません。発信元ネットワークが指定されていない場合、IPXPING 要求パケットを送信する IPX 回線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 回線が IPXWAN 無番号 RIP または静的ルーティング・サーキットである場合には、発信元ネットワーク番号に使用された IPX 回線のノード・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'

デフォルト値: 1

src-node
発信元 IPX ノード・アドレスを指定します。これはオプション・パラメーターです。この値は、直接接続された IPX 回線と関連付けられている既知のノード・アドレスでなければなりません。発信元ノードが指定されていない場合には、IPXPING 要求パケットを送信する IPX 回線のノード・アドレスが発信元 IPX ノードとして使用されます。IPX 回線が IPXWAN 無番号 RIP または静的ルーティング・サーキットである場合には、発信元ネットワーク番号に使用された IPX 回線のノード・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'

デフォルト値: なし

size
PING 要求に付加されるデータ・バイト数を指定します。これはオプション・パラメーターです。このデータには、要求が最初に送信される時間が含まれるので、指定する値は 4 バイトより小さくてはなりません。また、ルーターまたは出力回線によってサポートされる最大パケット・サイズより大きくすることもできません。この値は、構成によって異なります。

有効値: 4 ～ ルーターの最大値

デフォルト値: 56 バイト

rate
PING 要求の相互間の秒数を指定します。これはオプション・パラメーターです。

有効値: 1 ～ 60

デフォルト値: 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、パス上の各転送回線をあて先に報告し、再び報告を戻すのに使用します。パラメーターを何も付けずに recordroute を起動すると、すべてのパラメーターを入力するように促されます。あて先 IPX ネットワーク番号とあて先 IPX ノード・アドレスのみが必須です。

recordroute を終了させる事象は 2 つあります。第 1 は、ユーザーがキーを押した場合です。第 2 は、最大数の recordroute 要求パケットが送信された場合です。

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。このパラメーターは必須です。

有効値: X'1' ～ X'FFFFFFFD'

デフォルト値: 1

dest-node
あて先 IPX ノード・アドレスを指定します。このパラメーターは必須です。

有効値: X'1' ～ X'FFFFFFFFFFFE'

デフォルト値: なし

src-net
発信元 IPX ネットワーク番号を指定します。これはオプション・パラメーターです。この値は、直接接続された IPX 回線と関連付けられている既知のネットワーク番号でなければなりません。発信元ネットワークが指定されていない場合には、recordroute 要求パケットを送信する IPX 回線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 回線が IPXWAN 無番号 RIP または静的ルーティング・サーキットである場合には、IPXWAN 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ので、他の番号制 IPX 回線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。

有効値: X'1' ～ X'FFFFFFFD'

デフォルト値: 1

src-node
発信元 IPX ノード・アドレスを指定します。これはオプション・パラメーターで

す。この値は、直接接続された IPX 回線と関連付けられている既知のノード・アドレスでなければなりません。発信元ノードが指定されていない場合には、recordroute 要求パケットを送信する IPX 回線のノード・アドレスが発信元 IPX ノードとして使用されます。IPX 回線が IPXWAN 無番号 RIP または静的ルーティング・サーキットである場合には、発信元ネットワーク番号に使用された IPX 回線のノード・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'

デフォルト値: なし

rate

recordroute 要求の相互間の秒数を指定します。これはオプション・パラメーターです。

有効値: 1 ～ 60

デフォルト値: 1

number

送信される recordroute 要求の最大数を指定します。これはオプション・パラメーターです。ゼロの値を指定すると、recordroute はキーが押されるまで続きます。

有効値: 0 ～ 60

デフォルト値: 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
```

パス全体への報告は、最初のレスポンスまたはパスが変更されたときに 1 回だけ行われます。上の例では、パスが 2 回変更されています。

Reset

reset コマンドは、特定の IPX 回線、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、あるいはルーター、RIP、SAP、または IPX 回線ベースのフィルター (フィルター・リスト) をリセットするのに使用します。

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起動されます。

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、指定の IPX 回線上で IPX をリセットします。IPX 回線上の IPX 構成に対して行わ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 フィルター構成に対して行わ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回線ベースのフィルターをリセットします。回線ベースのフィルター構成に対して行われた変更が起動されます。有効な ***filter-types*** 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た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起動されます。

例: reset route-static

sap-static
構成メモリーに保管された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起動されます。

例: reset sap static

Sizes

sizes コマンドは、構成されたローカル・ノードおよびリモート・ネットワーク・キャッシュのサイズ、および現在使用されているキャッシュ・エントリーの数を表示するのに使用します。(このコマンドは、キャッシュのコンテンツは表示しません。)

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・テーブルのコンテンツ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 1 つを指定します。

SAP - このサービスは 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 - このサービスはタイムアウトになり、もう使用されていないことを示します。このサービスはもはや有効でないことを他のルーターに知ら

せるために、サービスは短時間だけテーブルに保持されています。その後、サービスは削除され、表示されなくなります。

Stat - このサービスは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。その他のタイプの数値が 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 文字のうちの最初の 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までのルーター・ホップ数を指定します。

Age サービス情報のエージ (経過時間) を指定します。SAP テーブル内のエントリーが更新されない場合、ルーターは次のアクションを取ります。

- 3 回の SAP 更新間隔が経過した後、そのサービスは Del として指定され、ルーターはそのルートがもはや有効でないことを公示します。SAP 更新間隔は **config** コマンドを使用して表示することができます。
- さらに 60 秒が経過すると、そのサービスは削除され、 **slist** ディスプレイ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・ホスト番号 (ネットワーク上の最初の回線のアドレス)
- サービスに到達できるソケット番号

ディスプレイの最下部に、使用されているエントリーの数と利用可能な総数が表示されます。すべてのエントリーが使用されている場合は、サービス・テーブルの大きさが不十分である可能性があります。サイズを大きくするには、IPX 構成 **set maximum services** コマンドを使用します。

Traceroute

traceroute コマンドは、PING 要求が最終あて先までの途中に通過する各ホップを報告するのに使用します。パラメーターを何も付けずに traceroute を起動すると、すべてのパラメーターを入力するように促されます。あて先 IPX ネットワーク番号とあて先 IPX ノード・アドレスのみが必須です。

traceroute を終了させる事象は 3 つあります。第 1 は、ユーザーがキーを押した場合です。第 2 は、あて先アドレスからレスポンスを受信した場合です。第 3 は、ホップの最大数に達した場合です。

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。このパラメーターは必須です。

有効値: X'1' ～ X'FFFFFFFD'

デフォルト値: 1

dest-node

あて先 IPX ノード・アドレスを指定します。このパラメーターは必須です。

有効値: X'1' ～ X'FFFFFFFFFFFE'

デフォルト値: なし

src-net

発信元 IPX ネットワーク番号を指定します。これはオプション・パラメーターです。この値は、直接接続された IPX 回線と関連付けられている既知のネットワーク番号でなければなりません。発信元ネットワークが指定されていない場合には、traceroute 要求パケットを送信する IPX 回線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 回線が IPXWAN 無番号 RIP または静的ルーティング・サーキットである場合には、IPXWAN 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ので、他の番号制 IPX 回線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。

有効値: X'1' ～ X'FFFFFFFD'

デフォルト値: 1

src-node

発信元 IPX ノード・アドレスを指定します。これはオプション・パラメーターです。この値は、直接接続された IPX 回線と関連付けられている既知のノード・アドレスでなければなりません。発信元ノードが指定されていない場合には、traceroute 要求パケットを送信する IPX 回線のノード・アドレスが発信元 IPX ノードとして使用されます。IPX 回線が IPXWAN 無番号 RIP または静的ルーティング・サーキットである場合には、発信元ネットワーク番号に使用された IPX 回線のノード・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'

デフォルト値: なし

size

traceroute 要求に付加されるデータ・バイト数を指定します。これはオプション・パラメーターです。このデータには、要求が最初に送信される時間が含まれるので、指定する値は 4 バイトより小さくてはなりません。また、ルーターまたは出力回線の最大パケット・サイズより大きくすることもできません。この値は、構成によって異なります。

有効値: 4 ～ ルーターの最大値

デフォルト値: 56

probes

ホップ当たりの送信 traceroute 要求の数を指定します。これはオプション・パラメーターです。

有効値: 1 ～ 10

デフォルト値: 3

rate

traceroute 要求に対して応答がない場合、プローブ相互間に待つ秒数を指定します。これはオプション・パラメーターです。

有効値: 1 ～ 60

デフォルト値: 1

hops

traceroute 要求を送信するホップの最大数を指定します。これはオプション・パラメーターです。NLSP がない場合、パケットは最大 16 ノードを通過することができます (したがって、デフォルトは 16 です)。NLSP または IBM 6611 ハーフ・ルーター・ソリューションを使用する場合は、限界は 16 ではなくなります。

有効値: 1 ～ 255

デフォルト値: 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 レスポンスの発信元 IPX アドレスは、変更されない限り、1 回だけ報告されます。上の例では、1 ホップ traceroute 要求に対して、2 つの異なるルーターが応答しています。このような状況が起こるのは、プローブとプローブの間にあて先へのルートが変更された場合です。

プローブの往復時間の他にも、traceroute によって報告される情報があります。

- '*' - 指定された時間にレスポンス・パケットを 1 つも受信しませんでした。
- 'H!' あて先ネットワークが到達不能です。これは traceroute がスタートした後であて先へのルートが失われた場合に報告されます。
- 'BF' - 利用可能なバッファーがありません。

IPX 回線フィルター監視コマンド

表40 は、IPX *type*-Lists> プロンプトから利用可能なコマンドをリストしています。この節では、これらのコマンドについて詳しく説明します。

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 40. IPX 回線フィルター・コマンドの要約

コマンド	機能
Cache	指定された回線のフィルター・キャッシュのコンテンツを表示します。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ます。
Clear	指定されたフィルターのカウンターをクリアするか、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のカウンターをクリアします。

表 40. IPX 回線フィルター・コマンドの要約 (続き)

コマンド	機能
Disable	指定されたフィルター、または現行タイプのすべてのフィルターを使用不可にします。
Enable	指定されたフィルター、または現行タイプのすべてのフィルターを使用可能にします。
List	指定されたフィルター、または現行タイプのすべてのフィルターをリストします。
Exit	直前のコマンド・レベルに戻ります。xxixページの『下位レベル操作環境の終了』 を参照してください。

Cache

cache コマンドは、フィルター・キャッシュのコンテンツを表示するのに使用します。IPX フィルターのみがキャッシュをサポートします。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、指定されたフィルターのカウンターをクリアするか、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のカウンターをクリアします。

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#*
指定され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、指定されたフィルターのカウンターを使用不可にするか、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のカウンターを使用不可にします。

構文:

disable 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を使用不可にします。

例: `disable all`

filter *filter#*
指定されたフィルター番号を使用不可にします。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、指定されたフィルターのカウンターを使用可能にするか、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のカウンターを使用可能にします。

構文:

enable 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を使用可能にします。

例: `enable all`

filter *filter#*
指定され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、指定されたフィルターに関する情報、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関する情報を表示します。

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#*

指定され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
```

付録A. IBM 6611 ルーターとの相互運用

IBM アクセス・インテグレーター・サービスの DLSw インプリメンテーションを IBM 6611 ルーターのインプリメンテーションと相互運用するためには、さまざまな構成上の考慮事項を検討する必要があります。

以下の節では、これらの考慮事項について概説し、IBM アクセス・インテグレーター・サービスの DLSw インプリメンテーションのフィーチャーのうち IBM 6611 のフィーチャーとは相互運用できないものを指摘します。

注: ここに示す考慮事項は、IBM 6611 の MPNP V1.2 ソフトウェアを使用して行ったテストから得られたものです。考慮事項は、他の MPNP ソフトウェア・バージョンには該当しないことがあります。

考慮事項は、以下の節に分類してあります。

- 『ブリッジ構成の考慮事項』
- 『DLSw 関連の考慮事項』
- 676ページの『IP 関連の構成の考慮事項』
- 676ページの『TCP 関連の考慮事項』
- 677ページの『その他の相互運用性に関する考慮事項』

ブリッジ構成の考慮事項

ブリッジ構成の考慮事項は、次のとおりです。

- DLSw の LAN 識別 (セグメント番号) は、IBM 2212 と IBM 6611 ルーターの双方で一致していることが必要です。不一致が継続的に存在する場合は、IBM アクセス・インテグレーター・サービス 構成プログラム (Talk 6) を入力し DLSw プロトコルを選択します。次に **set srb** コマンドを使用して、セグメント番号を IBM 6611 の値に一致するように設定します。
- ブリッジ・フレームに使用できる最大 MTU 値は 2100 バイトです。これは、現在 IBM 6611 によってサポートされている最大値です。2100 より小さい MTU 値を指定する場合は、構成された値が IBM 2212 と IBM 6611 ルーターの双方で一致していることが重要です。

DLSw 関連の考慮事項

DLSw 関連の相互運用性の考慮事項は、次のとおりです。

- IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションでは SSP_IAMOKAY メッセージ (SSP メッセージ・タイプ Type X'x1D') の生成がサポートされないのに対して、IBM 6611 DLSw インプリメンテーションではサポートされます。この SSP メッセージは RFC 1434 に文書化されておらず、IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションでは、受信すると通知せずに廃棄されます。

IBM 6611 ルーターとの相互運用

- IBM 6611 DLSw インプリメンテーションは、IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションから受信した 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した SSP メッセージは生成しません。
- IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションは、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。このメッセージを受信した場合、IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションは、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。このレスポンスは、IBM 6611 DLSw ルーターの APPN ネットワーク・ノード実現によって期待されます。

IP 関連の構成の考慮事項

IP 構成に関する考慮事項は、次のとおりです。

- IBM アクセス・インテグレーター・サービス DLSw 近隣が動的に相互を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/ピア DLSw グループ機能は、IBM 6611 DLSw インプリメンテーションとは相互運用できません。そのため、DLSw の **add tcp neighbor** 構成コマンドを使用して、隣接 IBM 6611 DLSw ピアの IP アドレスを定義することが必要になります。
- 上記の IBM アクセス・インテグレーター・サービス DLSw グループ機能の相互運用上の制約は、RIP/OSPF の選択にも意味を持ってきます。
  - 2212 上で DLSw グループを使用するためには、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 とは相互運用できないので、2212 では RIP のみを使用可能に構成し、OSPF は構成しないようにすることが可能です。
  - IBM 2212 側では OSPF と RIP の両方を使用可能にすることができますが、MOSPF (OSPF 構成を通して選択されている場合) は IBM 6611 によってサポートされません。
- IBM アクセス・インテグレーター・サービス IP 構成内で、特定インターフェース上の同報通信アドレスに対して構成した充てんパターンは、必ず IBM 6611 上の対応する定義に一致するようにします。
- DLSw を介して伝達する SNA トラフィック用の帯域幅を保証するのに使用できる、IBM アクセス・インテグレーター・サービスの帯域幅予約システム (BRS) は、IBM 6611 DLSw インプリメンテーションと相互運用できません。

  BRS のために IBM 2212 ハードウェアによって割り当てられた優先順位は、発信方向では実施できますが、中間 IP ルーターが BRS をサポートしていない場合には優先度の順序は保証されません。また、6611 は伝送路の自分の側では BRS をサポートしないので、BRS は単方向にしか適用できません。

TCP 関連の考慮事項

TCP の相互運用性に関する考慮事項は、次のとおりです。

TCP 接続切断の検出の相違

IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションは、キープアライブ応答を受信しない場合 (そのコネクションでキープアライブ・オプションが使用可能にされていると想定) またはデータを配信できない場合に、TCP コネクションが切断されていることを検出します。

TCP コネクションの再確立の相違

TCP コネクションが切断された場合、IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションは、エンド・ステーションから DLC TEST メッセージを受信して新規の DLSw SSP_CANUREACH が生成されたときに、TCP コネクションを再確立します。IBM 6611 は、これと同じ動作をしない場合があります。

キープアライブ使用不可/使用可能に関する相違

前述のように、IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションは、TCP 近隣 IP アドレスが追加 (構成) されている場合、キープアライブ・オプションを使用可能および使用不可にすることができます。IBM 6611 DLSw インプリメンテーションにおける TCP は、TCP セッションで受信したキープアライブ・メッセージには応答しますが、常駐の 6611 TCP が TCP キープアライブ・メッセージを生成するメカニズムは備えていません。

サポートされる TCP コネクションの最大数

IBM アクセス・インテグレーター・サービス DLSw インプリメンテーションには、サポートされる TCP コネクションの最大数に関するハード・コーディングされた制約はありません。したがって、サポートされる TCP コネクションの最大数は、IBM 2212 の利用可能なメモリーに直接関係します。IBM 6611 の場合は、DLSw インプリメンテーションでサポートできる TCP コネクションを 100 とする、ハード・コーディングされた内部制限があります。

その他の相互運用性に関する考慮事項

以下の相互接続性に関する種々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 コネクションの確立の試行中に問題が検出された場合は、IBM 6611 構成をチェックして、MAC アドレス・フィルターが関連の発信元またはあて先 MAC アドレスに対して誤って使用可能にされていないか確認してください。
- RFC 1434 ではオーファン DLSw セッションの問題 (たとえば、後続のアクティビティーがないのに DLSw 回線が確立された状態のまま残っている DLSw セッション) には特別な対応は取っていませんが、IBM アクセス・インテグレーター・サービスおよび IBM 6611 DLSw インプリメンテーションは両方とも、オーファン DLSw セッション・タイムアウトを提供することによってこの問題を解決しています。どちらのインプリメンテーションも、DLSw 回線確立状態のときに非アクティブのままの状態が 30 秒を超える DLSw セッションはないようにされています。

IBM 6611 ルーターとの相互運用

付録B. IBM 6611 ブリッジとの相互運用

IBM 2212 のブリッジングを IBM 6611 のブリッジングと相互運用可能にするためには、さまざまな構成問題を検討する必要があります。

この付録では、これらの問題について概説し、IBM 2212 で実現されたブリッジ機能のうち、IBM 6611 のブリッジ・インプリメンテーションと相互運用**できない**ものを指摘します。

整合性のないネットワークを構築するのを回避するために、IBM 6611 と IBM 2212 を、PPP およびフレーム・リレー・シリアル・リンクを介した 2 つのエンド・ブリッジとして使用する場合には、以下のブリッジ構成問題を考慮する必要があります。

PPP の場合、RFC 1638、*PPP ブリッジング制御プロトコル*に説明されているように、IBM 2212 ブリッジは異なる 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、IBM 2212 は RFC 1490 *フレーム・リレーを介したマルチプロトコル相互接続* 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 MAC タイプをサポートしていますが、 IBM 6611 ブリッジがトークンリング MAC フレームをサポートするのは、PPP またはフレーム・リレーに関連したブリッジ・ポートが**ソース・ルーティング**・ポートとして構成されている場合に限られます。そのため、IBM 6611 と IBM 2212 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に、ネットワーク・トポロジーにある種の制約が生じます。

RFC 1638 第 5.3 節に、ベンダーがピア・ブリッジに PPP 経由でサポートされる MAC タイプを通知し、ピアが PPP 経由でサポートされない MAC タイプを送信するのを防止する方法が記述されています。現在、IBM 2212 ブリッジは PPP ネットワークあての非イーサネット・フレームを廃棄しません。また PPP 上に送信する前に、すべてのフレームをイーサネット・フレームに変換することも試みません。その結果、IBM 6611 は PPP を介して非イーサネット・フレームを受信することになり、構成に一致しない場合は廃棄しています。

その他の PPP の考慮事項

ブリッジ・ネットワークに 2212 および 6611 を構成する際には、以下のことを念頭におく必要があります。

- PPP リンクを介してトラフィックをブリッジする場合は、交渉された最大受信単位 (MRU) が、ブリッジされたフレームを収容できる十分な大きさになるようにすることが必要です。ブリッジされたフレームには、データと発信元 LAN からの MAC レイヤー・ヘッダーが入っています。

  たとえば、イーサネット・フレームには 1500 バイトのデータが入ります。WAN リンクを介してブリッジされる場合、ブリッジされたトラフィックには追加の 14 バイトのイーサネット MAC ヘッダーが組み込まれ、パケット・サイズは 1514 になります。このことは、このフレームをブリッジするためには、交渉済みの PPP MRU が少なくとも 1514 でなければならないことを意味しています。

MRU サイズは、ブリッジされたフレームを保持できる十分な大きさにするのに加えて、さらに余裕をもたせるように考慮する必要があります。当初の MRU 値として 2000 ～ 2048 を使用してみてください。

- PPP リンクの両端の MRU が同じサイズに構成されていることを確認してください。2212 にデフォルト MRU を使用する場合は、6611 の MRU 値を 2212 MRU 値に一致させてください。

構成例

以下のネットワーク・トポロジーの例は、機能***しません***。可能な代替構成には、**代替**と表示してあります。WAN を考慮する際には、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 2212 (SR-TB) - PPP (TB) - IBM 6611 (TB) - イーサネット

代替: トークンリング (SR) - IBM 2212 (SRB) - PPP (SR) - IBM 6611 (SR-TB) - イーサネット

例 2: トークンリング (TB) - IBM 2212 (TB) - PPP (TB) - IBM 6611 (TB) - ETH/TKR

代替: トークンリング (SR) - IBM 2212 (SRB) - PPP (SR) - IBM 6611 (SR-TB) - ETH

代替: トークンリング (SR) - IBM 2212 (SRB) - PPP (SR) - IBM 6611 (SRB) - TKR

代替: トークンリング (TB) - IBM 2212 (SR-TB) - PPP (SR) - IBM 6611 (SRB) - TKR

代替: トークンリング (TB) - IBM 2212 (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、ソース・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の発信ブリッジ・ポートのブリッジ構成の状態に基づいて、IBM 2212 ブリッジは、ソース・ルート・トークンリング・フレームを、次のように変換します。

1. ETH (TB) イーサネット
2. PPP / FR / トンネル / トークンリング TB フォーマット
3. PPP / FR / トンネル / トークンリング SR フォーマット
4. TKR (TB) トークンリング TB フォーマット
5. TKR (SR) トークンリング SR フォーマット

略語集

AARP AppleTalk アドレス解決プロトコル (AppleTalk Address Resolution Protocol)

ABR エリア・ボーダー・ルーター (area border router)

ack 確認応答 (acknowledgment)

AIX 拡張対話式エグゼクティブ (Advanced Interactive Executive)

AMA 任意 MAC アドレス指定 (arbitrary MAC addressing)

AMP アクティブ・モニター・プレゼント (active monitor present)

ANSI 米国規格協会 (American National Standards Institute)

AP2 AppleTalk フェーズ 2 (AppleTalk Phase 2)

APPN 拡張ピアツーピア・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 (adaptive source routing transparent)

ASYNC
非同期 (asynchronous)

ATCP AppleTalk 制御プロトコル (AppleTalk Control Protocol)

ATP AppleTalk トランザクション・プロトコル（AppleTalk Transaction Protocol）

AUI 接続ユニット・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・ブロードキャスト・マネージャー (Bridging Broadcast Manager)

BECN 逆方向明示的輻輳 (ふくそう) 通知（backward explicit congestion notification）

BGP ボーダー・ゲートウェイ・プロトコル（Border Gateway Protocol）

BNC bayonet Niell-Concelman

BNCP ブリッジング・ネットワーク制御プロトコル (Bridging Network Control Protocol)

BOOTP
BOOT プロトコル (BOOT protocol)

BPDU ブリッジ・プロトコル・データ単位（bridge protocol data unit）

bps ビット/秒 (bits per second)

BR ブリッジング/ルーティング (bridging/routing)

BRS 帯域幅予約システム (bandwidth reservation system)

BSD Berkeley ソフトウェア配布 (Berkeley software distribution)

BTP BOOTP リレー・エージェント (BOOTP relay agent)

BTU 基本伝送単位 (basic transmission unit)

CAM コンテンツ・アドレス可能メモリー (content-addressable memory)

CCITT 国際電信電話諮問委員会 (Consultative Committee on International Telegraph and Telephone)

CD 衝突検出 (collision detection)

CGWCON
ゲートウェイ・コンソール (Gateway Console)

CIDR 無クラス・ドメイン間ルーティング (Classless Inter-Domain Routing)

CIP クラシカル IP (Classical IP)

CIR 認定情報速度 (committed information rate)

CLNP コネクションレス型モード・ネットワーク・プロトコル (Connectionless-Mode Network Protocol)

CPU 中央演算処理装置 (central processing unit)

CRC 巡回冗長検査 (cyclic redundancy check)

CRS 構成報告書サーバー（configuration report server）

CTS 送信可 (clear to send)

CUD 起呼ユーザー・データ (call user data)

DAF 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 国防データ・ネットワーク (Defense Data Network)

DDP データグラム送達プロトコル (Datagram Delivery Protocol)

DDT 動的デバッグ・ツール (Dynamic Debugging Tool)

DHCP 動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)

dir 直接接続 (directly connected)

DL データ・リンク (data link)

DLC データ・リンク制御 (data link control)

DLCI データ・リンク接続識別子 (data link connection identifier)

DLS データ・リンク交換 (data link switching)

DLSw データ・リンク交換 (data link switching)

DMA 直接メモリー・アクセス (direct memory access)

DNA ディジタル・ネットワーク体系 (Digital Network Architecture)

DNCP DECnet プロトコル制御プロトコル (DECnet Protocol Control Protocol)

DNIC データ・ネットワーク識別子コード (Data Network Identifier Code)

DoD 米国国防総省 (Department of Defense)

DOS ディスク・オペレーティング・システム (Disk Operating System)

DR 指定ルーター (designated router)

DRAM 動的ランダム・アクセス・メモリー (Dynamic Random Access Memory)

DSAP 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)

ELSCon
2 次 ELS コンソール (Secondary ELS Console)

ESI エンド・システム識別子 (End system identifier)

EST 東部標準時 (Eastern Standard Time)

Eth イーサネット (Ethernet)

fa-ga 機能アドレス・グループ・アドレス (functional address-group address)

FCS フレーム検査シーケンス (frame check sequence)

FECN 順方向明示的輻輳 (ふくそう) 通知 (forward explicit congestion notification)

FIFO 先入れ先出し (first in, first out)

FLT フィルター・ライブラリー (filter library)

FR フレーム・リレー (Frame Relay)

FRL フレーム・リレー (Frame Relay)

FTP ファイル転送プロトコル (File Transfer Protocol)

GMT グリニッジ標準時 (Greenwich Mean Time)

GOSIP
米国政府 OSI 調達仕様 (Government Open Systems Interconnection Profile)

GTE 一般電話会社 (General Telephone Company)

GWCON
ゲートウェイ・コンソール (Gateway Console)

HDLC ハイレベル・データ・リンク制御 (high-level data link control)

HEX 16 進法 (hexadecimal)

HPR 高性能ルーティング (high-performance routing)

HST TCP/IP ホスト・サービス (TCP/IP host services)

HTF ホスト・テーブル形式 (host table format)

IBD 統合ブート装置 (Integrated Boot Device)

ICMP インターネット制御メッセージ・プロトコル (Internet Control Message Protocol)

ICP インターネット制御プロトコル (Internet Control Protocol)

ID 識別 (identification)

IDP イニシアル・ドメイン・パート (Initial Domain Part)

IDP インターネット・データグラム・プロトコル (Internet Datagram Protocol)

IEEE 米国電気電子学会 (Institute of Electrical and Electronics Engineers)

Ifc# インターフェース番号 (interface number)

IGP 内部ゲートウェイ・プロトコル (interior gateway protocol)

InARP 逆アドレス解決プロトコル (Inverse Address Resolution Protocol)

IP インターネット・プロトコル (Internet Protocol)

IPCP IP 制御プロトコル (IP Control Protocol)

IPPN IP プロトコル・ネットワーク (IP Protocol Network)

IPX インターネットワーク・パケット交換 (Internetwork Packet Exchange)

IPXCP IPX 制御プロトコル (IPX Control Protocol)

ISDN サービス総合ディジタル網 (integrated services digital network)

ISO 国際標準化機構 (International Organization for Standardization)

Kbps キロビット/秒 (kilobits per second)

LAC L2TP ネットワーク・アクセス・コンセントレーター (L2TP Network Access Concentrator)

LAN ローカル・エリア・ネットワーク (local area network)

LAPB リンク・アクセス・プロトコル (link access protocol-balanced)

LAT ローカル・エリア・トランスポート (local area transport)

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)

LED 発光ダイオード (light-emitting diode)

LF 最大フレーム、改行 (largest frame; line feed)

LIS 論理 IP サブネット (Logical IP subnet)

LLC 論理リンク制御 (logical link control)

LLC2 論理リンク制御 2 (logical link control 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
軍用ネットワーク (military network)

MOS マイクロ・オペレーティング・システム (Micro Operating System)

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)

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 米国科学財団 (National Science Foundation)

NSFNET
米国科学財団ネットワーク (National Science Foundation NETwork)

NVCNFG
不揮発性構成 (nonvolatile configuration)

OPCON
オペレーター・コンソール (Operator Console)

OSI 開放型システム間相互接続 (open systems interconnection)

OSICP
OSI 制御プロトコル (OSI Control Protocol)

OSPF 最短パス最優先オープン (Open Shortest Path First)

OUI 組織固有識別子 (organization unique identifier)

PC パーソナル・コンピューター (personal computer)

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 (process identification)

P-P ポイント・ポイント (Point-to-Point)

PPP ポイント・ポイント・プロトコル (Point-to-Point Protocol)

PROM プログラム式読み取り専用メモリー (programmable read-only memory)

PU 物理装置 (physical unit)

PVC パーマネント・バーチャル・サーキット (permanent virtual circuit)

RAM ランダム・アクセス・メモリー (random access memory)

RD ルート記述子 (route descriptor)

REM リング・エラー監視 (ring error monitor)

REV 受信 (receive)

RFC Request for Comments（コメント要求）

RI リング標識、ルーティング情報 (ring indicator; routing information)

RIF ルーティング情報フィールド (routing information field)

RII ルーティング情報標識 (routing information indicator)

RIP ルーティング情報プロトコル (Routing Information Protocol)

RISC 縮小命令セット・コンピューター (reduced instruction-set computer)

RNR 受信不可 (receive not ready)

ROM 読み取り専用メモリー (read-only memory)

ROpcon
リモート・オペレーター・コンソール (Remote Operator Console)

RPS リング・パラメーター・サーバー (ring parameter server)

RTMP ルーティング・テーブル保守プロトコル (Routing Table Maintenance Protocol)

RTP ルーティング更新プロトコル (RouTing update Protocol)

RTS 送信要求 (request to send)

Rtype ルート・タイプ (route type)

rxmits 再送 (retransmissions)

rxmt 再送する (retransmit)

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)

seqno シーケンス番号 (sequence number)

SGID サーバー・グループ ID (sever group id)

SGMP シンプル・ゲートウェイ監視プロトコル (Simple Gateway Monitoring Protocol)

SL シリアル・ライン (serial line)

SMP 待機モニター・プレゼント (standby monitor present)

SMTP シンプル・メール転送プロトコル (Simple Mail Transfer Protocol)

SNA システム・ネットワーク体系 (Systems Network Architecture)

SNAP サブネットワーク・アクセス・プロトコル (Subnetwork Access Protocol)

SNMP シンプル・ネットワーク管理プロトコル (Simple Network Management Protocol)

SNPA サブネットワーク接続ポイント (subnetwork point of attachment)

SPF OSPF エリア内ルート (OSPF intra-area route)

SPE1 OSPF 外部ルート・タイプ 1 (OSPF external route type 1)

SPE2 OSPF 外部ルート・タイプ 2 (OSPF external route type 2)

SPIA OSPF エリア間ルート・タイプ (OSPF inter-area route type)

SPID サービス・プロファイル ID (service profile ID)

SPX 順次パケット交換 (Sequenced Packet Exchange)

SQE 信号品質エラー (signal quality error)

SRAM 静的ランダム・アクセス・メモリー (static random access memory)

SRB ソース・ルーティング・ブリッジ (source routing bridge)

SRF 特定ルート・フレーム (specifically routed frame)

SRLY SDLC リレー (SDLC relay)

SRT ソース・ルーティング透過 (source routing transparent)

SR-TB
ソース・ルーティング - 透過型ブリッジ (source routing-transparent bridge)

STA 静的 (static)

STB スパンニング・ツリー・ブリッジ (spanning tree bridge)

STE スパンニング・ツリー探索 (spanning-tree explorer)

STP シールド付き対より線、スパンニング・ツリー・プロトコル (shielded twisted pair; spanning tree protocol)

SVC スイッチド・バーチャル・サーキット (switched virtual circuit)

TB 透過型ブリッジ (transparent bridge)

TCN トポロジー変更通知 (topology change notification)

TCP 伝送制御プロトコル (Transmission Control Protocol)

TCP/IP
伝送制御プロトコル/インターネット・プロトコル (Transmission Control Protocol/ Internet Protocol)

TEI 端末終端点識別子 (terminal endpoint identifier)

TFTP トリビアル・ファイル転送プロトコル (Trivial File Transfer Protocol)

TKR トークンリング (token ring)

TMO タイムアウト (timeout)

TOS サービスのタイプ (type of service)

TSF 透過スパンニング・フレーム (transparent spanning frames)

TTL 活動回数 (time to live)

TTY テレタイプライター (teletypewriter)

TX 送信 (transmit)

UA 非番号制確認 (unnumbered acknowledgment)

UDP ユーザー・データグラム・プロトコル (User Datagram Protocol)

UI 非番号制情報 (unnumbered information)

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

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) すべての着信先に同じデータを伝送すること。 (T) (2) 複数の着信先に同時にデータを伝送すること。 (3) *マルチキャスト (multicast)* と対比。

同報通信アドレス (broadcast address). 通信において、リンク上のすべてのステーションに共通のアドレスとして確保されているステーション・アドレス (8 桁の 1 で構成)。*全ステーション・アドレス (all-stations address)* と同義。

C

キャッシュ (cache). (1) 主記憶装置から読み出した、プロセッサーが次に必要になる可能性がある命令とデータのコピーを入れておくために使用される、主記憶装置より小さくて高速の特殊用途バッファー記憶装置。 (T) (2) 頻繁にアクセスされる命令とデータを入れておくバッファー記憶装置。アクセス時間を短縮するために使用される。 (3) ディレクトリーの検索速度を上げるために、頻繁に使用されるディレクトリー情報を入れておくことができる、ネットワーク・ノード内のディレクトリー・データベースのオプション部。 (4) キャッシュに入れる、または保管すること。

コール・リクエスト・パケット (call request packet). (1) 呼のための接続を確立することを要求するために、データ端末装置 (DTE) がネットワーク全体に伝送する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。

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・パケットまたは発呼要求パケット内のビット。

デーモン (daemon). 標準サービスを行うために無人で実行されるプログラム。デーモンには、そのタスクを実行するために自動的に起動されるものと、定期的に動作するものがある。

データ・キャリア検出 (DCD) (data carrier detect (DCD)). *受信回線信号検出器 (RLSD) (received line signal detector (RLSD))* の同義語。

データ回線 (data circuit). (1) 両方向データ通信の手段を提供する、関連付けられた一対の送信チャネルと受信チャネル。 (I) (2) SNA においては、*リンク接続 (link connection)* の同義語。 (3) *物理サーキット (physical circuit)* およびバーチャル・サーキット *(virtual circuit)* も参照。

注:

1. データ交換装置相互間では、データ回線は、データ交換装置で使用するインターフェースのタイプによって、データ回線終端装置 (DCE) を含むことがある。
2. データ端末とデータ交換装置またはデータ集線装置との間では、データ回線は、データ装置側のデータ回線終端装置を含み、またデータ交換装置またはデータ集線装置側の DCE と類似の装置を含むことがある。

データ回線終端装置 (DCE) (data circuit-terminating equipment (DCE)). データ端末において、データ端末装置 (DTE) と回線の間で信号変換および符号化を行う装置。 (I)

注:

1. DCE は、独立した機器であるか、DTE または中間装置に組み込まれている。
2. DCE は、伝送路のネットワーク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。*送信元サービス・アクセス・ポイント (SSAP) (source service access point (SSAP))* と対比。

装置 (device). 特定の目的をもつ機械的、電気的、または電子的な仕組み。

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呼を受け入れることができない状態を表わす用語。

定義域、ドメイン (domain). (1) データ処理資源が共通制御下に置かれているコンピューター・ネットワーク部分。 (T) (2) 開放型システム間相互接続 (OSI) において、共通のポリシーが適用される、分散システムの部分または管理オブジェクトの集合。 (3) *管理領域 (Administrative Domain)* および*ドメイン名 (domain name)* を参照。

ドメイン名 (domain name). インターネット・プロトコルにおける、ホスト・システムの名前。ドメイン名は、区切り文字によって区切られた一連のサブネームから構成される。たとえば、ホスト・システムの完全修飾ドメイン名 (FQDN) が `ralvm7.vnet.ibm.com` である場合、以下がそれぞれドメイン名である。

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

ドメイン名サーバー (domain name server). インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップすることにより名前からアドレスへの変換を行うサーバー・プログラム。ネーム・サーバー *(name server)* と同義。

ドメイン名システム (DNS) (Domain Name System (DNS)). インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップするために使用される分散データベース・システム。

ドット 10 進表記 (dotted decimal notation). 基底を 10 とし、ピリオド (ドット) で相互を分離して書かれた、4 つの 8 ビット数字からなる 32 ビット整数の構文表記。 IP アドレスを表すのに使用される。

ダンプ (dump). (1) ダンプしたデータ。 (T) (2) 誤り情報を収集するために、バーチャル記憶装置のコンテンツの全部または一部をコピーすること。

動的再構成 (DR) (dynamic reconfiguration (DR)). 完全な構成テーブルを再生成したり、影響を受けるメジャー・ノードを停止せずに、ネットワーク構成 (周辺 PU および LU) を変更するプロセス。

動的ルーティング (Dynamic Routing). 初期化時に静的に構成されたルートではなく、動的に確認されたルートを使用するルーティング。

E

エコー (echo). データ通信において、通信チャネル上の反射信号。たとえば、通信端末装置では各信号は 2 度表示される。ローカル端末に入ったときに一度表示され、通信リンクを経由して戻ってきたときに再度表示される。これにより、信号が正確であるかどうかを検査することができる。

EIA 232. データ通信において、順次 2 進データ交換を使用して、データ端末装置 (DTE) とデータ回線終端装置 (DTE) 間のインターフェースを定義する米国電子工業会 (EIA) の仕様。

米国電子工業会 (EIA) (Electronic Industries Association (EIA)). 業界の技術成長を促進し、各メンバーの意見を代表し、業界標準を開発するために組織された電子機器製造業者の団体。

EIA 単位 (EIA unit). 米国電子工業会で確立された測定単位で、44.45 mm (1.7 インチ) に等しい。

カプセル化 (encapsulation). (1) 通信において、階層化されたプロトコルによって使用される技法で、これを用いて各レイヤーはサポートするレイヤーからのプロトコル・データ単位 (PDU) に制御情報を追加する。この場合、このレイヤーは、サポートするレイヤーからのデータをカプセル化する。インターネット・プロトコルでは、たとえば、パケットには、物理レイヤーからの制御情報が入り、その後にネットワーク・レイヤーからの制御情報が続き、その後にアプリケーション・プロトコル・データが入っている。 (2) データ・リンク交換 *(data link switching)* も参照。

コード化 (encode). 元の形に再び変換できるような方法で、規則を使用してデータを変換すること。 (T)

エンド・ノード (EN) (end node (EN)). (1) *拡張対等間通信ネットワーキング (APPN) エンド・ノード (Advanced Peer-to-Peer Networking (APPN) end node)* およびローエントリー・ネットワーキング *(LEN)* エンド・ノード *(low-entry networking (LEN) end node)* を参照。 (2) 通信において、頻繁に 1 つのデータ・リンクに接続されるノードで、中間ルーティング機能を実行できないもの。

入り口点 (EP) (entry point (EP)). SNA において、分散ネットワーク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。

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)。

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。発信元と着信先のアドレス、ユーザー・データ、および制御情報 (データグラムの長さ、ヘッダー・チェックサム、データグラムの分割が可能かどうか、あるいは分割されているかどうかを示すフラグなど) が入っている。

IP ルーター (IP router). ネットワーク上のトラフィックが流れるパスを決定する、IP インターネット内の装置。ルーティング・プロトコルを使用して、ネットワークに関する情報を収集し、データグラムを最終着側に転送する最善ルートを決める。データグラムは、IP 着信アドレスに基づいてルーティングされる。

IPXWAN. 広域ネットワーク (WAN) を介してインターネットワーク・パケット交換機能 (IPX) ルーティング情報を交換する前に、ルーター相互間で情報を交換するために使用される Novell プロトコル。

J

ジッター (jitter). (1) ディジタル信号の有意瞬間における、その理想位置からの短時間の非累積的な変動。 (2) 伝送されたディジタル信号の好ましくない変動。 (3) ネットワーク遅延の変動。

L

L2TP アクセス集線装置 (LAC) (L2TP Access Concentrator (LAC)). PPP プロトコルと L2TP プロトコルの両方を扱うことができる 1 つまたは複数の公衆サービス電話網 (PSTN) 回線または ISDN 回線に接続される集線装置。装置には、L2TP が稼働するためのメディアをサポートする必要がある。L2TP はトラフィックを 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) に渡す。L2TP は、PPP ネットワークによって搬送されたプロトコルをトンネルすることができる。

L2TP ネットワーク・サーバー (LNS) (L2TP Network Server (LNS)). LNS は PPP エンド・ステーションなど任意のプラットフォーム上で稼働する。 LNS は L2TP プロトコルのサーバー側を扱う。L2TP は、L2TP トンネルを通じて到着する単一の媒体にだけ依存しているので、LNS は単一の LAN または WAN インターフェースだけをもつが、LAC によってサポートされる全範囲の PPP インターフェースのうちどのインターフェースから到着する呼び出しも着信する。これらには、非同期 ISDN、同期 ISDN、V.120、およびその他のタイプの接続が含まれる。

LAN ブリッジ・サーバー (LBS) (LAN bridge server (LBS)). IBM トークンリング・ネットワーク・ブリッジ・プログラムにおいて、2 つ以上のリング間で (ブリッジを介して) 転送されたフレームに関する統計情報を保持しているサーバー。 LBS は、LAN 報告機構 (LRM) を通して、これらの統計を該当の LAN マネージャーに送信する。

LAN エミュレーション (LE) (LAN Emulation (LE)). ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

LAN エミュレーション・クライアント (LEC) (LAN Emulation Client (LEC)). エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

LAN エミュレーション構成サーバー (LECS) (LAN Emulation Configuration Server (LECS)). 構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

LAN エミュレーション・サーバー (LES) (LAN Emulation Server (LES)). LAN 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。

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。

マルチキャスト (multicast). (1) 選択された着信先グループに同じデータを伝送すること。 (T) (2) パケットのコピーが可能なすべての着信先のサブセットだけに伝達される、特殊な形式の同報通信。

マルチパス・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)). *拡張ピア間通信ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node)* を参照。

ネットワーク・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

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) エコー要求を宛先に送って応答を待つことにより、宛先に到達できるかどうかをテストする、TCP/IP ネットワーク・ノードで使用されるプログラム。 (2) 通信における、到達可能性のテスト。

パケット損失率 (packet loss ratio). パケットが指定の着信先に到達しない、または指定された時間内に到達しない確率。

パケット・モード動作 (packet mode operation). *パケット交換 (packet switching)* の同義語。

パケット交換 (packet switching). (1) アドレス指定されたパケットを用いてデータのルーティングと転送を行うことによって、パケットの伝送中だけチャネルが占有されるようにする処理。伝送が完了すると、そのチャネルは他のパケットの伝送に利用可能になる。 (I) (2) *パケット・モード動作 (packet mode operation)* と同義。*回線交換 (circuit switching)* も参照。

並列ブリッジ (parallel bridges). 同じ LAN セグメントに接続され、そのセグメントへの冗長パスを形成する 1 対のブリッジ。

並列伝送グループ (parallel transmission groups). 各グループが異なるグループ番号をもつ、隣接ノード間の複数の伝送グループ。

パス (path). (1) 通信ネットワークにおける 2 つのノード間のルート。パスは複数の分岐を含むことができる。 (T) (2) 2 つのネットワーク・アクセス可能装置間で交換される情報が通る、一連の伝送ネットワーク・コンポーネント (パス制御およびデータ・リンク制御)。*明示ルート (ER) (explicit route (ER))*、*ルート拡張 (route extension)*、および*バーチャル・ルート (VR) (virtual route (VR))* も参照。

パス制御 (PC) (path control (PC)). 通信ネットワークのネットワーク・アクセス可能装置間でメッセージをルーティングし、相互間のパスを提供する機能。伝送制御からの基本情報単位 (BIU) を (場合によっては分割して) パス情報単位 (PIU) に変換し、1 つまたは複数の PIU を含む基本伝送単位をデータ・リンク制御と交換する。パス制御はノード・タイプによって異なる。あるノード (たとえば、APPN ノード) は、ローカルに生成されたセッション識別子をルーティングに使用し、あるノード (サブエリア・ノード) は、ネットワーク・アドレスをルーティングに使用する。

パス・コスト (path cost). リンク状態ルーティング・プロトコルにおいて、2 つのノードまたはネットワーク・ノード間のパス上のリンク・コストの合計。

パス情報単位 (PIU) (path information unit (PIU)). 伝送ヘッダー (TH) のみから成る、または TH の後に基本情報単位 (BIU) または BIU セグメントが続いているメッセージ単位。

パターン突き合わせ文字 (pattern-matching character). 1 文字または複数の文字を表すために使用できる、アスタリスク (*) や疑問符 (?) のような特殊文字。任意の 1 文字または一組の文字を、パターン突き合わせ文字と置き換えることができる。*グローバル文字 (global character)* および*ワイルドカード文字 (wildcard character)* と同義。

パーマネント・バーチャル・サーキット (PVC) (permanent virtual circuit (PVC)). X.25 およびフレーム・リレー通信で、各データ端末装置 (DTE) に論理チャネルが固定的に割り当てられているバーチャル・サーキット。呼設定プロトコルは不要である。*スイッチド・バーチャル・サーキット (SVC) (switched virtual circuit (SVC))* と対比。

物理回線 (physical circuit). 多重化なしで確立されている回路。*データ回線 (data circuit)* も参照。*バーチャル・サーキット (virtual circuit)* と対比。

物理レイヤー (physical layer). 開放型システム間相互接続参照モデルにおいて、伝送媒体を介して物理接続を確立、維持、および解放するための機械的、電気的、機能的、および手順的な手段を提供するレイヤー。 (T)

物理装置 (PU) (physical unit (PU)). (1) SSCP-PU セッションを介した SSCP の要求に応じて、ノードに関連する資源 (接続リンクや隣接リンク・ステーションなど) を管理および監視するコンポーネント。 SSCP は、接続リンクのようなノードの資源を PU を介して間接的に管理するために、物理装置をもつセッションを起動する。この用語は、タイプ 2.0, タイプ 4, およびタイプ 5 ノードにのみ適用される。 (2) *周辺 PU (peripheral PU)* およびサブエリア *PU (subarea PU)* も参照。

PING コマンド (ping command). インターネット制御メッセージ・プロトコル (ICMP) エコー要求パケットをゲートウェイ、ルーター、またはホストに送信し、その応答を待つコマンド。

ポイント・ポイント・プロトコル (PPP) (Point-to-Point Protocol (PPP)). パケットをカプセル化し、シリアル・ポイント・ポイント・リンクを介して伝送する方法を提供するプロトコル。

ポーリング (polling). (1) 多地点接続またはポイント・ポイント接続において、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。

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、発信元ノードから着信先ノードまでのパスを形成する TG とノードを識別する、正しいシーケンスの制御ベクトルから構成される。

ルーター (router). (1) ネットワークのトラフィックの流れのパスを決めるコンピューター。パスの選択は、特定のプロトコル、最短または最善パスを識別するアルゴリズム、およびその他の基準 (メトリックやプロトコル特有の着信先アドレスなど) から得られた情報に基づいて、複数のパスから選ばれる。 (2) 参照モデル・ネットワーク・レイヤーにおいて、類似または異なる体系を使用する 2 つの LAN セグメントを接続する装置。 (3) OSI 用語では、エンティティーに到達できるパスを判別する機能。 (4) TCP/IP では、*ゲートウェイ (gateway)* と同義。 (5) *ブリッジ (bridge)* と対比。

ルーティング (routing). (1) メッセージを着側に到達させるためのパスを割り当てること。 (2) SNA において、メッセージ単位で運ばれるパラメーター (伝送ヘッダー内の着信先ネットワーク・アドレスなど) によって決められた、ネットワークの特定パスを通ってメッセージ単位を転送すること。

ルーティング・ドメイン (routing domain). インターネット通信において、ルーティング・プロトコルを使用してネットワーク全体の表示が各中間システム内で同一に

なるようにしている、中間システムのグループ。ルーティング・ドメインは、外部リンクによって相互に接続されている。

ルーティング情報プロトコル (RIP) (Routing Information Protocol (RIP)). インターネット・プロトコルにおいて、領域間のルーティング情報を交換し、インターネット・ホスト間の最適ルートを決めるために使用される、内部ゲートウェイ・プロトコル。 RIP は、リンク伝送速度ではなく、ルート・メトリックに基づいて最適ルートを決める。

ルーティング・ループ (routing loop). コンバージェンスが起こるまで、あるいは関係のネットワークが到達不能とみなされるまで、ルーターが相互間で情報を循環するときに発生する状態。

ルーティング・プロトコル (routing protocol). ルーターが他のルーターを見付け、到達可能なネットワークに達する最善ルートに関する情報を最新に保つために使用される技法。

ルーティング・テーブル (routing table). データグラムを転送したり、接続を確立するために使用されるルートの集まり。この情報は、ネットワーク・トポロジーと着側への到達可能性を識別するために、ルーター間で受け渡される。

ルーティング・テーブル保守プロトコル (RTMP) (Routing Table Maintenance Protocol (RTMP)). AppleTalk ネットワークにおいて、AppleTalk ルーティング・テーブルを用いて、トランスポート・レイヤーでルーティング情報を生成し、保守する機能を提供するプロトコル。 AppleTalk ルーティング・テーブルは、インターネットを通して、発信元ソケットから着信先ソケットにパケットを伝送する。

ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP)). ルーティング・データベースを維持しているバーチャル・ネットワーキング・システム (VIrtual NEtworking System (VINES)) プロトコルで、VINES ノード間でのルーティング情報の交換を可能にする。*インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP))* も参照。

rsh. ログイン・ステップを完全に飛ばして、リモート UNIX 機械上のコマンド解釈プログラムを呼び出し、そのコマンド解釈プログラムにコマンド行引き数を渡す、rlogin コマンドの変数。

S

SAP. サービス・アクセス・ポイント (service access point) を参照。

シード・ルーター (seed router). AppleTalk ネットワークにおいて、ネットワーク構成データ (たとえば、ネットワーク範囲の数やゾーン・リスト) を維持するルーター。各ネットワークには、少なくとも 1 つのシード・ルーターがある。シード・ルーターは、構成ツールを使用して、最初に設定する必要がある。*非シード・ルーター (nonseed router)* と対比。

セグメント (segment). (1) コンポーネント間または装置の相互間のケーブル区間。セグメントは、1 本のパッチ・ケーブル、相互接続された複数のパッチ・ケーブル、または相互接続された建物ケーブルとパッチ・ケーブルの組み合わせから成る。 (2) インターネット通信において、異なる機械にある TCP 機能の間の転送単位。各セグメントには、制御フィールドとデータ・フィールドが入っており、現在のバイト・ストリーム位置、実際のデータ・バイト、および受信データを妥当性検査するためのチェックサムが付加されている。

分割 (segmenting). OSI において、サポートするレイヤーからの 1 つのプロトコル・データ単位 (PDU) を複数の PDU にマップするためにレイヤーが実行する機能。

シーケンス番号 (sequence number). 通信において、伝送の流れやデータの受信を制御するために、フレームまたはパケットに割り当てられる番号。

シリアル・ライン・インターネット・プロトコル (Serial Line Internet Protocol) (SLIP). シリアル・ライン (たとえば、シリアル・ケーブルまたは電話回線を介したモデムへの RS232 接続) を介した 2 つの IP ホスト間のポイント・ポイント接続上で使用されるプロトコル。

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。

SNA 管理サービス (SNA/MS) (SNA management services (SNA/MS)). SNA ネットワークの管理を援助するために提供されるサービス。

ソケット (socket). (1) 処理間またはアプリケーション・プログラム間の通信のエンドポイント。 (2) カリフォルニア大学の Berkeley ソフトウェア配布 (一般には、 Berkeley UNIX または BSD UNIX と呼ばれる) によって提供される抽象概念で、プロセスまたはアプリケーション間の通信のエンドポイントとして働く。

ソース・ルート・ブリッジング (source route bridging). LAN において、フレームの IEEE 802.5 媒体アクセス制御 (MAC) ヘッダー内のルーティング情報を使用して、フレームが送信する必要があるリングまたはトークンリング・セグメントを判別するブリッジング方式。ルーティング情報は、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、送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・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。

トークン (token). (1) ローカル・エリア・ネットワークにおいて、あるデータ装置が一時的に伝送媒体を制御していることを示すために、そのデータ装置から別のデータ装置に連続的に渡される許可信号。各データ装置には、媒体を制御するためにトークンを獲得して使用する機会が与えられる。トークンというのは、伝送許可を示す特別のメッセージまたはビット・パターンである。 (T) (2) LAN において、伝送媒体上を、ある装置から別の装置に渡される一連のビット。トークンにデータが付加されるとフレームになる。

トークンリング (token ring). (1) IEEE 802.5 では、媒体に接続されたステーション間でトークン (特殊なパケットまたはフレーム) を渡すことによって媒体アクセスを制御するネットワーク技術。 (2) ある接続リング・ステーション (ノード) から別のノードにトークンを渡すリング・トポロジーを持つ、FDDI または IEEE 802.5 ネットワーク。 (3) *ローカル・エリア・ネットワーク (LAN) (local area network (LAN))* も参照。

トークンリング・ネットワーク (token-ring network). (1) トークン・パッシング手順により、データ・ステーション間で単方向のデータ伝送を行い、伝送されたデータが送信元ステーションに戻ってくる構造の環状ネットワーク。 (T) (2) ノードからノードへ順にトークンを渡すリング・トポロジーを使用するネットワーク。送信の準備ができているノードは、トークンを取り込み、伝送するデータを挿入することができる。

トポロジー (topology). 通信において、ネットワーク・ノード内のノードの物理的または論理的な配置。特に、ノードとそれを結ぶリンクの関係を表す。

トポロジー・データベース更新 (TDU) (topology database update (TDU)). ネットワーク・トポロジー・データベースを維持するために、APPN ネットワーク・ノード間に同報通信され、各ネットワーク・ノードに完全に複写される、新規または変更されたリンクまたはノードに関するメッセージ。 TDU には、以下のものを識別する情報が入っている。

- 送信元ノード
- ネットワークの各種資源のノード特性およびリンク特性
- 記述されている各資源の最新の更新のシーケンス番号

トレース (trace). (1) コンピューター・プログラムの実行の記録。命令が実行された順序を表す。 (A) (2) データ・リンクの場合は、送信または受信されたフレームとバイトの記録。

トランシーバー (送受信装置) (transceiver (transmitter-receiver)). LAN において、ホスト・インターフェースをイーサネットのようなローカル・エリア・ネットワークに接続する物理装置。イーサネット・トランシーバーには、ケーブルに信号を送って衝突を検出する電子機器が内蔵されている。

伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP)). インターネット、およびインターネットワーク・プロトコルに関する米国国防総省の規格に準拠するその他のすべての通信ネットワークで使用されている通信プロトコル。 TCP は、パケット交換通網のホストとそのネットワークの相互接続システムのホストとの間に、高信頼性ホスト間プロトコルを提供する。基礎となるプロトコルとして、インターネット・プロトコル (IP) を使用している。

伝送制御プロトコル/インターネット・プロトコル (TCP/IP) (Transmission Control Protocol/Internet Protocol (TCP/IP)). ローカル・エリア・ネットワークと広域ネットワーク・ノードの両方で、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呼のエコー制御装置を使用禁止にする手順を含めた、一般交換電話ネットワークの自動応答装置および並列自動発呼装置を定義する CCITT の仕様。

V.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。

バージョン (version). 通常は重要な新しいコードまたは新しい機能を含む、別個のライセンス・プログラム。

VINES. バーチャル・ネットワーキング・システム (VIrtual NEtworking System)。

バーチャル・サーキット (virtual circuit). (1) パケット交換で、実際の接続箇所をユーザーに見えるようにする、ネットワークによって提供される機能。 (T) *データ回線 (data circuit)* も参照。*物理回線 (physical circuit)* と対比。 (2) 2 台の DTE 間に確立された論理接続。

バーチャル・コネクション (virtual connection). フレーム・リレーにおいて、ポテンシャル接続の戻りパス。

バーチャル・リンク (virtual link). 最短パス最優先オープン (OSPF) において、非バックボーン中継エリアによって分離されたボーダー・ルーターに接続する、ポイント・ポイント・インターフェース。エリア・ルーターは OSPF バックボーンの一部なので、バーチャル・リンクはバックボーンに接続する。バーチャル・リンクは、OSPF バックボーンが不連続にならないようにする。

バーチャル・ネットワーキング・システム (VINES) (VIrtual NEtworking System (VINES)). Banyan Systems, Inc. からのネットワーク運用システムとネットワーク・ソフトウェア。VINES ネットワークにおけるバーチャル・リンクでは、たとえ実際には数百マイル離れていても、すべての装置およびサービスが相互に直接接続されているように見える。 *StreetTalk* も参照。

バーチャル・ルート (VR) (virtual route (VR)). (1) SNA において、次のような論理接続。(a) 特定の明示ルートとして物理的に実現されている 2 つのサブエリア・ノード間の論理接続。または (b) ノード内のセッション用のサブエリア・ノード内に完全に収まっている論理接続。別個のサブエリア・ノードの間のバーチャル・ルートは、使用する明示ルートに伝送優先順位を定め、バーチャル・ルート・ペーシングよってフロー制御を行い、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］

［ヤ行］

［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

SD88-6064-00

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

アクセス・インテグレーター・
サービス

AIS V3.2 プロトコル構成 解説書 第 1 巻