Nways
マルチプロトコル・アクセス・サービス

フィーチャーの使用と構成
バージョン 3.4

SD88-6112-02
(英文原典：SC30-3993-02)

Nways
マルチプロトコル・アクセス・サービス

フィーチャーの使用と構成
バージョン 3.4

SD88-6112-02
(英文原典：SC30-3993-02)

お願い

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

本書は、IBM Nways マルチプロトコル・アクセス・サービスのバージョン 3 リリース 4 に適用されます。また、改訂版や TNL で特に指示がない限り、以降のリリースや修正レベルにも適用されます。

本マニュアルについてご意見やご感想がありましたら

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

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

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

をご覧ください。（URL は、変更になる場合があります）

原　典： SC30–3993–02
Nways Multiprotocol Access Services
Using and Configuring Features Version 3.4

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2000.1

目次

図

表

特記事項

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

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

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

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

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

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

商標

次の用語は、IBM Corporation の米国およびその他の国における商標です。

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

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

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

NetView は、Tivoli Systems, Inc. の米国およびその他の国における商標です。

Java およびすべての Java ベースの商標とロゴは、Sun Microsystems, Inc. の米国またはその他の国、あるいは両方における商標です。

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

まえがき

本書には、ルーター・ユーザー・インターフェースを使用して Nways 装置 に導入されたフィーチャーを構成および操作するのに必要な情報が記載されています。本書で説明しているフィーチャーが、どの Nways 装置でもサポートされるわけではありません。 装置特定のフィーチャーの場合は、次の個所でそのことを示しています。

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

本書は、IBM 2216 をサポートし、これを “ルーター” または “装置” と読んでいます。本書の例は、IBM 2216 の構成を表しますが、実際の出力は本書のものとは異なる場合があります。ここに示されている例は、ユーザーが装置を構成する際に表示される内容のガイドラインとして使用してください。

本書の対象読者

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

追加情報の入手

資料が印刷された後で変更が行われる場合があります。追加情報をご利用いただける場合、または資料の印刷後に変更が必要になった場合は、CD-ROM のファイル (README という名前のファイル) に変更内容を収めてあります。このファイルは、ASCII テキスト・エディターを使用してご覧ください。

ソフトウェアについて

IBM Nways マルチプロトコル・アクセス・サービスは、 IBM 2216 (ライセンス・プログラム番号 5765-C90) をサポートするソフトウェアです。このソフトウェアには、以下の構成要素が含まれています。

- 基本コード (次のものから構成されます)
  - 装置に対してブリッジング、データ・リンク・スイッチ、および SNMP エージェントの各機能を提供するコード。
  - 装置に導入されているマルチプロトコル・アクセス・サービス基本コードの構成、監視、および使用を可能にするルーター・ユーザー・インターフェース。ルーター・ユーザー・インターフェースは、サービス・ポートに接続される ASCII 端末またはエミュレーターを介してローカルでアクセスすることも、Telnet セッションまたはモデム接続装置を介してリモートからアクセスすることもできます。

  基本コードは工場で 2216 に導入済みです。

- IBM Nways マルチプロトコル・アクセス・サービス用構成プログラム (本書では、*構成プログラム*と呼んでいます)。これは、独立型ワークステーションから装置を構成することを可能にするグラフィカル・ユーザー・インターフェースです。構成プログラムにはエラー検査およびオンライン・ヘルプ情報が含まれます。

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

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

本書における表記法

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

1. コマンドの省略形は、次のように下線を引いて表示しています。

   ```
   reload
   ```

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

2. キーワードの選択項目は大括弧で囲み、or (または) という語で区切っています。たとえば、次のようになります。

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

   パラメーターの値として、キーワードの 1 つを選択してください。

3. オプションの後に続く 3 つのピリオドは、オプションの後にユーザーが追加データ (たとえば、変数) を入力することを意味します。たとえば、次のようになります。

   ```
   time host ...
   ```

   この例では、コマンドの説明として、ピリオドの位置にホストの IP アドレスを入力します。

4. コマンドの応答として表示される情報の中で、オプションのデフォルト値はそのオプションの直後にある大括弧に入れて示します。たとえば、次のようになります。

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

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

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

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

6. キーボードのキーの名前は、次のように表示します。**Enter**
7. 変数 (すなわち、ユーザーが定義するデータを表すのに使用される名前) は、イタリック体で表示します。たとえば、次のようになります。

   File Name: *filename.ext*

ライブラリーの概要

ライブラリー構造への変更: バージョン 3.2 以降、ライブラリーの構成に次のような変更が行われました。

- **機能の概説、使用、および構成** という表題の部分は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* からフィーチャーの*使用と構成* に移されました。
- DIAL 機能の使用、構成、および監視の章は、フィーチャーの*使用と構成* に移されました。

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 2216 ホーム・ページを参照してください。

http://www.networking.ibm.com/216/216prod.html

次のリストは、IBM 2216 ライブラリーの資料をタスク別に並べてあります。

計画

GA27-4105

IBM 2216 Introduction and Planning Guide

この資料は IBM 2216 と一緒に出荷されます。ここでは、インストールの準備および初期構成の実行方法について説明しています。

インストール

GA88-6314

IBM 2216 Nways マルチアクセス・コネクター 導入および初期構成の手引き

この資料は IBM 2216 と一緒に出荷されます。ここでは、IBM 2216 のインストールおよびそのインストールの検証方法について説明しています。

GX27-3988

2216 Nways Multiaccess Connector Hardware Configuration Quick Reference

この参照カードは、IBM 2216 の正しい状態を判別するのに使用されるハードウェア構成情報の入力および保管に使用されます。

診断および保守

SY27-0350

2216 Nways Multiaccess Connector Service and Maintenance Manual

この資料は IBM 2216 と一緒に出荷されます。ここでは、IBM 2216 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

以下のリストには、マルチプロトコル・アクセス・サービス をサポートする資料が示してあります。

SC30-3886

ソフトウェア使用者の手引き

この資料には、次の説明が記載されています。

- マルチプロトコル・アクセス・サービス ソフトウェアの構成、監視、および使用
- マルチプロトコル・アクセス・サービスのコマンド行ルーター・ユーザー・インターフェースを使用して、IBM 2216 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・プロトコルの構成および監視。

SD88-6112

フィーチャーの使用と構成

SC88-6697

プロトコルの構成と監視 解説書 第 1 巻

SC88-6698

プロトコルの構成と監視 解説書 第 2 巻

これらの資料は、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・インターフェースにアクセスし、これを使用して、ルーターに同梱されているルーティング・プロトコル・ソフトウェアを構成および監視する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ついての情報も含まれています。

SC88-6373

イベント・ログ・システム・メッセージの手引き

この資料には、出される可能性のあるエラー・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説明しています。

安全

SD21-0030

Caution: Safety Information--Read This First

この資料は IBM 2216 に付属しているもので、IBM 2216 の導入および保守作業に適用される注意と危険についての注意書きが収められています。

マーケティング

次の IBM Web ページは、製品情報を提供します。

`http://www.networking.ibm.com/216/216prod.html`

IBM 2216 ソフトウェア・ライブラリーの変更の要約

次のリストは、バージョン 3 リリース 4 で行われた、ソフトウェアの変更に適用されます。

- フレーム・リレーの機能強化：
  - 新しいフレーム・ハンドラー (FH) のサポート
  - 3745 制御装置をサポートする、トラフィックのバーストを処理する PU スロットル
  - 同一の物理インターフェース上でバーチャル・インターフェースを使用できる新しいインターフェース・タイプ (フレーム・リレー・サブインターフェース)
  - 無番号 IP サポート
- VPN の拡張:
  - CPE の機能強化:
    - LDAP サーバーからのポリシー情報がローカルに保管される。
    - ポリシー・クィック構成
    - ポリシー整合性検査
    - 管理ドメイン内の LDAP サーバーからポリシー情報を取り出すことができる。
    - IPSec トンネル ping
  - IP の機能強化:
    - ボイス・ルーティングの機能強化:
      - PPP (RFC 2507、2508、2509)上での IP ヘッダー圧縮
      - マルチリンク PPP 上の断片化されたデータ・パケット間の音声トラフィックのインターリーブ
      - フレーム・リレー上の断片化されたデータ・パケット間の音声トラフィックのインターリーブ
      - PPP またはフレーム・リレーのパケット圧縮のバイパスと音声トラフィックの暗号化
    - IP ループバック・アドレス

      このサポートによって、TN3270 ゲートウェイ、ネットワーク・ディスパッチャー、および IPSec の要件をサポートするため、ユーザーは特定のインターフェース上での IP アドレスを定義できます。
    - IPv6
      - ドメイン間ルーティング機能 (BGP4+) が IPv6 についてサポートされ、IPv6 ルーティングおよびアドレッシング情報をサポートし、転送に TCP6 を使用します。
      - IPv6 トラフィックは、ATM イーサネット LAN エミュレーションを介してカプセル化やトンネルを用いずにサポートされます。
    - 複数送信パス

      IP ルーティングは、4 つまでの等価静的ルートを使用して、特定のアドレスおよびマスクへの複数並列リンクをサポートします。
    - IP ルート集合
    - マルチキャストの機能強化:
      - IPv4 用のプロトコル独立マルチキャスト高密度モード (PIM-DM)。

- ネットワーク管理者は、インバウンドおよびアウトバウンドのトラフィック・フィルターを使用して、ネットワークへのおよびネットワークからの IP マルチキャスト・データのフローを制御できるようになりました。

- Not-so-stubby area (NSSA)

  OSPF は、RFC 1587 に定義されている not-so-stubby area (NSSA) をサポートし、最新のインターネット・ドラフトがサポートされます。

- ランダム早期検出 (RED)
- ディファレンシャル (差別化された) サービス・ポリシーの機能強化
- VRRP の機能強化:
  - ハードウェア MAC アドレスを、バーチャル MAC アドレスの代わりに、使用して冗長ゲートウェイを識別できます。これによって、パフォーマンスを向上できます。
  - 複数のバックアップ候補が使用可能である場合には、優先使用オプションを構成できます。
  - マスター IP ルーターを選択する場合、使用可能ルートまたはネットワーク・インターフェースなどの追加の基準を使用して非 IP 機能をサポートできます。

- WAN リルートのための Dial-on-demand 代替インターフェース
- TN3270 の拡張機能
  - LU キャッピング
  - LU プール負荷バランス
  - TN3270 セッションの Talk 5 切断
  - 追加の報告情報
  - 1 から 255 までのアドレスのサポート
- ネットワーク・ディスパッチャーの機能強化
  - ルーティング・プロトコルによるネットワーク・ディスパッチャー・クラスター・アドレスの公示
  - 新しい SSL アドバイザー
- DLSw SDLC PU1 サポート
- 同一のインターフェース上でイーサネット・タイプ II (デフォルト) と 802.3 の両方を同時にサポートするイーサネット・カプセル化サポート
- DHCP に機能強化:
  - リース情報のハード・ディスク・バックアップ
  - DHCP インターフェースの複数 IP アドレスのサポート
  - 短期リース・サポート
- RADIUS の機能強化
  - Radius スケーラビリティー
  - Login of Last Resort
- L2TP スケーラビリティー
- シン・サーバーの機能強化

  代替またはバックアップのマスター・サーバーへの接続
- サービス・ファイル検索機能強化

変更個所の表示

ハードコピーおよび PDF では、技術上の変更や追加個所には、その変更の左側の欄外に縦線 (|) を引いて示してあります。

ネットワーク・ユーティリティー

ネットワーク・ユーティリティーは、2216 の各種モデルで構成されるプロダクトです。表1 に示すように、2216 の機能の各種サブセットを提供します。

ネットワーク・ユーティリティーによってサポートされるソフトウェア・フィーチャー

ネットワーク・ユーティリティーの各モデルは、表1 に示すように、2216 のソフトウェア・フィーチャーのサブセットを提供します。 2216 モデル 400 Web サーバー・キャッシュ (WSC) は、IP プロトコルをサポートしますが、APPN フィーチャーは提供しません。

表 1. 2216 モデル 400 およびネットワーク・ユーティリティーでサポートされるコード・フィーチャー

フィーチャーまたはプロトコル	2216 モデル 400 基本で使用可能	2216 モデル 400 WSC で使用可能	ネットワーク・ユーティリティー モデル TN1 で使用可能	ネットワーク・ユーティリティー モデル TX1 で使用可能
TN3720E	Yes[1]	--	Yes[1]	--
TN3720E IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュ	Yes[1]	--	Yes[1]	--
TN3720E ホストによって開始された動的 LU 定義	Yes[1]	--	Yes[1]	--
DLSw を介した TN3720E 多重 PU SA	Yes[1]	--	Yes[1]	--
ネットワーク・ディスパッチャー	Yes	Yes	Yes	Yes
TN3720E サーバー・アドバイザー (または、ネットワーク・ディスパッチャー・アドバイザー)	Yes	Yes[2]	Yes	Yes[2]
帯域幅予約および優先待ち行列	Yes	Yes	Yes	Yes
フレーム・リレー・パケットの断片化	Yes	Yes	Yes	Yes
フレーム・リレーを介した音声パケット転送	Yes	Yes	Yes	Yes
MAC フィルター	Yes	Yes	Yes	Yes
WAN レストラル	Yes	Yes	--	--
WAN リルート	Yes	Yes	--	--
データ圧縮	Yes	Yes	Yes	Yes
コード化サブシステム	Yes	Yes	Yes	Yes
暗号化	Yes	Yes	Yes	Yes
データ・リンク交換 (DLSw)	Yes	--	Yes	Yes

表 1. 2216 モデル 400 およびネットワーク・ユーティリティーでサポートされるコード・フィーチャー (続き)

フィーチャーまたはプロトコル	2216 モデル 400 基本で使用可能	2216 モデル 400 WSC で使用可能	ネットワーク・ユーティリティー モデル TN1 で使用可能	ネットワーク・ユーティリティー モデル TX1 で使用可能
サービス品質 (QoS)	Yes	Yes	Yes	Yes
IPSec (IP セキュリティー)	Yes	Yes	Yes	Yes
ディファレンシェーテッド・サービス	Yes	Yes	Yes	Yes
L2TP	Yes	Yes	Yes	Yes
L2F	Yes	Yes	Yes	Yes
PPTP	Yes	Yes	--	--
ネットワーク・アドレス変換	Yes	Yes	Yes	Yes
AAA (認証、許可、および会計セキュリティー)	Yes	Yes	Yes	Yes
RSVP	Yes	Yes	Yes	Yes
DHCP サービス	Yes	Yes	Yes	Yes
ディレクトリー・サービス : LDAP サポート	Yes	Yes	Yes	Yes
IPv6	Yes	--	Yes	Yes
シン・サーバー	Yes	--	--	--
Web サーバー・キャッシュ	--	Yes	--	--
SDLC 1 次グループ・ポーリング	Yes	--	Yes	Yes
SDLC 双方向同時通信	Yes	--	Yes	Yes
IPX	Yes	--	--	--
Appletalk	Yes	--	--	--
DECnet IV	Yes	--	--	--
OSI	Yes	--	--	--
Banyan Vines	Yes	--	--	--
DIAL	Yes	Yes	Yes[3]	Yes[3]
APPN フィーチャー				
ブランチ・エクステンダー	Yes	--	Yes	Yes
従属 LU リクエスター (DLuR)	Yes	--	Yes	Yes
エンタープライズ・エクステンダー	Yes	--	Yes	Yes
拡張ボーダー・ノード	Yes	--	Yes	Yes
高性能ルーティング (HPR)	Yes	--	Yes	Yes
ネットワーク・ノード (NN)	Yes	--	Yes	Yes

1. これは別売りのフィーチャーです。
2. IBM ルーティング・プロダクト上の TN3270E サーバーと通信する場合
3. トンネル伝送だけにアクセス可能。トンネル伝送機能には、L2TP、PPTP、および L2F が組み込まれています。

ヘルプの入手

コマンド・プロンプトで、そのレベルで利用可能なコマンドのリストという形で、ヘルプを入手することができます。 これを行うには、**?** (**help** コマンド) を入力し、**Enter** を押します。 **?** は、現在のレベルから利用可能なコマンドのリストを入手するのに使用します。通常は、特定のコマンド名の後に **?** を入力すると、そのオプションが表示されます。

下位レベル操作環境の終了

ソフトウェアは複数レベルの構造になっているので、2216 を構成または動作するときには、2 次、3 次、およびさらに下位レベルの環境に入ります。すぐ上のレベルに戻るためには、**exit** コマンドを入力します。 2 次レベルに達するためには、2 次レベルのプロンプト (Config> または +) が得られるまで繰り返し **exit** を入力します。

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

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

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

変更の要約

第1章 帯域幅予約および優先待ち行列の使用

この章では、フレーム・リレーおよび PPP インターフェースで現在利用可能な帯域幅予約システムおよび優先待ち行列機能について説明します。この章には、次の内容が記載されています。

帯域幅予約システム

帯域幅予約システム (BRS) は、あるネットワーク接続上で需要 (トラフィック) が供給 (スループット) を超えた場合、どのパケットを廃棄するかを決めることができます。帯域幅の使用率が 100% に達した場合、BRS はユーザーの構成に基づいて、廃棄するトラフィックを判別します。

帯域幅予約は、指定されたクラスのトラフィック用として伝送帯域幅を ″予約″ します。各クラスに、接続の帯域幅の最小比率が割り振られています。 2ページの図1 および 2ページの図2 を参照してください。

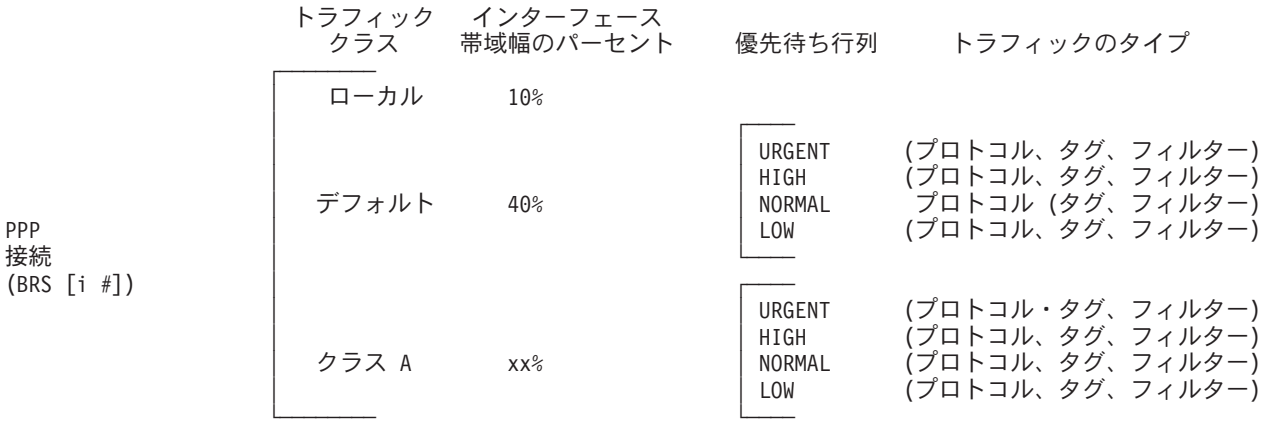
PPP インターフェースでは、トラフィック・クラス (t-class) を定義し、各トラフィック・クラスに PPP インターフェースの帯域幅の比率を割り振ります。少なくとも 2 種類のトラフィック・クラスがあります。

1. LOCAL クラス。ルーターによってローカルで発信されたパケット (たとえば、IP RIP パケット) のための帯域幅が割り振られます。
2. DEFAULT クラス。その他のすべての通信は、最初はこのクラスに割り当てられます。

ユーザーは、追加のトラフィック・クラスを作成し、トラフィック・クラス内の優先待ち行列に、プロトコル、フィルター、およびタグを割り当てることができます。 2ページの図1 を参照してください。

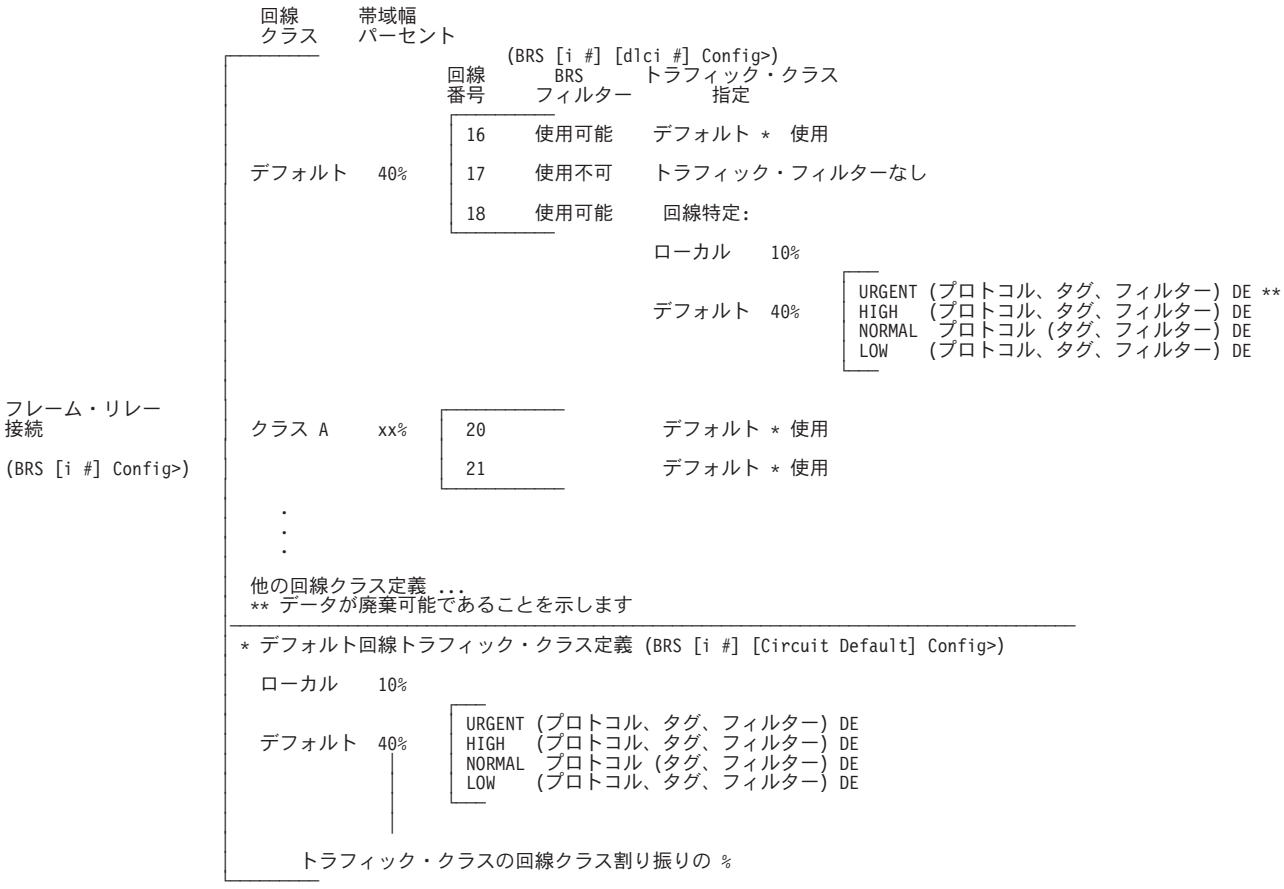
フレーム・リレー・インターフェースでは、回線クラス (c-class) を定義し、各回線クラスに、フレーム・リレー・インターフェースの帯域幅の比率を割り振ります。少なくとも 1 つの回線クラス (DEFAULT 回線クラス) が存在し、すべての回線が最初はこのクラスに割り当てられます。ユーザーは追加の回線クラスを作成し、それらの回線クラス (c-class) に回線を割り当てることができます。各フレーム・リレー回線では、トラフィック・クラス (t-class) を定義し、各トラフィック・クラスに、そのフレーム・リレーの帯域幅の比率を割り振ることができます。フレーム・リレー回線のトラフィック・クラス・サポートは、PPP インターフェースのトラフィック・クラス・サポートと同様です。フレーム・リレーの回線クラスとトラフィック・クラスの関係については、2ページの図2 を参照してください。

BRS および優先待ち行列の使用



注: すべてのプロトコルが、最初は DEFAULT トラフィック・クラスの NORMAL 優先待ち行列に割り当てられます。ユーザーは、トラフィック・クラス内の優先待ち行列に、プロトコル、フィルター、またはタグを割り当てることができます。

図 1. PPP BRS トラフィック・クラスとトラフィック・クラス優先待ち行列の関係



注: すべてのプロトコルが、最初は DEFAULT トラフィック・クラスの NORMAL 優先待ち行列に割り当てられます。ユーザーは、トラフィック・クラス内の優先待ち行列に、プロトコル、フィルター、またはタグを割り当てることができます。

図 2. フレーム・リレー BRS 回線クラスとトラフィック・クラスの関係

これらの予約される比率は、そのネットワーク接続の帯域幅の最小*配分* です。ネットワークが容量いっぱいで稼働している場合、あるクラスのメッセージは、そのクラスに割り振られた構成済み帯域幅までしか送信できません。この場合、他の帯域幅伝送が満たされるまで、追加の伝送は保留されます。トラフィック量の少ないパスの場合は、他にトラフィックがなければ、パケット・ストリームは許容最小値を最大 100% を超えるまで帯域幅を使用できます。

帯域幅予約は、実際には一種の*安全機能* です。一般的には、装置は回線速度の 100% を超える速度は使用しないようにすべきです。このような状態になる場合は、より高速の回線が必要と考えられます。ただし、トラフィックの “バースト性” により、要求された伝送速度が短時間 100% を超えてしまうことがあります。そのような場合には、帯域幅予約を使用可能にすることにより、優先順位の高いトラフィックが確実に送達される (つまり、廃棄されない) ようにすることができます。

帯域幅予約は、次の接続タイプ上で実行されます。
- フレーム・リレー (シリアル・ラインまたはダイヤル回線インターフェース)
- PPP (シリアル・ラインまたはダイヤル回線インターフェース)

フレーム・リレー上の帯域幅予約

帯域幅予約は、2 つのレベルで帯域幅を予約することができます。

- インターフェース・レベルでは、インターフェースの帯域幅の比率を回線クラス (*c-classes*) に割り当てることができます。各回線クラスには、1 つまたは複数の回線が含まれます。
- 回線レベルでは、トラフィック・クラス (*t-classes*) を定義し、回線の帯域幅の比率を割り振ることができます。 (**create-super-class** コマンドによって作成されたトラフィック・クラスは、どの帯域幅とも関連付けられませんが、常に、回線について定義されたその他すべての t-class に優先されます。)

BRS がフレーム・リレーからパケットを受信すると、構成済みの c-class および t-class を使用して、そのパケットをいつ送信するか決定されます。BRS は、c-class、回線、クラス、および t-class 内の優先順位にしたがって、そのパケットを待ち行列化します。回線が割り当てられている c-class が c-class の待ち行列に入れられると、c-class の待ち行列は明確な重み付けをもった待ち行列アルゴリズムにしたがってソートされます。c-class 内で、送信されるパケットをもつ回線は、ラウンドロビン式にサービスされます。各 c-class 内の t-class も、公正な重み付き待ち行列アルゴリズムにしたがってソートされます。 t-class 内では、パケットは、それぞれの優先順位 (urgent、high、normal、または low) に応じてさらに待ち行列化されます。

パケットは、次の基準のすべてに適合すると、待ち行列から除去されて送信されます。
1. 次の c-class 内の次のパケットである
2. c-class 内の次の回線の次のパケットである
3. その c-class の次の t-class 内のパケットの 1 つである
4. その t-class の次の優先グループ内の次のパケットである

インターフェースおよび BRS 用の 1 つまたは複数の回線を使用可能にし、c-class または t-class を構成しない場合、回線はすべて (*default*) と呼ばれる 1 つの c-class

に割り当てられます。この構成の場合、c-class の待ち行列上にはデフォルト c-class しかないので、送信用のパケットをもつ c-class 内の回線はそれぞれラウンドロビン順に処理されます。BRS にこれを行わせたい場合は、デフォルト c-class のすべての回線を残しておき、その他の回線クラスは作成しないでください。

孤立サーキットならびに BRS が明示的に使用可能になっていない回線は、あらゆる状況でこのデフォルト BRS 待ち行列化環境を使用します。BRS は、それらをデフォルト c-class に割り当てます。

BRS を構成するためには、次の順序で行います。

1. インターフェース上で BRS を使用可能にする。
2. 回線上で BRS を使用可能化し、c-class を追加する。
3. 回線を c-class に割り当てる。
4. 必要であれば、その c-class のそれぞれについて tclass を定義する。

特定インターフェースの回線クラスの予約カウンターを表示するための帯域幅予約監視コマンドがいくつかあります。

- clear-circuit-class
- counters-circuit-class
- last-circuit-class

BRS の監視について詳しくは、21ページの『第2章 帯域幅予約の構成と監視』を参照してください。

インターフェースは、帯域幅監視コマンド用のプロンプトに表示されるものです。たとえば、`BRS [i 5]` は、インターフェース 5 のプロンプトです。

待ち行列化のサポート

フレーム・リレー上の帯域幅予約を使用すると、インターフェースおよび回線の帯域幅予約が使用可能にされていない場合でも、各回線は輻輳 (ふくそう) 状態のときにフレームを待ち行列化することができます。

廃棄可能性

フレーム・リレー・ネットワークは、PVC 上の CIR を超えた転送データを廃棄することがあります。ルーターは、DE ビットをセットすることにより、一部のトラフィックを廃棄可能と見なすように指示することができます。該当する場合、フレーム・リレー・ネットワークは廃棄可能としてマーク付けされたフレームを廃棄します。これによって、廃棄可能のマークが付いていないフレームがネットワークを通過できるようになることがあります。ユーザーは、プロトコル、フィルター、またはトラフィック・クラスへのタグを割り当てるときに、そのプロトコル、フィルター、またはタグ・トラフィックが廃棄可能かどうかを指定することができます。トラフィックを廃棄可能として構成する方法については、28ページの『Assign』を参照してください。音声トラフィック (プロトコル VOFR によって識別される) は、必ず、**非**廃棄可能として構成する必要があります。

トラフィック・クラス処理のためのデフォルト回線定義

フレーム・リレー・インターフェースには、多数の回線を定義することができます。BRS では、各回線のトラフィック・クラス定義を完全に構成する必要はなく、

デフォルトの 1 組のトラフィック・クラスとプロトコル、フィルター、およびタグ割り当てを定義し (デフォルト回線定義と呼ばれます)、インターフェース上の任意の回線がこれを使用できるようにします。回線上で BRS を初期に使用可能にすると、回線はデフォルト回線定義を使用するように初期設定されます。回線がトラフィック・クラスの扱いに関するデフォルト回線定義を使用できない場合には、**add-class**、**change-class**、**assign**、**deassign**、**tag**、および **untag** コマンドを使用して、その回線に特定した定義を作成することができます。

回線が回線特定の定義を使用しているときに、それに代えてデフォルト回線定義を使用するように設定したい場合は、その回線の BRS プロンプトで **use-circuit-defaults** コマンドを使用することができます。

トラフィック・クラスの扱いに関するデフォルト回線定義は、BRS フレーム・リレー・インターフェース・プロンプトで **set-circuit-defaults** を使用して定義します。このコマンドは BRS 回線デフォルト・プロンプトを表示します。そこから、トラフィック・クラスの追加、変更、および削除、プロトコル、フィルター、およびタグの割り当てと割り当て解除、ならびに BRS タグの作成を行うことができます。トラフィック・クラスのデフォルト回線定義を変更すると、デフォルト回線定義を使用しているすべての回線のトラフィック・クラスの扱いが動的に更新されます。

フレーム・リレーを介した音声用の BRS の構成

音声フレームは、専用回線を介して転送できます。この状態では、インターフェース上および回線上で BRS を使用可能にして、音声と関連付けられた回線についてデフォルトを受け入れます。 c-class を複数個作成し、音声専用の回線を、高位の帯域幅比率と関連付けられた c-class に割り当て、データと関連付けられた回線を、低位の帯域幅パーセントと関連付けられた回線クラスに割り当てなければならない場合があります。

音声およびその他のトラフィックの両方が同じ回線を介して転送される場合には、インターフェースおよび回線上で BRS を使用可能にしてください。1 つまたは複数の回線を優先するのではなく、すべての回線をラウンドロビン式にサービスを受けさせたい場合には、デフォルト c-class のほかに追加の c-class を作成しないことを決める必要があります。その場合には、音声とデータの両方が転送される各回線について、**create-super-class** コマンドを使用して t-class を作成し、VOFR トラフィックをこのクラスに割り当ててください。必要に応じて追加の t-class も作成し、これらの t-class に他のタイプのトラフィックを割り当てます。この構成は、音声トラフィックが他のすべてのトラフィックに対して必ず優先されるようにして、断片化が使用可能であればセグメント化されていない音声フレームは、断片化されていたデータ・セグメント間に割り込みを入れることができるようにするのに役立ちます。同じインターフェースで音声とデータを送信しようとする場合は、フレーム・リレー・インターフェースで断片化を使用可能にしてください。断片化により、フレームがさらに小さくなるので、連続する音声フレーム間の遅延が短くなります。

断片化の使用可能化について詳しくは、*Nways マルチプロトコル・アクセス・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” の章に記載されている **enable fragmentation** コマンド を参照してください。

優先待ち行列

帯域幅予約は、指定されたトラフィック・クラス (*t-classes*) に対して、接続の総帯域幅の比率を割り振ります。他のすべての t-class に優先される、**create-super-class**pubs コマンドによって作成された t-class の場合を除き、BRS t-class は帯域幅比率と関連付けられます。プロトコルおよびフィルター・データを、t-class および t-class 内の特定の優先待ち行列に割り当てることができます。優先待ち行列を使用すると、プロトコルおよびフィルターを、設定値をもつトラフィック・クラス内の特定の待ち行列に割り当てることができます。BRS t-class は、同じ名前によって識別されたパケットの集りです。たとえば、“ipx” という名前のクラスは、すべての IPX パケットを表します。

優先待ち行列を用いて、各帯域幅 t-class に以下の優先順位の設定値の 1 つを割り当てることができます。

- Urgent
- High
- Normal (通常: デフォルト設定)
- Low

この割り当ては、ユーザーによって定義された、指定されたトラフィック・クラスまたは t-class に対して行われます。

各帯域幅 t-class の各優先順位ごとに、待ち行列で待っているパケットの数を設定することもできます。BRS **queue-length** コマンドは、各 BRS 優先待ち行列に待ち行列化できる出力バッファーの最大数、およびルーターの入力バッファーが不足しているときに各 BRS 優先待ち行列に待ち行列化できる出力バッファーの最大数を設定します。PPP とフレーム・リレーの両方の優先待ち行列の長さを設定できます。

重要: 待ち行列の長さの値を高く設定し過ぎると、ルーターの性能が大きく低下する可能性があります。

BRS の場合、PPP およびフレーム・リレー WAN 接続の優先待ち行列の長さを設定することができます。**queue-length** コマンドの説明は、41ページの『Queue-length』 を参照してください。

ある帯域幅 t-class の優先順位の設定値は、他の帯域幅クラスでは無効です。ある帯域幅クラスが他の帯域幅クラスより優先されるということはありません。

帯域幅予約なしの優先待ち行列

帯域幅予約なしで優先待ち行列が構成されている場合、最高の優先順位のトラフィックが最初に送達されます。高優先順位のトラフィックが大量にある場合には、低い優先順位のトラフィックは見過ごされる可能性がありますが、優先待ち行列と帯域幅予約を組み合わせれば、パケット転送をすべてのタイプのトラフィックに割り振ることができます。

トラフィック・クラスの構成

add-class コマンドを使用してトラフィック・クラスを作成し、次に **assign** コマンドを使用して、そのクラスにトラフィックのタイプを割り当てます。トラフィッ

クは、そのプロトコル・タイプ に基づいて、あるいは特定のタイプのプロトコル・トラフィック を識別する (たとえば、SNMP IP パケット) フィルターに基づいて、トラフィック・クラスに割り当てられます。

サポートされるプロトコル・タイプは、次のとおりです。
- IP
- ARP
- DNA
- VINES
- IPX
- OSI
- VOFR
- AP2
- ASRT
- SNA/APPN-ISR
- APPN-HPR®
- HPR/IP

BRS フィルター

帯域幅予約を使用すると、特定のプロトコル・トラフィックを、同じプロトコル・タイプを使用する他のトラフィックとは異なる扱いにすることができます。たとえば、SNMP IP トラフィックを、他の IP トラフィックとは異なるトラフィック・クラスおよび優先順位に割り当てるといったことが可能です。この例では、特定のプロトコル・トラフィックをフィルターに掛ける (つまり、固有に識別する) ので、SNMP は BRS フィルターです。IP、ASRT (ブリッジング)、および APPN-HPR プロトコル・トラフィックを帯域幅予約によってフィルターに掛けることが可能です。サポートされるフィルターは、次のとおりです。
- IP トンネル伝送
- IP 経由の SDLC トンネル伝送 (SDLC リレー)
- IP 経由の BSC トンネル伝送 (BSC リレー)
- Rlogin
- Telnet
- SNA/APPN-ISR
- APPN-HPR
- SNMP
- IP マルチキャスト
- DLSw
- MAC フィルター
- NetBIOS
- Network-HPR
- High-HPR
- Medium-HPR
- Low-HPR
- XTP
- TCP/UDP ポート番号またはソケット
- TOS バイト
- 優先順位ビット

BRS とフィルター

ここでは、BRS を各種のフィルターと一緒に使用する方法について説明します。

MAC アドレス・フィルターとタグ

MAC Address フィルターは、タグ を使用して、帯域幅予約と MACフィルター (MCF) の共同作業で処理されます。たとえば、帯域幅予約を使用しているユーザーは、ブリッジ・トラフィックにタグを割り当てることによって、それを分類することができます。

タグ付けプロセスは、MAC フィルター構成コンソールでフィルター項目を作成し、それにタグ番号を割り当てることによって行われます。このタグ番号は、このタグに対応するすべてのパケットのトラフィック・クラスを設定するのに使用されます。タグ値は、現在は 1 〜 64 の範囲でなければなりません。MAC フィルターについて詳しくは、51ページの『第3章 MAC フィルターの使用』を参照してください。

注: タグは、ブリッジされるパケットに***だけ*** 適用されます。PPP またはフレーム・リレー接続では、最高 5 つのタグ付けされた MAC フィルターを帯域幅予約フィルターとして割り当てることができ、それらを TAG1 〜 TAG5 として指定します。TAG1 が最初に検索され、次に TAG2 というようにして TAG5 まで続けられます。1 つの MAC フィルター・タグは、MCF に設定された任意の数の MAC アドレスから構成することができます。

MAC フィルター構成プロセスでタグ・フィルターを作成したら、BRS タグ構成コマンドを使用して、BRS タグ名 (TAG1、TAG2、TAG3、TAG4、または TAG5) を MAC フィルター・タグ番号に割り当てることができます。次に、BRS assign コマンドでその BRS タグ名を使用して、対応する MAC フィルターを帯域幅トラフィック・クラスと優先順位に割り当てます。

タグは、IP トンネルの例に見られるように、“グループ” とも呼ばれます。IP トンネルのエンドポイントは、任意の数のグループに属することができます。パケットは、MAC アドレス・フィルターのタグ付けフィーチャーによって、特定のグループに割り当てられます。MAC フィルターについての追加情報は、51ページの『第3章 MAC フィルターの使用』および 55ページの『第4章 MAC フィルターの構成と監視』を参照してください。

帯域幅予約と待ち行列優先順位をタグ付きパケットに適用するには、次のようにします。

1. `filter config>` プロンプトで MAC フィルター構成コマンドを使用して、ブリッジを通過するパケットのタグを設定する。詳しくは、51ページの『第3章 MAC フィルターの使用』を参照してください。
2. 帯域幅予約 **tag** コマンドを使用して、帯域幅予約のタグを参照する。
3. 帯域幅予約 **assign** コマンドを使用して、BRS タグを t-class に割り当てる。**assign** コマンドは、その BRS t-class 内の待ち行列優先順位も指定するように求めるプロンプトを出します。

TCP/UDP ポート番号フィルター

パケットの UDP または TCP ポート番号と (オプションで) ソケットに基づいて、一定範囲の TCP または UDP ポートからの TCP/IP パケットを、BRS t-class と優先順位に割り当てることができます。最高 5 つの UDP/TCP ポート番号フィルターを指定することができます。フィルターに、個々の TCP または UDP ポート番号、一定範囲の TCP または UDP ポート番号、あるいはソケット識別子 (ポート番号と IP アドレスの組み合わせ) を指定します。そのフィルターを、BRS トラフィック・クラスとそのクラス内の優先順位に割り当てることができます。

UDP/TCP ポート・フィルターが使用可能のとき、BRS は各 TCP または UDP パケットを調べて、宛先または発信元ポート番号が、フィルターに指定したポート番号の 1 つに一致しているかどうかをチェックします。ユーザーが IP アドレスを BRS UDP/TCP フィルターの一部として定義しており、宛先または発信元 IP アドレスが、ユーザーの定義したフィルター・アドレスと一致している場合にも、BRS はパケットを、そのポート番号フィルターのトラフィック・クラスと優先順位に割り当てます。

たとえば、ポート番号フィルターを 25 ～ 29 の範囲の UDP ポート番号に構成し、そのフィルターをトラフィック・クラス 'A' の優先順位 'normal' に割り当てるといったことができます。この場合、BRS は、発信元または宛先ポート番号が 25 ～ 29 のすべての UDP パケットを、トラフィック・クラス 'A' の Normal 優先順位待ち行列に入れます。

TCP ポート番号フィルターを IP アドレス 5.5.5.25 の TCP ポート番号に構成し、そのフィルターをトラフィック・クラス 'B' の優先順位 'urgent' に割り当てるといったこともできます。この場合、BRS は、発信元または宛先ポート番号が 50 で、宛先または発信元 IP アドレスが 5.5.5.25 のすべての TCP パケットを、トラフィック・クラス 'B' の Urgent 優先待ち行列に入れます。

IPv4 TOS ビット・フィルター

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

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

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

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

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

IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィック用の IP バージョン 4 優先順位ビット処理の使用

BRS は通常、ポート番号によって IP TCP トラフィックと UDP トラフィックを区別します。しかし、BRS は、IP 保護トンネルを通して伝送されたり、2 次 UDP または TCP フラグメントに入れて伝送される IP トラフィックのように、2 度カプセル化されたトラフィックのポートは識別することができません。BRS が IP 保護トンネル伝送パケットや TCP および UDP 2 次フラグメント・パケットをフィルター処理できるようにするために、IP バージョン 4 優先順位ビット処理が BRS に追加されました。

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

APPN/HPR トラフィックが IP を介してルートされるときに、APPN-HPR の各伝送優先順位 (network、high、medium、および low) が、3 つの IP バージョン 4 優先順位ビットの特定の値にマップされます。

- HPR Network 伝送優先順位は、IPv4 優先順位値 '110'b にマップされます。
- HPR high 伝送優先順位は、IPv4 優先順位値 '100'b にマップされます。
- HPR medium 伝送優先順位は、IPv4 優先順位値 '010'b にマップされます。
- HPR low 伝送優先順位は、IPv4 優先順位値 '001'b にマップされます。

BRS に対して IPv4 優先順位フィルターが使用可能にされており、IP パケット内の優先順位ビットが APPN/HPR トラフィックに使用される値の 1 つに一致している場合、そのパケットは、対応する HPR 伝送優先順位が割り当てられている BRS t-class の優先順位待ち行列に入れられます。たとえば、IP パケットの優先順位値が '110'b で、BRS HPR-Network フィルターが t-class A、優先順位レベルが normal に割り当てられている場合、パケットは t-class A の normal 優先順位待ち行列に入れられます。BRS HPR 伝送優先順位フィルターは構成されていないが、APPN-HPR

フィルターは構成されている場合には、パケットは APPN-HPR フィルターが割り当てられている優先順位待ち行列と t-class に入れられます。

次の 3 種類のトラフィックは、IPv4 優先順位値 '011'b にマップされます。
- APPN/HPR が IP を介してルート指定されるときに送信される APPN/HPR XID トラフィック
- DLSw トラフィック
- TN3270 トラフィック

複数のタイプのトラフィックが 1 つの値にマップされるので、IPv4 優先順位ビットに基づくフィルターが使用可能にされている場合には、BRS はトラフィックを区別することができません。そのため、優先順位値 '011'b を持つ IP パケットを検出すると、BRS は次の順序で BRS フィルターを評価して、フィルターが使用可能にされているかどうかを調べます。構成されている BRS フィルターが見つかると、パケットはその BRS フィルターが割り当てられている優先順位待ち行列と t-class に入れられます。
- SNA/APPN-ISR (APPN/HPR XID 交換に使用される)
- DLSw
- Telnet

パケットが BRS によってフィルター処理される優先順位値の 1 つを持っているが、適用できる BRS フィルター・タイプが構成されていない場合、パケットは IP プロトコルが割り当てられている優先順位待ち行列と BRS t-class に入れられます。

TN3270 トラフィックが、クライアントによって、BRS が使用可能な広域ネットワークを介して 2216 に送信される場合、クライアントが優先順位ビットを '011'b に設定していない限り、BRS はクライアントからのトラフィックに優先順位を付けることはできません。

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

1. BRS では、BRS が IPv4 優先順位ビットに基づいてフィルター処理する必要があるかどうかを構成します。BRS は、IP 保護トンネル伝送パケット、または TCP および UDP 2 次フラグメント・パケットに対してだけ、このタイプのフィルター処理を実行します。
2. DLSw、IP 経由 HPR、および TN3270 を構成する場合、これらのプロトコル・タイプのそれぞれについて、2216 が発信するパケットに対して IPv4 優先順位ビットを設定する必要があるかどうかを指定します。

IPv4 優先順位ビット・フィルター処理を使用するためには、次のステップを実行します。

1. BRS で IPv4 優先順位フィルターをアクティブにする。
2. 各種のカテゴリーの SNA トラフィックに対して BRS t-classes を構成し、プロトコルとフィルターを割り当てる。これは、IP 保護トンネルを通して伝送されない、あるいはフラグメント化されない SNA トラフィックの場合と同様の方法で行います。
3. DLSw、IP 経由 HPR、および TN3270 プロトコルを構成するときに、IPv4 優先順位ビットの設定を使用可能にする。

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

ブリッジ・トラフィックの SNA および APPN フィルター

SNA/APPN-ISR フィルターは、ブリッジされる SNA および APPN-ISR トラフィックを、BRS トラフィック・クラスに割り当てることができます。SNA および APPN-ISR トラフィックは、宛先または発信元 SAP が 0x04、0x08、または 0x0C で、その LLC (802.2) 制御フィールドが非番号制情報 (UI) フレームでないことを示しているブリッジ・パケットとして識別されます。

注: フレーム・リレー BAN パケットが、このカテゴリーに入ります。

APPN-HPR フィルターは、ブリッジされる HPR トラフィックを BRS t-class に割り当てることができます。HPR トラフィックは、宛先または発信元 SAP が X'04'、X'08'、X'0C' 、または X'C8' で、その LLC (802.2) 制御フィールドが非番号制情報 (UI) フレームであることを示してブリッジ・パケットとして識別されます。

Network-HPR、High-HPR、Medium-HPR、および Low-HPR フィルターは、さらに HPR ブリッジ・パケットを HPR 伝送優先順位に従ってフィルターに掛けるすることができます。たとえば、Network 伝送優先順位を持つ HPR トラフィックをある t-class と優先順位に割り当て、その他のすべての HPR ブリッジ・トラフィックを異なる t-class または優先順位に割り当てたい場合、Network-HPR フィルターを該当する t-class と優先順位に割り当て、その APPN-HPR フィルターを使用して、残りの HPR トラフィックを異なる t-class または優先順位に割り当てることができます。

IP を介してルーティングされる APPN-HPR トラフィックは、network、high、medium、および low HPR 伝送優先順位に割り当てられた UDP ポート番号を使用してフィルターに掛けられます。 XID 交換には、追加の UDP ポート番号が使用されます。IP を介する APPN-HPR をサポートするのに使用される UDP ポート番号はすべて構成可能です。

IP ネットワークの中間ルーターで APPN が使用可能にされていない場合は、`BRS Config>` コマンド・プロンプトから、IP 経由 HPR 用の UDP ポート番号を構成することができます。装置で APPN が使用可能にされている場合には、BRS は `APPN Config>` コマンド・プロンプトで構成された値を使用します。

その他のフィルターも、トラフィックを割り当てるのに役立つ場合があります。たとえば、DLSw フィルターは、TCP 接続を介して送信される SNA-DLSw トラフィックを BRS t-class に割り当てることができます。

SNA/APPN-ISR および APPN-HPR フィルターは、上記以外の SAP をチェックしたい場合に、MAC フィルターを使用してスライディング・ウィンドウ・フィルターを作成し、そのフィルターにタグを付けます。次に、タグ付けされた MAC フィルターを BRS t-class に割り当てます。

フィルターの優先順位

1 つのパケットが複数の BRS フィルター・タイプに一致することもあり得ます。たとえば、SNA が入っている IP トンネル伝送ブリッジ・パケットは、IP トンネル

伝送フィルターと SNA/APPN-ISR フィルターに一致する可能性があります。パケットが BRS フィルター・タイプに一致するかどうかを判別するときのフィルターの評価順序は、次のとおりです。

1. TOS フィルター (IP)
2. IPv4 優先順位処理
3. ブリッジ・パケットの MAC フィルター・タグの一致 (IP/ASRT)
4. ブリッジングの NetBIOS (IP/ASRT)
5. ブリッジングの SNA/APPN-ISR (IP/ASRT)
6. HPR-Network (IP/ASRT/APPN-HPR)
7. HPR-High (IP/ASRT/APPN-HPR)
8. HPR-Medium (IP/ASRT/APPN-HPR)
9. HPR-Low (IP/ASRT/APPN-HPR)
10. APPN-HPR (IP/ASRT)
11. UDP/TCP ポート番号フィルター (IP)
12. IP トンネル伝送 (IP)
13. SDLC/BSC リレー (IP)
14. DLSw (IP)
15. マルチキャスト (IP)
16. SNMP (IP)
17. Rlogin (IP)
18. Telnet (IP)
19. XTP (IP)

注: 括弧内は、フィルターが適用されるプロトコルです。

サンプル構成

フレーム・リレー回線のトラフィック・クラス処理にデフォルト回線定義を使用する場合

注:

1 フィーチャー BRS を構成します。

2 インターフェース 1 の BRS を使用可能にします。

3 回線 16、17、18 の BRS を使用可能にします。これらの回線では、トラフィック・クラス処理のデフォルト回線定義が使用されます。

4 トラフィック・クラス処理のデフォルト回線定義を定義するために set-circuit-defaults メニューにアクセスします。

5 トラフィック・クラスを追加し、そのトラフィック・クラスにプロトコルとフィルターを割り当てます。

6 回線 16 の BRS 定義をリストおよび表示します。回線 16 はデフォルト回線定義を使用しているので、デフォルト回線定義で定義されたトラフィック・クラスと、プロトコルおよびフィルター割り当てが表示されます。

7 固有のクラス CIRC171 を作成して、回線 17 がトラフィック・クラス処理にデフォルト回線定義ではなく、回線特定の定義を使用するように変更します。このクラスに、プロトコル、フィルター、またはタグを割り当てることができます。

8 デフォルト回線定義を変更して DEF1 および DEF2 トラフィック・クラスがそれぞれ帯域幅の 10% を予約するようにし、これらの変更が、回線 16 には反映されているが、回線 17 には反映されていない (回線 17 は現在、回線特定の定義を使用しているので) ことを表示します。

9 回線 17 がトラフィック・クラス処理に回線特定の定義ではなく、デフォルト回線定義を使用するように変更します。

```
t 6
 Gateway user configuration
 Config>feature brs      1
 Bandwidth Reservation User Configuration
 BRS Config>interface 1     2
 BRS [i 1]Config>enable
 Please reload router for this command to take effect.
 BRS [i 1] Config>circuit 16    3
 BRS [i 1][dlci 16] Config>enable
 Defaults are in effect for this circuit.
 Please reload router for this command to take effect.
 BRS [i 1][dlci 16] Config>exit
 BRS [i 1]Config>circuit 17
 BRS [i 1][dlci 17] Config>enable
 Defaults are in effect for this circuit.
 Please reload router for this command to take effect.
 BRS [i 1][dlci 17] Config>exit
 BRS [i 1]Config>circuit 18
 BRS [i 1][dlci 18] Config>enable
 Defaults are in effect for this circuit.
 Please reload router for this command to take effect.
 BRS [i 1][dlci 18] Config>
 *reload
 Are you sure you want to reload the gateway? (Yes or [No]): yes



 *t 6
 Gateway user configuration
 Config>feature brs
 Bandwidth Reservation User Configuration
 BRS Config>interface 1
 BRS[i 1] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 10%
 total circuit classes defined (counting one default) 1


 class DEFAULT has 10% bandwidth allocated
   the following circuits are assigned:
       16  using defaults.
       17  using defaults.
       18  using defaults.

 default class is DEFAULT


BRS [i 1] Config>?
 ENABLE
 DISABLE
 SET-CIRCUIT-DEFAULTS
 CIRCUIT
 ADD-CIRCUIT-CLASS
 DEL-CIRCUIT-CLASS
 CHANGE-CIRCUIT-CLASS
 DEFAULT-CIRCUIT-CLASS
 ASSIGN-CIRCUIT
 DEASSIGN-CIRCUIT
 QUEUE-LENGTH
 LIST
 SHOW
 CLEAR-BLOCK
 EXIT
 BRS [i 1] Config>set-circuit-defaults     4
 BRS [i 1] [circuit defaults] Config>?
```

```
ADD-CLASS
DEL-CLASS
CHANGE-CLASS
DEFAULT-CLASS
TAG
UNTAG
ASSIGN
DEASSIGN
LIST
EXIT
BRS [i 1] [circuit defaults] Config>add    5
Class name [DEFAULT]?DEF1
Percent bandwidth to reserve [10]? 5
BRS [i 1] [circuit defaults] Config>add
Class name [DEFAULT]?DEF2
Percent bandwidth to reserve [10]?5
BRS [i 1] [circuit defaults] Config>assign ip
Class name [DEFAULT]?DEF1
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES> [NO]?
BRS [i 1] [circuit defaults] Config>assign asrt
Class name [DEFAULT]? DEF2
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES> [NO]?
BRS[i 1] [circuit defaults] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, default circuit
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.



class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS  [i 1] [circuit defaults] Config>exit
BRS  [i 1] Config>circuit 16     6
BRS  [i 1][dlci 161] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 16 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
```

```
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

 class DEF1 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol IP with priority NORMAL is not discard eligible


 class DEF2 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ASRT with priority NORMAL is not discard eligible

 assigned tags:

 default class is DEFAULT with priority NORMAL



BRS  [i 1] [dlci 16] Config>show

 BANDWIDTH RESERVATION currently in RAM
 interface number 1, circuit number 16 using defaults.
 maximum queue length 10, minimum queue length 3
 4 current defined classes:
   class LOCAL has 10% bandwidth allocated
   class DEFAULT has 40% bandwidth allocated
   class DEF1 has 5% bandwidth allocated
   class DEF2 has 5% bandwidth allocated

 protocol and filter assignments:

 Protocol/Filter      Class              Priority    Discard Eligible
 ---------------      -----              --------    ----------------
 IP                   DEF1                 NORMAL             NO
 ARP                  DEFAULT              NORMAL             NO
 DNA                  DEFAULT              NORMAL             NO
 VINES                DEFAULT              NORMAL             NO
 IPX                  DEFAULT              NORMAL             NO
 OSI                  DEFAULT              NORMAL             NO
 VOFR                 DEFAULT              NORMAL             NO
 AP2                  DEFAULT              NORMAL             NO
 ASRT                 DEF2                 NORMAL             NO

 BRS [i 1] [dlci 16] Config>exit


BRS [i 1] Config>circuit 17
 BRS [i 1] [dlci 17] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, circuit number 17 using defaults.
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 60%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible

 class DEF1 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol IP with priority NORMAL is not discard eligible
```

```
 class DEF2 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ASRT with priority NORMAL is not discard eligible

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 1] [dlci 17] Config>add-class    7
 This circuit is currently using circuit defaults...
 Are you sure you want to override the defaults ?(Yes or [No]): yes
 Class name [DEFAULT]? CIRC171
 Percent bandwidth to reserve [10]? 5
 BRS[i 1] [dlci 17] Config>assign vines
 Class name [DEFAULT]? CIRC171
 Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
 Frame Relay Discard Eligible <NO/YES>[NO]?


BRS [i 1] [dlci 17] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, circuit number 17
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 65%
 total classes defined (counting one local and one default) 5


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ARP with default priority is not discard eligible
     protocol DNA with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible


 class DEF1 has 5% bandwidth allocated
   the following protocols and filters assigned:
     protocol IP with priority NORMAL is not discard eligible


 class DEF2 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol ASRT with priority NORMAL is not discard eligible


 class CIRC171 has 5% bandwidth allocated
   the following protocols and filters are assigned:
     protocol VINES with priority NORMAL is not discard eligible

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 1] [dlci 17] Config>show

 BANDWIDTH RESERVATION currently in RAM
 interface number 1, circuit number 17
 maximum queue length 10, minimum queue length 3
 5 current defined classes:
   class LOCAL has 10% bandwidth allocated
   class DEFAULT has 40% bandwidth allocated
   class DEF1 has 5% bandwidth allocated
   class DEF2 has 5% bandwidth allocated
   class CIRC171 has 5% bandwidth allocated



 protocol and filter assignments:

 Protocol/Filter      Class              Priority    Discard Eligible
 ---------------      -----              --------    ----------------
 IP                   DEF1                 NORMAL            NO
```

```
ARP                 DEFAULT             NORMAL              NO
DNA                 DEFAULT             NORMAL              NO
VINES               CIRC171             NORMAL              NO
IPX                 DEFAULT             NORMAL              NO
OSI                 DEFAULT             NORMAL              NO
VOFR                DEFAULT             NORMAL              NO
AP2                 DEFAULT             NORMAL              NO
ASRT                DEF2                NORMAL              NO

BRS [i 1] [dlci 17] Config>exit
BRS [i 1] Config>set-circuit-defaults
BRS [i 1] [circuit defaults] Config>change DEF1     8
Percent bandwidth to reserve [ 5]? 10
BRS [i 1] [circuit defaults] Config>change DEF2
Percent bandwidth to reserve [5]? 10
BRS [i 1] [circuit defaults] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, default circuit
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [circuit defaults] Config>exit


BRS [i 1] Config>circuit 16
  BRS [i 1] [dlci 16] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 16 using defaults.
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 70%
  total classes defined (counting one local and one default) 4


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol VINES with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol VOFR with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible

  class DEF1 has 10% bandwidth allocated
```

```
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 10% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 16] Config>exit


BRS [i 1] Config>circuit 17
  BRS [i 1[ [dlci 17] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 17
  maximum queue length 10, minimum queue length 3
  total bandwidth allocated 65%
  total classes defined (counting one local and one default) 5


  class LOCAL has 10% bandwidth allocated
    protocols and filters cannot be assigned to this class.


  class DEFAULT has 40% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ARP with default priority is not discard eligible
      protocol DNA with default priority is not discard eligible
      protocol IPX with default priority is not discard eligible
      protocol OSI with default priority is not discard eligible
      protocol VOFR with default priority is not discard eligible
      protocol AP2 with default priority is not discard eligible


  class DEF1 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol IP with priority NORMAL is not discard eligible


  class DEF2 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol ASRT with priority NORMAL is not discard eligible


  class CIRC171 has 5% bandwidth allocated
    the following protocols and filters are assigned:
      protocol VINES with priority NORMAL is not discard eligible

  assigned tags:

  default class is DEFAULT with priority NORMAL

  BRS [i 1] [dlci 17] Config>use-circuit-defaults     9
  This circuit is currently NOT using circuit defaults...
  Are you sure you want to delete current definitions and use defaults ? (Yes or
  [No]): yes
  Defaults are in effect for this circuit.
  Please reload router for this command to take effect.
  BRS [i 1] [dlci 17] Config>
  *reload
  Are you sure you want to reload the gateway? (Yes or [No] ):yes


  *t 6
  Gateway user configuration
  Config>feature brs
  Bandwidth Reservation User Configuration
  BRS Config>interface 1
  BRS [i 1] Config>circuit 17
  BRS [i 1] [dlci 17] Config>list

  BANDWIDTH RESERVATION listing from SRAM
  bandwidth reservation is enabled
  interface number 1, circuit number 17 using defaults.
```

```
maximum queue length 10, minimum queue length 3
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible


class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL



BRS [i 1] [dlci 17] Config>show

BANDWIDTH RESERVATION currently in RAM
interface number 1, circuit number 17 using defaults.
maximum queue length 10, minimum queue length 3
4 current defined classes:
  class LOCAL has 10% bandwidth allocated
  class DEFAULT has 40% bandwidth allocated
  class DEF1 has 10% bandwidth allocated
  class DEF2 has 10% bandwidth allocated

protocol and filter assignments:

Protocol/Filter      Class              Priority    Discard Eligible
---------------      -----              --------    ----------------
IP                   DEF1                 NORMAL            NO
ARP                  DEFAULT              NORMAL            NO
DNA                  DEFAULT              NORMAL            NO
VINES                DEFAULT              NORMAL            NO
IPX                  DEFAULT              NORMAL            NO
OSI                  DEFAULT              NORMAL            NO
VOFR                 DEFAULT              NORMAL            NO
AP2                  DEFAULT              NORMAL            NO
ASRT                 DEF2                 NORMAL            NO

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

第2章 帯域幅予約の構成と監視

この章では、帯域幅予約システム (BRS) の構成コマンドおよび監視コマンドについて説明します。

この章には、次の内容が記載されています。

帯域幅予約構成の概説

ルーター上で帯域幅予約構成コマンドにアクセスし、帯域幅予約を構成するには、次のようにしてください。

1. OPCON (*) プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **feature brs** と入力する。
3. BRS Config> プロンプトで **interface #** と入力する。インターフェースは、ポイントツーポイントまたはフレーム・リレー・インターフェースです。BRS は、フレーム・リレー・サブインターフェース上で構成できません。詳細については、*Nways マルチプロトコル・アクセス・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使用』を参照してください。
4. BRS [i 0] Config> プロンプトで **enable** と入力する。

   これはインターフェース・プロンプト・レベルで、この例では、インターフェース番号はゼロになっています。構成する各インターフェースごとに、ステップ 3 とステップ 4 を繰り返す必要があります。

   フレーム・リレー・インターフェースの BRS を構成している場合は、ステップ 4a を続けます。

   その他のインターフェースの BRS を構成している場合は、直接、ステップ 5 に進みます。

   a. BRS [i 0] Config> プロンプトで **circuit** # と入力する。ただし、# は構成する回線の番号です。
   b. BRS [i 0] [dlci 16] Config> プロンプトで **enable** と入力する。これは回線プロンプト・レベルで、この例では、回線 (DLCI) 番号は 16 です。
   c. BRS [i 0] [dlci 16] Config> プロンプトで **exit** と入力して、インターフェース・レベル・プロンプトに戻る。
   d. BRS t-classes を定義したい各回線ごとに、ステップ 4a ～ 4c を繰り返します。
5. ルーターを再ロードします。
6. 使用可能にした特定のインターフェースに対して帯域幅予約を構成するために、ステップ 1 ～ 3 を繰り返します。

7. PPP インターフェースの BRS を構成している場合は、BRS[i 0]Config> プロンプトで、24ページの表4 に表示されている構成コマンドを使用して、トラフィック・クラスを構成し、そのトラフィック・クラスにプロトコル、フィルター、およびタグを割り当てます。FR インターフェースの BRS を構成している場合は、ステップ 8 〜 10 に従ってください。
8. FR インターフェースの BRS を構成している場合は、24ページの表3 に示されているコマンドを使用して、回線クラスを構成し、その回線クラスに回線を割り当てることができます。
9. デフォルトの回線定義を使用したい場合は、BRS[i 0]Config> プロンプトで **set-circuit-defaults** コマンドを入力します。これにより BRS[i 0][circuit defaults] プロンプトが表示されるので、ここで 24ページの表4 からの該当するコマンドを使用して、トラフィック・クラスを構成し、そのトラフィック・クラスにプロトコル、フィルター、およびタグを割り当てることができます。トラフィック・クラス処理のデフォルト回線定義を定義する作業が完了したら、"exit" と入力して、BRS[i 0] Config> プロンプトに戻ります。
10. トラフィック・クラス処理のデフォルト回線定義を使用できない FR 回線がある場合には、**circuit** *permanent-virtual-circuit circuit_number* と入力します。これで回線プロンプトにアクセスできるので、ここから 24ページの表4 に示されたコマンドを使用して、トラフィック・クラス処理の回線特定の定義を作成します。

注: t-class および c-class 構成変更を有効にするために、ルーターを再ロードする必要はありません。

talk 6 (t 6) コマンドは、構成プロセスにアクセスします。

feature brs コマンドは、BRS 構成プロセスにアクセスします。このコマンドは、フィーチャー名 (brs) またはフィーチャー番号 (1) を使用して入力できます。

interface # コマンドは、帯域幅予約を構成する特定のインターフェースを選択します。BRS クラスを構成する前に、**enable** コマンドを使用して、インターフェース上の BRS を使用可能にしておく必要があります。21ページの4 のステップのプロンプトは、選択されたインターフェースの番号がゼロであることを示しています。

circuit # コマンドは、BRS トラフィック・クラスを構成する FR インターフェース上の回線を選択します。回線の BRS t-classes を構成する前に、**enable** コマンドを使用して、回線上の BRS を使用可能にしておく必要があります。ステップ 21ページの4b のプロンプトは、インターフェース 0 上の回線 16 が選択されたことを示しています。

選択したインターフェースおよび回線の帯域幅予約を使用可能にした後、ルーターを再ロードした上で、回線クラス (フレーム・リレーだけ) およびトラフィック・クラスを構成することが必要です。

種々のレベルの BRS プロンプトから Config> プロンプトが表示されるまで **exit** コマンドを入力することによって、いつでも Config> プロンプトに戻ることができます。

帯域幅予約の構成コマンド

ここでは、帯域幅予約の構成コマンドについて説明します。使用できるコマンドは、表示されているBRS 構成プロンプト (`BRS Config>`、`BRS [i x] Config>`、`BRS [i x] [dlci y] Config>`、または `BRS [i x] [circuit defaults] Config>`) によって異なります。

表 2. 帯域幅予約構成コマンドの要約 (BRS Config> プロンプトから利用可能)

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Activate-IP-precedence-filtering	保護 IP トンネルを介して送信される、または 2 次 TCP または UDP フラグメントに入れて送信される APPN および SNA パケットの BRS IPv4 優先順位フィルターを起動します。DLSw、IP 経由 HPR、および TN3270 を構成する場合は、IPv4 優先順位ビットの設定値を構成することも必要です。
Deactivate-IP-precedence-filtering	IPv4 優先順位フィルター処理を停止します。
Enable-hpr-over-ip-port-numbers	IP 経由 APPN-HPR トラフィックの BRS フィルター処理を使用可能にし、IP 経由 HPR パケットを識別するのに使用する UDP ポート番号を構成できるようにします。 **注:** APPN がロード・イメージに存在する場合は、このコマンドはサポートされません。BRS は APPN から、IP 経由 HPR が構成されているかどうかを確認し、構成されている場合には、APPN サポートから、IP 経由 HPR に使用される UDP ポート番号を確認します。
Disable-hpr-over-ip-port-numbers	IP 経由 APPN-HPR トラフィックの BRS フィルター処理を使用不可にします。 **注:** APPN がロード・イメージに存在する場合は、このコマンドはサポートされません。BRS は APPN から、IP 経由 HPR が構成されているかどうかを確認します。
Interface	帯域幅予約を構成するインターフェースを選択します。 **注:** このコマンドは、他の構成コマンドを使用する前に入力する必要があります。 24ページの表3 および 24ページの表4 を参照してください。
List	帯域幅予約をサポートするインターフェースを表示し、各インターフェースについて、帯域幅予約が使用可能か使用不可かを示します。

表 2. 帯域幅予約構成コマンドの要約 (BRS Config> プロンプトから利用可能) (続き)

コマンド	機能
Exit	直前のコマンド・レベルに戻ります。 xxxv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 3. フレーム・リレー・インターフェースの BRS [i #] Config> プロンプトから利用可能な構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add-circuit-class	帯域幅 c-class の名前とその帯域幅の比率を設定します。
Assign-circuit	指定された回線を指定された帯域幅 c-class に割り当てます。
Change-circuit-class	帯域幅 c-class に構成された帯域幅の量を変更します。
Circuit	BRS 回線レベル・プロンプト (BRS [i x][dlci y] Config>) にアクセスします。ここから 表4 に示されたコマンドを使用して、フレーム・リレー回線上の帯域幅予約を構成することができます。
Clear-block	現行インターフェースに関連した構成データを SRAM からクリアします。回線クラス構成データおよびトラフィック・クラスのデフォルト回線定義がクリアされます。
Deassign-circuit	指定された回線をデフォルトの c-class に復元します。
Default-circuit-class	デフォルト帯域幅 c-class の名前とそのインターフェース帯域幅の比率を設定します。
Del-circuit-class	指定された帯域幅 c-class を削除します。
Disable	インターフェース上の帯域幅予約を使用不可にします。
Enable	インターフェース上の帯域幅予約を使用可能にします。
List	c-classes と割り当てられた回線定義を SRAM から表示します。
Queue-length	優先待ち行列内のパケット数の最大値と最小値を設定します。
Set-circuit-defaults	BRS [i x] [circuit defaults] Config> コマンド・プロンプトにアクセスし、表4 から該当するコマンドを使用して、トラフィック・クラス処理のデフォルト回線定義を作成できるようにします。
Show	現在定義されている c-classes と、割り当てられている回線を、SRAM から表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

次の表は、PPP インターフェースの BRS [i x] Config> プロンプト、フレーム・リレー回線の BRS [i x] dlci [y] Config> プロンプト、および BRS [i x] [circuit defaults] Config> プロンプトから利用可能な BRS 回線コマンドを示しています。

表 4. BRS トラフィック・クラス処理コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add-class	指定された量の帯域幅をユーザー定義のトラフィック・クラスに割り当てます。
Create-super-class	*super-class (スーパークラス)* と呼ばれる t-class を定義します。
Assign	プロトコルまたはフィルターを、構成されたトラフィック・クラスに割り当てます。
Change-class	帯域幅 t-class に対して構成された帯域幅の量を変更します。

表 4. BRS トラフィック・クラス処理コマンド (続き)

コマンド	機能
Clear-block	PPP インターフェースまたはフレーム・リレー回線のトラフィック・クラスとプロトコル、フィルター、およびタグ割り当て構成データを、SRAM からクリアします。 **注:** このコマンドは BRS [i x] [circuit defaults] Config> プロンプトからは使用できません。
Deassign	指定されたパケットまたはフィルターの待ち行列化を、デフォルトの t-class と優先順位に復元します。
Default-class	デフォルトの t-class と優先順位を必要な値に設定し、すべての未割り当てプロトコルを新しいデフォルト t-class に割り当てます。
Del-class	以前に構成した帯域幅 t-class を削除します。
Disable	PPP インターフェースまたはフレーム・リレー回線上の帯域幅予約を使用不可にします。 **注:** BRS [i x] [circuit defaults] Config> プロンプトからは、BRS を使用可能または使用不可にすることはできません。
Enable	PPP インターフェースまたはフレーム・リレー回線上の帯域幅予約を使用可能にします。 **注:** BRS [i x] [circuit defaults] Config> プロンプトからは、BRS を使用可能または使用不可にすることはできません。
List	SRAM に保管されている構成済み t-classes とプロトコル、フィルター、およびタグ割り当てを表示します。
Queue-length	優先待ち行列内のパケット数の最大値と最小値を設定します。 **注:** このコマンドは、BRS [i x] [circuit defaults] Config> プロンプトではサポートされません。
Show	RAM に保管されている現在定義済みの t-classes とプロトコル、フィルター、およびタグ割り当てを表示します。 **注:** このコマンドは、BRS [i x] [circuit defaults] Config> プロンプトではサポートされません。
Tag	MAC フィルター・フィーチャーの構成時にタグ付けされた MAC フィルターに、BRS タグ名 (TAG1-TAG5) を割り当てます。
Untag	BRS タグ名 (TAG1-TAG5) と MAC フィルター・フィーチャーの構成時にタグ付けされた MAC フィルターとの関係を除去します。
Use-circuit-defaults	ユーザーがトラフィック・クラス処理の circuit-specific 定義を削除して、circuit-defaults 定義を使用することができるようにします。このコマンドは、フレーム・リレーの BRS [i x] dlci [y] Config> プロンプトでだけ有効です。 **注:** デフォルトを有効にするためには、ルーターを再ロードする必要があります。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

該当するコマンドを使用して、ポイント・ポイント・プロトコル (PPP) およびフレーム・リレーの帯域幅予約を構成してください。フレーム・リレーの場合は、回線とネットワーク・インターフェースを構成することが必要です。PPP の場合は、ネットワーク・インターフェースを構成するだけで済みます。

注:

1. BRS インターフェース・メニュー内から **clear-block**、**disable**、**enable**、**list**、および **show** コマンドを出すと、選択されたインターフェースに構成されている帯域幅予約情報に影響を与えたり、表示したりします。BRS 回線メニュー内

からこれらのコマンドを出した場合は、パーマネント・バーチャル・サーキット (PVC) に構成されているフレーム・リレー帯域幅予約情報にだけ影響を与えたり、表示したりします。

2. 帯域幅予約コマンドを使用する前に、次のことを念頭に入れてください。
   - 他の構成コマンドを使用する前に、**interface** コマンドを使用して、インターフェースを選択しておくことが必要です。(BRS 構成は、これを強制的に要求します。)
   - *Class-name* パラメーターは、大文字小文字の区別をします。
   - 現行の *class-names* を見たい場合は、**list** または **show** コマンドを使用します。
   - インターフェースまたは回線上の帯域幅予約を使用可能にした後は、回線およびトラフィック・クラスを追加/削除/変更したり、回線またはプロトコルを動的に割り当てたりすることができます。有効にするために、ルーターを再ロードする必要があるコマンドは、**enable**、**disable**、**use-circuit-defaults**、および **clear-block** コマンドだけです。
3. t-class および c-class 構成変更を有効にするために、ルーターを再ロードする必要はありません。

Activate-IP-precedence-filtering

activate-ip-precedence-filtering コマンドは、保護 IP トンネルを介して送信される、または 2 次 TCP または UDP フラグメントに入れて送信される APPN および SNA パケットの BRS IPv4 優先順位フィルターを起動するのに使用します。DLSw、IP 経由 HPR、および TN3270 を構成する場合は、IPv4 優先順位ビットの設定値を構成することも必要です。詳しくは、10ページの『IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィック用の IP バージョン 4 優先順位ビット処理の使用』を参照してください。

構文:

activate-ip-precedence-filtering

Add-circuit-class

注: フレーム・リレーの構成時にだけ使用されます。

add-circuit-class コマンドは、インターフェース・レベルで、ユーザー定義の帯域幅 c-class に割り当てられた回線グループが使用する指定量の帯域幅を割り振るのに使用します。

構文:

add-circuit-class *class-name %*

Add-class

add-class コマンドは、指定量の帯域幅をユーザー定義の帯域幅 t-class に割り振るのに使用します。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオ

ーバーライドするかどうかを尋ねられます。『Yes』と応答すると、回線はトラフィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。『No』と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、BRS [i x][circuit defaults]Config> コマンド・プロンプトに行く必要があります。

構文:

add-class [*class-name* または *class#*] *%*

例 1: A フレーム・リレー回線上に CIRC17 という名前のクラスを 1 つ追加する

```
BRS [i 1] [dlci 17] Config>add-class
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults ?(Yes or [No]):y
Class name [DEFAULT]? CIRC17
Percent bandwidth to reserve [10]?5
BRS [i 1] [dlci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17
maximum queue length 10, minimum queue length 3
total bandwidth allocated 65%
total classes defined (counting one local and one default) 5


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible
    protocol ASRT with default priority is not discard eligible


class DEF1 has 5% bandwidth allocated
  protocol IP with priority NORMAL is not discard eligible.


class DEF2 has 5% bandwidth allocated
 protocol ARP with priority NORMAL is not discard eligible.


class CIRC171 has 5% bandwidth allocated
  no protocols or filters are assigned to this class.

assigned tags:

default class is DEFAULT with priority NORMAL
```

例 2: A フレーム・リレー回線上に class1 という名前のクラスを 1 つ追加する

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

BRS [i 2] [dlci 128]>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 2, circuit number 128
```

```
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with default priority is not discard eligible
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible
    protocol ASRT with default priority is not discard eligible

class class1 has 10% bandwidth allocated
  no protocols or filters are assigned to this class.

assigned tags:

default class is DEFAULT with priority NORMAL

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

Assign

assign コマンドは、指定されたタグ、プロトコル・パケット、またはフィルターを、そのクラス内の特定の t-class と優先順位に割り当てるのに使用します。4 つの優先順位タイプは、次のとおりです。

- Urgent
- High
- Normal (デフォルト優先順位)
- Low

注: プロトコル「ボイス・オーバー・フレーム・リレー (VOFR)」は、音声パケットがフレー ム・リレー・インターフェースを介して送信されるときに使用されます。回線が音声パケットだけ を伝送する場合は、回線上で t-class を 1 つだけ割り当て、プロトコルを VOFR と指定してください。t-class が 1 つだけ割り当てられるのは、ある t-class を別の t-class に対して優先することができないためです。t-class が複数個ある場合には、音声を伝送しない t-class が帯域幅の制御を獲得し、音声トラフィックの伝送と衝突します。音声トラフィックが即時伝送を受け取るようにするには、VOFR トラフィックおよび VOFR トラフィックにタイプ *Urgent* の優先順位を与えるしかありません。

回線で音声トラフィックだけでなく、データ・トラフィックも伝送しようとする場合は、*Nways マルチプロトコル・アクセス・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 ” の章の **enable fragmentation** コマンド に記載されているようなフレーム・リレーを介した断片化を回線に対して設定する必要があります。大きなデータ・パッケージが帯域幅を使いきれず、音声パケットが短時間で通過できなくならないようにするには、このようにすることが必要です。

構文:

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

assign コマンドは、フレーム・リレーのフレームの廃棄可能性 (DE) ビットを設定するのにも使用できます。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。『Yes』と応答すると、回線はトラフィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。『No』と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、BRS [i x][circuit defaults]Config> コマンド・プロンプトに行く必要があります。

例 1:

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

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

```
BRS [i 2] [dlci 128]>assign ?
IP
ARP
DNA
VINES
IPX
OSI
VOFR
AP2
ASRT
TUNNELING-IP
SDLC/BSC-IP
RLOGIN-IP
TELNET-IP
NETBIOS
SNA/APPN-ISR
SNMP-IP
MULTICAST-IP
DLSW-IP
TAG1
TAG2
TAG3
TAG4
TAG5
APPN-HPR
NETWORK-HPR
HIGH-HPR
MEDIUM-HPR
LOW-HPR
XTP-IP
UDP_TCP1
UDP_TCP2
UDP_TCP3
UDP_TCP4
UDP_TCP5
TOS1
TOS2
TOS3
TOS4
TOS5
Protocol or filter name [IP]? TOS1  1
Class name [DEFAULT]? class1  2
Priority  [NORMAL]?
Frame Relay Discard Eligible  [NO]?
TOS Mask [1-FF] [FF]?
TOS Range (Low) [0-FF] [0]? 1
```

```
TOS Range (High) [1]? 3
BRS [i 2] [dlci 128]> list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 2, circuit number 128
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with default priority is not discard eligible
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible
    protocol ASRT with default priority is not discard eligible


class class1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    filter TOS1 with priority NORMAL is not discard eligible
       with TOS range x1 - x3 and TOS mask xFF

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 2] [dlci 128]>show

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

protocol and filter assignments:

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

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

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

Assign-circuit

注: フレーム・リレーの構成時にだけ使用されます。

assign-circuit コマンドは、インターフェース・レベルで、指定された回線を指定された帯域幅 c-class に割り当てるのに使用します。PVC を回線クラスに割り当てるときは DLCI を使用し、SVC を回線クラスに割り当てるときは回線名を使用します。

注: **circuit** コマンドを使用してバーチャル・サーキット上の BRS を使用可能にし、ルーターを再ロードしてからでなければ、このコマンドを使用して回線に回線クラスを割り当てることはできません。

構文:

assign-circuit *# class name*

Change-circuit-class

注: フレーム・リレーの構成時にだけ使用されます。

change-circuit-class コマンドは、インターフェース・レベルで、指定された c-class に割り当てられた回線グループが使用する帯域幅の比率を変更するのに使用します。

構文:

change-circuit-class *class-name %*

Change-class

change-class コマンドは、帯域幅 t-class に構成された帯域幅の量を変更するのに使用します。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。『Yes』と応答すると、回線はトラフィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。『No』と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

構文:

change-class [*class-name* または *class#*] *%*

Circuit

注: フレーム・リレーの構成時にだけ使用されます。

circuit コマンドは、フレーム・リレーのパーマネント・バーチャル・サーキット (PVC) またはスイッチド・バーチャル・サーキット (SVC) を構成するのに使用します。このコマンドは、BRS インターフェース構成プロンプト (`BRS [i #] Config>`) からしか出せません。

構文:

circuit

add-class、**assign**、**default-class**、 **del-class**、**deassign**、または **change-class** コマンドを使用する前に、回線上の BRS を使用可能にし、ルーターを再ロードしておく必要があります。

PVC の例:

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

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

SVC の例:

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

BRS [i 1 ] [svc svc01] Config>  enable
```

フレーム・リレー回線に対して **enable** コマンドを出し、ルーターを再ロードすると、その回線に対して以下の構成コマンドが利用可能になります。

add-class	deassign	enable	tag
assign	default-class	exit	untag
change-class	del-class	list	clear-block
disable	show	use-circuit-defaults	

Clear-block

clear-block コマンドは、現行の帯域幅予約構成データを SRAM からクリアするのに使用します。

構文:

clear-block

- このコマンドを PPP のインターフェース・プロンプトから入力すると、そのインターフェースのすべての BRS 構成データがクリアされます。
- このコマンドをフレーム・リレーのインターフェース・プロンプトから入力すると、そのインターフェースまたはインターフェース上の回線は使用可能でなくなり、すべての回線クラス構成データとトラフィック・クラス処理のデフォルト回線定義がクリアされます。ただし、個々の回線のトラフィック・クラス構成データはクリアされず、インターフェース上の BRS を再び使用可能にすれば利用可能です。
- 回線のトラフィック・クラス構成データをクリアするためには、最初にインターフェース・レベル・プロンプトから **circuit** コマンドを入力し、次に回線レベル・プロンプトから **clear-block** コマンドを入力します。各回線のトラフィック・クラス構成データをクリアした後で、インターフェース・レベル・プロンプトから **clear-block** コマンドを入力して、回線クラス構成データをクリアします。この変更は、ルーターを再ロードするまで有効になりません。

例:

```
clear-block
You are about to clear BRS configuration information for this interface
Are you sure you want to do this (Yes or No): y
BRS [i 1] Config>
```

Create-super-class

create-super-class コマンドは、PPP インターフェースまたはフレーム・リレー回線上でスーパークラス と呼ばれる t-class を構成するために使用します。各 PPP インターフェースまたはフレーム・リレー回線について構成できるスーパークラスは 1 つだけです。このスーパークラスと関連付けられる帯域幅パーセントはありません。スーパークラスに割り当てられたプロトコルまたはフィルター・データは、PPP インターフェースまたはフレーム・リレー回線上の他のどの t-class に割り当てられたプロトコルまたはフィルター・データよりも優先して送信されます。ボイス・オーバー・フレーム・リレー (VOFR) プロトコルのスー パークラスは、音声パケットとデータ・パケットの両方を転送する回線用に構成する必要があります。この環境では、音声を伝送するようスーパークラスを構成すると、音声パケットが上位の優先順位をもつようにする上で役立ちます。

構文:

create-super-class

Deactivate-IP-precedence-filtering

deactivate-ip-precedence-filtering コマンドは、IPv4 優先順位フィルター処理を停止にするのに使用します。

構文:

deactivate-ip-precedence-filtering

Deassign

deassign コマンドは、指定されたプロトコル・パケットまたはフィルターの待ち行列化を、デフォルトの t-class と優先順位に復元するのに使用します。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。『Yes』と応答すると、回線はトラフィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。『No』と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

構文:

deassign [*prot-class* または *filter-class*]

Deassign-circuit

注: フレーム・リレーの構成時にだけ使用されます。

deassign-circuit コマンドは、インターフェース・レベルで、指定された回線の待ち行列化をデフォルト c-class に復元するのに使用します。

構文:

deassign-c #

Default-circuit-class

注: フレーム・リレーの構成時にだけ使用されます。

default-circuit-class コマンドは、インターフェース・レベルで、デフォルト帯域幅 c-class のユーザー定義名と、そのクラスの回線 (帯域幅 c-class に割り当てられていない孤立回線を含む) に割り振られる帯域幅の比率を設定するのに使用します。

構文:

default-circuit-class *class-name %*

Del-circuit-class

注: フレーム・リレーの構成時にだけ使用されます。

del-circuit-class コマンドは、インターフェース・レベルで、指定された帯域幅 c-class を削除するのに使用します。

構文:

del-circuit-class *class-name*

Default-class

default-class コマンドは、デフォルト t-class と優先順位を必要な値に設定するのに使用します。以前に値が指定されていない場合、システム・デフォルト値が使用されます。そうでない場合は、最後に指定された値が使用されます。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。『Yes』と応答すると、回線はトラフィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。『No』と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

構文:

default-cl [*class-name* または *class#*] *priority*

Del-class

del-class コマンドは、指定されたインターフェースまたは回線から、以前に構成された帯域幅 t-class を削除するのに使用します。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。『Yes』と応答すると、回線はトラ

フィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。『No』と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、BRS [i x][circuit defaults]Config> コマンド・プロンプトに行く必要があります。

構文:

del-class [*class-name* または *class#*]

Disable

disable コマンドは、インターフェース上 (インターフェース・プロンプトから入力した場合) または回線上 (回線プロンプトから入力した場合) の帯域幅予約を使用不可にするのに使用します。この変更は、ルーターを再ロードするまで有効になりません。

帯域幅予約が使用不可にされたかどうかを確認するには、**list** コマンドを入力します。

構文:

disable

Disable-hpr-over-ip-port-numbers

disable-hpr-over-ip-port-numbers コマンドは、IP 経由 HPR トラフィックの BRS フィルター処理を使用不可にするのに使用します。

構文:

disable-hpr-over-ip-port-numbers

IP 経由 HPR トラフィックの BRS フィルター処理が使用不可にされたかどうかを確認するには、**list** コマンドを入力します。

注: APPN がロード・イメージに含まれている場合は、APPN Config> コマンド・プロンプトで、IP 経由 HPR トラフィックを使用するかどうかを構成します。

Enable

enable コマンドは、インターフェース上 (インターフェース・プロンプトから入力した場合) または回線上 (回線プロンプトから入力した場合) の帯域幅予約を使用可能にするのに使用します。この変更は、ルーターを再ロードするまで有効になりません。

構文:

enable

BRS と優先待ち行列の構成

注:

1. PPP インターフェース上の BRS を構成するときは、インターフェース・プロンプトで **enable** コマンドを出し、ルーターを再ロード　した後で、トラフィック・クラスを構成し、トラフィック・クラスにプロトコルとフィルターを割り当てます。
2. 回線上で BRS を初期に使用可能にすると、回線はデフォルト回線定義を使用するように初期設定されます。インターフェース・プロンプトおよびトラフィック・クラスを定義したい各回線の回線プロンプトで、**enable** コマンドを出します。その後、ルーターを再ロードしてから、インターフェースの回線クラスおよび各回線のトラフィック・クラスを構成します。たとえば、次のようになります。

```
t 6
Gateway user configuration
Config>f brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1] Config>enable
Please reload router for this command to take effect
BRS [i 1] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1
maximum queue length 10, minimum queue length 3
total bandwidth allocated 10%
total circuit classes defined (counting one default) 1


class DEFAULT has 10% bandwidth allocated
  no circuits are assigned to this class.

default class is DEFAULT

BRS [i 1] Config>circ 16
BRS [i 1] [dlci 16] Config>enable
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1] [dlci 16] Config>ex
Please reload router for this command to take effect.
BRS [i 1] [dlci 16] Config>

*reload  Are you sure you want
to reload the gateway? (Yes or [No]): y
```

Enable-hpr-over-ip-port-numbers

enable-hpr-over-ip-port-numbers コマンドは、IP 経由 APPN-HPR トラフィックの BRS フィルター処理を使用可能にし、IP 経由 HPR パケットを識別するのに使用する UDP ポート番号を構成するのに使用します。

注: APPN がロード・イメージに含まれている場合は、APPN Config> コマンド・プロンプトで、IP 経由 HPR を使用可能にし、IP 経由 HPR トラフィックに使用する UDP ポート番号を指定します。

構文:

enable-hpr-over-ip-port-numbers

例:

```
BRS Config> enable-hpr-over-ip-port-numbers
XID exchange port number [12000]?
HPR net  trans prio port number [12001]?
```

```
HPR high trans prio port number [12002]?
HPR medium trans prio port number [12003]?
HPR low    trans prio port number [12004]?
```

XID exchange port number

このパラメーターは、XID 交換に使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12000

Network priority port number

このパラメーターは、network 優先順位トラフィックに使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12001

High exchange port number

このパラメーターは、high 優先順位トラフィックに使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12002

Medium exchange port number

このパラメーターは、medium 優先順位トラフィックに使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12003

Low exchange port number

このパラメーターは、low 優先順位トラフィックに使用される UDP ポート番号を指定します。このポート番号は、ネットワーク上の他の装置に定義された番号と同じでなければなりません。

有効値: 1024 ～ 65535

デフォルト値: 12004

Interface

interface コマンドは、帯域幅予約構成コマンドが適用されるシリアル・インターフェースを選択するのに使用します。*帯域幅予約は、PPP (ポイントツーポイント・プロトコル) およびフレーム・リレー・インターフェースを稼働するルーター上でサポートされます。*

注: 帯域幅予約は、フレーム・リレー・サブインターフェース経由でサポートされません。詳細については、*Nways* マルチプロトコル・アクセス・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使用を参照してください。

構文:

interface *interface#*

注:

1. 新しいインターフェースに対する帯域幅予約コマンドを入力する場合は、他の帯域幅予約構成コマンドを使用する***前に*** このコマンドを入力する必要があります。帯域幅予約プロンプトを終了した後で、前に構成したインターフェースの帯域幅予約を変更するためにこのプロンプトに戻りたい場合には、再びこのコマンドを最初に入力する必要があります。
2. WAN レストラルが使用されており、1 次インターフェースに BRS が構成されている場合、2 次インターフェースにも BRS を構成する必要があります。通常、WAN レストラルが使用されている場合には、2 次インターフェースは 1 次インターフェースと同じ識別を取りますが、BRS の場合はそうではないので、1 次インターフェースと 2 次インターフェースの両方で BRS を構成することが必要です。

特定のインターフェース上の帯域幅予約を使用可能にするには、`BRS Config>`プロンプトで、その特定プロトコルまたはフィーチャーをサポートするインターフェースの番号を入力します。これにより、この章で説明している BRS Talk 6 **enable** コマンドを使用できるようになります。インターフェース番号を使用可能にした後、2216 を 再ロードして、このコマンドを有効にしてからでないと、インターフェースに他の構成変更を加えることはできません。

注: フレーム・リレー・インターフェースの BRS を構成している場合は、ルーターを再ロードする前に、**circuit** コマンドを使用して回線を選択し、それらの回線の帯域幅予約を使用可能にすることができます。

List

list コマンドは、現在定義されている帯域幅クラスとそれぞれに保証されている比率を表示するのに使用します。

list コマンドと **show** コマンドは似ています。 **list** コマンドは現行の SRAM 定義を表示し、**show** コマンドは現行の RAM 定義を表示します。

構文:

list *interface#*

list コマンドを出すプロンプトに応じて、さまざまな出力が表示されます。**list** コマンドは、次のプロンプトから出すことができます。

- `BRS [i 1] [dlci 16] Config>`
- `BRS [i 1] Config>`
- `BRS Config>`
- `BRS [i 1] [circuit defaults] Config>`

注: このコマンドをフレーム・リレー回線プロンプト (BRS [i x] [dlci y] Config>) から使用すると、回線がトラフィック・クラス処理のデフォルト回線定義を使用しているのか、回線特定の定義を使用しているのかが示されます。回線がデフォルト回線定義を使用している場合、デフォルト回線定義に現在定義されているトラフィック・クラス、プロトコル、フィルター、およびタグが表示されます。ただし、デフォルト回線定義を変更したい場合には、BRS[i x] [circuit defaults] Config> プロンプトに行かないと変更できません。

PPP インターフェースの BRS インターフェース・レベル・プロンプト (BRS [i 0]) およびフレーム・リレー・インターフェースの BRS 回線レベル・プロンプト (BRS [i 0] [dlci 16] Config>) では、**list** コマンドは、構成された帯域幅の比率、および割り当てられたプロトコルとフィルターを表示します。

フレーム・リレーの BRS インターフェース・レベル・プロンプトでは、**list** コマンドは、回線クラス、それぞれに構成された帯域幅の比率、および割り当てられた回線を表示します。

例 1

```
BRS Config>list
 Bandwidth Reservation is available for 2 interfaces.

 Interface   Type            State
 ---------   ----            -----
         1   FR              Enabled
         2   PPP             Enabled

 The use of HPR over IP port numbers is disabled

 BRS Config>interface 1
 BRS [i 1] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 10%
 total circuit classes defined (counting one default) 1


 class DEFAULT has 10% bandwidth allocated
   the following circuits are assigned:
       17
       16  using defaults.
       18  using defaults.

 default class is DEFAULT

 BRS [i 2] Config>exit
 BRS Config>interface 2
 BRS [i 2] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 2
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 50%
 total classes defined (counting one local and one default) 2


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.


 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol IP with default priority
     protocol ARP with default priority
     protocol DNA with default priority
     protocol VINES with default priority
     protocol IPX with default priority
     protocol OSI with default priority
     protocol VOFR with default priority
     protocol AP2 with default priority
```

```
    protocol ASRT with default priority

 assigned tags:

 default class is DEFAULT with priority NORMAL

 BRS [i 2] Config>
```

例 2

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

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3


class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.


class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
   protocol ASRT with priority NORMAL is not discard eligible
   filter NETBIOS with priority NORMAL is not discard eligible


class CLASS1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
   protocol IP with priority NORMAL is not discard eligible
   protocol ARP with priority NORMAL is not discard eligible
   protocol DNA with priority NORMAL is not discard eligible
   protocol VINES with priority NORMAL is not discard eligible
   protocol IPX with priority NORMAL is discard eligible
   protocol OSI with priority NORMAL is not discard eligible
   protocol VOFR with priority NORMAL is not discard eligible
   protocol AP2 with priority NORMAL is not discard eligible
```

例 3

```
 BRS [i 1] [circuit defaults] Config>list

 BANDWIDTH RESERVATION listing from SRAM
 bandwidth reservation is enabled
 interface number 1, default circuit
 maximum queue length 10, minimum queue length 3
 total bandwidth allocated 70%
 total classes defined (counting one local and one default) 4


 class LOCAL has 10% bandwidth allocated
   protocols and filters cannot be assigned to this class.



 class DEFAULT has 40% bandwidth allocated
   the following protocols and filters are assigned:
     protocol DNA with default priority is not discard eligible
     protocol VINES with default priority is not discard eligible
     protocol IPX with default priority is not discard eligible
     protocol OSI with default priority is not discard eligible
     protocol VOFR with default priority is not discard eligible
     protocol AP2 with default priority is not discard eligible
     protocol ASRT with default priority is not discard eligible


 class DEF1 has 10% bandwidth allocated
   protocol IP with priority NORMAL is not discard eligible.


 class DEF2 has 10% bandwidth allocated
  protocol ARP with priority NORMAL is not discard eligible.

 assigned tags:

 default class is DEFAULT with priority NORMAL

  BRS [i 1] [circuit defaults] Config>
```

例 4

```
BRS Config>list
 Bandwidth Reservation is available for 2 interfaces.

 Interface   Type            State
```

```
---------   ----            -----
        1   FR              Enabled
        2   PPP             Enabled

The use of HPR over IP port numbers is enabled.

   Transmission Type   Port Number
   -----------------   -----------
       XID exchange        12000
       HPR network         12001
       HPR high            12002
       HPR medium          12003
       HPR low             12004
```

Queue-length

queue-length コマンドは、各 BRS 優先待ち行列に待ち行列化できるパケットの数を設定するのに使用します。各 BRS クラスには、そのプロトコル、フィルター、およびタグに割り当てられた優先順位値があり、各優先待ち行列に、このコマンドで指定したパケット数を保管することができます。

構文:

queue-length *maximum-length minimum-length*

このコマンドは、各 BRS 優先待ち行列に待ち行列化できるバッファーの最大数、およびルーターの入力バッファーが不足しているときに各 BRS 優先待ち行列に待ち行列化できる最大数を設定します。

PPP インターフェースに対して **queue-length** を出すと、このコマンドは、そのインターフェースに定義されている各 BRS t-class の各優先待ち行列の queue-length 値を設定します。

フレーム・リレー・インターフェースに対して **queue-length** を出すと (プロンプト `BRS [i 0] Config>` で)、このコマンドは、そのインターフェースの各パーマネント・バーチャル・サーキットに対して定義されている各 BRS t-class の各優先待ち行列のデフォルト queue-length 値を設定します。

フレーム・リレー PVC に対して **queue-length** を出すと (プロンプト `BRS [i 0] [dlci 16] Config>` などで)、このコマンドは、その PVC に定義されている各 BRS t-class の各優先待ち行列の待ち行列長さ値を設定します。これらの値は、そのフレーム・リレー・インターフェースに設定されているデフォルトの待ち行列長さ値をオーバーライドします。

重要: このコマンドは、その使用が不可欠のとき以外は、使用しないでください。待ち行列長さのデフォルト値は、ほとんどのユーザーに推奨できる値です。待ち行列の長さの値を高く設定し過ぎると、ルーターの性能が大きく低下する可能性があります。

Set-circuit-defaults

set-circuit-defaults コマンドは、トラフィック・クラス処理のデフォルト回線定義を定義するのに必要なコマンドにアクセスするのに使用します。これらのデフォルト回線定義は、同じトラフィック・クラスと、プロトコル、フィルター、およびタグ割り当てを使用できるインターフェース上のすべてのフレーム・リレー回線で使用できます。

構文:

set-circuit-defaults

Show

show コマンドは、RAM に保管されている現行の定義済み帯域幅クラスを表示するのに使用します。

構文:

show *interface#*

show コマンドを出すプロンプトに応じて、さまざまな出力が表示されます。**show** コマンドは、次のプロンプトから出すことができます。

- BRS [i *x*] Config> - インターフェース番号 *x* のインターフェース・レベル・プロンプト。
- BRS [i *x*] [dlci *y*] Config> - フレーム・リレー・インターフェース番号 *x* 上の回線 *y* の回線レベル・プロンプト。次の例は、回線レベル・プロンプトからの show コマンドの出力を示しています。

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

Protocol/Filter      Class             Priority    Discard Eligible
---------------      -----             --------    ----------------
IP                   CLASS1              NORMAL            NO
ARP                  CLASS1              NORMAL            NO
DNA                  CLASS1              NORMAL            NO
VINES                CLASS1              NORMAL            NO
IPX                  CLASS1              NORMAL            YES
OSI                  CLASS1              NORMAL            NO
VOFR                 CLASS1              NORMAL            NO
AP2                  CLASS1              NORMAL            NO
ASRT                 DEFAULT             NORMAL            NO
NETBIOS              DEFAULT             NORMAL            NO
```

PPP のインターフェース・プロンプトおよびフレーム・リレーの回線プロンプトでは、トラフィック・クラス情報が表示されます。フレーム・リレーのインターフェース・プロンプトでは、回線クラス情報が表示されます。

注:

1. このコマンドをフレーム・リレー回線プロンプト (BRS [i x] [dlci y] Config>) から使用すると、回線がトラフィック・クラス処理のデフォルト回線定義を使用しているのか、回線特定の定義を使用しているのかが示されます。回線がデフォルト回線定義を使用している場合、デフォルト回線定義に現在定義されているトラフィック・クラス、プロトコル、フィルター、およびタグが表示されます。ただし、デフォルト回線定義を変更したい場合には、BRS[i x] [circuit defaults] Config> プロンプトに行かないと変更できません。
2. このコマンドは BRS [i x] [circuit defaults] Config> プロンプトからは使用できません。

Tag

tag コマンドは、MAC フィルター機能の構成時にタグ付けされた MAC フィルター項目を、次に利用可能な BRS タグ名に割り当てるのに使用します。BRS タグ名は、TAG1、TAG2、TAG3、TAG4、および TAG5 です。assign コマンドで BRS タグ名を指定して、タグを BRS トラフィック・クラスに割り当てます。

構文:

tag *mac_filter_tag#*

list コマンドを使用すると、どの MAC フィルター・タグが BRS タグ名に割り当てられており、どの BRS タグ名が帯域幅トラフィック・クラスに割り当てられているかが表示されます。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。『Yes』と応答すると、回線はトラフィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。『No』と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

Untag

untag コマンドは、MAC フィルター・タグ番号と BRS タグ名の関係を除去するのに使用します。タグを除去できるのは、対応する BRS タグ名が帯域幅トラフィック・クラスに割り当てられていないときだけです。

構文:

untag *mac_filter_tag#*

list コマンドを使用すると、どの MAC フィルター・タグが BRS タグ名に割り当てられており、どの BRS タグ名が帯域幅トラフィック・クラスに割り当てられているかが表示されます。

注: 現在、トラフィック・クラス処理のデフォルト回線定義を使用しているフレーム・リレー回線に対してこのコマンドを使用すると、デフォルト回線定義をオーバーライドするかどうかを尋ねられます。『Yes』と応答すると、回線はトラフィック・クラス処理の回線特定の定義を使用するように変更され、コマンドの使用が認められます。『No』と応答すると、コマンドは放棄され、その回線では引き続きデフォルト回線定義が使用されることになります。デフォルト回線定義を変更したい場合は、`BRS [i x][circuit defaults]Config>` コマンド・プロンプトに行く必要があります。

Use-circuit-defaults

use-circuit-defaults コマンドは、インターフェース・レベルで、回線特定の定義を削除して、トラフィック・クラス処理のデフォルト回線定義を使うようにするのに使用します。回線デフォルト値を使用することの確認を求めるプロンプトが出ます。

構文:

use-circuit-defaults

注:

1. このコマンドは、フレーム・リレーの構成時にだけ使用されます。
2. デフォルトを有効にするためには、ルーターを再ロードする必要があります。

例:

```
BRS [i 1] [dlci 17] Config>use-circuit-defaults
This circuit is currently NOT using circuit defaults...
 Are you sure you want to delete current definitions and use defaults ? (Yes or
 [No]): y
 Defaults are in effect for this circuit.
 Please reload router for this command to take effect.
 BRS [i 1] [dlci 17] Config>
 *reload  Are you sure you want to reload the gateway? (Yes or [No]): y
```

帯域幅予約監視プロンプトへのアクセス

帯域幅予約監視コマンドにアクセスし、ルーター上の帯域幅予約を監視するには、次のようにします。

1. OPCON プロンプト (*) で **talk 5** と入力する。
2. GWCON プロンプト (+) で **feature brs.** と入力する。
3. BRS> プロンプトで **interface #** と入力する。ただし、# は監視するインターフェースの番号です。これにより、インターフェース・レベル・プロンプト BRS [i x]> が表示されます。ただし、x はインターフェース番号です。
4. フレーム・リレーの場合だけ、インターフェース・プロンプトで **circuit #** と入力して、このインターフェース上の監視する回線を指定する。

   これにより、回線レベル・プロンプト BRS [i x] [dlci y]> が表示されます。ただし、x はインターフェース番号で、y は回線番号です。
5. プロンプトで、該当する監視コマンドを入力する。 (『帯域幅予約監視コマンド』 を参照してください。)

   talk 5 (t 5) コマンドは、監視プロセスにアクセスします。

   feature brs コマンドは、BRS 監視プロセスにアクセスします。このコマンドは、フィーチャー名 (brs) またはフィーチャー番号 (1) を使用して入力できます。

   interface # コマンドは、帯域幅予約を監視する特定のインターフェースを選択します。

   circuit # コマンドは、フレーム・リレーのパーマネント・バーチャル・サーキット (PVC) の DLCI を選択します。

   BRS> プロンプトで **exit** コマンドを入力すれば、いつでも GWCON プロンプトに戻ることができます。

   帯域幅予約監視プロンプト (BRS>) にアクセスしたら、45ページの表5 に説明されている特定の監視コマンドのどれでも入力できます。

帯域幅予約監視コマンド

ここでは、帯域幅予約監視コマンドの要約を示し、個々のコマンドについて説明します。 表5 は、帯域幅予約監視コマンドを示しています。使用できるコマンドは、BRS 監視プロンプト (BRS>、BRS [i x]>、または BRS [i x] [dlci y]>) によって異なります。

表 5. 帯域幅予約監視コマンドの要約

コマンド	FR でだけ使用	機能
? (ヘルプ)		このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxv ページの『ヘルプの入手』を参照してください。
Circuit	yes	フレーム・リレーのパーマネント・バーチャル・サーキット (PVC) の DLCI を選択します。フレーム・リレーの帯域幅予約トラフィックを監視するには、回線プロンプト・レベルにあることが必要です。
Clear		現在の t-class カウンターをクリアし、それらを **last** t-class カウンターとして保管します。カウンターはクラス別に表示されます。
Clear-circuit-class	yes	現在の c-class カウンターをクリアし、それらを **last** c-class カウンターとして保管します。カウンターはクラス別に表示されます。
Counters		現在の t-class カウンターを表示します。
Counters-circuit-class	yes	現在の c-class カウンターを表示します。
Interface		監視するインターフェースを選択します。 **注:** このコマンドは、他の帯域幅予約監視コマンドを使用する前に入力する必要があります。
Last		最後に保管された t-class カウンターを表示します。
Last-circuit-class	yes	最後に保管された c-class カウンターを表示します。
Exit		直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』 を参照してください。

Circuit

注: フレーム・リレーを監視するときにだけ使用します。

circuit コマンドは、監視するフレーム・リレー PVC の DLCI を選択するのに使用します。このコマンドは、BRS インターフェース監視プロンプト (BRS [i #]>) からしか出せません。

構文:

circuit *permanent-virtual-circuit-#*

フレーム・リレー回線を選択した後、回線プロンプトで次のコマンドを使用することができます。

```
CLEAR
COUNTERS
LAST
EXIT
```

Clear

clear コマンドは、現行の帯域幅予約 t-class カウンターを保管して **last** コマンドを用いて検索できるようにし、値をクリアするのに使用します。カウンターは、帯域幅トラフィック・クラスに基づいて保持されます。

構文:

clear

Clear-Circuit-Class

注: フレーム・リレーを監視するときにだけ使用します。

clear-circuit-class コマンドは、現行の帯域幅予約 c-class カウンターを保管して **last-circuit-class** コマンドを用いて検索できるようにし、値をクリアするのに使用します。カウンターは、回線クラスに基づいて保持されます。

構文:

clear-circuit-class

Counters

counters コマンドは、PPP インターフェースまたはフレーム・リレー回線に対して構成されたトラフィック・クラスの帯域幅予約トラフィックを説明する統計を表示するのに使用します。

構文:

counters

例: **counters**

```
Bandwidth Reservation Counters
interface number 1
Class            Pkt Xmit     Bytes Xmit     Bytes Ovfl     Pkt Ovfl    Q_len

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

TOTAL              140          11502              0            0
```

Bytes Ovfl

優先待ち行列の最大 queue-length に達したか、あるいは優先待ち行列が最小待ち行列長さ限界値にあるときに、受信バッファーが不足しているインターフェースからパケットが来たためにパケットを待ち行列化できなかったかのいずれか理由で転送できなかったパケットのバイト数を表示します。

Pkt Ovfl

優先待ち行列の最大 queue-length に達したか、あるいは優先待ち行列が最小待ち行列長さ限界値にあって、低い受信バッファーで稼働していたインターフェースからパケットが来たためにパケットを待

ち行列化できなかったかのどちらかの理由で、転送できなかったパケットのパケット数を表示します。

Q_len 各トラフィック・クラス内のそれぞれの優先待ち行列で送信を待機している現行パケット数。

Counters-circuit-class

注: フレーム・リレーを監視するときにだけ使用します。

counters-circuit-class コマンドは、フレーム・リレー回線に対して構成されたトラフィック・クラスの統計を表示するのに使用します。

構文:

counters-circuit-class

例: **counters-circuit-class**

```
Bandwidth Reservation Circuit Class Counters
Interface 1


Class         Pkt Xmit     Bytes Xmit     Bytes Ovfl
DEFAULT             25           3402             26
CIRCLASS1            1             56              0
CIRCLASS2            0              0              0

TOTAL               26           3458             26
```

Interface

interface コマンドは、帯域幅予約監視コマンドが適用されるシリアル・インターフェースを選択するのに使用します。*帯域幅予約は、PPP (ポイントツーポイント・プロトコル) およびフレーム・リレー・インターフェースを稼働するルーター上でサポートされます。*

構文:

interface *interface#*

注: 新しいインターフェースに対する帯域幅予約コマンドを入力する場合は、他の帯域幅予約監視コマンドを使用する前にこのコマンドを入力する必要があります。帯域幅予約監視プロンプト (BRS>) を終了した後で、帯域幅予約を監視するためにこのプロンプトに戻りたい場合には、再びこのコマンドを最初に入力する必要があります。

特定のインターフェースの帯域幅予約を監視するには、BRS> 監視プロンプトで、そのインターフェースの番号を入力します。これにより、この章で説明している帯域幅予約監視コマンドを使用できるようになります。

Last

last コマンドは、最後に保管された t-class 統計を表示するのに使用します。t-class 統計は、**counters** コマンドの場合と同じフォーマットで表示されます。

構文:

last

Last-circuit-class

注: フレーム・リレーを監視するときにだけ使用します。

last-circuit-class コマンドは、最後に保管された回線クラス統計を表示するのに使用します。c-class 統計は、**counters-circuit-class** コマンドの場合と同じフォーマットで表示されます。

構文:

last-circuit-class

帯域幅予約動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

帯域幅予約は、CONFIG (Talk 6) **delete interface** コマンドを制限なしでサポートします。

GWCON (Talk 5) Activate Interface

帯域幅予約は、GWCON (Talk 5) **activate interface** コマンドを制限なしでサポートします。

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

GWCON (Talk 5) Reset Interface

帯域幅予約は、GWCON (Talk 5) **reset interface** コマンドを制限なしでサポートします。

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

CONFIG (Talk 6) 即時変更コマンド

帯域幅予約は、装置の操作状態を即時に変更する、次の CONFIG コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行する場合には、保管されて保存されます。

コマンド
GWCON, feature brs, activate-ip-precedence-filtering
GWCON, feature brs, deactivate-ip-precedence-filtering
GWCON, feature brs, enable-hpr-over-ip-port-numbers
GWCON, feature brs, disable-hpr-over-ip-port-numbers
GWCON, feature brs, interface, add-circuit-class
GWCON, feature brs, interface, assign-circuit

GWCON, feature brs, interface, change-circuit-class
GWCON, feature brs, interface, deassign-circuit
GWCON, feature brs, interface, default-circuit-class
GWCON, feature brs, interface, del-circuit-class
GWCON, feature brs, interface, disable
GWCON, feature brs, interface, enable
GWCON, feature brs, interface, queue-length
GWCON, feature brs, interface, add-class **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, assign **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, change-class **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, create-super-class **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, deassign **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, default-class **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, del-class **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, disable **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, enable **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, tag **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。
GWCON, feature brs, interface, untag **注:** このコマンドは、フレーム・リレー・インターフェースについて回線レベルで使用できます。

第3章 MAC フィルターの使用

この章では、処理時にパケットに適用するパケット・フィルターを指定するための媒体アクセス制御 (MAC) の使用法について説明します。この章には、次の内容が記載されています。

- 『MAC フィルターと DLSw トラフィック』
- 52ページの『MAC フィルター・パラメーター』

フィルターとは、ブリッジするときのパケットの扱い方を決めるためにパケットに適用される 1 組の規則です。MAC フィルターは、ブリッジされるトラフィックにだけ影響を与えます。

注: MAC フィルターはトンネル・トラフィックにも適用できます。

フィルター・プロセスでは、ブリッジング時にパケットは処理されるか、フィルターに掛けられるか、またはタグ付けされます。アクションは、次のとおりです。

- **処理** - パケットは、影響を受けずにブリッジをパスすることができます。
- **フィルター** - パケットは、ブリッジをパスすることができません。
- **タグ付け** - パケットは、ブリッジをパスすることができますが、構成可能なパラメーターに基づいて、1 ～ 64 の範囲の番号でマーク付けされます。

MAC フィルターは、次の 3 つのオブジェクトから構成されます。

1. フィルター項目 - パケット内のアドレス・フィールドまたは任意のウィンドウのデータに適用される 1 つの規則です。この規則を適用した結果は、真 (一致する) または偽 (一致しない) のどちらかの状態です。
2. フィルター・リスト - 1 つまたは複数のフィルター項目のリストが入っています。
3. フィルター - 1 組のフィルター・リストが入っています。

MAC フィルターと DLSw トラフィック

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

LLC に対するフィルターを設定するときは、*Bridge Net* 番号を、そのフィルターのインターフェース番号として使用します。Bridge Net 番号は、ルーターに構成したインターフェースの数に 2 を加算して決めます。インターフェースのリストを見たい場合は—`hConfig>` プロンプトで **list devices** コマンドを入力するか、または `+` プロンプトで **configuration** を入力します。

次の例では、Bridge Net 番号は 7 です。

```
Ifc 0 Token Ring                    Slot: 1  Port: 1
Ifc 1 Token Ring                    Slot: 1  Port: 2
Ifc 2 Token Ring                    Slot: 2  Port: 1
Ifc 3 Token Ring                    Slot: 2  Port: 2
Ifc 4 Ethernet                      Slot: 4  Port: 1
Ifc 5 Ethernet                      Slot: 4  Port: 2
```

たとえば、この Bridge Net に対してフィルターを設定した場合、ルーターは除外フィルターに一致するフレームをドロップしません。代わりに、これらのフレームをブリッジに転送します。

MAC フィルター・パラメーター

フィルターを作成するときには、次のパラメーターの一部または全部を指定することができます。

- 発信元 MAC アドレスまたは着信先 MAC アドレス
- パケット内の照合するデータ
- フィルターに掛けるパケットのフィールドに適用されるマスク
- インターフェース番号
- 入力 / 出力の指定
- 包含 / 除外 / タグの指定
- タグ値 (タグが指定されている場合)

フィルター項目パラメーター

次のパラメーターは、アドレス・フィルター項目 (address-filter-item) を構成するのに使用されます。

- アドレス・タイプ: SOURCE または DESTINATION
- タグ: *tag-value*
- アドレス・マスク: *hex-mask*

各フィルター項目 (filter-item) は、パケット内のタイプと照合するアドレス・タイプ (SOURCE または DESTINATION のどちらか) を指定します。

アドレス・マスクは、16 進法で入力する数字の列で、パケットのアドレスと比較するのに使用されます。マスクは、指定された MAC アドレスと比較する前に、パケットの SOURCE または DESTINATION MAC アドレスに適用されます。

アドレス・マスクは、MAC アドレスと長さが等しくなければならず、指定の MAC アドレスと等しいかどうかを比較する前に MAC アドレス内のバイトとの論理積を取るバイトを指定します。マスクが指定されていない場合は、オール 1 として想定されます。

フィルター・リスト・パラメーター

次のパラメーターは、フィルター・リスト (filter-list) を構成するのに使用されます。

- 名前: an *ASCII-string*
- フィルター項目リスト: *filter-item 1 . . . filter-item n*
- アクション: INCLUDE、EXCLUDE、TAG(*n*)

フィルター・リストは、1 つまたは複数のフィルター項目で構成されます。各フィルター・リストには、固有の名前が与えられます。

パケットにフィルター・リストを適用するということは、各フィルター項目を、リストに追加された順序で比較することを表します。リスト内の任意のフィルター項目が TRUE 条件を戻した場合、フィルター・リストはそれに指定されているアクションを戻します。

フィルター・パラメーター

次のパラメーターは、フィルターを構成するのに使用されます。

- フィルター・リスト名: *ASCII-string 1 . . . ASCII-string n*

- インターフェース番号: *IFC-number*
- ポート方向: INPUT または OUTPUT
- デフォルト・アクション: INCLUDE、EXCLUDE、または TAG
- デフォルト・タグ: *tag-value*

フィルターの構成は、1 組のフィルター・リスト名をインターフェース番号に対応付け、INPUT または OUTPUT を指定することによって行います。フィルターをパケットに適用するということは、対応付けられたフィルター・リストのそれぞれを、指定の番号のインターフェースで受信 (INPUT) または送信 (OUTPUT) されるパケットに適用することを意味しています。

フィルターがパケットを INCLUDE 条件と評価した場合、そのパケットは転送されます。フィルターがパケットを EXCLUDE 条件と評価した場合、そのパケットはドロップされます。フィルターが TAG 条件と評価した場合、対象のパケットはタグを付けて転送されます。

各フィルターの追加パラメーターとして、デフォルト・アクションがあります。これは、フィルター・リストのすべてが一致しなかった結果として取られるアクションです。このデフォルト値は INCLUDE ですが、INCLUDE、EXCLUDE、または TAG を設定できます。デフォルト・アクションが TAG の場合は、タグ値も指定します。

MAC フィルター・タグの使用

次に、MAC フィルター・タグの使用法のいくつかを表示します。

- MAC アドレス・フィルターは、タグを使用して、帯域幅予約と MAC フィルター・フィーチャー (MCF) が共同で処理します。帯域幅予約を使用しているユーザーは、たとえばブリッジ・トラフィックにタグを割り当て、それを分類することができます。
- タグ付けプロセスは、MAC フィルター構成コンソールでフィルター項目を作成し、それにタグを割り当てます。次に、このタグを使用して、このタグに関連するすべてのパケットを対象にした帯域幅クラスを設定します。タグ値は、現行は 1 ～ 64 の範囲でなければなりません。
- MAC フィルター構成プロセスでタグ付きフィルターを作成したら、帯域幅予約 (BRS) **tag** 構成コマンドを使用して、MAC フィルター・タグ番号に BRS タグ名 (TAG1、TAG2、TAG3、TAG4、または TAG5) を割り当てます。次に、BRS **assign** 構成コマンドでこの BRS タグ名を使用して、対応する MAC フィルターを帯域幅トラフィック・クラスと優先順位に割り当てます。
- 最高 5 つのタグ付き MAC アドレスを、1 ～ 5 の値に設定することができます。TAG1 が最初に検索され、次に TAG2 という具合に TAG5 まで続けられます。

タグによって、IP トンネルの『グループ』を参照することもできます。MAC アドレス・フィルターのタグ付けフィーチャーを使用して、パケットを特定のグループに割り当てることによって、IP トンネルのエンドポイントを任意の数のグループに所属させることができます。

第4章 MAC フィルターの構成と監視

この章では、MAC フィルターの構成および監視プロンプトにアクセスする方法、および利用可能なコマンドの使用法について説明します。この章には、次の内容が記載されています。

MAC フィルター構成プロンプトへのアクセス

MAC フィルター構成コマンドにアクセスするには、CONFIG プロセスから **feature** コマンドを使用します。**feature** コマンドを使用すると、プロトコルおよびネットワーク・インターフェースの構成プロセスの外部の特定フィーチャーの構成コマンドにアクセスできます。

feature コマンドの後に疑問符を入力すると、使用しているソフトウェア・リリースで利用可能なフィーチャーのリストを入手できます。たとえば、次のようになります。

```
Config> feature ?
WRS
BRS
MCF
Feature name or number [MCF]?
```

MAC フィルター構成プロンプトにアクセスするには、**feature** コマンドに続けて *feature number* (3) または *short name* (MCF) を入力します。たとえば、次のようになります。

```
Config> feature mcf
MAC Filtering user configuration
Filter config>
```

MAC フィルター構成プロンプトにアクセスしたら、特定の構成コマンドの入力を開始することができます。MAC フィルター構成プロンプトから **exit** コマンドを入力すれば、いつでも CONFIG プロンプトに戻ることができます。

MAC フィルター構成コマンド

ここでは、MAC フィルター構成コマンドの要約を示します。これらのコマンドは `Filter config>` プロンプトで入力します。

次のコマンドを使用して、MAC フィルター・フィーチャーを構成します。

表 6. MAC フィルター構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Attach	フィルター・リストをフィルターに追加します。
Create	フィルター・リスト、あるいは INPUT または OUTPUT フィルターを作成します。

表 6. MAC フィルター構成コマンドの要約 (続き)

コマンド	機能
Default	指定されたデフォルト・アクションを EXCLUDE、INCLUDE、または TAG に設定します。
Delete	フィルター・リストに関連するすべての情報を除去します。create filter コマンドを使用して作成されたフィルターも削除します。
Detach	フィルター・リストをフィルターから除去します。
Disable	MAC フィルター全体を使用不可にするか、または特定のフィルターを使用不可にします。
Enable	MAC フィルター全体を使用可能にするか、または特定のフィルターを使用可能にします。
List	ユーザーによって構成されたすべてのフィルター・リストおよびフィルターの要約を表示します。このフィルターに追加されたフィルター・リストのリスト、およびフィルターに関するすべての後続情報も生成します。
Move	指定のフィルターに追加されたフィルター・リストを配列し直します。
Reinit	ルーターの残りの部分に影響を与えずに、更新された構成から MAC フィルター・システム全体を再初期設定します。
Set-Cache	フィルターのキャッシュ・サイズを変更します。
Update	特定のフィルター・リストの情報を追加または削除します。該当するサブコマンドのメニューが表示されます。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Attach

attach コマンドは、フィルター・リストをフィルターに追加するのに使用します。

フィルターの構成は、1 組のフィルター・リストをインターフェース番号に関連付けることによって行います。フィルター・リストは、1 つまたは複数のフィルター項目で構成されます。

構文:

attach *filter-list-name filter-number*

Create

create コマンドは、フィルター・リスト、あるいは INPUT または OUTPUT フィルターを作成するのに使用します。

構文:

create list *filter-list-name*

filter [input or output] *interface-number*

list *filter-list-name*
フィルター・リストを作成します。リストには、ユーザーが選択した最大 16 文字の固有のストリング (Filter-list-name) の名前を付けます。この名前は、作成しているフィルター・リストを識別するのに使用します。また、この名前は、そのフィルター・リストに関連した他のコマンドでも使用されます。

filter [input or output] *interface-number*
フィルターを作成し、それをインターフェース番号で指定されたインターフェース上の INPUT または OUTPUT 方向に対応するネットワークに置きま

す。デフォルトでは、このフィルターはフィルター項目を付加せずに作成され、デフォルト・アクションは INCLUDE であり、ENABLED にされます。

Default

default コマンドは、指定されたフィルター番号を持つフィルターのデフォルト・アクションを EXCLUDE、INCLUDE、または TAG に設定するのに使用します。

構文:

default exclude *filter-number*

include *filter-number*

tag *tag-number filter-number*

exclude *filter-number*
指定されたフィルター番号のフィルターのデフォルト・アクションを EXCLUDE に設定します。

include *filter-number*
指定されたフィルター番号のフィルターのデフォルト・アクションを INCLUDE に設定します。

tag *tag-number filter-number*
指定されたフィルター番号のフィルターのデフォルト・アクションを TAG に設定し、関連のタグ値をタグ番号に設定します。

Delete

delete コマンドは、フィルター・リストに関連するすべての情報を除去し、割り当てられた名前を新規フィルター・リストの名前として解放するのに使用します。ユーザーがすでに作成したフィルターにフィルター・リストが付いている場合、このコマンドは何も削除せずに、コンソールにエラー・メッセージを表示します。また、このリストに属するすべてのフィルター項目も削除されます。

create filter コマンドを使用して作成されたフィルターも、このコマンドで削除されます。

構文:

delete list *filter-list*

filter *filter-number*

list *filter-list*
フィルター・リストに関連するすべての情報を除去し、割り当てられたストリングを新規フィルター・リストの名前として解放します。フィルター・リストは、以前に **create list** コマンドで入力されたストリングでなければなりません。

ユーザーがすでに作成したフィルターにフィルター・リストが付いている場合、このコマンドは何も削除せずに、コンソールにエラー・メッセージを表示します。このコマンドが使用されると、このリストに属しているすべてのフィルター項目も削除されます。

filter *filter-number*
create filter コマンドを使用して作成されたフィルターを削除します。

Detach

detach コマンドは、フィルター・リスト名 (filter-list パラメーター) をフィルター (filter-number パラメーター) から削除するのに使用します。

構文:

detach *filter-list-name filter-number*

Disable

disable コマンドは、MAC フィルター全体を使用不可にするか、または特定のフィルターを使用不可にするのに使用します。

構文:

disable all
filter *filter-number*

all MAC フィルター全体を使用不可にします。ただし、前に使用可能にされたフィルターは、ENABLED として設定されたままになります。

filter *filter-number*
特定のフィルターを使用不可にします。filter-number パラメーターは、**list filters** コマンドで表示された番号に対応します。

Enable

enable コマンドは、MAC フィルター全体を使用可能にするか、または特定のフィルターを使用可能にするのに使用します。

構文:

enable all
filter *filter-number*

all MAC フィルター全体を使用可能にします。ただし、フィルター自体は DISABLED に設定されたままになる場合もあります。

filter *filter-number*
特定のフィルターを使用可能にします。filter-number パラメーターは、**list filters** コマンドで表示された番号に対応します。

List

list コマンドは、ユーザーによって構成されたすべてのフィルター・リストとフィルターの要約を表示するのに使用します。フィルターに付けられたすべてのフィルター・リストのリストは表示されません。その他に、次の情報が表示されます。

- フィルター・システムの状態 (ENABLE, DISABLE) が入っているリスト
- 構成済みフィルター・リスト・レコードの集合
- 個々の構成済みフィルター・レコード

さらに、各フィルターについて、次の情報が表示されます。

- フィルター番号
- インターフェース番号
- フィルターの方向 (INPUT、OUTPUT)
- フィルターの状態 (ENABLE、DISABLE)
- フィルターのデフォルト・アクション (TAG、INCLUDE、EXCLUDE)

このコマンドは、フィルターに付加されたフィルター・リストのリスト、およびフィルターに関するすべての後続情報も生成します。

構文:

list all

filter *filter-number*

all 構成されたすべてのフィルター・リストおよびフィルターの要約を表示します。

filter *filter-number*
指定されたフィルターに付加されたフィルター・リストのリスト、およびそのフィルターに関するすべての後続情報を生成します。

Move

move コマンドは、指定されたフィルター (filter-number パラメーターによって示される) に追加されたフィルター・リストを配列し直すのに使用します。
Filter-list-name1 によって示されるリストは、Filter-list-name2 によって示されるリストの直前に移動されます。

構文:

move *filter-list-name1 filter-list-name2 filter-number*

Reinit

reinit コマンドは、ルーターの残りの部分に影響を与えずに、更新された構成から MAC フィルター・システム全体を再初期設定するのに使用します。

構文:

reinit

Set-Cache

set-cache コマンドは、デフォルトのキャッシュ・サイズ (16) を 4 ～ 32768 の範囲の数に変更するのに使用します。

構文:

set-cache *cache-size filter-number*

Update

update コマンドは、特定のフィルター・リストを情報を追加または削除するのに使用します。必要なフィルター・リスト名を指定してこのコマンドを使用すると、そ

の特定フィルター・リストの Filter filter-list-name Config> プロンプトが表示されます。こうして表示された新たなプロンプトから、指定されたリストの情報を変更することができます。

新たに表示されたプロンプト・レベルを使用して、フィルター・リストにフィルター項目を追加または削除します。フィルター・リストにフィルター項目を指定する順序は重要です。それによって、フィルター項目がパケットに適用される順序が決まるからです。

構文:

update *filter-list-name*

更新サブコマンド

ここでは、MAC フィルター構成サブコマンドの要約を示します。これらのサブコマンドは Filter filter-list-name config> プロンプトで入力します。

表 7. 更新サブコマンドの要約

サブコマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add	発信元または宛先 MAC アドレス・フィルターまたはウィンドウ・フィルターを追加します。フィルター項目をフィルター・リストに追加します。
Delete	フィルター項目をフィルター・リストから削除します。
List	ユーザーによって構成されたすべてのフィルター・リストとフィルターの要約を表示します。このフィルターに付加されたフィルター・リストのリスト、およびフィルターに関するすべての後続情報も生成します。
Move	指定されたフィルターに付加されたフィルター・リストを配列し直します。
Set-Action	INCLUDE、EXCLUDE、または TAG (タグ番号オプション付き) 条件を評価するように、フィルター項目を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

次のサブコマンドを使用して、フィルター・リストを更新します。

Add

add サブコマンドは、フィルター項目をフィルター・リストに追加するのに使用します。このサブコマンドでは特別に、発信元または宛先 MAC アドレスと比較するための 16 進数を追加したり、あるいはパケット・データと比較するためのマスク付きの一連のウィンドウ・データを追加したりすることができます。

フィルター・リストにフィルター項目を指定する順序は重要です。それによって、フィルター項目がパケットに適用される順序が決まるからです。

add サブコマンドを使用するたびに、フィルター・リスト内にフィルター項目が作成されます。最初に作成されたフィルター項目にはフィルター項目番号 1 が割り当てられ、次の項目には番号 2 が割り当てられるというようになります。**add** サブコマンドを正常に入力すると、ルーターは追加されたばかりのフィルター項目の番号を表示します。

最初の一致が見つかると、フィルター項目の適用は停止され、フィルター・リストの指定のアクションに基づいて、フィルター・リストは INCLUDE、EXCLUDE、または TAG に評価します。フィルター・リストのどのフィルター項目にも一致しない場合には、フィルターのデフォルト・アクション (INCLUDE、EXCLUDE、または TAG) が戻されます。

構文: add

source *hex-MAC-addr hex-Mask*

destination *hex-MAC-addr hex-Mask*

window MAC *offset-value hex-data hex-mask*

window INFO *offset-value hex-data hex-mask*

source *hex-MAC-addr hex-Mask*

発信元 MAC アドレスと比較するための 16 進数を追加します。***hex-MAC-addr*** は、最大 16 桁の偶数の 16 進数で、前に 0x を付けずに入力する必要があります。

hex-mask パラメーターは hex-MAC-address と同じ長さであることが必要であり、パケット内の指定された MAC アドレスと論理 AND されます。デフォルトの hex-mask 引き数は、すべてが 2 進数の 1 になります。

hex-MAC-addr パラメーターは、標準または非標準のビット配列で指定することができます。標準ビット配列は、単に 16 進数として指定します (たとえば、000003001234)。一連の 16 進数を 2 桁ずつハイフン (-) で区切って表すこともできます (たとえば、00-00-03-00-12-34)。

非標準ビット配列は、一連の 16 進数を 2 桁ずつコロン (:) で区切って指定します (たとえば、00:00:C9:09:66:49)。フィルター項目の MAC は、標準表記と非標準表記を区別するために、常にハイフン (-) またはコロン (:) のいずれかを使用して表示します。

destination *hex-MAC-addr hex-Mask*

照合の対象がパケットの発信元 MAC アドレスではなく、宛先 MAC アドレスであることを除いて、add source サブコマンドと同様に機能します。

window MAC *offset-value hex-data hex-mask*

マスク付き 16 進数をパケット・データに照合するための指定のオフセット (フレームの先頭から計算された) を使用して、スライディング・ウィンドウ・フィルター項目を追加します。

window INFO *offset-value hex-data hex-mask*

オフセットが情報フィールドの先頭から計算されることを除いて、**add window mac** コマンドと同様です。

Delete

delete サブコマンドは、フィルター項目をフィルター・リストから除去するのに使用します。フィルター項目を削除するには、その項目を追加したときに割り当てたフィルター項目番号を指定します。

delete サブコマンドが使用されたときに生じた番号順のすき間は埋められます。たとえば、フィルター項目 1、2、3、および 4 が存在し、フィルター項目 3 が削除された場合、フィルター項目 4 の番号が 3 に変更されます。

MAC フィルターの構成

構文:

delete *filter-item-number*

List

list サブコマンドは、すべてのフィルター項目レコードのリストを印刷出力するのに使用します。各 MAC アドレス・フィルター項目に関する次の情報が表示されます。

- 標準形式および非標準形式の MAC アドレスとアドレス・マスク
- フィルター項目番号
- アドレス・タイプ (発信元または宛先)
- フィルター・リストのアクション

構文:

list canonical

noncanonical

mac-address canonical

mac-address noncanonical

window

canonical

フィルター・リスト内のすべてのフィルター項目レコードのリストを印刷出力して、項目番号、アドレス・タイプ (SRC、DST)、標準形式 MAC アドレス、および標準形式アドレス・マスクを表示します。フィルター・リストのアクションも示されます。

mac-address canonical

フィルター・リスト内のすべてのフィルター項目レコードのリストを印刷出力して、項目番号、アドレス・タイプ (SRC、DST)、標準形式 MAC アドレス、および標準形式アドレス・マスクを表示します。フィルター・リストのアクションも示されます。

noncanonical

フィルター・リスト内のすべてのフィルター項目レコードのリストを印刷出力して、項目番号、アドレス・タイプ (SRC、DST)、非標準形式 MAC アドレス、および非標準形式アドレス・マスクを表示します。フィルター・リストのアクションも示されます。

mac-address noncanonical

フィルター・リスト内のすべてのフィルター項目レコードのリストを印刷出力して、項目番号、アドレス・タイプ (SRC、DST)、非標準形式 MAC アドレス、および非標準形式アドレス・マスクを表示します。フィルター・リストのアクションも示されます。

window

フィルター・リスト内のすべてのスライディング・ウィンドウ・フィルター項目レコードのリストを印刷出力して、項目番号、基底、オフセット、データ、およびマスクを表示します。フィルター・リストのアクションも示されます。

Move

move サブコマンドは、フィルター・リスト内のフィルター項目を配列し直します。番号が *filter-item-name1* によって指定されているフィルター項目は、*filter-item-name2* の直前に移動され、番号が付け直されます。

構文:

move *filter-item-name1 filter-item-name2*

Set-Action

set-action サブコマンドは、INCLUDE、EXCLUDE、または TAG (タグ番号オプション付き) 条件を評価するように、フィルター項目を設定することができます。フィルター・リストのフィルター項目の 1 つが、フィルター対象と見なされるパケットのコンテンツに一致している場合、フィルター・リストは指定された条件に評価します。デフォルト設定値は INCLUDE です。

構文:

set-action [INCLUDE or EXCLUDE or TAG] *tag-number*

MAC フィルター監視プロンプトへのアクセス

MAC フィルター監視コマンドにアクセスするには、GWCON プロセスから **feature** コマンドを入力します。**feature** コマンドを使用すると、プロトコルおよびネットワーク・インターフェースの監視プロセスの外部の特定ルーター機能の監視コマンドにアクセスできます。

feature コマンドの後に疑問符を入力すると、使用しているソフトウェア・リリースで利用可能なフィーチャーのリストを入手できます。たとえば、次のようになります。

```
+ feature ?
WRS
BRS
MCF
```

MAC フィルター監視プロンプトにアクセスするには、**feature** コマンドに続けて、フィーチャー番号 (3) または短縮名 (MCF) を入力します。たとえば、次のようになります。

```
+ feature mcf
MAC Filtering user monitoring
Filter>
```

MAC フィルター監視プロンプトにアクセスしたら、特定の監視コマンドの入力を開始することができます。MAC フィルター監視プロンプトから **exit** コマンドを入力すれば、いつでも GWCON プロンプトに戻ることができます。

MAC フィルター監視コマンド

ここでは、MAC フィルター監視コマンドの要約を示します。次のコマンドは Filter> プロンプトで入力します。

表 8. MAC フィルター監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Clear	list filter コマンドでリストされた "フィルター単位" 統計をクリアします。
Disable	MAC フィルターをグローバルに使用不可にするか、または "フィルター単位 " で使用不可にします。
Enable	MAC フィルターをグローバルに使用可能にするか、または "フィルター単位 " で使用可能にします。
List	現在ルーターで実行されている各フィルターの統計および設定値の要約を表示します。
Reinit	ルーターの残りの部分に影響を与えずに、更新された構成から MAC フィルター・システム全体を再初期設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

次のコマンドを使用して、MAC フィルター・フィーチャーを監視します。

Clear

clear コマンドは、フィルター統計をクリアするのに使用します。

構文:

clear all

filter *filter-number*

all **list all** コマンドによって表示された統計をクリアします。

filter *filter-number*
list filter コマンドによって表示された統計をクリアします。

Disable

disable コマンドは、MAC フィルターをグローバルに使用不可にするのに使用します。このコマンドは、各フィルターを個別には使用不可にしません。

このコマンドは、フィルター番号によって指定されたフィルターも使用不可にします。このフィルターは、構成レコードを変更せずに、使用不可にされます。引き数が指定されていない場合、MAC フィルターはグローバルに使用不可にされます。

構文:

disable all

filter *filter-number*

all MAC フィルターをグローバルに使用不可にします。このコマンドは、各フィルターを個別には使用不可にしません。

filter ***filter-number***
フィルター番号によって指定されたフィルターを使用不可にします。このフィルターは、構成レコードを変更せずに、使用不可にされます。フィルター番号が指定されていない場合、MAC フィルターはグローバルに使用不可にされます。

Enable

enable コマンドは、MAC フィルターをグローバルに使用可能にするのに使用します。このコマンドは、各フィルターを個別には使用可能にしません。

このコマンドは、フィルター番号によって指定されたフィルターも使用可能にします。このフィルターは、構成レコードを変更せずに、使用可能にされます。引き数が指定されていない場合、MAC フィルターはグローバルに使用可能にされます。

構文:

enable all
filter *filter-number*

all MAC フィルターをグローバルに使用可能にします。このコマンドは、各フィルターを個別には使用可能にしません。

filter *filter-number*
フィルター番号によって指定されたフィルターを使用可能にします。このフィルターは、構成レコードを変更せずに、使用可能にされます。フィルター番号が指定されていない場合、MAC フィルターはグローバルに使用可能にされます。

List

list コマンドは、現在ルーターで実行されている各フィルターの統計および設定値の要約を表示するのに使用します。**list all** コマンドを使用すると、各フィルターの次の情報が表示されます。
- デフォルト・アクション
- キャッシュ・サイズ
- デフォルト・タグ
- 状態 (使用可能 / 使用不可)
- INCLUDE、EXCLUDE、または TAG としてフィルターされたパケットの数

さらに、指定のフィルターに対する **list filter** コマンドでは、次の情報も表示されます。
- list all コマンドによって表示されるすべての情報
- 現在このフィルターで実行されているすべてのフィルター・リスト。次のものが含まれます。
  - リスト名
  - リスト・アクション
  - リスト・タグ
  - 各フィルター・リストによってフィルターされたパケットの数

構文:

list all

filter *filter-number*

all 現在ルーターで実行されている各フィルターの統計および設定値を表示します。

filter *filter-number*
各フィルターの統計および設定値に加えて、現在このフィルターで実行されているすべてのフィルター・リストの統計および設定値を生成します。

Reinit

reinit コマンドは、ルーターの残りの部分に影響を与えずに、更新された構成から MAC フィルター・システム全体を再初期設定するのに使用します。

構文:

reinit

MAC フィルター動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

MAC フィルターは、CONFIG (Talk 6) **delete interface** コマンドを制限なしでサポートします。

GWCON (Talk 5) Activate Interface

MAC フィルターは、GWCON (Talk 5) **activate interface** コマンドをサポートしますが、次の考慮が必要です。

新たに活動化されたインターフェースに定義された MAC フィルターがある場合には、それぞれのインターフェースごとにすべての MAC フィルターが再初期設定されます。

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

GWCON (Talk 5) Reset Interface

MAC フィルターは、GWCON (Talk 5) **reset interface** コマンドをサポートしますが、次の考慮が必要です。

新たにリセットされたインターフェースに定義された MAC フィルターがある場合には、それぞれのインターフェースごとにすべての MAC フィルターが再初期設定されます。

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

GWCON (Talk 5) 構成要素リセット・コマンド

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

GWCON, Feature MCF, Reinit コマンド

説明: すべての構成済み MAC フィルターを動的に再初期設定します。

ネットワークへの影響:
なし。

制限事項:
なし。

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

CONFIG (Talk 6) Activate コマンド

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

CONFIG, Feature MCF, Reinit コマンド

説明: すべての構成済み MAC フィルターを動的に再初期設定します。

ネットワークへの影響:
なし。

制限事項:
なし。

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

第5章 WAN レストラルの使用

この章には、次の内容が記載されています。

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

WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローの各フィーチャーは、機能が似ているので混同する可能性があります。ここでは、いずれの機能がユーザーにとって便利であるかを判断し、それを構成するのに必要な情報を見つけるのに役立つ事柄を概説します。

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

WAN レストラル

WAN レストラルは、最も基本的なフィーチャーです。WAN レストラルを使用する場合は、1 次リンクと 2 次リンクを構成します。1 次リンクに障害が起きた場合、2 次リンクがスタートし、1 次の特性を引き継ぎます。2 次リンクは 1 次リンクからのプロトコル定義を使用するので、2 次リンクにプロトコル定義を構成する必要はありません。

WAN レストラルの場合:

- 1 次リンクと 2 次リンクがペアになっています。
- 1 つの 1 次リンクだけが特定の 2 次リンクを使用するように構成できます。
- 2 次リンクではプロトコル定義 (たとえば、プロトコル・アドレス) を構成しません。
- 1 次リンクには、PPP シリアル・インターフェースまたはマルチリンク・インターフェースを使用することができます。PPP ダイヤル回線インターフェースは使用できません。
- 2 次リンクは、PPP ダイヤル回線またはマルチリンク PPP インターフェースでなければなりません。
- **enable wrs** コマンドを使用して、WRS フィーチャーを使用可能にする必要があります。
- **enable secondary-circuit** コマンドを使用して、1 次 / 2 次のペアを使用可能にする必要があります。

WAN レストラルの使用

注: 1 次リンクに BRS が構成されており、その 1 次リンクが WAN レストラルの 1 次 / 2 次のペアの片方である場合、2 次リンクにも BRS を構成する必要があります。通常は、WAN レストラルが構成されている場合には、2 次リンクは 1 次リンクと同じ機能を引き継ぎます。しかし BRS については、これは該当しません。そのため、BRS は 1 次リンクと 2 次リンクの両方で構成する必要があります。

WAN リルート

WAN リルートは、より拡張された機能です。WAN リルートを使用する場合は、1 次リンクと代替リンクを構成します。1 次リンクに障害が起きた場合、代替リンクがスタートします。ルーティング・プロトコル (たとえば、RIP または OSPF) は、新たに利用可能になったリンクを検出し、パケットの転送に使用されるルートを調整します。

WAN リルートの場合:

- 1 次リンクと代替リンクがペアになっています。
- 複数の 1 次リンクが同じ代替リンクを使用するように構成できます。
- 代替リンクでプロトコル定義を構成する必要があります。
- 1 次リンクには、ルート可能プロトコル (たとえば、IP、IPX) を構成できる任意のリンクを使用できます。たとえば、1 次リンクには、LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線を使用することができます。1 次リンクに使用できないインターフェース・タイプの例としては、SDLC シリアル・インターフェース、SRLY シリアル・インターフェース、および V.25bis や ISDN のような基本ネットがあります。
- 代替リンクは、ルート可能プロトコル (たとえば、IP、IPX) を構成できる任意のリンクを使用することができ、代替リンクのデータ・リンク・タイプは、1 次リンクのデータ・リンク・タイプと一致している必要はありません。たとえば、代替リンクには、LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線などを使用できます。代替リンクに使用できないインターフェース・タイプの例としては、SDLC シリアル・インターフェース、SRLY シリアル・インターフェース、および V.25bis や ISDN のような基本ネットがあります。
- 1 次リンクがダイヤル回線である場合は、代替リンクは、ダイヤル・オンデマンド・ダイヤル回線であってはなりません。ダイヤル回線がダイヤル・オンデマンド・サーキット回線でないように構成するには、そのダイヤル `Circuit Config>` プロンプトに **set idle 0** を指定して構成する必要があります。詳細については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の『ダイヤル回線の構成および監視』を参照してください。

  I.430、I.431、およびチャネル化 T1/E1 ダイヤル回線は暗黙的に固定されているので、WRS 1 次として使用できます。

  注: I.430/I.431 およびチャネル化 T1/E1 ダイヤル回線は、明示的に構成することなく、WRS 1 次として使用することができます。
- **enable wrs** コマンドを使用して、WRS フィーチャーを使用可能にする必要があります。

- **enable alternate-circuit** コマンドを使用して、1 次 / 代替のペアを使用可能にする必要があります。
- オプションで、1 次リンクへの復帰を制御するための安定化時間、ルーティング安定化時間、および復帰開始時刻と終了時刻も構成できます。
- 代替リンクが X.25 の場合、WAN リルートを使用可能にしたルーターの X.25 インターフェースを構成するときは **national-personality set disconnect-procedure active** コマンドを使用し、他方のルーターの X.25 インターフェースを構成するときは **national-personality set disconnect-procedure passive** コマンドを使用することが必要です。

ダイヤル・オン・オーバーフロー

ダイヤル・オン・オーバーフローは WAN リルートに似ていますが、1 次リンクに障害が起きなくても、代替リンクをスタートさせることができます。1 次リンクの使用状況を監視し、限界値を超えると、代替リンクがスタートします。すべてのプロトコルが代替リンクで起動されるわけではありません。IP だけが代替リンクで起動され、その他のプロトコルは、1 次リンクがダウンしない限り、引き続き 1 次リンクを使用します。

1 次リンクがダウンすると、WAN リルートが引き継ぎ、代替インターフェース上に構成されているプロトコルが、代替インターフェース上のルートを検出し、そのルートを使い始めることができます。

ダイヤル・オン・オーバーフローの場合:

- ダイヤル・オン・オーバーフローは、WAN リルートの組み合わせである 1 次 / 代替のペアを使用します。
- ダイヤル・オン・オーバーフローを使用するためには、WAN リルートのペアを構成する必要があり、WAN リルート構成のすべての制約が適用されます。
- ダイヤル・オン・オーバーフローに使用される WAN リルートのペアの 1 次リンクは、フレーム・リレーでなければなりません。
- ダイヤル・オン・オーバーフローを使用するためには、OSPF ルーティング・プロトコルを使用することが必要です。
- **enable dial-on-overflow** コマンドを使用して、追加限界値と廃棄限界値、帯域幅監視間隔、および最小代替アップ・タイムを構成する必要があります。
- 安定化時間 (Stabilization time)、ルーティング安定化時間 (routing-stabilization time) 、復帰開始時刻 (start-time-of-day-revert-back) および復帰停止時刻 (stop-time-of-day-revert-back) は、ダイヤル・オン・オーバーフローの動作には影響を与えません。

WAN リルートについて詳しくは、97ページの『第7章 WAN リルート・フィーチャー』を参照してください。

始める前に

WAN レストラルを構成する前に、次の用意が必要です。

1. 1 次シリアル・インターフェース (専用回線) が PPP 用に構成されている。ルーター上の任意のシリアル・インターフェースを使用できます。

2. 対応するダイヤル回線をもつインターフェースがルーター上に構成されている。ISDN インターフェースまたは V.25bis インターフェースを基本ネットとして使用することができます。
3. 2 次ダイヤル回線が、1 次インターフェースがダウンしたときにダイヤルするように構成されている。ダイヤル回線をこのように構成するには、ダイヤル Circuit Config> プロンプトで **set idle** コマンドを使用して、アイドル・タイマーをゼロに設定します。このコマンドを指定すると、ダイヤル回線はダイヤル・オンデマンドになりません。
4. リンクの一方の端の 2 次ダイヤル回線が発信専用に構成されている。Circuit Config> プロンプトで **set calls outbound** コマンドを使用して構成します。

   注: 2 次インターフェースにはプロトコル・アドレスを構成しないでください。2 次リンク (ダイヤル回線) が活動状態になると、1 次インターフェースのプロトコル割り当てが使用されます。
5. リンクの他方の端の 2 次ダイヤル回線が受信専用に構成されている。Circuit Config> プロンプトで **set calls inbound** コマンドを使用して構成します。

WAN レストラルの構成手順

ここでは、WAN レストラルを構成するのに必要な手順について説明します。構成を開始する前に、Config> プロンプトで **list device** コマンドを使用して、種々の装置のインターフェース番号を表示します。

次のステップに従って、ルーター上の WAN レストラルを構成します。

1. Config> プロンプトで **feature wrs** コマンドを入力して、WRS Config> プロンプトを表示する。たとえば、次のようになります。

```
Config>feature wrs
WAN Restoral user configuration
WRS Config>
```

2. 1 次インターフェースに 2 次ダイヤル回線を割り当てる。このダイヤル回線は、1 次インターフェースをバックアップします。たとえば、次のようになります。

```
WRS Config>add secondary-circuit
Secondary interface number  [0]? 3
Primary interface number  [0]? 1
```

3. 追加した 2 次ダイヤル回線上の WAN レストラルを使用可能にする。たとえば、次のようになります。

```
WRS Config>enable secondary-circuit
Secondary interface number  [0]? 3
```

4. ルーター上の WAN レストラルをグローバルに使用可能にする。たとえば、次のようになります。

```
WRS Config>enable wrs
```

5. ルーターをリスタートして、構成変更を有効にする。

2 次ダイヤル回線の構成

ダイヤル回線を構成するには、次の手順で行います。

1. ダイヤル回線インターフェース番号を調べる。これを行うには、次のように入力します。

```
Config> list device
```

PPP ダイヤル回線インターフェースがリストされない場合は、次のように入力して、ダイヤル回線インターフェースを追加します。

```
Config> add device dial-circuit

Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
```

2. Config> プロンプトから次のように入力して、2 次インターフェース (ダイヤル回線) が 1 次インターフェース (PPP) と同じデータ・リンク・タイプを持つように構成する。

```
Config> set data PPP
Interface Number [0]? 3
```

3. **network** *interface#* を入力して、ダイヤル回線構成プロンプト (Circuit Config>) にアクセスする。

```
Config> network 3
```

4. ダイヤル回線の基本ネット・インターフェースを選択する。基本ネットは V.25bis、または ISDN です。

```
Circuit Config> set net 2
```

5. ダイヤル回線アイドル・タイマーを 0 (0 = 固定) に設定するために、次のように入力する。

```
Circuit Config> set idle 0
```

6. バックアップ・コネクションの一方の端 (たとえば、ルーター A) を受信用に設定するために、次のように入力する。

```
Circuit Config> set calls inbound
```

7. バックアップ・コネクションの他方の端 (たとえば、ルーター B) を発信用に設定するために、次のように入力する。

```
Circuit Config>  set calls outbound
```

注:

1. **set calls both** コマンドは使用しないでください。これらを個別に設定することにより、着信と発信の接続試行が衝突するのを防止できます。
2. ダイヤル回線には、転送プロトコル (たとえば、IP、IPX など) アドレスは構成しないでください。2 次インターフェース (ダイヤル回線) が活動状態になると、1 次インターフェースのプロトコル割り当てが使用されます。
3. ISDN の構成方法については、*Nways* マルチプロトコル・アクセス・サービス ソフトウェア*使用者の手引き* の 『ISDN インターフェースの使用』の項を参照してください。
4. V.25 の構成方法については、*Nways* マルチプロトコル・アクセス・サービス ソフトウェア*使用者の手引き* の 『V.25 インターフェースの使用』の項を参照してください。

第6章 WAN レストラルの構成と監視

この章では、WAN レストラルの構成コマンドおよび作動可能コマンドについて説明します。この章には、次の内容が記載されています。

- 83ページの『WAN レストラル・インターフェース監視プロセスへのアクセス』
- 83ページの『WAN レストラル監視コマンド』
- 94ページの『WAN レストラルおよび WAN レストラル動的再構成サポート』

注: ダイヤル回線の構成については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の『ダイヤル回線の構成および監視』を参照してください。ダイヤル回線は、WAN リルートを構成する際にインターフェースとして使用できます。

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

WAN レストラル構成コマンドを用いて、WAN レストラル・インターフェース構成を作成または変更することができ ます。ここでは、WAN レストラル構成コマンドの要約を示し、個々のコマンドについて説明します。

表9 は、WAN レストラル構成コマンドとそのフィーチャーを表示しています。これらのコマンドは `WRS Config>` プロンプトで入力します。`WRS Config>` にアクセスするには、`Config>` プロンプトで **feature wrs** と入力します。

表 9. WAN レストラル構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add	1 次から 2 次へ (WAN レストラルの場合) または 1 次から代替へ (WAN リルートの場合) のマッピングを追加します。
Disable	WRS、個々の 2 次回線マッピング、または代替回線マッピングを使用不可にします。
Enable	WRS、個々の 2 次回線マッピング、または代替回線マッピングを使用可能にします。
List	現行の復元構成を表示します。
Remove	add によって作成された 1 次から 2 次へのマッピングまたは 1 次から代替へのマッピングを除去します。
Set	安定化 (stabilization) タイマー、ルート安定化 (route-stabilization)、および復帰時刻 (time-of-day-revert-back) タイマーの値を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Add

add コマンドは、2 次または代替ダイヤル回線、あるいは 1 次シリアル・リンクの専用リンク・インターフェースを識別するのに使用します。

構文:

add alternate-circuit

secondary-circuit

alternate-circuit

add alternate-circuit コマンドは、WAN リルートのために、代替インターフェースを 1 次インターフェースに結合します。複数の 1 次リンクを単一の代替インターフェースに割り当てることができます。代替リンク・タイプは、1 次リンク・タイプと同じである必要はありません (たとえば、代替リンク・タイプが PPP ダイヤル回線で、1 次リンク・タイプがフレーム・リレー専用回線であっても構いません)。

例:

```
WRS Config>add alt
Alternate interface number  [0]? 6
Primary interface number [0]? 1
```

Alternate interface number

これは、以前に代替インターフェースに割り当てたインターフェース番号です。任意の LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線を、代替インターフェースとして使用できます。デフォルトは 0 です。

Primary interface number

これは、以前に装置が追加されたときに割り当てられた 1 次インターフェースのインターフェース番号です。1 次インターフェースは、以前に定義された任意の LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線を使用できます。デフォルトは 0 です。

secondary-circuit

add secondary-circuit コマンドは、WAN レストラルのために、2 次インターフェースを 1 次インターフェースに結合します。両方のインターフェースとも、以前に構成されていることが必要です。1 つの 2 次インターフェースを 1 次に (または、その逆に) 割り当てることしかできません。

例:

```
WRS Config>add secondary-circuit
Secondary interface number  [0]? 4
Primary interface number [0]? 1
```

Secondary interface number

これは、以前に装置が追加されたときに、2 次インターフェースに割り当てられたダイヤル回線インターフェース番号です。任意の PPP ダイヤル回線またはマルチリンク PPP インターフェースを、2 次インターフェースとして使用できます。デフォルトは 0 です。

Primary interface number

これは、以前に装置が追加されたときに割り当てられた 1 次インターフェースのインターフェース番号です。1 次インターフェースには、PPP を実行する任意の定義済み専用回線を使用できます。デフォルトは 0 です。

Disable

disable コマンドは、WAN レストラル・フィーチャー、WAN レストラルにおける 1 次 / 2 次のペア、WAN リルートにおける 1 次 / 代替のペア、または 1 次 / 代替のペアに対するダイヤル・オン・オーバーフローを使用不可にするのに使用します。

構文:

disable alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit *interface#*
WAN リルートの 1 次 / 代替のペアを使用不可にします。

例:

```
WRS Config> disable alternate-circuit
Alternate interface number  [0]? 6
```

Alternate interface number
これは、以前に **add alternate-circuit** コマンドを使用して構成された代替インターフェースの番号です。デフォルトは 0 です。

dial-on-overflow *alt-intfc#*
指定された代替リンクを使用するすべての 1 次 / 代替のペアに対するダイヤル・オン・オーバーフローを使用不可にします。

例:

```
WRS Config> disable dial-on-overflow
alternate interface number  [0]? 6
```

Alternate interface number
これは、以前に **add alternate-circuit** コマンドを使用して構成された代替インターフェースの番号です。デフォルトは 0 です。

secondary-circuit *interface#*
WRS コンソールから次の **enable secondary-circuit** コマンドが出されるまで、関連の 2 次インターフェースによる特定の 1 次インターフェースの復元を使用不可にします。両方のインターフェースとも構成済みであり、WRS 構成内で相互が結合されていることが必要です。

例:

```
WRS Config> disable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number
これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

wrs ルーター上の WAN レストラル・フィーチャーをグローバルに使用不可にします。これは、WAN リルートおよびダイヤル・オン・オーバーフローも使用不可にされることを意味しています。

Enable

enable コマンドは、WAN レストラル・フィーチャー、WAN レストラルにおける 1 次 / 2 次のペア、WAN リルートにおける 1 次 / 代替のペア、または 1 次 / 代替のペアに対するダイヤル・オン・オーバーフローを使用可能にするのに使用します。

構文:

enable alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit *interface#*

代替回線を使用可能にします。

例:

```
WRS Config>enable alternate-circuit
Alternate interface number  [0]? 6
```

Alternate interface number

これは、以前に **add alternate-circuit** コマンドを使用して構成された代替インターフェースの番号です。デフォルトは 0 です。

dial-on-overflow

ダイヤル・オン・オーバーフローを使用可能にし、ダイヤル・オン・オーバーフローの動作方法を制御するパラメーターを設定できるようにします。

例:

```
WRS>enable dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate
interface.
Primary interface number  ]0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!
```

Primary interface number

これは、ダイヤル・オン・オーバーフローを使用可能にする 1 次インターフェースのインターフェース番号です。デフォルトは 0 です。

add-threshold

帯域幅の追加のために代替インターフェースを起動する時期を決めます。この値は、1 次インターフェースに構成された回線速度の比率として表すことが必要です。デフォルトは 90% です。

drop-threshold

帯域幅の追加のための代替インターフェースが不要になる時期を決めます。この値は、1 次インターフェースに構成された回線速度の比率として表すことが必要です。デフォルトは 60% です。

bandwidth monitoring interval

add-threshold および *drop-threshold* のために 1 次インターフェースの帯域幅を監視する頻度を決めます。デフォルトは 15 秒です。

Minimum time to keep alternate up

この時間枠には、ローカル・ルーター上の IP トラフィックを代替インターフェースに再ルートするときに、ルーターが新規ルートを確立できる十分な時間を含める必要があります。デフォルトは 5 分です。

secondary-circuit *interface#*

指定された 2 次リンクによる 1 次リンクの復元を使用可能にします。

例:

```
WRS Config> enable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number

これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

wrs ルーター上の WAN レストラル・フィーチャーの機能を使用可能にします。これは、WAN リルートおよびダイヤル・オン・オーバーフローも構成されている場合には、それらも使用可能になることを意味しています。

List

list コマンドは、そのフィーチャーのグローバル構成情報を表示したり、WAN レストラルの 1 次 / 2 次のペア、WAN リルートの 1 次 / 代替のペア、およびダイヤル・オン・オーバーフローに関する構成情報を表示するのに使用します。

構文:

list

例:

```
WRS Config>list all
WAN Restoral is enabled.
Default Stabilization Time:       0 seconds
Default First Stabilization Time: 0 seconds

                                                Secondary
   Primary Interface       Secondary Interface  Enabled
----------------------  ----------------------  --------
 4 - WAN PPP             7 - PPP Dial Circuit       No
                                        Alt.     1st  Subseq TOD Revert Back  Stab
Primary Interface  Alternate Interface  Enabled  Stab  Stab  Start    Stop
-----------------  -------------------  -------  ----  ----  -------  ------- ----

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


Dial-on-overflow is enabled.
Primary    add-       drop-      test       minimum
Interface  threshold  threshold  interval   alt up time
---------  ---------  ---------  ---------  -----------
     1         29%        20%      15 sec.   300 sec.
```

Remove

remove コマンドは、代替インターフェースまたは 2 次 (バックアップ) インターフェースの 1 次インターフェースへのマッピングを削除するのに使用します。

WAN レストラルの構成

構文:

remove alternate-circuit

secondary-circuit

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

WAN リルートの代替 (バックアップ) インターフェースの 1 次インターフェースへのマッピングを除去します。両方のインターフェースとも割り当て済みであり、**add alternate-circuit** コマンドを使用して相互が結合されていることが必要です。

Alternate-interface#

これは、以前に **add alternate-circuit** コマンドを使用して構成された代替インターフェースの番号です。デフォルトは 0 です。

Primary-interface#

これは、以前に 2 次インターフェースに除去され結合された 1 次インターフェースのインターフェース番号です。デフォルトは 0 です。

例:

```
WRS Config> remove alternate-circuit
Alternate interface number  [0]? 3
Primary interface number  [0]? 1
```

secondary-circuit *secondary-interface# primary-interface#*

WAN レストラルの 2 次 (バックアップ) インターフェースの 1 次インターフェースへのマッピングを除去します。両方のインターフェースとも割り当て済みであり、**add secondary-circuit** コマンドを使用して相互が結合されていることが必要です。

Secondary-interface#

これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

Primary-interface#

除去される 2 次インターフェースにバインド済みの 1 次インターフェースのインターフェース番号です。デフォルトは 0 です。

例:

```
WRS Config> remove secondary-circuit
Secondary interface number  [0]? 3
Primary interface number [0]? 1
```

Set

set コマンドは、WAN リルートのパラメーターを設定するのに使用します。

構文:

set ? default

first-stabilization

routing-stabilization

stabilization

start-time-of-day-revert-back

stop-time-of-day-revert-back

デフォルト (default)

set default コマンドは、安定化 (stabilization) 期間および最初の安定化 (first-stabilization) 期間が構成されていないリンクで使用されるデフォルト値を設定するのに使用します。

first-stabilization

最初の安定化時間 (first-stabilization time) が構成されていないリンクで使用されるデフォルトの最初の安定化時間の値を設定します。

```
WRS Config>set default first
Default first primary stabilization time (0 - 3600 seconds)  [0]? 20
```

stabilization

安定化時間 (stabilization time) が構成されていないリンクで使用されるデフォルトの安定化時間の値を設定します。

```
WRS Config>set default stab
Default primary stabilization time (0 - 3600 seconds)  [0]? 30
```

first-stabilization

1 次リンクがアップにならない場合、この 1 次リンクのルーティングを代替リンクに切り替える前の、ルーター初期化の秒数を設定します。

例:

```
WRS Config>set first
Primary interface number [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

First primary stabilization time

この 1 次インターフェースの安定化時間。デフォルトは 1 です。

routing-stabilization

ルーティング安定化 (routing-stabilization) の値を設定します。このパラメーターは、1 次リンクが起動していることが検知され、安定化タイマー (指定されている場合) が満了した後で 1 次リンクと代替リンクの両方が起動したままになっている秒数を定義します。ルーティング安定化時間が与えられると、OSPF または RIP のようなルーティング・プロトコルは新しいルートの可用性を認識する時間が充分与えられます。ルーティング安定化タイマー (routing-stabilization timer) を指定しないと、代替ルートは使用不可になったが 1 次ルートがまだ見つからないという数秒の間トラフィックが中断されることがあります。

代替リンクがリルートより前にアップになっていた場合は、代替リンクはアップのままとなり、ルーティング安定化タイマー (routing-stabilization timer) は無視されます。代替リンクがリルートより前にダウン、あるいはリルート中であった場合は、代替リンクはダウンしたままで、ルーティング安定化タイマー (routing-stabilization timer) および安定化タイマー (stabilization timer) は両方とも無視されます。

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

Primary interface number

有効値 : 0 ～ルーター上に構成されたインターフェースの数

デフォルト値 : 0

Routing-stabilization timer

有効値 : 1 ～ 3600 秒

デフォルト値 : 0

stabilization

1 次リンクが起動していることが最初に検出された後、その 1 次リンク上でのルーティングの再初期設定プロセスが始まるまでに必要な秒数を設定します。ルーティング安定化タイマー (routing-stabilization timer) が設定されていない場合は、stabilization (安定化) タイマーが満了すると、代替リンクはダウンします。ルーティング安定化タイマー (routing-stabilization timer) は、安定化 (stabilization) タイマーが満了すると同時に開始し、代替リンク上にトラフィックを維持するのに充分なだけ 1 次リンクと代替リンクの両方をアップにしておき、この間に OSPF および RIP のようなルーティング・プロトコルは 1 次リンクを介してルートを再確立します。

例:

```
WRS Config>set first
Primary interface number [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

これは、安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Primary stabilization time

1 次インターフェースの安定化時間。デフォルトは 1 です。

start-time-of-day-revert-back

ルーターが 1 次ルートに戻ることができる最も早い時刻。ルーターは、復帰開始時刻 (start-time-of-day-revert-back) と復帰停止時刻 (stop-time-of-day-revert-back) の間の任意の時刻に、1 次に復帰することができます。1 次への復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 0 です。

例:

```
WRS Config>set start
Primary interface number  [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number

これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Time-of-day-revert-back-window start

この時刻は、復帰ウィンドウの開始時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに復帰することができます。1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 1 です。

stop-time-of-day-revert-back

この時刻は、復帰ウィンドウの終了時刻をマークします。ルーターは、復帰

開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに復帰することができます。1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 1 です。

例:

```
WRS Config>set stop
Primary interface number [0]? 1
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured)  [0]?5
```

Primary interface number

これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Time-of-day-revert-back-window stop

この時刻は、復帰ウィンドウの終了時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに復帰することができます。1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 1 です。

WAN レストラル・インターフェース監視プロセスへのアクセス

WAN レストラルインターフェース監視プロセスにアクセスするには、GWCON (+) プロンプトから、次のコマンドを入力します。

```
+ feature wrs
```

WAN レストラル監視コマンド

WAN レストラル (WRS) 監視コマンドを用いて、WAN レストラルの 1 次 / 2 次のペア、WAN リルートの 1 次 / 代替のペア、およびダイヤル・オン・オーバーフローの状態を監視することができます。監視インターフェースを通して行われた WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローの動作状態の変更は、ルーターのリスタートを経ると保持されません。

WRS プロンプトにアクセスするには、GWCON (+) プロンプトで **feature wrs** と入力します。表10 は、WRS コマンドとその機能を示しており、後でそれぞれのコマンドについて説明しています。

表 10. WAN レストラル監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Clear	**list** コマンドを使用して表示した監視統計をクリアします。
Disable	WRS を使用不可にするか、または個々の 2 次、代替、またはダイヤル・オン・オーバーフローを使用不可にします。
Enable	WRS を使用不可にするか、または個々の 2 次、代替、またはダイヤル・オン・オーバーフローを使用可能にします。
List	代替または 2 次回線の 1 つまたはすべてに関する監視情報を表示します。
Set	stabilization (安定化)、route-stabilization (ルート安定化)、および time-of-day-revert-back-timer (復帰時刻タイマー) の値を設定します。

表 10. WAN レストラル監視コマンド (続き)

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

Clear

clear コマンドは、**list** コマンドを使用して表示された 、WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローの統計をクリアするのに使用します。

構文:

clear

注: このコマンドは *Longest restoral period* はクリアしますが、*Most recent restoral period* はクリアしません。画面の表示については、**list** コマンドの項に示されている例を参照してください。

Disable

disable コマンドは、WAN レストラル・フィーチャーを完全に使用不可にする、特定の 1 次インターフェースに対応する 2 次インターフェースによる復元を使用不可にする、代替インターフェースを使用不可にする、またはダイヤル・オン・オーバーフローを使用不可にするのに使用します。

構文:

disable alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit

WAN リルートの 1 次 / 代替のペアを使用不可にします。同じ代替を使用する複数のペアが存在することもあります。このコマンドは、指定された代替回線を使用するすべてのペアを使用不可にします。

例:

```
WRS>disable alternate-circuit
Alternate circuit number  [0]? 6
```

Alternate circuit number

これは、代替回線の番号です。デフォルトは 0 です。

dial-on-overflow

指定された 1 次 / 代替のペアのダイヤル・オン・オーバーフローを、そのペアに対する WAN リルートの使用可能/使用不可状態を変更せずに、使用不可にします。ダイヤル・オン・オーバーフローがルーティングを実行中の場合は、次の監視インターバルが満了した時点で終了されます。

secondary-circuit

特定の 1 次インターフェースに対応する 2 次インターフェースによる復元を、次の **restart**、**reload**、または **enable secondary-circuit** コマンドま

で使用不可にします。両方のインターフェースとも構成済みであり、WRS 構成内で相互が結合されていることが必要です。

通常は、**talk 5** (GWCON) の **disable** コマンドによりインターフェースは非活動状態にされ、非活動状態のままになりますが、WAN レストラルの 2 次の場合は、そうではありません。2 次インターフェースに適用される **disable** コマンドは、インターフェース自体は使用不可にしません。現行のコールだけを使用不可にします (つまり、活動状態のコールが切断されます)。2 次回線を使用不可にするためには、WAN レストラル監視プロンプトで **disable secondary-circuit** と入力し、トップ・レベルの GWCON プロンプトで 2 次インターフェースを使用不可にすることが必要です。**例:**

```
WRS>disable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number
これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

wrs WRS を使用不可にすると、ルーター上の WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローが、次の **restart**、**reload**、または **enable WRS** コマンドまで使用不可になります。

Enable

enable コマンドは、WAN レストラル・インターフェースを使用可能にする、1 次リンクの 2 次回線による復元を使用可能にする、代替回線を使用可能にする、またはダイヤル・オン・オーバーフローを使用可能にするのに使用します。

構文:

enable alternate-circuit
dial-on-overflow
secondary-circuit
wrs

alternate-circuit
指定された代替を使用するすべてのペアに対して、WAN リルートの 1 次 / 代替のペアを使用可能にします。

例:

```
WRS> enable alternate-circuit
Alternate circuit number  [0]? 3
```

Alternate circuit number
これは、代替回線のインターフェース番号です。デフォルトは 0 です。

dial-on-overflow
ダイヤル・オン・オーバーフローを使用可能にし、ダイヤル・オン・オーバーフローを制御するパラメーターを設定できるようにします。オプションで、ただちに IP プロトコルを代替に切り替える (追加限界値を超えたときのように) ことも可能です。

例:

```
WRS>  dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate interface.
Primary interface number [0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!

Do you want to switch IP traffic to the alternate now?(Yes or [No]):
WRS>
```

secondary-circuit

指定された 2 次リンクによる 1 次リンクの復元を使用可能にします。

例:

```
WRS>  enable secondary-circuit
Secondary interface number  [0]? 3
```

Secondary interface number

これは、以前に **add secondary-circuit** コマンドを使用して構成された 2 次インターフェースの番号です。デフォルトは 0 です。

wrs ルーター上の WAN レストラル・フィーチャーの機能を使用可能にします。WAN レストラル、WAN リルート、またはダイヤル・オン・オーバーフローを行うためには、この機能を使用可能にすることが必要です。

Set

set コマンドは、WAN リルートのパラメーターを設定するのに使用します。

構文:

set ?

default

first-stabilization

routing-stabilization

stabilization

start-time-of-day-revert-back

stop-time-of-day-revert-back

デフォルト (default)

set default コマンドは、安定化 (stabilization) 期間および最初の安定化 (first-stabilization) 期間が構成されていないリンクで使用されるデフォルト値を設定するのに使用します。

例:

```
WRS Config> set default ?
FIRST-STABILIZATION
STABILIZATION
```

first-stabilization

最初の安定化時間 (first-stabilization time) が構成されていないリンクで使用されるデフォルトの最初の安定化時間の値を設定します。

```
WRS Config>set default first

Default first primary stabilization time (0 - 3600 seconds)  [0]? 20
```

stabilization

安定化時間 (stabilization time) が構成されていないリンクで使用されるデフォルトの安定化時間の値を設定します。

```
WRS Config>set default stab
Default primary stabilization time (0 - 3600 seconds)  [0]? 30
```

first-stabilization

1 次リンクがアップにならない場合、この 1 次リンクのルーティングを代替リンクに切り替える前の、ルーター初期化の秒数を設定します。

例:

```
WRS Config>set first
Primary interface number [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number

これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

First primary stabilization time

この 1 次インターフェースの安定化時間。デフォルトは 1 です。

routing-stabilization

ルーティング安定化 (routing-stabilization) の値を設定します。このパラメーターは、1 次リンクが起動していることが検知され、安定化タイマー (指定されている場合) が満了した後で 1 次リンクと代替リンクの両方が起動したままになっている秒数を定義します。ルーティング安定化時間が与えられると、OSPF または RIP のようなルーティング・プロトコルは新しいルートの可用性を認識する時間が充分与えられます。ルーティング安定化タイマー (routing-stabilization timer) を指定しないと、代替ルートは使用不可になったが 1 次ルートがまだ見つからないという数秒の間トラフィックが中断されることがあります。

代替リンクがリルートより前にアップになっていた場合は、代替リンクはアップのままとなり、ルーティング安定化タイマー (routing-stabilization timer) は無視されます。代替リンクがリルートより前にダウン、あるいはリルート中であった場合は、代替リンクはダウンしたままで、ルーティング安定化タイマー (routing-stabilization timer) および安定化タイマー (stabilization timer) は両方とも無視されます。

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

Primary interface number

有効値 : 0 ～ルーター上に構成されたインターフェースの数

デフォルト値 : 0

Routing-stabilization timer

有効値 : 1 ～ 3600 秒

デフォルト値 : 0

stabilization

1 次リンクが起動していることが最初に検出された後、その 1 次リンク上でのルーティングの再初期設定プロセスが始まるまでに必要な秒数を設定します。ルーティング安定化タイマー (routing-stabilization timer) が設定され

ていない場合は、stabilization (安定化) タイマーが満了すると、代替リンクはダウンします。ルーティング安定化タイマー (routing-stabilization timer) は、安定化 (stabilization) タイマーが満了すると同時に開始し、代替リンク上にトラフィックを維持するのに充分なだけ 1 次リンクと代替リンクの両方をアップにしておき、この間に OSPF および RIP のようなルーティング・プロトコルは 1 次リンクを介してルートを再確立します。

例:

```
WRS Config>set first
Primary interface number [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
```

Primary interface number
これは、安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Primary stabilization time
1 次インターフェースの安定化時間。デフォルトは 1 です。

start-time-of-day-revert-back
ルーターが 1 次ルートに戻ることができる時刻を設定します。ルーターは、復帰開始時刻 (start-time-of-day-revert-back) と復帰停止時刻 (stop-time-of-day-revert-back) の間の任意の時刻に、1 次に復帰することができます。1 次への復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 0 です。

例:

```
WRS Config>set start
Primary interface number [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number
これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Time-of-day-revert-back-window start
この時刻は、復帰ウィンドウの開始時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに復帰することができます。1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 1 です。

stop-time-of-day-revert-back
この時刻は、復帰ウィンドウの終了時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに復帰することができます。1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 1 です。

例:

```
WRS Config>set stop
Primary interface number [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]?
5
```

Primary interface number
これは、最初の安定化時間を設定している 1 次インターフェースの 1 次インターフェース番号です。デフォルトは 0 です。

Time-of-day-revert-back-window stop
この時刻は、復帰ウィンドウの終了時刻をマークします。ルーターは、復帰開始時刻と復帰停止時刻の間の任意の時刻に、1 次インターフェースに復帰することができます。1 次インターフェースへの復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 1 です。

List

list コマンドは、WAN レストラルの 1 次 / 2 次のペアの 1 つまたはすべて、あるいは WAN リルートの 1 次 / 代替のペアの 1 つまたはすべてに関する情報を表示するのに使用します。

構文:

list all
alternate-circuit
secondary-circuit
summary

all 各 2 次インターフェースについて、要約情報を表示し、続いて特定の情報を表示します。

例:

```
list all
WAN Restoral/Re-route is enabled with 2 circuits configured
    Total restoral attempts =          7 completions   =          7
    Total packets forwarded =         39
    Longest completed restoral period in hrs:min:sec     0:03:27

    Total overflow attempts =         20 completions   =         19
    Longest completed overflow period in hrs:min:sec     0:05:00

   Primary       Secondary    Restoral  Restoral   Current/Longest
Net Interface  Net Interface  Enabled    Active       Duration
-------------  -------------  --------  --------   --------------------
  4  PPP/0       7  PPP/1       No         No       00:03:27/ 00.06.00

                               Re-route/ Re-route/         Recent
   Primary       Alternate    Overflow  Overflow     Reroute/Overflow
Net Interface  Net Interface  Enabled    Active       Duration
-------------  -------------  --------  --------   --------------------
  1   FR/0       2   FR/1     Yes/Yes    No /No     00:00:56/ 00:05:00
```

Total restoral attempts
1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

Completions
復元の試みに成功した (2 次がアップになり、使用された) 回数

Total packets forwarded
2 次インターフェースを介して転送されたパケットの合計数。これは両方向の合計数で、restart または clear restoral-statistics コマンドが出されるまでの、すべての正常な復元期間における累計です。

Longest Completed Restoral Period
このフィールドは、現行の使用期間はカウントせずに、復元が動作していた最長時間を時間、分、秒数で表示します。

Total Overflow Attempts
オーバーフローが原因での試行回数

Completions
オーバーフローが原因での試行に成功した (2 次リンクがアップになり、使用された) 回数

Longest Completed Overflow Period
現行の使用時間はカウントせずに、1 つのオーバーフローが動作していた最長時間を時間、分、秒数で表示します。

Primary Net Interface
対応する 2 次インターフェースによってバックアップされているインターフェース

Secondary Net Interface
対応する 1 次インターフェースをバックアップするのに使用されるダイヤル回線

Restoral Enabled
この 1 次インターフェースの復元が現在使用可能になっていることを示します。

Restoral Active
復元が活動状態かどうか (Yes または No) を示します。

Current/Longest Duration
現行の時間と、2 次ネットワーク・インターフェースがアップであった最長時間を時間、分、秒数で表示します。

Primary Net Interface
対応する代替インターフェースによってバックアップされるインターフェース

Alternate Net Interface
対応する 1 次インターフェースのバックアップとして使用されるインターフェース

Re-route/Overflow Enabled
リルートおよびオーバーフローが使用可能であるかどうか (Yes または No) を示します。

Re-route/Overflow Active
リルートおよびオーバーフローが活動状態かどうか (Yes または No) を示します。

Recent Re-route Overflow Duration
代替ネットワーク・インターフェースの最新のリルートおよびオーバーフローの時間数を、時間、分、秒数で示します。

Alternate-circuit

代替回線の合計数を提供します。監視オペレーターは、WAN リルートの状態、および各代替インターフェースと対応の 1 次マッピングに関する統計を検索することができます。

例:

```
WRS>li alt 7
Primary    1:FR/0 Frame Relay V.35/V.36
Alternate  7:PPP/1 Point to Point V.25bis Dial Circuit
reroute Enabled, currently inactive
overflow Enabled, currently inactive
Primary first stabilization time: default (0 seconds)
Primary stabilization time: default (0 seconds)
Routing-stabilization time: 15 seconds
Time-of-day revert back not configured: start = 0, stop = 0
Restored 0 times (0 attempts)
Overflow 0 times (0 attempts)
```

Primary Interface

この代替インターフェースによってバックアップされるインターフェース

Alternate Interface

対応する 1 次インターフェースをバックアップするのに使用されるダイヤル回線

Reroute Enabled

この 1 次インターフェースのリルートが現在使用可能になっているかどうかを示します。

Overflow Enabled

この 1 次インターフェースのオーバーフローが現在使用可能になっているかどうかを示します。

Primary first stabilization

1 次リンクがアップにならない場合、この 1 次リンクのルーティングを代替リンクに切り替える前のルーター初期設定の秒数

First stabilization

1 次リンクがアップであることが最初に検出されてから、ルーティングが代替リンクから 1 次リンクに戻されるまでに必要な秒数。1 次リンクがこの秒数だけアップ状態に保たれるまでは、ルーティングは代替リンクを介して継続されます。

Routing stabilization

ルーティングが 1 次リンクに戻されてから、代替リンクがダウンにされるまでに必要な秒数。この時間中、1 次リンクと代替リンクは両方ともアップのままです。このインターバルは、OSPF および RIP 時間のようなルーティング・プロトコルが 1 次インターフェースを介してルートの可用性を認知できるようにするためのものです。

Time-of-day revert back

ルーターが 1 次ルートに戻すことができる時刻。ルーターは、復帰開始時刻 (start-time-of-day-revert-back) と復帰停止時刻 (stop-time-of-day-revert-back) の間の任意の時刻に、1 次に復帰する

ことができます。1 次への復帰は、1 次がアップになり、安定化パラメーターが満たされた場合にだけ実行されます。デフォルトは 0 です。

Restored times
1 次インターフェースをリルートするための試行回数

Overflow times
ダイヤル・オン・オーバーフローの試行回数

secondary-circuit
各 2 次回線の合計数を提供します。監視オペレーターは、WAN レストラルの状態、および各 2 次インターフェースと対応の 1 次とのマッピングに関する統計を検索することができます。

例:

```
list secondary-circuit
Secondary interface number  [0]? 1

                                                    Secondary
Primary Interface          Secondary Interface      Enabled
-------------------        -------------------      ---------
1  PPP/0  Point to Poi     3  PPP/1  Point to Poi     Yes

Router primary interface state = Up
Router secondary interface state = Available
Restoral Statistics:

  Primary restoral attempts =       6   completions =    5
  Restoral packets forwarded =    346
    Most recent restoral period in hrs:min:sec          00:08:20
```

Primary Interface
この対応する 2 次インターフェースによってバックアップされているインターフェース

Secondary Interface
対応する 1 次インターフェースをバックアップするのに使用されるダイヤル回線

Secondary Enabled
この 1 次インターフェースの復元が現在使用可能になっているかどうかを示します。

Router Primary Interface State
1 次インターフェースの状態が、次のどれか 1 つであることを示します。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。

Disabled - オペレーターがリンクを使用不可にしたことを示します。

Not present - リンクは構成されているが、ハードウェアに問題があることを示します。

Router Secondary Interface State
対応する 2 次インターフェースの状態が、次のどれか 1 つであることを示します。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。これは、Config> プロンプトまたはオペレーター・コンソールで、2 次の基本ネットが使用不可にされている場合にも起こります。

Available - リンクが待機モードにあることを示します。

Testing - リンクが接続確立中であることを示します。

復元の統計:

Primary Restoral Attempts
1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

Restoral Packets forwarded
このフィールドには、転送されたパケットの合計数が表示されます。

Most Recent Restoral Period
これは、前回の使用時または現行の復元の使用時の、2 次がアップであった時間数を示します。

summary

各 2 次回線の合計数を提供します。

例:

```
list summary
WAN Restoral is enabled with 3 circuit(s) configured

  Total restoral attempts =      3 completions =      2
  Total packets forwarded =    346
  Longest restoral period in hrs:min:sec   00:08:20

Primary Interface and State      Secondary Interface and State
---------------------------   ----------------------------------
 1  PPP/0  - Up                 3  PPP/1  - Available
```

Total restoral attempts
1 次に障害が発生し、ルーターが 2 次リンクの起動を試みた回数

Completions
復元の試みに成功した (2 次がアップになり、使用された) 回数

Total packets forwarded
2 次インターフェースを介して転送されたパケットの合計数。これは両方向の合計数で、restart または clear restoral-statistics コマンドが使用されるまでの、すべての復元期間における累計です。

Longest restoral period
このフィールドは、現行の使用期間はカウントせずに、復元が使用された最長時間を時間、分、秒数で表示します。

Primary Interface and State
対応する 2 次によってバックアップされるインターフェース。有効な状態は、次のとおりです。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。

Disabled - オペレーターがリンクを使用不可にしたことを示します。

Not present - リンクは構成されているが、ハードウェアに問題があることを示します。

Secondary Interface and State

対応する 1 次をバックアップするのに使用されているダイヤル回線。有効な状態は、次のとおりです。

Up - リンクがアップであることを示します。

Down - リンクがダウンであることを示します。これは、`Config>` プロンプトまたはオペレーター・コンソールで、2 次の基本網が使用不可にされている場合にも起こります。

Testing - リンクが接続確立中であることを示します。

Available - リンクが待機モードにあることを示します。

WAN レストラルおよび WAN レストラル動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

WAN レストラルおよび WAN リルートは、CONFIG (Talk 6) **delete interface** コマンドを制限なしでサポートします。

GWCON (Talk 5) Activate Interface

WAN レストラルおよび WAN リルートは、GWCON (Talk 5) **activate interface** コマンドをサポートしますが、次の考慮が必要です。

- WAN レストラルの 1 次インターフェースは、その 2 次インターフェースが別の 1 次インターフェースを活発に復元している場合に、活動化できません。
- WAN レストラル 1 次インターフェースは、その 2 次インターフェースが WAN レストラル 1 次インターフェース、WAN リルート 1 次インターフェース、または **activate interface** コマンドの前の WAN リルート代替インターフェースであった場合には、活動化できません。
- WAN レストラルの 2 次インターフェースは、別の 2 次インターフェースがその 1 次インターフェースを活発に復元している場合に、活動化できません。
- WAN レストラル 2 次インターフェースは、その 1 次インターフェースが WAN レストラル 2 次インターフェース、WAN リルート 1 次インターフェース、または **activate interface** コマンドの前の WAN リルート代替インターフェースであった場合には、活動化できません。
- WAN リルート 1 次インターフェースは、その代替インターフェースが WAN リルート 1 次インターフェース、WAN レストラル 1 次インターフェース、または **activate interface** コマンドの前の WAN リルート代替インターフェースとして使用された場合には、活動化できません。
- WAN リルート代替インターフェースは、その 1 次インターフェースが別の代替インターフェースの 1 次インターフェースであったか、WAN リルート代替インターフェースであったか、WAN リルート 1 次インターフェースであったか、または WAN レストラル 1 次インターフェース、または WAN リルート 2 次インターフェースであった場合には、活動化できません。

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

GWCON (Talk 5) Reset Interface

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

GWCON (Talk 5) 一時変更コマンド

WAN レストラルおよび WAN リルートは、装置の操作状態を一時変更する、次の GWCON コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行すると、行われません。

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

第7章 WAN リルート・フィーチャー

この章では、WAN リルート・フィーチャーについて説明します。この章には、次の内容が記載されています。

WAN リルートの概説

WAN リルートは、代替ルートを設定することによって、1 次リンクに障害が起きたときに、ルーターが自動的に代替ルートを通る宛先への新しい接続を開始できるようにします。WAN レストラルの説明、および WAN リルートとダイヤルオン・オーバーフローを合わせて使用する方法については、69ページの『WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローの概説』を参照してください。

WAN リルート・プロセスは、次のとおりです。

1. 1 次リンクの障害を検出する。
2. 代替リンクに切り替える。
3. 1 次リンクの回復を検出する。
4. 1 次リンクに戻す。

代替リンクは、ルート可能プロトコル (たとえば、IP、IPX) を構成できる任意のリンクを使用することができ、代替リンクのデータ・リンク・タイプは、1 次リンクのデータ・リンク・タイプと一致している必要はありません。たとえば、代替リンクには、LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ダイヤル回線などを使用できます。代替リンクに使用できないインターフェース・タイプの例としては、SDLC シリアル・インターフェース、SRLY シリアル・インターフェース、および V.25bis や ISDN のような基本ネットがあります。

注: 1 次リンクまたは代替リンクがダイヤル回線の場合、そのダイヤル回線はダイヤル・オンデマンド用に構成することはできません。`Circuit Config>` プロンプトで **set idle 0** コマンドを使用して、ダイヤル回線がダイヤル・オンデマンドを実行できないように構成してください。詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の『ダイヤル回線の構成および監視』を参照してください。

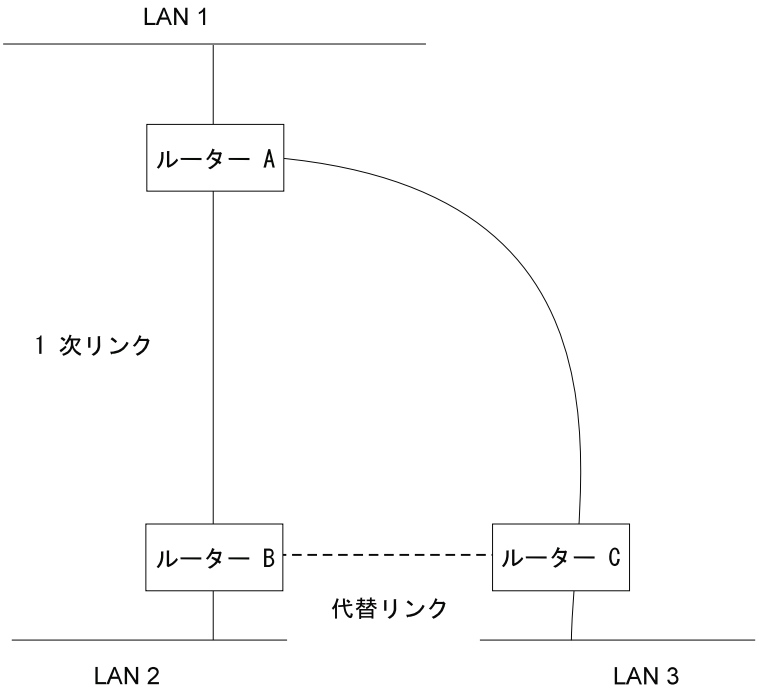


図 3. WAN リルート. 通常は、ルーター A と B の間、およびルーター A と C の間にコネクションがあります。ルーター A と B の間の 1 次リンクに障害が起きた場合、WAN リルートは、ルーター B と C の間に代替リンクを確立します。これにより、ルーター A と B は、ルーター C を介して通信できるようになります。

ダイヤル・オン・オーバーフロー

ダイヤル・オン・オーバーフローでは、1 次リンクのトラフィック速度が指定の限界値に達すると、IP トラフィック用の代替インターフェースを使用することができます。これは、1 次インターフェースが必ずしもダウンしなくても、代替リンクが起動されることを意味しています。1 次インターフェースのトラフィックが指定の限界値に達すると、ルーターは代替リンクを起動します。ダイヤル・オン・オーバーフローを使用するためには、WAN リルートが構成されており、1 次インターフェースがフレーム・リレーであることが必要です。ダイヤル・オン・オーバーフローで代替インターフェースに切り替えることができる唯一のプロトコルは、IP です。ダイヤル・オン・オーバーフローを使用する場合も、RIP の代わりに、OSPF を IP ルーティング・プロトコルとして使用する必要があります。

ダイヤル・オン・オーバーフローの構成については、75ページの『WAN レストラル、WAN リルート、およびダイヤル・オン・オーバーフローの構成コマンド』 を参照してください。

帯域幅の監視

WAN リルートの構成時に、ダイヤル・オン・オーバーフローの帯域幅監視のインターバルを指定することができます。1 次インターフェースの送受信の帯域幅が監視されます。1 次インターフェースの帯域幅が*追加* 限界値に達すると、代替インターフェースを起動するための WAN リルート要求が生成されます。WAN リルートが代替インターフェースの起動に成功すると、IP は 1 次インターフェースを介したルーティングを停止し、代替インターフェースを介してルーティングを開始します。

WAN リルートが代替ルートの起動に失敗すると、1 次インターフェースの帯域幅使用率が*ドロップ* 限界値を下回るまで、代替インターフェースの起動を定期的に試みます。

1 次インターフェースの送受信の帯域幅使用率が*ドロップ* 限界値に達し、構成された最小アップ・タイムが満了すると、代替インターフェースはドロップされます。これにより、IP は代替インターフェースを介したルーティングを停止し、1 次インターフェースの使用を開始します。

追加限界値およびドロップ限界値は、1 次リンクに構成された回線速度の比率として指定します。構成された回線速度は、必ずしもリンクの実際の速度と一致するとは限りません。リンク上の各方向のトラフィックの量は、別々に計算されます。どちらかの方向のトラフィックが指定の比率より大きい場合、限界値を超したと見なされます。

WAN リルートの構成

次に示すのは、WAN リルートを構成するのに必要なステップです。次に、これらのタスクを実行する方法の例を示します。

WAN リルートを構成するには、次の作業が必要です。

1. 1 次リンクを構成する。
2. 代替リンクを構成する。
3. 代替リンクを 1 次リンクに割り当てる。1 次リンクの安定化 (stabilization) 期間も指定できます。

   安定化時間が終わった後 (構成されている場合) に行われる 1 次リンクへの復帰時刻 (time-of-day revert-back) を指定することができます。これにより、ユーザーが希望する時刻まで 2 次をアップに維持し、オフ・ピーク時に 1 次に復帰させるといったことが可能になります。

   注: 1 次リンクと代替リンクは、異なるデータ・リンク・タイプであっても構いません。1 次リンクおよび代替リンクには、次のものを使用できます。
   - LAN インターフェース
   - PPP シリアル・インターフェース
   - フレーム・リレー・シリアル・インターフェース
   - X.25 シリアル・インターフェース
   - PPP ダイヤル回線
   - フレーム・リレー・ダイヤル回線

サンプル WAN リルート構成

100ページの図4 は、ISDN を介するフレーム・リレー・ダイヤル回線を代替リンクとして使用している WAN リルートを示しています。ルーター A とルーター C 間のフレーム・リレー DLCI に障害が起きた場合、WAN リルートはダイヤル回線を使用してルーター D を経由する代替コネクションを確立します。支社から本社への 1 次リンクの 1 つに障害が起きた場合、WAN リルートは別の支社を経由して本社に接続する代替ルートを確立します。

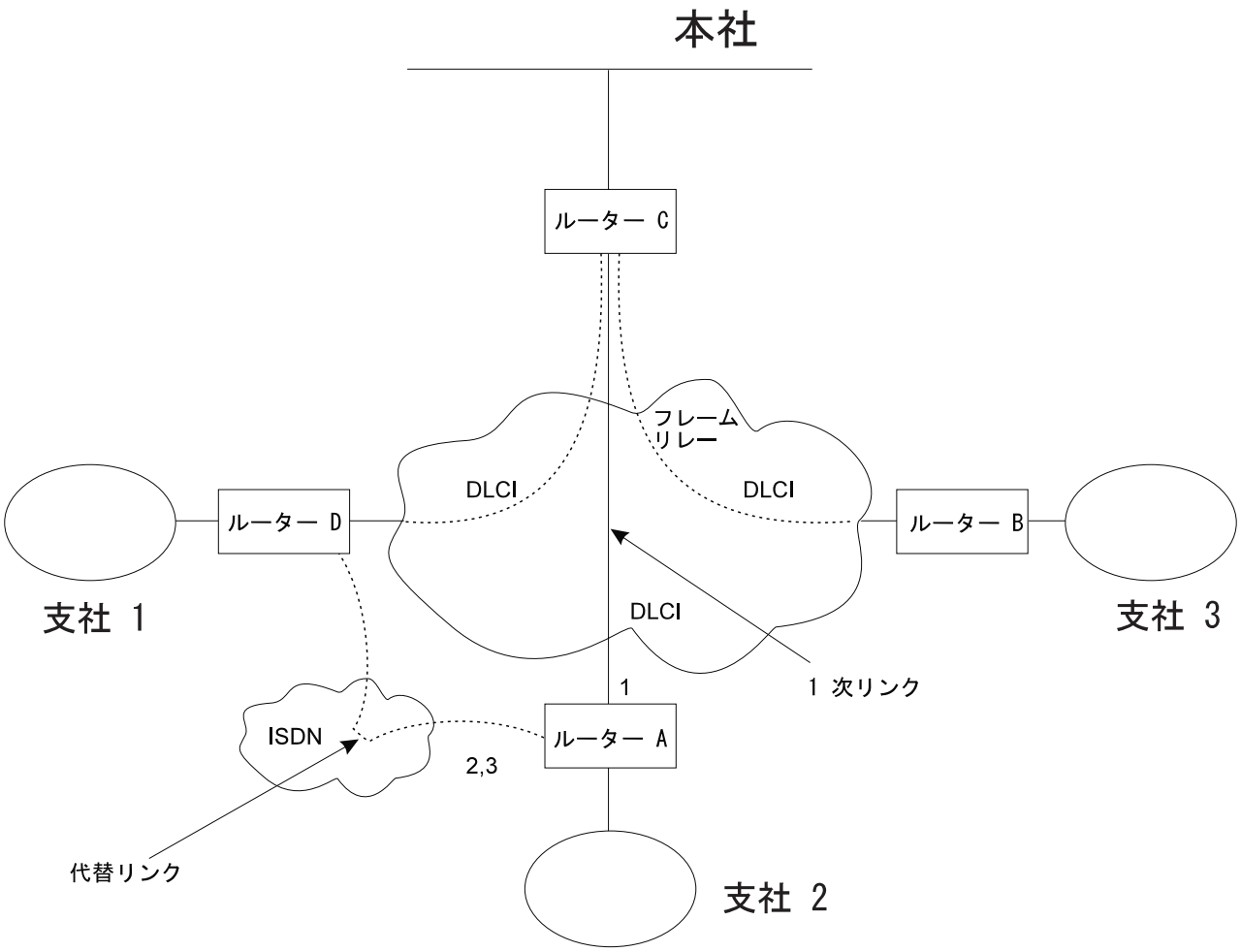


図 4. サンプル WAN リルート構成. 支社はフレーム・リレーを使用して本社に接続。

次では、図4 のルーター A 上の WAN リルートを設定する方法について説明します。次のタスクが必要になります。

- 1 次フレーム・リレー・インターフェース (1) を構成して、そのフレーム・リレー・インターフェースに必要な PVC または必要な PVC グループを設定するか、あるいは No-PVC フィーチャーを使用可能にする。
- ISDN インターフェース (2) およびそのフレーム・リレー・ダイヤル回線 (3) を構成する。
- この回線についてダイヤル・オンデマンドを使用不可にするために、ダイヤル回線を、1 次フレーム・リレー・インターフェースの代替リンクとして割り当て、ダイヤルの `Circuit Config>` プロンプトで **set idle 0** コマンドを出す。
- 任意により、次のものも指定できます。
  - 1 次リンクの安定化 (stabilization) 期間
  - 1 次リンクの復帰時刻 (time-of-day revert-back) ウィンドウ

これらのタスクについて、次で詳しく説明します。

フレーム・リレー・インターフェースの構成

ルーター A 上に WAN リルート用のフレーム・リレー・インターフェースを構成するには、1 次フレーム・リレー・インターフェース上のルーター A と C 間に PVC を追加します。

他のルーターへの接続が失われたときに、1 次 FR インターフェースが自身をダウンとして宣言するようにさせるには、3 通りの方法を選択できます。

1. No-PVC フィーチャーを使用可能にする。このフィーチャーが使用可能のとき、活動状態の PVC がないと、FR インターフェースはダウンします。
2. ある PVC を必須として構成するが、その PVC を必須 PVC グループの中に含めない。この場合、その PVC が非活動状態になると、FR インターフェースはダウンします。
3. 1 組の PVC を必須として構成し、必須 PVC グループに含める。この場合、必須 PVC グループのすべての PVC が非活動状態になると、FR インターフェースはダウンします。

フレーム・リレー・インターフェースの構成は、次の手順で行います。

1. ISDN インターフェース上のデータ・リンクをフレーム・リレーに設定する (まだ行っていない場合)。

   ```
   Config>set data-link frame relay
   Interface Number [0]? 2
   ```

2. フレーム・リレー構成プロセスに入る。

   ```
   Config>network
   What is the network number [0]?2
   Frame Relay user configuration
   FR Config>
   ```

   注: 1 次フレーム・リレー・インターフェースを構成するために、残りの 2 つのステップのうちの *1* つ だけを実行します。

3. **add permanent-virtual-circuit** コマンドを使用して、PVC を追加する。

   PVC を必須として構成するには、次のようにします。

   『Is circuit required for interface operation ?』 という問いに対して **y** と入力する。

   PVC を必須 PVC グループのメンバーとして構成するには、次のようにします。

   a. 『Does circuit belong to a Required PVC group ?』 という問いに対して **y** を入力する。

   b. 『What is the group name ?』 の問いに応答して、グループ名を入力する。

   すでに PVC が追加されている場合は、**change permanent-virtual-circuit** コマンドを使用して、PVC を必須として構成し、該当する場合は、それを必須 PVC グループに割り当てます。詳しくは、*Nways* マルチプロトコル・アクセス・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使用’ の項を参照してください。

   ```
   FR Config> add permanent-virtual-circuit
   Circuit number [16]?
   Committed Information Rate (CIR) in bps [64000]?
   Committed Burst Size (Bc) in bits [64000]?
   Excess Burst Size (Be) in bits [0]?
   ```

```
Assign circuit name []?
Is circuit required for interface operation [N]? y
Does the circuit belong to a required PVC group [N]?  y
What is the group name []?group1
```

4. 必要な場合は、No-PVC フィーチャーを使用可能にする。

   注: このステップは、直前のステップを飛ばした場合にだけ 実行してください。

   ```
   FR Config>enable no-pvc
   ```

この他にも、フレーム・リレーに対して設定できるパラメーターがあります。詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の ‘フレーム・リレーの使用’ の項を参照してください。

ISDN インターフェースとダイヤル回線の構成

ルーター A とルーター D 間の ISDN インターフェースとダイヤル回線を構成します。ISDN インターフェースおよびダイヤル回線の構成方法についての詳しい説明は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の ‘ISDN インターフェースの使用 ’ の項を参照してください。

WAN レストラルとは異なり、代替リンクとして使用されるダイヤル回線には、ルーティング・プロトコルを構成する必要があります。このルート可能プロトコルは、保守パケットを送信するのを防止できないので、代替リンクは再ルートの必要がなくても接続を確立します。この場合、代替リンクを再ルートにだけ使用したいときは、ダイヤル回線を使用不可に設定します。ダイヤル回線を使用不可にするには、`Config>` プロンプトで **disable interface** コマンドを入力します。

ISDN インターフェースに複数のダイヤル回線を割り当てた場合、ダイヤル回線に優先順位を設定することができます。すべての B チャネルが、物理インターフェース上に活動状態のダイヤル回線を持っており、高い優先順位の回線がパケットを受信する場合、最低優先順位の接続は終了され、高い優先順位の回線が接続を確立します。

優先順位は 0 ～ 15 に設定できます。15 が最高優先順位の回線で、0 が最低優先順位の回線です。新規ダイヤル回線のデフォルト優先順位は 8 です。優先順位を変更する場合は、`Circuit Config>` プロンプトで **set priority** と入力します。

代替リンクの割り当てと構成

WAN リルート構成プロセスに入って、ダイヤル回線を LAN インターフェース、PPP、フレーム・リレー、または X.25 シリアル・インターフェース、あるいは PPP またはフレーム・リレー・ ダイヤル回線の代替リンクとして割り当て、必要な場合には、安定化期間 (stabilization periods) または復帰時刻 (time-of-day revert-back) ウィンドウ (もしくは、その両方) を指定します。

安定化期間には、次の 3 種類があります。

- *最初の安定化期間 (First stabilization period)* は、ルーターが最初に 1 次インターフェースの起動を試みたときに、1 次インターフェースが活動状態になるのを待つ時間の長さです。最初の安定化期間が経過しても 1 次がアップにならない場合、WAN リルートは代替リンクを起動します。
- *安定化期間 (Stabilization period)* は、ルーターが代替リンクから 1 次リンクに戻す前に、1 次リンクの信頼性を確認するために待つ時間の長さです。

- *ルーティング安定化期間 (Routing stabilization period)* は、ルーターが代替リンクから 1 次リンクに戻す前に、1 次リンクの信頼性を確認するために待つ時間の長さです。この時間は、OSPF または RIP などのルーティング・プロトコルが、代替リンクがダウンする前に 1 次リンクを介してルートの可用性を認知するのに使用します。

復帰時刻 (time-of-day revert-back) ウィンドウは、1 次がアップになり、構成された安定化期間が経過した後で 1 次に戻す具体的な時刻です。

ユーザーは 24 時間クロックを使用して、復帰ウィンドウの開始時刻と停止時刻を指定します。開始時刻に達するまで、2 次はアップのまま維持され、ダウンにされません。1 次がアップになる時刻が、開始時刻と停止時刻 (ウィンドウ内の) の間にある場合、安定化期間が経過した後、ただちに 1 次リンクに切り替わります。

代替リンクの割り当てと構成は、次の手順で行います。

1. WAN レストラル構成プロセスに入る。

```
Config>feature wrs
WAN Restoral user configuration
```

2. ダイヤル回線を、1 次フレーム・リレー・インターフェースの代替リンクとして割り当てる。

```
WRS Config>add alternate-circuit
Alternate interface number  [0]? 4
Primary interface number  [0]? 1
```

3. 代替回線を使用可能にする。

```
WRS Config>enable alternate-circuit
Alternate interface number  [0]? 4
```

4. オプションで、最初の安定化期間を指定する。

   特定の 1 次インターフェースに対する最初の安定化期間を設定するには、**set first-stabilization-period** コマンドを使用します。特定の期間が設定されていないすべてのインターフェースに対するデフォルトの最初の安定化期間を設定するには、**set default first-stabilization-period** コマンドを使用します。

```
WRS Config>set first-stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?

WRS Config>set default first-stabilization-period
Default first primary stabilization time (0 - 3600 seconds) [0]?
```

5. オプションで、安定化期間を設定する。特定のインターフェースに対する安定化期間を設定するには、**set stabilization-period** コマンドを使用します。特定の期間が設定されていないすべてのインターフェースに対するデフォルトの安定化期間を設定するには、**set default stabilization-period** コマンドを使用します。

```
WRS Config>set stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1 = default)  [-1]?
WRS Config>set default stabilization-period
Default first primary stabilization time (0 - 3600 seconds) [0]?
```

6. 任意により、ルーティング安定化期間 (routing stabilization period) を設定する。特定のインターフェースに対するルーティング安定化期間を設定するには、**set routing-stabilization** コマンドを使用します。

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

7. 任意により、復帰時刻 (time-of-day-revert-back) ウィンドウを指定する。

   特定のインターフェース・ウィンドウの開始時刻と停止時刻を設定するには、start-time-of-day-revert-back コマンドと stop-time-of-day-revert-back コマンドを使用します。デフォルト値のゼロは、ウィンドウが構成されないことを意味します。24 時間クロックは、午前 1 時に開始して、夜中の 24時に終了します。開始時刻と停止時刻が同じ (ただし、ゼロでない) 場合、復帰は正確にその時刻に起こります。

   次は、復帰ウィンドウの設定を示す 2 つの例です。

   a. 開始時刻が 23 で、停止時刻が 3 のとき、午後 11 時から午前 3 時までの復帰ウィンドウを生成します。

   b. 開始時刻が 1 で、停止時刻が 5 のとき、午前 1 時から午前 5 時までの復帰ウィンドウを生成します。

```
WRS Config> set start-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]?
WRS Config> set stop-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured) [0]?
```

第8章 ネットワーク・ディスパッチャー・フィーチャーの使用

この章では、ネットワーク・ディスパッチャー・フィーチャーの使用法について説明します。この章には、次の内容が記載されています。

- 『ネットワーク・ディスパッチャーの概説』
- 106ページの『ネットワーク・ディスパッチャーの使用による TCP および UDP トラフィックのバランス』
- 107ページの『ネットワーク・ディスパッチャーの高可用性』
- 110ページの『ネットワーク・ディスパッチャーの構成』
- 118ページの『TN3270 でのネットワーク・ディスパッチャーの使用』
- 122ページの『クラスター・アドレス公示でのネットワーク・ディスパッチャーの使用』
- 124ページの『Web サーバー・キャッシュでのネットワーク・ディスパッチャーの使用』
- 124ページの『eNetwork ホスト・オンデマンド・クライアント・キャッシュでのネットワーク・ディスパッチャーの使用』
- 124ページの『スケーラブル高可用性キャッシュ (SHAC) でのネットワーク・ディスパッチャーの使用』

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

ネットワーク・ディスパッチャーの概説

ネットワーク・ディスパッチャーとは、TCP/IP セッション要求をサーバー・グループ内の種々のサーバーに転送し、すべてのサーバー間で要求のロード・バランシングを取ることによって、サーバーの性能を高めるフィーチャーです。この転送は、ユーザーおよびアプリケーションには透過的に行われます。ネットワーク・ディスパッチャーは、E メール、ワールド・ワイド・ウェブ (WWW) サーバー、分散並列データベース照会、およびその他の TCP/IP アプリケーションなどのサーバー・アプリケーションに役立ちます。

ネットワーク・ディスパッチャーは、サーバー・グループへのステートレス UDP アプリケーション・トラフィックのロード・バランシングを取るにも使用することができます。

ネットワーク・ディスパッチャーは、ピーク需要時の問題に対処するための、強力で、柔軟で、拡張が容易なソリューションを提供することにより、ユーザーのサイトの潜在的な能力を最大限に発揮させることができます。ネットワーク・ディスパッチャーは、ピーク需要時に、着信要求を処理するための最適なサーバーを自動的に見つけます。

ネットワーク・ディスパッチャー機能は、ロード・バランシングを取るためにドメイン名サーバーを使用しません。ロード・バランシングと管理ソフトウェアの固有な組み合わせを介して、サーバー間のトラフィックのバランスを取ります。ネット

ワーク・ディスパッチャーは、障害のあるサーバーを検出し、他の利用可能なサーバーにトラフィックを転送することもできます。

ネットワーク・ディスパッチャー・マシンに送られるすべてのクライアント要求は、ネットワーク・ディスパッチャーが、動的に設定される重みに基づいて最適サーバーと判断したサーバーに転送されます。これらの重みは、接続カウント、サーバーの負荷およびサーバーの使用可能性を含む多くの係数に基づいて、ネットワーク・ディスパッチャーによって計算されます。

サーバーからクライアントへの応答には、ネットワーク・ディスパッチャーは介入しません。ネットワーク・ディスパッチャーと通信するために、サーバー上にソフトウェアを追加する必要はありません。

ネットワーク・ディスパッチャー機能は、大規模で、拡張が容易なサーバー・ネットワークを、安定した状態で効率的に管理するためのかぎになります。ネットワーク・ディスパッチャーを使用すると、多数の個別のサーバーをリンクして、単一のバーチャル・サーバーのように見せることができます。世界は、ユーザーのサイトは単一の IP アドレスのように見えます。ネットワーク・ディスパッチャーは、ドメイン名サーバーから独立して機能します。要求はすべてネットワーク・ディスパッチャー・マシンの IP アドレスに送られます。

ネットワーク・ディスパッチャーでは、SNMP ベースの管理アプリケーションを使用して、基本的な統計および潜在的なアラート状態を受信し、ネットワーク・ディスパッチャーを監視することができます。詳しくは、*プロトコルの構成と監視 解説書 第 1 巻*の『SNMP 管理』の項を参照してください。

ネットワーク・ディスパッチャーは、クラスター化されたサーバーへのトラフィックのロード・バランシングに大きく貢献し、サイトの安定した効率的な管理を実現します。

ネットワーク・ディスパッチャーの使用による TCP および UDP トラフィックのバランス

ロード・バランシングには、さまざまなアプローチがあります。ある方法では、最初のサーバーが遅かったり応答しない場合、ユーザーが任意に異なるサーバーを選択することができます。ある方法はラウンドロビン方式を採用し、ドメイン名サーバーが、要求を処理するサーバーを選択します。この方法は比較的優れていますが、ターゲット・サーバー上の現在のロードは考慮に入れられず、ターゲット・サーバーが利用可能であるかどうかさえ考慮されません。

ネットワーク・ディスパッチャーは、要求のタイプ、サーバー上のロードの分析、またはユーザーが割り当てる 1 組の構成可能な重みに基づいて、種々のサーバーへの要求のロード・バランスを取ることができます。異なるタイプのバランスを個別に管理するために、ネットワーク・ディスパッチャーには、次のコンポーネントが装備されています。

実行プログラム

受信した要求のタイプに基づいて、接続のロード・バランスを取ります。一般的なな要求のタイプとしては、HTTP、FTP、および Telnet があります。このコンポーネントは、常に実行されます。

アドバイザー

サーバーに照会し、各サーバーのプロトコルを用いて結果を分析します。アドバイザーは適切な重みを設定するために、この情報を**マネージャー** に渡します。アドバイザーは、任意選択のコンポーネントです。しかし、アドバイザーを使用しない場合には、ネットワーク・ディスパッチャーはサーバーに障害がいつ発生したかを検出できず、下位のサーバーに新しい接続を送信し続けます。

ネットワーク・ディスパッチャーは、FTP、HTTP、SMTP、NNTP、POP3、および Telnet 用のアドバイザーをサポートするだけでなく、IBM 2210、IBM 2212、および IBM 2216 内の TN3270 サーバーと一緒に稼働する TN3270 アドバイザー、および MVS システム上のワークロード・マネージャー (WLM) と一緒に稼働する MVS™ アドバイザーもサポートします。WLM は、個々の MVS ID の作業負荷の量を管理します。ネットワーク・ディスパッチャーは、WLM を利用して、OS/390® V1R3 以降のリリースを稼働する MVS サーバーへの要求のロード・バランスを取ることができます。

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

マネージャー

次に基づいて、サーバーの重みを設定します。

- 実行プログラムの内部カウンター
- プロトコル・アドバイザーによって提供されたサーバーからのフィードバック
- システム・モニター (MVS アドバイザー) からのフィードバック

マネージャーは、任意選択のコンポーネントです。ただし、マネージャーを使用しない場合、ネットワーク・ディスパッチャーは、サーバーごとに修正したサーバーの重みに基づいてラウンドロビン・スケジューリング方式でロードのバランスを取ります。

ネットワーク・ディスパッチャーを使用してステートレス UDP トラフィックのロード・バランスを取る場合は、要求内の宛先 IP アドレスを使用してクライアントに応答したサーバーだけを使用する必要があります。詳しくは、115ページの『ネットワーク・ディスパッチャー用のサーバーの構成』を参照してください。

ネットワーク・ディスパッチャーの高可用性

ネットワーク・ディスパッチャーの基本機能には次のような特性があり、いろいろな観点から、これが単一障害点になることを示しています。

- 入ってくるすべてのトラフィックを調べます。既存の接続への一部のパケットが、異なるネットワーク・ディスパッチャーを経由する異なるパスを使用してサーバーに達する場合、サーバーは即時にその接続をリセットします。

- 確立されたすべての接続を追跡し、それを終了することはありませんが、ネットワーク・ディスパッチャーの接続テーブルからエントリーが失われると、接続はリセットされます。
- それより前のホップ・ルーターからは、それが最終ホップであり、接続の終端であるように見えます。

これらの特性により、次のような障害が発生した場合、クラスター全体にとって重大なものになります。

- 何らかの理由でネットワーク・ディスパッチャーに障害が生じた場合、すべての接続テーブルが失われます。したがって、クライアントからサーバーへの既存の接続もすべて失われます。クライアントをサーバーに誘導できる第 2 のネットワーク・ディスパッチャーが存在すると仮定しても、通常のルーティング・プロトコル遅延 (数分かかることもある) の後でしか、新しい接続を確立することができません。
- 直前の IP ルーターへの構成済みネットワーク・ディスパッチャー・インターフェースに障害が生じた場合、同じネットワーク・ディスパッチャーに到達できる別のインターフェースが存在する必要があります。その場合は IP ルーターによって回復されますが (ARP エージング機構を使用して、数分の遅れで)、そうでない場合は、すべての接続が失われます。
- サーバーにインターフェースするネットワーク・ディスパッチャーに障害が生じた場合、直前のホップ・ルーターはそのネットワーク・ディスパッチャーが最終ホップであるものと想定するので、新しい接続を再ルートしません。既存の接続は失われ、新しい接続は確立されないことになります。

いずれの障害の場合も (これらは、ネットワーク・ディスパッチャーの障害だけでなく、ネットワーク・ディスパッチャーの近隣の障害でもあります)、すべての既存の接続は失われます。標準 IP 回復機構を搭載したバックアップ用のネットワーク・ディスパッチャーを備えている場合でも、最善の場合でも、回復に時間がかかり、しかも新規の接続にしか適用されません。最悪の場合には、接続は回復しません。

ネットワーク・ディスパッチャーの可用性を高めるために、ネットワーク・ディスパッチャー高可用性機能は、次の機構を使用しています。

- 同じクライアント、同じサーバー・クラスターへの接続性、およびネットワーク・ディスパッチャー相互間の接続性を備えている 2 つのネットワーク・ディスパッチャー。
- ネットワーク・ディスパッチャーの障害を検出するための、2 つのネットワーク・ディスパッチャー間の『ハートビート』機構
- 各ネットワーク・ディスパッチャーから到達できる IP ホストと到達できないホストを識別するための到達可能性基準
- ネットワーク・ディスパッチャー・データベース (つまり、接続テーブル、到達可能性テーブル、およびその他のテーブル) の同期化
- アクティブ・ネットワーク・ディスパッチャー (特定のサーバー・クラスターを担当する) とスタンドバイ・ネットワーク・ディスパッチャー (そのサーバー・クラスターに継続的に同期化される) を選ぶ論理
- 論理またはオペレーターがアクティブとスタンドバイを切り替えることに決定した場合、迅速に IP の引き継ぎを実行する機構

障害の検出

障害検出の基本的基準 (ハートビート・メッセージによって検出されるアクティブ・ネットワーク・ディスパッチャーとスタンドバイ・ネットワーク・ディスパッチャー間の接続性の損失) の他に、『到達可能性基準』と呼ばれるもう 1 つの障害検出機構があります。ネットワーク・ディスパッチャーの構成時に、各ネットワーク・ディスパッチャーが正しく作動するために到達可能でなければならないホストのリストを指定します。ホストは、ルーター、IP サーバー、またはその他のタイプのホストが可能です。ホスト到達可能性は、そのホストに PING することによって入手します。

ハートビート・メッセージを送れない場合、あるいはアクティブ・ネットワーク・ディスパッチャーが到達可能性基準を満たさなくなり、スタンドバイ・ネットワーク・ディスパッチャーが到達可能である場合、切り替えが行われます。利用可能なあらゆる情報に基づいて決定を下せるように、アクティブ・ネットワーク・ディスパッチャーは、その到達可能性の機能をスタンドバイ・ネットワーク・ディスパッチャーに定期的に送信します。スタンドバイ・ネットワーク・ディスパッチャーは、その機能を自身の機能と比較して、切り替えるかどうかを決定します。

データベースの同期

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

回復方法

ネットワーク・ディスパッチャー・マシンやインターフェースに障害が生じた場合、IP 引き継ぎ機構が、速やかにすべてのトラフィックをスタンドバイ・ネットワーク・ディスパッチャーに転送します。既存のクライアント/サーバー接続が維持されるように、データベース同期機構によって、スタンドバイはアクティブ・ネットワーク・ディスパッチャーと同じエントリーを持つことが保証されています。

IP 引き継ぎ

注: クラスター IP アドレスは、クラスター・アドレス公示を使用していない限り、直前のホップ・ルーター (IP ルーター) と同じ論理サブネット上に存在するものと想定しています。

IP ルーターは、ARP プロトコルを介してクラスター・アドレスを解決します。IP 引き継ぎを行うために、ネットワーク・ディスパッチャー (スタンドバイがアクティブになる) は、自分自身に対して ARP 要求を出します。これは、そのクラスターの論理サブネットに属するすべての直接接続ネットワークにブロードキャストされます。それより前のホップの IP ルーターは、それぞれの ARP テーブルを更新し

て (RFC826 に従って)、そのクラスターへのすべてのトラフィックを、新たにアクティブになった (前はスタンドバイだっ た) ネットワーク・ディスパッチャーに送るようにします。

ネットワーク・ディスパッチャーの構成

ユーザー・サイトをサポートするネットワーク・ディスパッチャーを構成するには、いろいろな方法があります。ユーザー・サイトにホスト名が 1 つしかなく、すべてのカスタマーがそれに接続する場合は、1 つのクラスターと任意の数のポート (接続を受信する) を定義することができます。この構成を 図5 に示します。

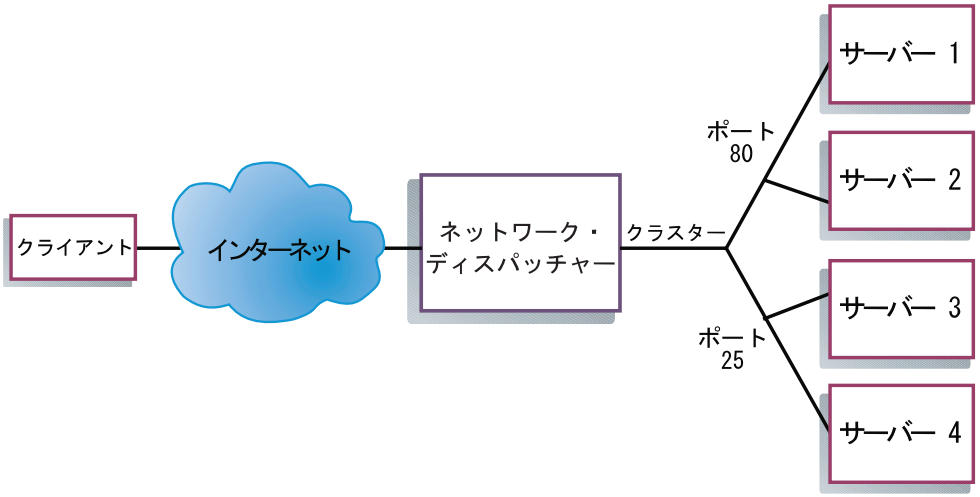


図5. 1 つのクラスターと 2 つのポートを持つように構成されたネットワーク・ディスパッチャーの例

ユーザーのサイトで、複数の会社または部門がそれぞれ異なる URL を使用してサイトにアクセスする競合タイプのホスト接続を行っている場合には、ネットワーク・ディスパッチャーを別の方法で構成することが必要になります。この場合は、111ページの図6 に示すように、各会社または部門ごとに 1 つのクラスターを定義し、その URL で接続を受け取る任意の数のポートを構成することができます。

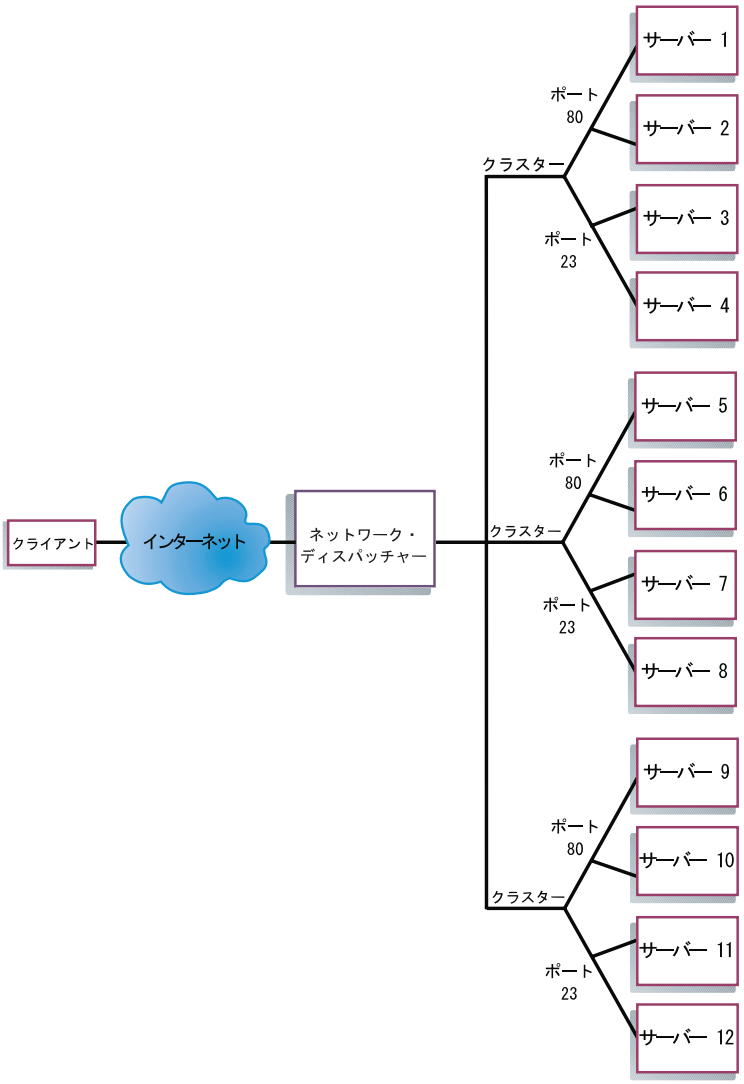


図 6. 3 つのクラスターと 3 つの URL を持つように構成されたネットワーク・ディスパッチャーの例

第 3 のネットワーク・ディスパッチャー構成方法は、サポートされる各プロトコル専用のサーバーが多数ある非常に大規模なサイトに適しています。たとえば、大きなダウンロード可能ファイル専用の直接 T3 回線を、個別の FTP サーバーに構成するといったことが可能です。この場合は、112ページの図7 に示すように、各プロトコルについて、1 つのポートで複数のサーバーを持つクラスターを定義することができます。

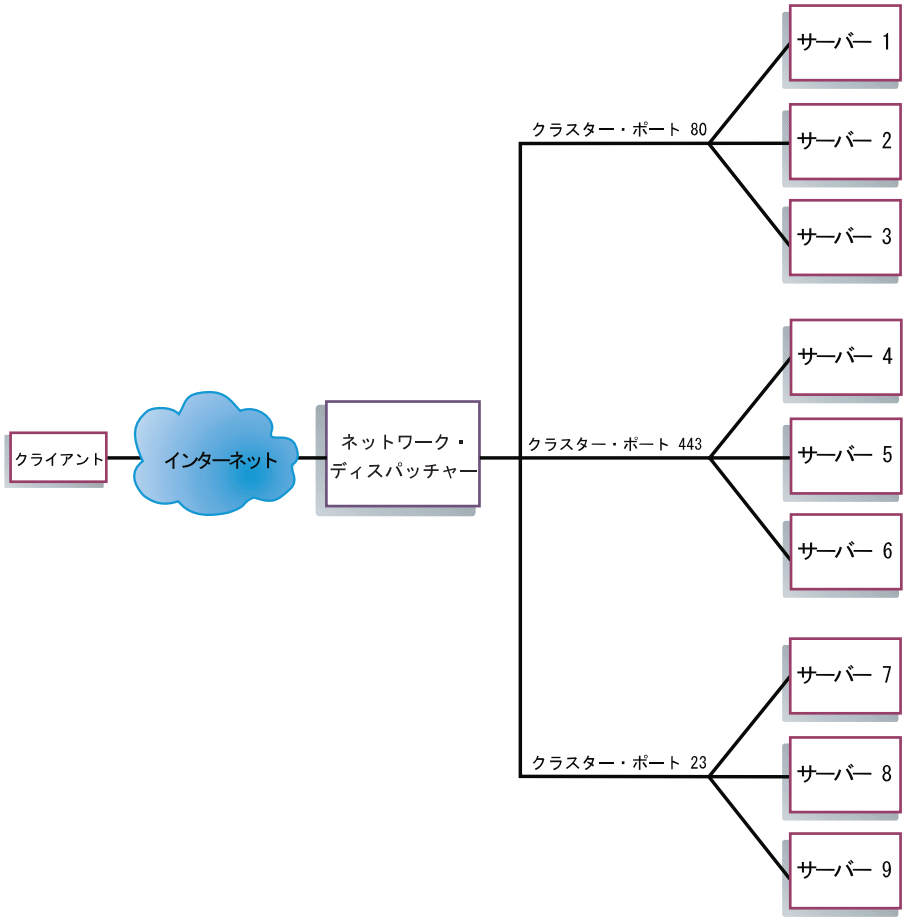


図7. 3 つのクラスターと 3 つのポートを持つように構成されたネットワーク・ディスパッチャーの例

構成ステップ

ネットワーク・ディスパッチャーを構成する前に、次のことを行います。

1. ネットワーク・ディスパッチャーにはサーバーへの直接インターフェースがあることを確認する (すなわち、各サーバー・マシンは、ネットワーク・ディスパッチャー・マシンだけに限られたサブネットに直接接続する必要があります)。ネットワーク・ディスパッチャー・フィーチャーはクライアントからサーバーへの受信トラフィックだけを見るため、サーバーはエンタープライズ・ルーターまたはインターネットへの独立した接続を持つことができ、これによりサーバーからクライアントへの発信トラフィックは、ネットワーク・ディスパッチャー・マシンをバイパスすることができます。これらのタイプの発信接続を可能にするために必要となる、特別のネットワーク・ディスパッチャー構成はありません。

   ユーザーのネットワークにとって高可用性が重要である場合は、113ページの図8に示した標準的な高可用性構成を参照してください。

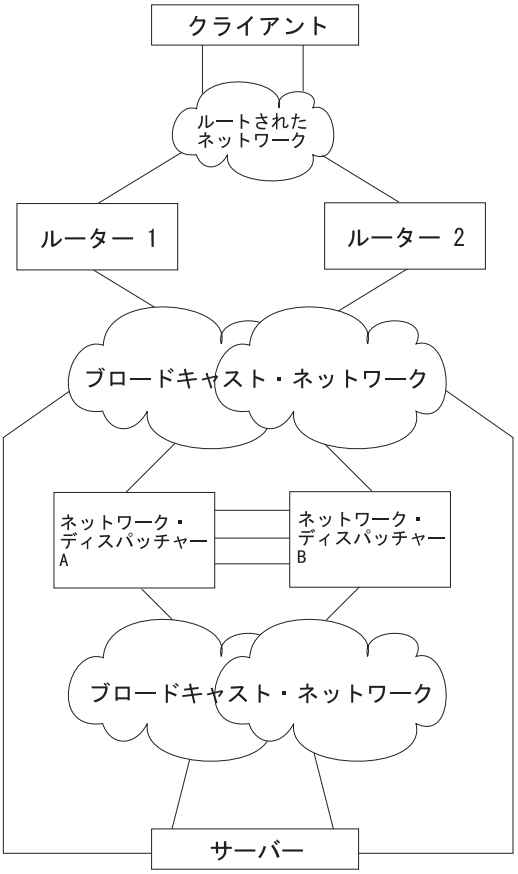


図 8. 高可用性ネットワーク・ディスパッチャー構成

2. ネットワーク・ディスパッチャー・マシンのインターフェースを構成する。この構成には、すべてのインターフェース、すべてのインターフェース上の IP アドレス、およびすべての該当するプロトコルが含まれます。ルーターの内部 IP アドレスはネットワーク・ディスパッチャーが使用するため、set internal-ip-address コマンドを使用して構成することも必要です。この内部 IP アドレスは、ネットワーク・ディスパッチャーに構成されているクラスター・アドレスに一致するものであってはなりません。**set internal-ip-address** コマンドについて詳しくは、*プロトコルの構成と監視 解説書 第 1 巻*「IP の構成と監視」を参照してください。
3. ネットワーク・ディスパッチャー・マシンをリブートまたはリスタートする。

IBM 2216 上のネットワーク・ディスパッチャーの構成

IBM 2216 上のネットワーク・ディスパッチャーを構成するには、次のようにします。

1. talk 6 では、**feature ndr** コマンドを使用して、ネットワーク・ディスパッチャー・フィーチャーにアクセスする。
2. **enable executor** および **enable manager** コマンドを使用して、実行プログラムとマネージャーを使用可能にする。
3. **add cluster** コマンドを使用してクラスターを構成する。クラスター・アドレスを公示するように構成する場合、詳細については、122ページの『クラスター・アドレス公示でのネットワーク・ディスパッチャーの使用』を参照してく

ださい。ネットワーク・ディスパッチャーにクラスター・アドレスを公示させないようにした場合、ネットワーク・ディスパッチャー・ルーターだけに限られた公示サブネットの一部であるクラスター・アドレスを選択する必要があります。このサブネットは、通常、ネットワーク・ディスパッチャーが次のホップ・クラスターからクライアント・トラフィックを受け取るサブネットです。

注: クラスター IP アドレスは、ルーターの内部 IP アドレスと一致するものであってならず、ルーター上で定義されているインターフェース IP アドレスと一致するものであってもなりません。同一のマシンでネットワーク・ディスパッチャーと TN3270 サーバーを稼働している場合、クラスター・アドレスは、ループバック・インターフェースに定義されている IP アドレスと一致させることができます。詳しくは、118ページの『TN3270 でのネットワーク・ディスパッチャーの使用』を参照してください。

4. 対応するプロトコルにサービスする各サーバー・クラスターに対して、**add port** コマンドを使用して、TCP および UDP 宛先ポートを構成する。通常のポートの例は、HTTP の場合は 80、FTP の場合は 20 または 21、および Telnet の場合は 23 です。
5. **add server** コマンドを使用して、サーバーを構成する。サーバーは、常にポートとクラスターに対応しています。1 つのサーバーは複数のポートにサービスすることができ (すなわち、同じクラスター用の複数のポートに 1 つのサーバーを定義できます)、サーバーのオペレーティング・システムが複数の別名をサポートする場合は、1 つのサーバーが複数のクラスターに所属することもできます。
6. **add advisor** コマンドを使用して、アドバイザーを構成する。

   注:

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

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

高可用性のネットワーク・ディスパッチャーを構成している場合は、次のステップを続けてください。そうでない場合は、これで構成は完了です。

注: 以下のステップは、1 次ネットワーク・ディスパッチャーで実行した後、バックアップでも実行してください。データベースが正しく同期化されるのを確認するために、バックアップの実行プログラムを使用可能にする前に、1 次ネットワーク・ディスパッチャーの実行プログラムを使用可能にしておくことが必要です。

8. **add backup** コマンドを使用して、このネットワーク・ディスパッチャーが 1 次であるかバックアップであるか、切り替えが手動であるか自動であるかを構成する。
9. **add heartbeat** コマンドを使用して、1 次ネットワーク・ディスパッチャーとバックアップ・ネットワーク・ディスパッチャー間のハートビートを実行するすべてのパスを構成する。パスは、発信元と宛先の IP アドレスで指定します。

   注: 1 つのインターフェースに障害が起きても、1 次とバックアップ・マシン間のハートビート通信が中断しないようにするために、1 次とバックアップ・ネットワーク・ディスパッチャー間には、複数のハートビート・パスを構成しておくことが必要になります。

   2 つのネットワーク・ディスパッチャー間の既存の LAN 接続が 1 つだけの場合、2 番目のハートビートを簡単な LAN 接続 (たとえば、クロス・ケーブルを 2 つのイーサネット・ポート間に直接接続できます) またはポイントツーポイントの逐次接続 (たとえば、無番号 IP を使用してヌル・モデム・ケーブルを介してのバックツーバック PPP 接続) で設定することもできます。
10. 完全なサービスを保証するために、**add reach** コマンドを使用して、ネットワーク・ディスパッチャーが到達できなければならないホスト IP アドレスのリストを構成する。通常は、これはサーバー、エンタープライズ・ルーター、または管理ステーションのサブセットになります。ネットワーク・ディスパッチャーのトラフィックが流入できるインターフェースごとに少なくとも 1 つの到達アドレスを構成する必要があります。

set、**remove**、および **disable** コマンドを使用して、構成を変更することができます。これらのコマンドの詳細については、127ページの『第9章 ネットワーク・ディスパッチャー・フィーチャーの構成と監視』を参照してください。

ネットワーク・ディスパッチャー用のサーバーの構成

サーバーをネットワーク・ディスパッチャーで使用できるように構成するには、次のようにします。

1. ループバック装置に別名を付ける。

   TCP および UDP サーバーが機能するためには、ループバック装置 (通常は ***lo0*** と呼ばれる) をクラスター・アドレスに設定する (できれば、別名を付ける) ことが必要です。ネットワーク・ディスパッチャーは、パケットをサーバー・マシンに転送する前に、IP パケット内の 宛先 IP アドレスを変更しません。ループバック装置をクラスター・アドレスに設定または別名指定した場合、サーバー・マシンはクラスター・アドレスあてのパケットを受け入れます。

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

ネットワーク・ディスパッチャーの使用

ネットワーク・インターフェースの別名指定をサポートするオペレーティング・システム (AIX、Solaris、または Windows NT など) を使用している場合は、ループバック装置の別名をクラスター・アドレスに指定する必要があります。別名をサポートするオペレーティング・システムを使用する利点は、複数のクラスター・アドレスにサービスするようにサーバー・マシンを構成できることです。

別名をサポートしないオペレーティング・システム (HP-UX および OS/2 など) を使用している場合は、***lo0*** をクラスター・アドレスとして設定する必要があります。

サーバーが、TCP/IP V3R2 を実行する MVS システムの場合、VIPA アドレスをクラスター・アドレスとして設定する必要があります。これはループバック・アドレスとして機能します。VIPA アドレスは、MVS ノードに直接接続されたサブネットに属していてはなりません。MVS システムが TCP/IP V3R3 を実行している場合は、ループバック装置をクラスター・アドレスとして設定する必要があります。高可用性を使用している場合、高可用性引き継ぎ機構を正しく機能させるためには、MVS システム内の RouteD を使用可能にしなければなりません。

注: この章に示されているコマンドは、次のオペレーティング・システムおよびレベルでテスト済みです。すなわち、AIX 4.1.5 と 4.2、HP-UX 10.2.0、Linux、OS/2 Warp Connect バージョン 3.0、OS/2 Warp バージョン 4.0、Solaris 2.6 (Sun OS 5.6)、Windows NT 3.51 および OS/390 です。

ループバック装置の設定または別名指定には、表11 に示すように、ご使用のオペレーティング・システムのコマンドを使用してください。

表 11. ディスパッチャーのループバック装置の別名指定用のコマンド

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

表 11. ディスパッチャーのループバック装置の別名指定用のコマンド (続き)

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

OS/390	OS/390 システム上にループバック別名を構成する。
	• IP パラメーター・メンバー (ファイル) で、管理者はホーム・アドレス・リストに 1 つのエントリーを作成することが必要になる。たとえば、次のようにします。
	`HOME`
	`;Address Link`
	`192.168.252.11 tr0`
	`192.168.100.100 ltr1`
	`192.168.252.12 loopback`
	• いくつかのアドレスをループバックに定義できる。
	• デフォルトとして 127.0.0.1 が構成される。

2. 余分なルートがないかチェックする。

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

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

   b. 次のコマンドを使用してすべての UNIX® システムおよび OS/2® に余分なルートがないかどうかチェックする。**netstat -nr**

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

```
Active Routes:
      Network Address          Netmask  Gateway Address       Interface  Metric
              0.0.0.0          0.0.0.0       9.67.128.1     9.67.133.67     1
```

```
      9.0.0.0        255.0.0.0     9.67.133.158     9.67.133.158     1
    9.67.128.0    255.255.248.0     9.67.133.67      9.67.133.67     1
   9.67.133.67  255.255.255.255       127.0.0.1        127.0.0.1     1
  9.67.133.158  255.255.255.255       127.0.0.1        127.0.0.1     1
 9.255.255.255  255.255.255.255     9.67.133.67      9.67.133.67     1
     127.0.0.0        255.0.0.0       127.0.0.1        127.0.0.1     1
     224.0.0.0        224.0.0.0     9.67.133.158     9.67.133.158     1
     224.0.0.0        224.0.0.0     9.67.133.67      9.67.133.67     1
255.255.255.255  255.255.255.255     9.67.133.67      9.67.133.67     1
```

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

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

```
      9.0.0.0        255.0.0.0     9.67.133.158     9.67.133.158     1
```

3. 余分なルートを削除する。

   余分なルートを削除するには、表12 から、該当するオペレーティング・システムのコマンドを使用します。

表 12. 各種オペレーティング・システムのルート削除コマンド

オペレーティング・システム	コマンド
AIX	**route delete -net** *network_address cluster_address*
HP-UNIX	**route delete** *cluster_address cluster_address*
Solaris	ルートを削除する必要はありません。
OS/2	ルートを削除する必要はありません。
Windows NT	**route delete** *network_address cluster_address* **注:** a. このコマンドは MS-DOS プロンプトで入力する必要があります。 b. Windows NT の場合、サーバーをリブートするたびに余分のルートを削除する必要があります。 c. サーバーをリブートするたびに余分のルートを手作業で除去しなくてもよいようにするには、サーバーをリブートしたあとで余分のルート自動的に削除する Windows NT リソース・キットを使用して、サービスを作成して導入することもできます。

TN3270 でのネットワーク・ディスパッチャーの使用

ネットワーク・ディスパッチャーは、大規模な 3270 環境に TN3270E サーバー・サポートを提供するために TN3270E サーバー機能を稼働している 2210、2212、ネットワーク・ユーティリティー、または 2216 のクラスターで使用することができます。TN3270 アドバイザーを使用して、ネットワーク・ディスパッチャーは各 TN3270E サーバーからロードの統計をリアルタイムで収集し、ロードを TN3270E サーバー間に可能な限り最適に配分することができます。ネットワーク・ディスパ

ッチャー・ルーターの外部の TN3270E サーバーに加えて、クラスター内の TN3270E サーバーの中の 1 台を内部にする、つまりネットワーク・ディスパッチャーと同じルーター内で稼働することができます。

構成の要点

外部 TN3270E サーバーの構成 (すなわち、TN3270E サーバーはネットワーク・ディスパッチャーと同じルーターでは稼働していない) は、スタンドアロンの TN3270E サーバーを設定するのと本質的に同一です。実際に、TN3270E サーバーは、クライアントからのトラフィックが別のマシンを経由して転送されたかどうかを認識しません。ただし、次のように、ネットワーク・ディスパッチャー用に外部 TN3270E サーバーを設定する際には、いくつかの点に注意する必要があります。

- TN3270E サーバーを設定するときには、TN3270E サーバーの IP アドレスをインターフェース・アドレスとしてサーバー・マシン上に構成する必要もあります。クライアントはパケットを TN3270E サーバーの IP アドレスに送信し、サーバー・マシンは、この場合 TN3270E サーバー機能であるローカル機能へ送信するためにパケットを受信します。 TN3270E サーバーの前にネットワーク・ディスパッチャーを使用して、クライアントはパケットをネットワーク・ディスパッチャー・クラスターの IP アドレスに送信し、ネットワーク・ディスパッチャーはパケットを変更せずにサーバーに転送し、パケットは、クラスター IP アドレスと同じ宛先 IP アドレスをもつサーバー・マシンに到達します。したがって、それぞれのサーバーにある TN3270 サーバーの IP アドレスは、クラスターの IP アドレスと同じに設定されなければならず、クラスターの IP アドレスをインターフェース・アドレス (どの IP 使用可能のインターフェースでもかまわない) として各サーバー・マシンで定義することも必要となり、これによって、パケットは TN3270E サーバー機能へローカル送信されるためにサーバー・マシンによって受信されます。
- TN3270E サーバー上で使用されているルーティング・プロトコル (たとえば、OSPF または RIP) の中に、クラスター・アドレスを公示するものが含まれていないことを確認しなければなりません。クライアント・ネットワークに関する限り、ネットワーク・ディスパッチャー・ルーターはクラスター・アドレスを 『独占』 している必要があります。
- クライアントからネットワーク・ディスパッチャーへのトラフィックが、ネットワーク・ディスパッチャーからサーバーへのトラフィックと同じ LAN 上を流れる場合、クラスター・アドレスへの ARP に対してサーバーが応答しないようにする必要があります。すなわち、サーバーのインターフェース上では、クラスター・アドレスをこの LAN に定義することはできません。ネットワーク・ディスパッチャーだけがクライアントのトラフィックをネットワークから受け取る LAN (または複数の LAN) 上の ARP に応答するようにする必要があります。別の方法として、クラスター・アドレスを別のインターフェース上のインターフェース・アドレスとして TN3270E サーバー上に構成したり、TN3270E サーバーの内部 IP アドレスとして構成することもできます。
- ネットワーク・ディスパッチャーでは、各 TN3270E サーバーを固有のサーバー IP アドレスで構成する必要があります。これは、ネットワーク・ディスパッチャーがサーバーを見つけるために使用するアドレスです。このアドレスを、TN3270E サーバー機能を実行するルーター上でインターフェース・アドレスとして構成することも必要です。固有なサーバーの IP アドレスが、ネットワーク・ディスパッチャーに対してローカルなサブネットの一部でない場合には、ネット

ワーク・ディスパッチャーは、このネットワーク・ディスパッチャー・マシンに定義された静的ルートを経由してか、またはこのサーバーの固有な IP アドレスを公示するルーティング・プロトコルを経由するかのいずれかによって、サーバーを必ず見付けることができます。

- 非活動期間がクラスターのステール・タイムアウトを超過したときに TN3270 接続がネットワーク・ディスパッチャー接続テーブルから早過ぎる時点で除去されないようにするために、 TN3270E サーバーのキープアライブ・タイマーを、クラスターのステール・タイムアウトより小さいタイムアウト値を用いたタイミング・マーク・モードで構成する必要があります。 TN3270E サーバーはメッセージをクライアントに送信し、接続がステールにならないようにする応答を期待します。

TN3270E サーバーがネットワーク・ディスパッチャーと同じルーター内にある場合は、次のことが適用されます。

- 内部 TN3270E サーバーに対してロード・バランスされているパケットは、パケットの宛先 IP アドレスとしてクラスター・アドレスを引き続きもつため、TN3270E サーバー IP アドレスをクラスター・アドレスとして構成する必要があります。
- TN3270E サーバーがネットワーク・ディスパッチャー・マシンの外部である場合は、パケットが TN3270E サーバー機能にローカルに送信できるようにするため、TN3270E サーバー IP アドレスをルーター上で内部 IP アドレスまたはインターフェース・アドレスとして定義する必要があります。TN3270E サーバーがネットワーク・ディスパッチャー・ルーターの内部である場合は、TN3270E サーバー IP アドレスをルーター上で内部 IP アドレスまたはインターフェース・アドレスとして定義してはなりません。TN3270E サーバー IP アドレス (すなわち、クラスター・アドレス) が内部 IP アドレスまたはインターフェース・アドレスとして定義されている場合、パケットはネットワーク・ディスパッチャーには到達せず、ルーター内の TN3270E サーバー機能に直接送られます。
- ネットワーク・ディスパッチャーでは、各 TN3270E サーバーを固有のサーバー IP アドレスで構成する必要があります。内部 TN3270E サーバーの場合、サーバーの固有の IP アドレスをネットワーク・ディスパッチャー・マシンの内部 IP アドレスと同じにして構成します。
- V3.4 より前では、TN3270E サーバーをネットワーク・ディスパッチャーによる内部または外部アクセスのいずれかに設定することもできますが、内部および外部の両方にはできず、また切り替えることもできません。したがって、両方のネットワーク・ディスパッチャー・ルーター内で内部 TN3270E サーバーについてネットワーク・ディスパッチャー高可用性ソリューションを導入する際に、一方のルーター内のネットワーク・ディスパッチャーが他方のネットワーク・ディスパッチャー・ルーター内の TN3270E サーバーに対してロード・バランスを取ることはできません。

  両方のネットワーク・ディスパッチャー・ルーター内で内部 TN3270E サーバーについてネットワーク・ディスパッチャー高可用性ソリューションを導入する際に、MAS V3.4 からは、内部 TN3270E サーバーをどちらかのネットワーク・ディスパッチャーがアクセスするように設定できます。このためには、両方のネットワーク・ディスパッチャー・ルーターにループバック装置を追加して、各ループバック・インターフェース上に TN3270E サーバー IP アドレス (すなわち、クラスター・アドレス) を定義するだけです。ネットワーク・ディスパッチャーが

活動状態にある場合、ループバック・インターフェース上のクラスター・アドレスは使用不能になるため、このクラスター・アドレスあてのパケットはネットワーク・ディスパッチャーに到達します。ネットワーク・ディスパッチャーが待機状態にある場合、ループバック・インターフェース上のクラスター・アドレスは使用可能になるため、このクラスター・アドレスあてのパケットは TN3270E サーバーにローカルで送信されます。このようにして、内部 TN3270E サーバーを高可用性設定で両方のネットワーク・ディスパッチャーが使用することができます。

活動ネットワーク・ディスパッチャー・マシンは、クラスター・アドレス用の ARP に対応する唯一のマシンでなければなりません。クラスター・アドレスがループバック・インターフェース上の両方のネットワーク・ディスパッチャー・マシンに定義されるため、プロキシー ARP を両方のネットワーク・ディスパッチャー・マシンで使用不能にして待機ネットワーク・ディスパッチャーがこのクラスター・アドレスの ARP に応答できなくする必要があります。

活動ネットワーク・ディスパッチャー・マシンは、クライアント・ネットワークに関する限り、クラスター・アドレスを所有もしなければならず、したがって、待機ネットワーク・ディスパッチャー・マシン (ループバック・インターフェース上に定義されたクラスター・アドレスをもつ) は、クラスター・アドレスを公示できません。RIP はデフォルトで、ホスト・ルート (マスク 255.255.255.255 をもつルート) を公示しませんが、ホスト・ルートの公示を使用可能にした場合には、RIP ポリシーを定義してクラスター・アドレスの公示を明確に使用不能にする必要があります。

次の例は、RIP がクラスター IP アドレス (ここでは、10.0.0.1 を想定) を公示できなくするポリシーを示します。2 番目のポリシー項目は RIP がすべての他のルートを公示できるようにすることに注意してください。

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

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

OSPF の場合、AS バウンダリー・ルーティングおよび直接ルートのインポートが使用可能になっている場合、または OSPF がループバック・インターフェース上で使用可能になっている場合には、ループバック・インターフェース上に定義さ

れたクラスター・アドレスは公示され、ユーザーはこのクラスター・アドレスの公示を明確に使用不能にする OSPF ポリシーを定義する必要があります。

次の例は、OSPF がクラスター IP アドレス (ここでは、10.0.0.1 を想定) をインポートできなくするポリシーを示します。2 番目のポリシー項目は OSPF がすべての他のルートをインポートできるようにすることに注意してください。

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

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

明示的な LU とネットワーク・ディスパッチャー

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

クラスター・アドレス公示でのネットワーク・ディスパッチャーの使用

クラスター・アドレス公示を使用すると、ネットワーク・ディスパッチャーに定義された各クラスター・アドレスを必ずネットワーク・ディスパッチャー・マシンで使用可能にされたルーティング・プロトコルによって公示されるように構成できます。公示されないクラスター・アドレスの場合、ネットワーク・ディスパッチャー・マシンに対してローカルな公示サブネットの一部であるクラスター・アドレスを選択する必要があります。公示されるように構成されているクラスター・アドレ

スは、ホスト・ルートとして公示され、公示サブネットの一部である必要はありません。クラスター・アドレスの公示は、次の使用例において有用です。

- 同じ内容をもつ、地理的に分散された複数のサーバー・サイトがあって、クライアントにもっとも近いサーバー・サイトに接続させたい。これは、すべてのサーバー・サイトで同じクラスター・アドレスを構成し、これらのサイトすべてからこれらのクラスター・アドレスを公示することによって、クラスター・アドレスの公示を使用して行うことができます。次に、ネットワークにあるルーティング・プロトコルは、それぞれのクライアント接続をもっとも近いサーバー・サイトに送信します。もっとも近いサイトがダウンしている場合には、接続は次にもっとも近いサーバー・サイトに向けられます。ネットワークでの変更 (ルーターまたは通信リンクがダウンしたり、アップする)またはサーバー・サイトの可用性の変更は、既存のクライアント/サーバー接続の最中であっても、もっとも近いサーバーを変更できることに注意してください。HTTP のような短い接続についての問題ではなくて、Telnet または TN3270 のような長い接続についての問題と考えることができます。
- クラスター・アドレス公示を使用すると、古典的な IP ATM ネットワーク上でネットワーク・ディスパッチャー高可用性を利用することができます。待機ネットワーク・ディスパッチャーが活動ネットワーク・ディスパッチャーから引き継ぐと、すべてのインターフェース上で余分の ARP を送信して、クラスター・アドレスあてのそれ以降のトラフィックが新しい MAC アドレスに送信されます。古典的な IP ATM では、ARP サーバーは更新されますが、ARP サーバーはクライアントにキャッシュのリフレッシュを強制することはできません。クライアント・キャッシュは、当該クライアントに構成されたリフレッシュ・タイムアウトが期限切れになるまでは更新されません。これは、数分かかります。1 次ネットワーク・ディスパッチャーの ATM アドレスをキャッシュしていないクライアントからの新しい接続は、即刻バックアップのネットワーク・ディスパッチャーに対して行われますが、引き継ぎの時点で存在する接続は切断され、このクライアントのクライアント・リフレッシュ・タイマーの設定時間を経過して、クライアントのキャッシュが更新されるまでは再確立されることはありません。ルーターをもつ ATM サブネットの一部ではないクラスター・アドレスを定義して、これらのクラスター・アドレスを公示することによって、ルーティング・プロトコルは、ここでクラスター・アドレスあてのトラフィックが正しいネットワーク・ディスパッチャーにルートされるようにします。1 次ネットワーク・ディスパッチャーは、待機状態に入るときにクラスター・アドレスの公示を停 止し、バックアップが活動ネットワーク・ディスパッチャーになるときにバックアップはクラスター・アドレスの公示を開始します。

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

- RIP の場合、ホスト・ルートの送信を使用可能にする必要がある。
- OSPF の場合、AS バウンダリー・ルーティングを使用可能にし、直接およびサブネットの両方のルートをインポートする必要がある。
- BGP の場合、発信ポリシーのアドレス範囲には公示済みクラスター・アドレスが含まれていることを確認し、無クラス bgp を使用可能にする必要があります。

Web サーバー・キャッシュでのネットワーク・ディスパッチャーの使用

Web サーバー・キャッシュ用のクラスターとポートを定義するには、ネットワーク・ディスパッチャーを使用する必要があります。*cache* モードのポートを定義すると、キャッシュ区画を構成するように指示するプロンプトが出ます。例については、221ページの『第12章 Web サーバー・キャッシュの構成と監視』の **add port** コマンドの項を参照してください。キャッシュ区画の構成値は、後で `Config>` プロンプトで **f webc** コマンドを入力して Web サーバー・キャッシュ・フィーチャー構成に直接進み、ここで変更することができます。Web サーバー・キャッシュについて詳しくは、179ページの『第11章 Web サーバー・キャッシュの使用』および 221ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。

eNetwork ホスト・オンデマンド・クライアント・キャッシュでのネットワーク・ディスパッチャーの使用

ホスト・オンデマンド・クライアント・キャッシュ用のクラスターとポートを定義するには、ネットワーク・ディスパッチャーを使用する必要があります。*hod client cache* モードのポートを定義すると、キャッシュ区画を構成するように指示するプロンプトが出ます。例については、162ページの『ホスト・オンデマンド・クライアント・キャッシュの構成』の **add port** コマンドの項を参照してください。キャッシュ区画の構成値は、後で `Config>` プロンプトで **f hod** コマンドを入力してホスト・オンデマンド・クライアント・キャッシュ・フィーチャー構成に直接進み、ここで変更することができます。ホスト・オンデマンド・クライアント・キャッシュについて詳しくは、161ページの『第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの構成と監視』を参照してください。

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

Web サーバー・キャッシュのグループをもつネットワーク・ディスパッチャーを使用してスケーラブル高可用性キャッシュを作成できます。スケーラブル高可用性キャッシュ (SHAC)は、1 台または複数台のネットワーク・ディスパッチャー・マシン (2 番目は 1 番目のバックアップになるために使用される)、2 台以上の Web サーバー・キャッシュ・マシン、および少なくとも 1 台のバックエンド・サーバーから構成されます。 125ページの図9 は、SHAC セットアップの例を示します。ネットワーク・ディスパッチャー・マシンは、キャッシュ・マシンへのクライアント・トラフィックをロード・バランスして、キャッシュ・マシンは、キャッシュからファイルをサービスする、またはファイルがキャッシュされている場合にはファイルをバックエンド・サーバーから入手します。

ネットワーク・ディスパッチャーを Web サーバー・キャッシュ・マシン (『Web サーバー・キャッシュでのネットワーク・ディスパッチャーの使用』を参照) で使用する必要があり、これによってネットワーク・ディスパッチャーはネットワーク・ディスパッチャー・マシンおよびすべてのキャッシュ・マシンで実際に実行しています。

ネットワーク・ディスパッチャー・マシンでは、クラスターとポートを構成し、ポートのモードを *extcache* に設定して外部スケーラブル・キャッシュ・アレイをロード・バランスしていることを示す必要があります。 128ページの『Add』の **add port** コマンドを参照してください。ポートの下では、キャッシュ・マシンはサーバーとして構成されます。他のサーバーと同様に、キャッシュのインターフェース IP アドレスは、ネットワーク・ディスパッチャー・マシンに構成された固有なサーバー IP アドレスのために使用されます。SHAC にとって、アドバイザーおよびマネージャーは重要です。HTTP アドバイザーは、外部キャッシュ (すなわち、ポート・モードは extcache) があるどのポートのネットワーク・ディスパッチャー・マシンでも使用可能にする必要があります。キャッシュが作動可能であるかどうかを判別するためにアドバイザー照会が使用されます。マネージャーを使用可能にし、重み計算にアドバイザー入力を含めるようにマネージャー比率を設定する (すなわち、アドバイザー・パーセントを 0 より大きい値に設定する) 必要があります。

ネットワーク・ディスパッチャー・マシンのクラスター/ポートの下でサーバーとしてキャッシュを構成するとき、同じクラスターとポートをキャッシュ・マシンのネットワーク・ディスパッチャー機能に構成する必要もあります。キャッシュ・マシンに定義されたポートは、モード cache に設定しなければならず、バックエンド・サーバーはこれらのポートの下のサーバーとして定義されます。また、HTTP アドバイザーは、キャッシュ・マシンで実行され、これらのマシンはバックエンド・サーバーのロードと使用可能性を判別できるようになります。

1 つのネットワーク・ディスパッチャー・マシンは、複数の SHAC クラスターのロード・バランスができます。詳しくは、186ページの『スケーラブルな高可用性キャッシュ』 を参照してください。

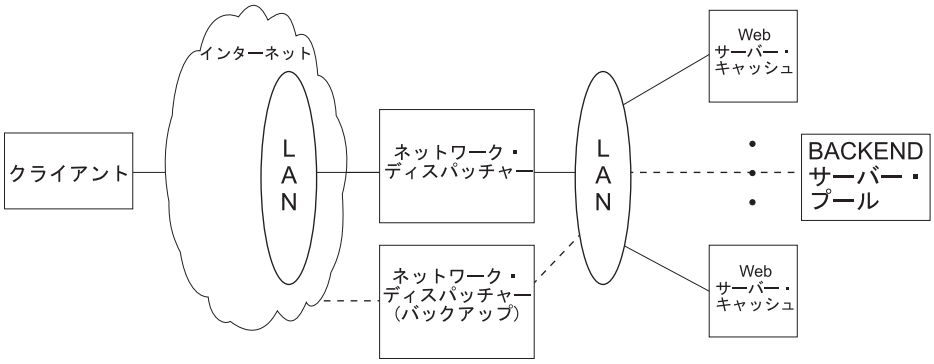


図 9. Lan 接続サーバー

第9章 ネットワーク・ディスパッチャー・フィーチャーの構成と監視

この章では、ネットワーク・ディスパッチャー・フィーチャーの構成コマンドおよびオペレーショナル・コマンドについて説明します。この章には、次の内容が記載されています。

- 『ネットワーク・ディスパッチャー構成コマンドへのアクセス』
- 『ネットワーク・ディスパッチャー構成コマンド』
- 148ページの『ネットワーク・ディスパッチャー監視コマンドへのアクセス』
- 148ページの『ネットワーク・ディスパッチャー監視コマンド』
- 157ページの『ネットワーク・ディスパッチャー動的再構成サポート』

ネットワーク・ディスパッチャー構成コマンドへのアクセス

ネットワーク・ディスパッチャー構成環境にアクセスするには、次のようにします。

1. OPCON プロンプト (*) で **talk 6** と入力する。
2. `Config >` プロンプトで **feature ndr** コマンドを入力する。

ネットワーク・ディスパッチャー構成コマンド

表13 は、ネットワーク・ディスパッチャー構成コマンドの要約を示しており、表の後に個々のコマンドの説明があります。これらのコマンドは `NDR Config >` プロンプトで入力します。

表 13. ネットワーク・ディスパッチャー構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add	ネットワーク・ディスパッチャーの各種のコンポーネント (アドバイザー、クラスター、ポート、およびサーバーを含む) を構成します。
Clear	ネットワーク・ディスパッチャー構成全体をクリアします。
Disable	ネットワーク・ディスパッチャーのバックアップ、実行プログラム、およびマネージャー・コンポーネントを使用不可にします。特定のアドバイザーも使用不可にします。
Enable	ネットワーク・ディスパッチャーのバックアップ、実行プログラム、およびマネージャー・コンポーネントを使用可能にします。特定のアドバイザーも使用可能にします。
List	ネットワーク・ディスパッチャー構成全体または構成の特定部分を表示します。
Remove	ネットワーク・ディスパッチャー構成の特定部分を除去します。
Set	アドバイザー、クラスター、ポート、サーバー、またはネットワーク・ディスパッチャー・マネージャーの構成パラメーターを変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Add

add コマンドは、アドバイザー、クラスター、ポート、サーバー、および到達可能アドレスを構成するのに使用します。高可用性の場合には、このネットワーク・ディスパッチャーが 1 次かバックアップかを構成することができ、ハートビートおよびデータベース同期に使用する IP アドレスも構成できます。

構文:

add

advisor . . .

backup . . .

cluster . . .

heartbeat . . .

port . . .

reach . . .

server . . .

Advisor *name port# interval timeout comm-port*

アドバイザーの名前とポートを指定します。このパラメーターは、アドバイザーが特定のプロトコルに関する情報を収集する頻度、およびアドバイザー・レポートの有効期限が切れたと見なすまでに必要な時間数も指定します。

name アドバイザーのタイプを指定します。追加したいアドバイザーのタイプに対応するアドバイザー番号を入力します。

表 14. アドバイザー名とポート番号

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

有効値 : 0 ～ 8

デフォルト値 : 1

port# このアドバイザーのポート番号を指定します。

有効値 : 1 ～ 65535

デフォルト値 : 表14 を参照

interval

アドバイザーが各サーバーのプロトコルを照会する頻度 (秒数) を指定します。この値の半分の時間、サーバーから応答がないと、アドバイザーはそのプロトコルを利用不能と見なします。

有効値 : 1 ～ 65535

デフォルト値 : 5

timeout

アドバイザー・レポートの有効期限が切れたと見なすまでの、時間間隔 (秒数) を指定します。

マネージャーは、負荷平衡を決めるのに期限切れ情報を使用するのを防止するために、このパラメーターに設定された時刻より古いタイム・スタンプをもつアドバイザーからの情報を使用しません。アドバイザー・タイムアウトは、アドバイザー・ポーリング間隔より大きい値でなければなりません。タイムアウトの方が小さいと、マネージャーは使用する必要がある報告を無視してしまいます。デフォルトでは、アドバイザーの報告はタイムアウトになりません。

このタイムアウト値は通常、アドバイザーを使用不可にした場合に適用されます。このパラメーターを、前に説明した interval/2 タイムアウト (これは、サーバーの応答がない時間に関するものです) と混同しないでください。

有効値 : 0 〜 65535

デフォルト値 : 0。これは、アドバイザー・レポートが期限切れにならないことを意味しています。

comm-port

TN3270 アドバイザーが TN3270 サーバーと通信するのに使用するポート番号を指定します。このパラメーターは、TN3270 アドバイザーの入力にだけ使用します。 TN3270 サーバー構成に設定されたアドバイザーのポート番号に一致する必要があります。

有効値 : 1 〜 65535

デフォルト値 :

- TN3270 デフォルト値 : 10008

注: マネージャー・コンポーネントはアドバイザーの前提条件なので、アドバイザーを使用可能にする前に、マネージャーを使用可能にしておく必要があります。ロード・バランシングの決定を行うのに使用されるサーバーの重みを設定する際にマネージャーがアドバイザー入力を考慮するようにマネージャーの比率を設定することも必要です。アドバイザーが正しく稼働するためには、**set internal-ip-address** コマンドを使用して、内部 IP アドレスを設定しておくことも必要です。 **set internal-ip-address** コマンドについて詳しくは、*プロトコルの構成と監視 解説書 第 1 巻* の「IP の構成と監視」を参照してください。

例 1:

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

例 2:

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

backup *role strategy*

このネットワーク・ディスパッチャーがバックアップであるか、1 次であるかを指定します。

role これが 1 次ネットワーク・ディスパッチャーであるか、バックアップ・ネットワーク・ディスパッチャーであるかを定義します。このコマンドは、冗長構成を使用し、高可用性機能を実行したい場合にだけ使用します。その場合には、ハートビート (**add heartbeat**) および到達可能性 (**add reach**) も構成する必要があります。

有効値 : 0 または 1

0 = 1 次

1 = バックアップ

デフォルト値 : 0

strategy

ネットワーク・ディスパッチャーは、自動的に 1 次モードに戻るのか、手動で戻すのかを指定します。1 次ネットワーク・ディスパッチャーに障害が起きてスタンドバイになり (バックアップが IP 引き継ぎ機能を実行したことを意味します)、その後で再び利用可能になったとき、strategy が *automatic* に設定されている場合は、データベースが同期されるとただちに自動的にアクティブ・ネットワーク・ディスパッチャーになります。strategy が *manual* に設定されている場合、元の 1 次はスタンドバイ・モードになり、オペレーターが talk 5 で **switchover** コマンドを使用しないと、再びそれをアクティブ状態にすることはできません。156ページの『Switchover』を参照してください。

有効値 : 0 または 1

0 = 自動

1 = 手動

デフォルト値 : 0

例:

```
add backup
Role (0=Primary, 1=Backup) [0]?
Switch back strategy (0=Auto, 1=Manual) [0]?
```

cluster *address FIN-count FIN-timeout Stale-timer Advertise-cluster-address Advertise-route-cost*

クラスターの IP アドレス、および実行プログラムがネットワーク・ディスパッチャー・データベースから不要情報収集を行う頻度を指定します。クラスター・アドレスを公示するように構成する場合、詳細については、122ページの『クラスター・アドレス公示でのネットワーク・ディスパッチャーの使用』を参照してください。公示されるように構成されていないクラスター・アドレスの場合、ネットワーク・ディスパッチャー・マシンに対してローカルな公示サブネットの一部であるクラスター・アドレスを選択する必要

があります。このサブネットは、通常、ネットワーク・ディスパッチャーが次のホップ・クラスターからクライアント・トラフィックを受け取るサブネットです。

注: クラスター IP アドレスは、ルーターの内部 IP アドレスと一致するものであってならず、ルーター上で定義されているインターフェース IP アドレスと一致するものであってもなりません。同一のマシンでネットワーク・ディスパッチャーと TN3270 サーバーを稼働している場合、クラスター・アドレスは、ループバック・インターフェースに定義されている IP アドレスと一致させることができます。詳しくは、118ページの『TN3270 でのネットワーク・ディスパッチャーの使用』 を参照してください。

アドレス (address)
クラスターの IP アドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

FIN-count
実行プログラムが *FIN-timeout* または *Stale-timer* の経過後にネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に、FIN 状態にあることが必要な接続の数を指定します。

有効値 : 0 〜 65535

デフォルト値 : 4000

FIN-timeout
接続が FIN 状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みます。

有効値 : 0 〜 65535

デフォルト値 : 30

Stale-timer
接続が非アクティブ状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから接続の情報の除去を試みます。

有効値 : 0 〜 65535

デフォルト値 : 1500

Advertise-cluster-address
クラスター・アドレスを公示するかどうかを指定します。

有効値 : yes または no

デフォルト値 : no

Advertise-route-cost
公示したルートのコストを指定します。この質問が出されるのは、**advertise cluster address** への応答が *yes* の場合だけです。

有効値 : 0 ～ 4294967295

デフォルト値 : 0

例:

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

heartbeat *address1 address2*

ハートビート・メッセージ用の 1 つのパスを指定します。ハートビート・メッセージは、*address1* (このネットワーク・ディスパッチャーに属する) から *address2* (相手のネットワーク・ディスパッチャーに属する) へ流れます。

注: 1 つのインターフェースに障害が起きても、1 次とバックアップ・マシン間のハートビート通信が中断しないようにするために、1 次とバックアップ・ネットワーク・ディスパッチャー間には、複数のハートビート・パスを構成しておくことが必要になります。

2 つのネットワーク・ディスパッチャー間の既存の LAN 接続が 1 つだけの場合、2 番目のハートビートを簡単な LAN 接続 (クロス・ケーブルを 2 つのイーサネット・ポート間に直接接続できます) またはポイントツーポイントの逐次接続 (無番号 IP を使用してヌル・モデム・ケーブルを介してのバックツーバック PPP 接続) で設定することもできます。

address1

ハートビート・メッセージの発信元のこのネットワーク・ディスパッチャーのインターフェースの IP アドレスを指定します。

有効値 : 任意の IP アドレス

デフォルト値 : 0.0.0.0

address2

ハートビート・メッセージの着信先のピア・ネットワーク・ディスパッチャーのインターフェースの IP アドレスを指定します。このアドレスは、*address1* に指定されたインターフェースから到達可能でなければなりません。

有効値 : 任意の IP アドレス

デフォルト値 : 0.0.0.0

例:

```
add heartbeat
Source Heartbeat address [0.0.0.0]? 131.2.25.90
Target Heartbeat Address [0.0.0.0]? 131.2.25.92
```

port *cluster-address port# port-type max-weight port-mode*

ポートとポートの属性を指定します。

cluster-address
クラスターの IP アドレスを指定します。

有効値 : 任意の IP アドレス

デフォルト値 : 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : 80

port-type
このポートでロード・バランスを取ることができる IP トラフィックのタイプを指定します。サポートされるタイプは、次のとおりです。

- 1 = TCP
- 2 = UDP
- 3 = 両方

有効値 : 1、2、3

デフォルト値 : 3

max-weight
このポート上のサーバーの最大重みを指定します。これは、実行プログラムが各サーバーに与える要求数の差異に影響します。

有効値 : 0 〜 100

デフォルト値 : 20

port-mode
ポートが、1 つのクライアントからのすべての要求を 1 つのサーバーに送る (sticky と呼ばれる) か、パッシブ ftp を使用する (pftp) か、 Web サーバー・キャッシュを使用する (cache) か、外部スケーラブル・キャッシュ・アレイを送る (extcache) か、ホスト・オンデマンド・クライアント・キャッシュを使用するか、あるいはこのクラスターでは特定のプロトコルを使用しない (none) かを指定します。

有効値 : 0 〜 5。値は、それぞれ次のものを示します。

- 0 = none
- 1 = sticky
- 2 = pftp
- 3 = cache
- 4 = extcache
- 5 = hod client cache

デフォルト値 : 0

例:

```
Config>feature ndr
NDR>add cluster 1.2.3.4 4000 30 1500
NDR>add port
Cluster address [0.0.0.0]? 1.2.3.4
```

```
Port number [80]? 80
Port type [3]?
Maximum weight [20]?
Port mode [0=none, 1=sticky, 2=pftp, 3=cache 4=extcache 5=hod client cache ]? 0
```

注:

1. ポート・モード 3 (cache=3) を選択した場合は、221ページの『第12章 Web サーバー・キャッシュの構成と監視』でWeb サーバー・キャッシュに関する情報を参照してください。
2. ポート・モード 5 (hod client cache=5) を選択した場合は、161ページの『第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの構成と監視』でWeb サーバー・キャッシュに関する情報を参照してください。

reach *address*

ネットワーク・ディスパッチャーが正しく作動するために到達可能であることが必要なホスト・アドレスを指定します。これは、サーバー・アドレス、ルーター・アドレス、管理ステーション・アドレス、あるいはその他の IP ホストのいずれでも構いません。

アドレス (address)

ターゲット IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値 : 0.0.0.0

例:

```
add reach
Address to reach [0.0.0.0]?
```

server *cluster-address port# server-address server-weight server-state*

クラスター内のサーバーの属性を指定します。

cluster-address

このサーバーが属するクラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値 : 0.0.0.0

port# このサーバーへの接続を介して実行されるプロトコルを指定します。

有効値 : 1 〜 65535

デフォルト値 : 80

server-address

サーバーの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値 : 0.0.0.0

server-weight

実行プログラムのために、サーバーの重みを指定します。これは、ネットワーク・ディスパッチャーがこの特定サーバーに要求を送信する頻度に影響を与えます。

有効値 : 0 〜 add port コマンドで指定した *max-weight* の値

デフォルト値 : port コマンドの max-weight

server-state

実行プログラムが処理を開始するときに、サーバーを利用可能と見なすか、利用不能と見なすかを指定します。

有効値 : 0 (ダウン) または 1 (アップ)

デフォルト値 : 1

例:

```
add server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [80]? 80
Server address [0.0.0.0]? 131.2.25.94
Server weight [35]?
Server state (down=0 up=1) [1]?
```

パラメーター構成の制限

表15 は、ネットワーク・ディスパッチャーに構成できる種々の項目の制限を示しています。

表 15. パラメーター構成の制限

パラメーター	制限
Advisors (アドバイザー)	2216 当たり 32
Clusters (クラスター)	2216 1 台あたり 100
Heartbeats (ハートビート)	2216 1 台あたり 32
Ports (ポート)	クラスター 1 台あたり 32
Reachs (リーチ)	2216 1 台あたり 32
サーバー (Servers)	構成済みポート 1 つ当たり 128、2216 用に構成されたすべてのクラスターの下の各ポート番号ごとに 512。
固有サーバー IP アドレス	2216 1 台あたり 128

Clear

clear コマンドは、ネットワーク・ディスパッチャー構成全体をクリアするのに使用します。

構文:

clear

Disable

disable コマンドは、ネットワーク・ディスパッチャーのコンポーネントを使用不可にするのに使用します。

構文:

disable advisor . . .
backup
executor
manager

advisor *name port#*

ネットワーク・ディスパッチャーからアドバイザーを使用不可にします。

name アドバイザーのタイプを指定します。使用不可にしたいアドバイザーのタイプに対応するアドバイザー番号を入力します。

詳しくは、128ページの表14 を参照してください。

有効値 : 0 〜 8

デフォルト値 : 0

port# このアドバイザーのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : なし。ユーザーがポート番号を入力する必要があります。

例:

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

backup

ネットワーク・ディスパッチャーのバックアップ機能を使用不可にします。

例:

```
disable backup
Backup is now disabled.
```

executor

ネットワーク・ディスパッチャーの実行プログラムを使用不可にします。実行プログラムを使用不可にすると、ネットワーク・ディスパッチャー・フィーチャーは使用不可になります。

例:

```
disable executor
Executor is now disabled.
```

注: 実行プログラムを使用不可にすると、マネージャー、アドバイザー、および高可用性機能は停止します (現在、稼働している場合)。

manager

ネットワーク・ディスパッチャーのマネージャーを使用不可にします。マネージャーは、任意選択のコンポーネントです。ただし、マネージャーを使用しない場合、ネットワーク・ディスパッチャーは、現行のサーバーの重みに基づいてラウンドロビン・スケジューリング方式でロードのバランスを取ります。

例:

```
disable manager
Manager is now disabled.
```

注: マネージャーはアドバイザーの前提条件なので、マネージャーを使用不可にすると、すべてのアドバイザーは稼働を停止します。

Enable

enable コマンドは、ネットワーク・ディスパッチャーのコンポーネントを使用可能にするのに使用します。

構文:

enable advisor . . .
backup
executor
manager

advisor *name port#*

ネットワーク・ディスパッチャーに対してアドバイザーを使用可能にします。

name アドバイザーのタイプを指定します。使用可能にしたいアドバイザーのタイプに対応するアドバイザー番号を入力します。

詳しくは、128ページの表14 を参照してください。

有効値 : 0 〜 8

デフォルト値 : 0

port# このアドバイザーのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : なし。ユーザーがポート番号を入力する必要があります。

例:

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

注: マネージャー・コンポーネントはアドバイザーの前提条件なので、アドバイザーを使用可能にする前に、マネージャーを使用可能にしておく必要があります。ロード・バランシングの決定を行うのに使用されるサーバーの重みを設定する際にマネージャーがアドバイザー入力を考慮するようにマネージャーの比率を設定することも必要です。アドバイザーが正しく稼働するためには、**set internal-ip-address** コマンドを使用して、内部 IP アドレスを設定しておくことも必要です。**set internal-ip-address** コマンドについて詳しくは、*プロトコルの構成と監視 解説書 第 1 巻*「IP の構成と監視」を参照してください。

backup

ネットワーク・ディスパッチャーのバックアップ機能を使用可能にします。

例: enable backup

注: バックアップを使用可能にする前に、少なくとも 1 つのハートビートを追加する必要があります。

executor

ネットワーク・ディスパッチャーの実行プログラムを使用可能にします。

例:

```
enable executor
Executor is now enabled.
```

manager

ネットワーク・ディスパッチャーのマネージャーを使用可能にします。

例:

```
enable manager
Manager interval was set to 2.
Manager proportions were set to  50   50   0   0
Manager refresh cycle was set to 2
Manager sensitivity was set to 5.
Manager smoothing factor was set to 1.50.
```

初めてマネージャーを使用可能にすると、次のデフォルト値を使用して、マネージャー・レコードが作成されます。

Interval: 2 秒

Refresh-Cycle: 2

Sensitivity: 5 %

Smoothing: 1.5

Proportions:

Active: 50%

New: 50%

Advisor: 0

System: 0

上記のパラメーターについての説明は、142ページの『Set』を参照してください。

List

list コマンドは、ネットワーク・ディスパッチャーに関する情報を表示するのに使用します。

構文:

list all
advisor
backup
cluster
manager
port
server

all すべてのネットワーク・ディスパッチャー構成情報を表示します。これには、アドバイザー、バックアップ、クラスター、マネージャー、ポート、およびサーバーに対して表示される情報と同じものが含まれています。

例:

```
NDR Config> list all

Executor: Enabled

Manager: Enabled

        Interval        Refresh-Cycle   Sensitivity     Smoothing
        2               2               5 %             1.50
        Proportions:    Active  New     Advisor         System
```

```
                        50 %    50 %    0 %             0 %

Advisor:
        Name    Port    Interval        TimeOut         State     CommPort
        http    80      5               0               Enabled
        MVS     10007   15              0               Enabled
        TN3270  23      5               0               Enabled   10008

Backup: Enabled
        Role            Strategy
        PRIMARY         AUTOMATIC

        Reachability:   Address         Mask            Type
                        131.2.25.93     255.255.255.255 HOST
                        131.2.25.94     255.255.255.255 HOST

        HeartBeat Configuration:
           Source Address:  131.2.25.90 Target Address:   131.2.25.92
           Source Address:  132.2.25.90 Target Address:   132.2.25.92

Clusters:
        Cluster-Addr    FIN-count       FIN-timeout     Stale-timer  Advertise/Cost
        131.2.25.91     4000            30              1500         Yes      / 20

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

Servers:
        Cluster-Addr    Port#   Server-Addr     Weight  State
        131.2.25.91     23      131.2.25.93     20 %    up
        131.2.25.91     23      131.2.25.94     20 %    up
        131.2.25.91     80      131.2.25.93     20 %    up
        131.2.25.91     80      131.2.25.94     20 %    up
```

advisor
ネットワーク・ディスパッチャーのアドバイザーの構成を表示します。

backup
ネットワーク・ディスパッチャーのバックアップ構成を表示します。

cluster
ネットワーク・ディスパッチャーのクラスターの構成を表示します。

manager
ネットワーク・ディスパッチャーのマネージャーの構成を表示します。

ポート (port)
ネットワーク・ディスパッチャーのポートの構成を表示します。

サーバー (server)
ネットワーク・ディスパッチャーのクラスターに対応するサーバーの構成を表示します。

Remove

remove コマンドは、ネットワーク・ディスパッチャー構成の一部を削除するのに使用します。

構文:

remove
- advisor . . .
- backup
- cluster . . .
- heartbeat . . .
- port . . .

reach . . .

server . . .

advisor *name port#*

ネットワーク・ディスパッチャー構成から特定のアドバイザーを除去します。

name アドバイザーのタイプを指定します。除去したいアドバイザーのタイプに対応するアドバイザー番号を入力します。

詳しくは、128ページの表14 を参照してください。

有効値 : 0 〜 8

デフォルト値 : 0

port# このアドバイザーのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : なし。ユーザーがポート番号を入力する必要があります。

例:

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

backup

高可用性機能を除去します。

注: バックアップは、ハートビートおよびリーチ機能の前提条件なので、バックアップを除去すると、ハートビートおよびリーチは稼働を停止します。

例: remove backup

cluster *address*

ネットワーク・ディスパッチャー構成からクラスターを除去します。

アドレス (address)

クラスターの IP アドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

注: クラスターを除去すると、そのクラスターに関連したすべてのポートおよびサーバーも除去されます。

例:

```
remove cluster
WARNING: Deleting a cluster will make any port or server
         associated with it to also be deleted.
Cluster address [0.0.0.0]? 131.2.25.91
```

heartbeat *address*

ネットワーク・ディスパッチャー構成からハートビート・アドレスを除去します。

アドレス (address)

ターゲット・ネットワーク・ディスパッチャーの IP アドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

例:

```
remove heartbeat
Target address [0.0.0.0]? 131.2.25.92
```

port *cluster-address port#*

ネットワーク・ディスパッチャー構成内の特定クラスターからポートを除去します。

cluster-address

クラスターの IP アドレスを指定します。

有効値 : 任意の IP アドレス

デフォルト値 : 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : なし。ユーザーがポート番号を入力する必要があります。

注:

1. ポートを除去すると、そのポートに関連したすべてのサーバーも除去されます。
2. 除去するポートのモードが「キャッシュ」の場合、関連の Web サーバー・キャッシュ・プロキシー構成も除去されます。
3. 除去するポートのモードが「ホスト・オンデマンド・クライアント・キャッシュ」の場合、関連のホスト・オンデマンド・クライアント・キャッシュ・プロキシー構成も除去されます。

例:

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

reach *address*

ネットワーク・ディスパッチャーが到達可能であることが必要なホストのリストからサーバーを除去します。

アドレス (address)

クラスターの IP アドレスを指定します。

有効値 : 任意の IP アドレス

デフォルト値 : 0.0.0.0

例:

```
remove reach
Target address [0.0.0.0]? 9.82.142.15
```

server *cluster-address port# server-address*
ネットワーク・ディスパッチャー構成内のクラスターとポートからサーバーを除去します。

cluster-address
クラスターの IP アドレスを指定します。

有効値 : 任意の IP アドレス

デフォルト値 : 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : なし。ユーザーがポート番号を入力する必要があります。

server-address
クラスターの IP アドレスを指定します。

有効値 : 任意の IP アドレス

デフォルト値 : 0.0.0.0

例:

```
remove server
Cluster address [0.0.0.0]? 7.82.142.15
Port number  [0]? 80
Server address [0.0.0.0]? 20.21.22.15
```

Set

set コマンドは、既存のアドバイザー、クラスター、ポート、またはサーバーの属性を変更するのに使用します。ネットワーク・ディスパッチャーのマネージャーの属性を定義することもできます。

構文:

set advisor . . .
cluster . . .
manager . . .
port . . .
server . . .

advisor *name port# interval timeout comm-port*
アドバイザーのポート番号、インターバル、およびタイムアウトを変更します。

name アドバイザーのタイプを指定します。設定したいアドバイザーのタイプに対応するアドバイザー番号を入力します。

詳しくは、128ページの表14 を参照してください。

有効値 : 0 〜 8

デフォルト値 : 0

port# このアドバイザーのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : なし。ユーザーがポート番号を入力する必要があります。

interval

アドバイザーが各サーバーのプロトコルを照会する頻度を指定します。この値の半分の時間が、サーバーから応答がないまま満了すると、アドバイザーはそのプロトコルを利用不能とみなします。

有効値 : 0 〜 65535

デフォルト値 : 5

timeout

アドバイザーがプロトコルを利用不能と見なすまでに必要な時間間隔 (秒数) を指定します。

マネージャーは、負荷平衡を決めるのに期限切れ情報を使用するのを防止するために、このパラメーターに設定された時刻より古いタイム・スタンプをもつアドバイザーからの情報を使用しません。アドバイザー・タイムアウトは、アドバイザー・ポーリング間隔より大きい値でなければなりません。タイムアウトの方が小さいと、マネージャーは使用する必要がある報告を無視してしまいます。デフォルトでは、アドバイザーの報告はタイムアウトになりません。

このタイムアウト値は通常、アドバイザーを使用不可にした場合に適用されます。このパラメーターを、前に説明した interval/2 タイムアウト (これは、サーバーの応答がない時間に関するものです) と混同しないでください。

有効値 : 0 〜 65535

デフォルト値 : 0。これは、プロトコルは常に利用可能とみなされることを意味しています。

comm-port

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

有効値 : 1 〜 65535

デフォルト値 :

- TN3270 デフォルト値 : 10008

例:

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

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

ネットワーク・ディスパッチャー構成内のクラスターの FIN-count、FIN-timeout、および Stale-timer を変更します。

アドレス (address)

クラスターの IP アドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

FIN-count

実行プログラムが *FIN-timeout* または *Stale-timer* の経過後にネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に、FIN 状態にあることが必要な接続の数を指定します。

有効値 : 0 〜 65535

デフォルト値 : 4000

FIN-timeout

実行プログラムがネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に経過する必要がある秒数を指定します。

有効値 : 0 〜 65535

デフォルト値 : 30

Stale-timer

接続が非アクティブ状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから接続情報の除去を試みます。

有効値 : 0 〜 65535

デフォルト値 : 1500

例:

```
set cluster
Cluster address [0.0.0.0]? 131.2.25.91
FIN count [4000]? 4500
FIN timeout [30]? 40
Stale timer [1500]? 2000
```

manager *interval proportion refresh sensitivity smoothing*

マネージャーが要求を満たす最善サーバーを判別するのに使用する値を設定します。

interval

実行プログラムが接続のロード・バランシングに使用するサーバーの重みが、マネージャーによって更新される前に経過する時間 (秒数) を指定します。

有効値 : 0 〜 65535

デフォルト値 : 2

proportion

マネージャーが重み付けを決定する際の外部ファクターの相対的な重要度を指定します。比率の合計は 100 に等しくなければなりません。ファクターには、次のものがありあす。

アクティブ (active)

実行プログラムによって追跡される各 TCP/IP サーバー上のアクティブ状態の接続の数

有効値 : 0 〜 100

デフォルト値 : 50

new 実行プログラムによって追跡される各 TCP/IP サーバー上の新規接続の数

有効値 : 0 〜 100

デフォルト値 : 50

advisor
ネットワーク・ディスパッチャーに定義されたプロトコル・アドバイザーからの入力

有効値 : 0 〜 100

デフォルト値 : 0

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

有効値 : 0 〜 100

デフォルト値 : 0

refresh
マネージャーが実行プログラムから状態を要求する頻度を指定します。このパラメーターは、*intervals* の回数として指定します。

有効値 : 0 〜 100

デフォルト値 : 2

sensitivity
ポート上のすべてのサーバーの重みの比率の変動を指定します。この後、マネージャーは、実行プログラムが接続のロード・バランシングに使用する重みを更新します。

有効値 : 0 〜 100

デフォルト値 : 5

smoothing
サーバーの重みが変動できる量の限界を指定します。平滑化 (smoothing) は、要求の分配が変動する頻度を最小化します。平滑化インデックスが高くなると、重みの変動は少なくなります。平滑化インデックスが低くなると、重みの変動は大きくなります。

有効値 : 1.0 〜 42 949 673.00 の間の 10 進値

デフォルト値 : 1.5

注: 小数点以下 2 桁までしか指定できません。

例:

```
set manager
Interval (in seconds) [2]? 3
Active proportion [50]? 40
New proportion [50]? 38
Advisor proportion [0]? 20
```

```
System proportion [0]? 2
Refresh cycle [2]? 4
Sensitivity threshold [5]? 10
Smoothing index (>1.00) [1.50]? 200
```

port *cluster-address port# port-type max-weight port-mode*

特定のクラスターとポート番号の port-type、max-weight、および port-mode を変更します。

cluster-address

クラスターの IP アドレスを指定します。

有効値 : 任意の IP アドレス

デフォルト値 : 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : なし。ユーザーがポート番号を入力する必要があります。

port-type

このポートでロード・バランスを取ることができる IP トラフィックのタイプを指定します。

有効値 :

- 1 = TCP
- 2 = UDP
- 3 = 両方

デフォルト値 : 3

max-weight

このポート上のサーバーの重みを指定します。これは、実行プログラムが各サーバーに与える要求数の差異に影響します。

有効値 : 0 〜 100

デフォルト値 : 20

port-mode

ポートが、1 つのクライアントからのすべての要求を 1 つのサーバーに送る (sticky と呼ばれる) か、パッシブ ftp を使用する (pftp) か、Web サーバー・キャッシュを使用する (cache) か、外部スケーラブル・キャッシュ・アレイを送る、ホスト・オンデマンド・クライアント・キャッシュを使用するか、あるいはこのクラスターでは特定のプロトコルを使用しない (none) かを指定します。

有効値 :

- 0 = none
- 1 = sticky
- 2 = pftp
- 3 = cache
- 4 = extcache
- 5 = hod client cache

デフォルト: 0 (none)

例:

```
set port
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]? 23
Port type (tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]? 30
Port mode (none=0, sticky=1, pftp=2, cache=3, extcache=4 hod client cache=5) [0]?
```

注:

1. ポート・モード 3 (cache=3) を選択した場合、詳細については、221ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。
2. ポート・モード 5 (hod client cache=5) を選択した場合、詳細については、161ページの『第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの構成と監視』を参照してください。

server *cluster-address port# server-address weight state*

クラスター内の特定のサーバーの状態およびサーバーの重みを変更します。

cluster-address

このサーバーが属するクラスターの IP アドレスを指定します。

有効値: 任意の IP アドレス

デフォルト値 : 0.0.0.0

port# このクラスターのプロトコルのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : なし。ユーザーがポート番号を入力する必要があります。

server-address

サーバーの IP アドレスを指定します。

有効値 : 任意の有効なサーバー・アドレス

デフォルト値: 0.0.0.0

state 実行プログラムが処理を開始するときに、サーバーを利用可能と見なすか、利用不能と見なすかを指定します。

有効値 : 0 (ダウン) または 1 (アップ)

デフォルト値 : 1

weight

実行プログラムのための、サーバーの重みを指定します。これは、ネットワーク・ディスパッチャーがこの特定サーバーに要求を送信する頻度に影響を与えます。

有効値 : 0 〜 add port コマンドで指定した *max-weight* の値

デフォルト値 : port コマンドの max-weight

例:

```
set server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]?
Server address [0.0.0.0]?
Server weight [20]? 25
Server state (down=0, up=1) [1]? 1
```

ネットワーク・ディスパッチャー監視コマンドへのアクセス

ネットワーク・ディスパッチャー監視環境にアクセスするには、次のようにします。

1. OPCON プロンプト (*) で **talk 5** と入力する。
2. GWCON プロンプト (+) で **feature ndr** と入力する。

ネットワーク・ディスパッチャーは、SNMP を使用して監視することもできます。詳しくは、*プロトコルの構成と監視 解説書 第 1 巻*の『SNMP 管理』の項を参照してください。

ネットワーク・ディスパッチャー監視コマンド

表16 は、ネットワーク・ディスパッチャー監視コマンドの要約を示しており、表の後に個々のコマンドの説明があります。これらのコマンドは NDR > プロンプトで入力します。

表 16. ネットワーク・ディスパッチャー監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
List	現在構成されているアドバイザー、クラスター、ポート、またはサーバーの属性を表示します。
Quiesce	これ以上の接続要求をサーバーに送信してはならないことを指定します。ハートビートおよびリーチ機能も一時的に停止します。
Report	アドバイザーおよびマネージャーに関する情報の報告を表示します。
Status	カウンター、クラスター、ポート、サーバー、アドバイザー、マネージャー、およびバックアップの現在の状態を表示します。
Switchover	スタンバイ・モードで動作しているネットワーク・ディスパッチャーを、強制的にアクティブ・ネットワーク・ディスパッチャーにします。このコマンドは、切り替えモードとして「手動」を指定した場合に使う必要があります。
Unquiesce	サーバーが構成されている各ポート上の以前に静止されたサーバーに対して、ネットワーク・ディスパッチャーのマネージャーが 0 より大きい重みを割り当てることができるようにします。このアクションにより、選択されたサーバーに対して新規の接続要求を送ることができるようになります。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

List

list コマンドは、ネットワーク・ディスパッチャーに関する情報を表示するのに使用します。

構文:

list advisor

cluster

port

server

advisor

現在使用可能になっている、ネットワーク・ディスパッチャー・アドバイザーの構成を表示します。

例:

```
list advisor
Advisor list requested.

-----------------------------------------
| ADVISOR |  PORT  |  TIMEOUT  |  STATUS  |
-----------------------------------------
|  ftp    |    21  |       5   |  ACTIVE  |
|  Http   |    80  | unlimited |  ACTIVE  |
|  MVS    | 10007  | unlimited |  ACTIVE  |
|  TN3270 |    23  | unlimited |  ACTIVE  |
-----------------------------------------
```

cluster

ネットワーク・ディスパッチャーのクラスターの構成を表示します。

例:

```
list cluster
EXECUTOR INFORMATION:
 ---------------------
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996
Number of defined clusters: 2

CLUSTER LIST:
-------------
  131.2.25.91
  10.11.12.2
```

ポート (port)

ネットワーク・ディスパッチャーのポートの構成を表示します。

例:

```
list port
Cluster Address [0.0.0.0]? 131.2.25.91

  ---------------------------------------------------------
| CLUSTER:       131.2.25.91                              |
|---------------------------------------------------------|
|   PORT   |    MAXWEIGHT   |  PORT MODE  |  PORT TYPE   |
|---------------------------------------------------------|
|     23   |         30     |    none     |     TCP      |
|     80   |         20     |    none     |     both     |
 ---------------------------------------------------------
```

サーバー (server)

ネットワーク・ディスパッチャーのクラスターに対応するサーバーの構成を表示します。

例:

```
list server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
```

```
Currently marked down.......... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
PORT 80 INFORMATION:
 -------------------
Maximum weight................. 20
Port mode...................... NONE
Port type...................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes............. 2
Currently marked down.......... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
```

表示された情報の説明については、155 ページを参照してください。

Quiesce

quiesce コマンドは、ハートビートまたはリーチ機能を一時的に停止するか、それ以上の接続要求をサーバーに送信しないように指定するのに使用します。

構文:

quiesce heartbeat
manager
reach

heartbeat *address*

ハートビート機能用に選択されたパスを停止します。*address* は、このネットワーク・ディスパッチャーのハートビート・メッセージの送信先のリモート・ネットワーク・ディスパッチャーの IP アドレスです。

例:

```
quiesce heartbeat
Remote Address [0.0.0.0]? 131.2.25.94
```

manager *address*

指定されたサーバーには、それ以上の接続要求をしてはならないことを指定します。*Address* は、そのサーバーの IP アドレスです。

例:

```
quiesce manager
Server Address [0.0.0.0]? 131.2.25.93
```

reach *address*

到達可能かどうかを判別するためのネットワーク・ディスパッチャーによる指定のアドレスへのポーリングを停止します。ただし、*address* は、到達可能性基準に含まれている IP アドレスです。

例:

```
quiesce reach
Reach Address [0.0.0.0]? 131.2.25.92
```

Report

report コマンドは、アドバイザーまたはマネージャーの報告を表示するのに使用します。

構文:

report advisor

manager

advisor *type port#*

特定のアドバイザーに関する情報の報告を表示します。

type アドバイザーのタイプです。アドバイザーのタイプに対応するアドバイザー番号を入力します。アドバイザー・タイプについては、128 ページの表14 を参照してください。

port# ポート番号です。

例:

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

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

サーバー・アドレスごとに示された値は、次のとおりです。

≥0 サーバーのロード

-1 アドバイザーがサーバーに接続できませんでした。

manager

現行のマネージャー情報の報告書を表示します。

例:

```
report manager

---------------------------------
|  HOST TABLE LIST  |   STATUS    |
---------------------------------
|  131.2.25.93      |    ACTIVE   |
|  131.2.25.94      |    ACTIVE   |
---------------------------------
```

報告書の情報は、次のとおりです。

Status サーバー・アドレスの状態を表示します。

Quiesce サーバーが静止しています。

Active サーバーが静止していません。

```
-------------------------------------------------------------------------------
|131.2.25.91    |WEIGHT | ACTIVE % 50  |  NEW % 50    | PORT %  0 |SYSTEM %  0|
|               ---------------------------------------------------------------
|PORT:   23     |NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
|-----------------------------------------------------------------------------|
|131.2.25.93    | 10| 10|  10|        0|  10|        0|   0|     0|-999|    -1|
|131.2.25.94    | 10| 10|  10|        0|  10|        0|   0|     0|-999|    -1|
|-----------------------------------------------------------------------------|
```

```
|PORT TOTALS:   | 20| 20|    |        0|    |        0|    |     0|    |    -2|
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
|131.2.25.91    |WEIGHT | ACTIVE % 50  |  NEW % 50    | PORT %  0 |SYSTEM %  0|
|               ---------------------------------------------------------------
|PORT:   80     |NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
|-----------------------------------------------------------------------------|
|131.2.25.93    | 10| 10|  10|        0|  10|        1|  16|     0|-999|    -1|
|131.2.25.94    | 10| 10|  10|        0|  10|        1|   3|    16|-999|    -1|
|-----------------------------------------------------------------------------|
|PORT TOTALS:   | 20| 20|    |        0|    |        0|    |    16|    |    -2|
-------------------------------------------------------------------------------


-----------------------------------------
| ADVISOR |  PORT  |  TIMEOUT  |  STATUS  |
-----------------------------------------
|  http   |    80  | unlimited |   ACTIVE |
|  MVS    | 10007  | unlimited |   ACTIVE |
-----------------------------------------
Manager report requested.
```

レポートの情報は、次のとおりです。

Weight このサーバーの全体的な重み計算

Now このサーバーに割り当てられていた直前の重み

New このサーバーに割り当てられた最新の重み

Active % 全体のサーバー重み計算でのアクティブ接続の比率。このパラメーターの値は、**set manager proportions** コマンドを使用して、決められます。 144 ページを参照してください。

Wt 全体の重み計算に使用された重み

Connect このサーバーについてのアクティブ接続回数

New % 全体のサーバー重み計算での新しい接続の比率。このパラメーターの値は、**set manager proportions** コマンドを使用して、決められます。144 ページを参照してください。

Wt 全体の重み計算に使用された重み

Connect
このサーバーについての新しい接続回数

Port % 全体のサーバー重み計算でのアドバイザーの比率。このパラメーターの値は、**set manager proportions** コマンドを使用して、決められます。144 ページを参照してください。

Wt 全体の重み計算に使用された重み

Load このサーバーについてアドバイザーが報告したサーバー・ロード

System % 全体のサーバー重み計算でのシステム監視の比率。このパラメーターの値は、**set manager proportions** コマンドを使用して、決められます。 144 ページを参照してください。

Wt 全体の重み計算に使用された重み

Load システム監視によってレポートされたサーバー・ロード

Status

status コマンドは、アドバイザー、バックアップ、カウンター、クラスター、マネージャー、ポート、およびサーバーの状態を入手するのに使用します。

構文:

status advisor
backup
cluster
counter
manager
ports
servers

advisor *name port#*

特定のアドバイザーの状態を入手します。

name アドバイザーのタイプを指定します。アドバイザーのタイプに対応するアドバイザー番号を入力します。アドバイザー・タイプについては、128ページの表14 を参照してください。

port# ポート番号です。

例:

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

Advisor ftp on port 21 status:
==============================
Interval.................. 10
```

backup

バックアップ機能の状態を入手します。

例:

```
status backup
 Dumping status ...
 Role : PRIMARY   Strategy : AUTOMATIC  State : ND_ACTIVE Sub-State : ND_SYNCHRONIZED
 <<Preferred Target : 132.2.25.92>>

 Dumping HeartBeat Status ...
 .....Heartbeat target : 131.2.25.92 Status : UNREACHABLE
 .....Heartbeat target : 132.2.25.92 Status : REACHABLE

 Dumping Reachability Status ...
 .....Host:131.2.25.93   Local:REACHABLE
 .....Host:131.2.25.94   Local:REACHABLE
```

cluster *address*

指定されたクラスターの状態を入手します。ただし、*address* は、クラスターの IP アドレスです。

例:

```
status cluster
Cluster Address [0.0.0.0]? 131.2.25.91

EXECUTOR INFORMATION:
 --------------------
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996

CLUSTER INFORMATION:
 -------------------
Address......................... 131.2.25.91
Number of target ports.......... 2
FIN clean up count.............. 4000
Connection FIN timeout.......... 30
Active connection stale timer... 1500
Advertise cluster address....... Yes
Advertise route cost............ 20

PORT 23 INFORMATION:
 -------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0  Active:
0 FIN 0 Complete 0 Status: up Saved Weight: -1  Address: 131.2.25.94 Weight:
20 Count: 0 TCP Count: 0 UDP Count: 0  Active: 0 FIN 0 Complete 0 Status:
up Saved Weight: -1
PORT 80 INFORMATION:
 -------------------
Maximum weight.................. 20
Port type....................... BOTH
Port mode....................... NONE
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UDP Count: 0  Active:
0 FIN 0 Complete 0 Status: up Saved Weight: -1  Address: 131.2.25.94 Weight:
20 Count: 0 TCP Count: 0 UDP Count: 0  Active: 0 FIN 0 Complete 0 Status:
up Saved Weight: -1
```

表示されたフィールドの定義については、155 ページを参照してください。

counter

すべてのカウンターの状態を入手します。

例:

```
status counter
Internal counters from executor:
--------------------------------
Total number of packets into executor...... 2684
Total packets for cluster processing (C)... 2684
Packets not addressed to a cluster(port)... 0

Cluster processing results:
---------------------------
Errors...................................... 0
Discarded................................... 0
Own address................................0
Forward requested........................... 2684
Forward discarded with error............... 0

Other processing problems:
--------------------------
Total packets dropped (C).................. 0
```

manager

マネージャーの状態を入手します。

例:

```
status manager
Number of defined hosts... 2
Sensitivity............... 0%
Smoothing factor.......... 2
Interval.................. 3
Weights refresh cycle..... 4

Active connections gauge proportion......... 40%
New connections counter(delta) proportion... 38%
```

```
Advisor gauge proportion..................... 20%
System Metric proportion.....................  2%

Manager status requested.
```

port *cluster-address port#*

特定のポートの状態を入手します。ただし、

cluster-address
クラスターの IP アドレスです。

port# クラスターのポート番号です。

例:

```
status port
Cluster Address [0.0.0.0]? 131.2.25.91
Port number  [0]? 80

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP count 2345
Active: 3431 FIN 3780 Complete 3431  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890  Active: 2980 FIN 2390 Status: up
Saved Weight: -1
```

報告されたサーバーの情報は、次のとおりです。

Address サーバー IP アドレス

Weight このサーバーに現在割り当てられている重み

Count TCP 接続と UDP パケットの累積カウント

TCP Count TCP 接続の累積カウント

UDP Count UDP パケットの累積カウント

Active アクティブ TCP 接続回数

FIN TCP 接続は FIN 状態です

Complete 完了 (FIN の後で ACK があった) している TCP 接続

Status 構成済みサーバーの状態:

active (アクティブ)	サーバーはアクティブである。
down (ダウン)	サーバーがダウンしている。
quiesced (静止)	サーバーが静止している。
not responding (応答しない)	サーバーはアドバイザーに応答していない。

Saved weight (保管済みの重み)
ダウンとサーバーがマークされる前のサーバーの重み

server *address*

特定のサーバーの状態を入手します。ただし、*address* は、サーバーが属するクラスターの IP アドレスです。

例:

```
status server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... TCP
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 140 TCP Count: 100 UDP Count: 40
Active: 50 FIN 45 Complete 50  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 250 TCP Count: 100 UDP Count: 40
Active: 60 FIN 54 Complete 50  Status: up Saved Weight: -1

PORT 80 INFORMATION:
 --------------------
Maximum weight.................. 20
Port mode....................... NONE
Port type....................... BOTH
All up nodes are weight zero.... FALSE
Total target nodes.............. 2
Currently marked down........... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP Count: 2345
Active: 3431 FIN 3780 Complete 3431  Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890  TCP Count: 10000 UDP Count: 2345
Active: 2980 FIN 2390 Complete 3431  Status: up Saved Weight: -1
```

Switchover

switchover コマンドは、切り替え方式が「手動」の場合、スタンドバイ・モードで作動しているネットワーク・ディスパッチャーを、強制的にアクティブ・ネットワーク・ディスパッチャーにするのに使用します。このコマンドは、スタンドバイ・モードのネットワーク・ディスパッチャーが稼働しているホストで入力する必要があります。

構文:

switchover

Unquiesce

unquiesce コマンドは、以前に **quiesce** コマンドを使用して停止したハートビート、マネージャー、またはリーチ機能をリスタートするのに使用します。

構文:

unquiesce heartbeat
manager
reach

heartbeat *address*

ハートビート・メッセージ用のパスをリスタートします。ただし、*address* は、このネットワーク・ディスパッチャーのキープアライブ・メッセージの送信先のリモート・ネットワーク・ディスパッチャーの IP アドレスです。

例:

```
unquiesce heartbeat
Remote Address [0.0.0.0]? 9.10.11.1
```

manager *address*

指定のサーバーへの接続要求の送信をリスタートします。*Address* は、そのサーバーの IP アドレスです。

例:

```
unquiesce manager
Server Address [0.0.0.0]? 20.21.22.15
```

reach *address*

到達可能かどうかを判別するためのネットワーク・ディスパッチャーによる指定のアドレスへのポーリングをリスタートします。ただし、*address* は到達可能性基準に含まれている IP アドレスです。

例:

```
unquiesce reach
Reach address [0.0.0.0]? 20.3.4.5
```

ネットワーク・ディスパッチャー動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

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

GWCON (Talk 5) Activate Interface

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

GWCON (Talk 5) Reset Interface

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

CONFIG (Talk 6) 即時変更コマンド

NDR は、装置の操作状態を即時に変更する、次の CONFIG コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行する場合には、保管されて保存されます。

・コマンド
CONFIG, feature ndr, add advisor
CONFIG, feature ndr, add backup
CONFIG, feature ndr, add cluster
CONFIG, feature ndr, add heartbeat

CONFIG, feature ndr, add port **注:** 選択されたポート・モードが Web サーバー・クライアント・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュである場合には、HTTP プロキシーの変更は、即時に行われません。
CONFIG, feature ndr, add reach
CONFIG, feature ndr, add server
CONFIG, feature ndr, disable advisor
CONFIG, feature ndr, disable backup
CONFIG, feature ndr, disable executor **注:** 実行プログラムを使用不可にした場合、実行時コード構造から、*NOT SRAM*を除くすべてのクラスター、ポートおよびサーバーが除去されます。ポート・モードが、除去されたポートの Web サーバー・クライアント・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュであった場合、すべての Web サーバー・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュの区画は使用不可にされ、HTTP プロキシーはクローズされます。
CONFIG, feature ndr, disable manager
CONFIG, feature ndr, enable advisor
CONFIG, feature ndr, enable backup
CONFIG, feature ndr, enable executor **注:** 実行プログラムを使用可能で、Web サーバー・クライアント・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュのポートがある場合には、HTTP プロキシーと区画は自動的でも即時でもありません。
CONFIG, feature ndr, enable manager
CONFIG, feature ndr, remove advisor
CONFIG, feature ndr, remove backup
CONFIG, feature ndr, remove cluster **注:** クラスターを除去すると、そのクラスターに関連したすべてのポートやサーバーは実行時コード構造と SRAM から除去されます。除去されたポートに Web サーバー・クライアント・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュがあった場合、HTTP プロキシーもダウンし、その SRAM は除去されます。
CONFIG, feature ndr, remove heartbeat
CONFIG, feature ndr, remove port **注:** 除去中のポートに Web サーバー・クライアント・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュのポート・モードがある場合には、HTTP プロキシーもダウンし、その SRAM は除去されます。
CONFIG, feature ndr, remove reach
CONFIG, feature ndr, remove server
CONFIG, feature ndr, set advisor
CONFIG, feature ndr, set cluster
CONFIG, feature ndr, set manager

CONFIG, feature ndr, set port **注:** このポートのポート・モードが Web サーバー・クライアント・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュであって、今他のものに設定中である場合には、これらのポートの HTTP プロキシーはクローズされ、その SRAM は除去されます。また、運用ソフトウェアがポート・モードを他のものから cache または hod client cache に設定している場合には、HTTP プロキシーの変更は即時に行われません。
CONFIG, feature ndr, set server

非動的再構成可能コマンド

すべての NDR 構成パラメーターは動的に変更できます。

第10章 IBM eNetwork ホスト・オンデマンド・クライアント・キャッシュの構成と監視

ホスト・オンデマンド・クライアント・キャッシュにより、Web ベースのクライアントは、Java™ ベースの端末エミュレーション・プログラムを使用して SNA ホスト・アプリケーションに接続できます。このエミュレーション・プログラムは、TN3270 を使用してクライアントをホストに接続します。ホスト・オンデマンド機能の余り一般的でないアプリケーションには、非 TN3270 端末のエミュレーション用の Telnet があります。これは、3270、5250、VT (VT52、VT100、VT220_7_BIT、VT220_8_BIT)、および CICS ゲートウェイ・セッションをサポートします。

Telnet サーバーの IP アドレスのデフォルトは、ホスト・オンデマンド・サーバーのアドレスです。これは、もっとも簡単な構成では、TN3270E サーバーはルーターに対して外部の位置に入ります。

より高度なセットアップでは、ホスト・オンデマンド管理者は、ホスト・オンデマンド・サーバーを特に、Telnet サーバー・アドレスがホスト・オンデマンド・クライアント・キャッシュのクラスター・アドレスと同じ (すなわち、ルーター (または複数のルーター) は TN3270E サーバーとして利用される) であるのが普通のセッションであるように設定します。これは、作成者が予期したとおりの、ホスト・オンデマンド・クライアント・キャッシュの標準的な使用法です。この構成では、ネットワーク・ディスパッチャーのクラスター・アドレスは、いくつかの関連ポートをもつことになります。いくつかはホスト・オンデマンド機能用で、1 つ (通常ポート 23) は TN3270E 機能用です。ネットワーク・ディスパッチャーを使用した TN3270E の構成に関する詳細については、105ページの『第8章 ネットワーク・ディスパッチャー・フィーチャーの使用』を参照してください。ホスト・オンデマンド・サーバーの観点から、任意の Telnet サーバー・アドレスを使用してプログラムされます。HOD セッションは、示されたアプレットがブラウザーによってサポートされている (一般的にこのようになっていますが、OS/2 に必要な条件については、*eNetwork Host On-Demand Version 3.0 Administrator's Guide*、IBM 資料番号 SC31-8627、を参照してください) のであれば、任意 Telnet サーバーを使用するようにプログラムされます。端末機能をクライアントに提供するために使用されたホスト・オンデマンド・サーバーは、Telnet サーバーから独立しています。Telnet サーバーは、クライアントが通信したいコンピューターに直接関係しています。

一方では、大規模な構成の場合、多くの TN3270E サーバーを、ネットワーク・ディスパッチャー構成のもとで Telnet ポート (ポート 23) に追加できます。極めて大規模な構成の場合、追加のポートは、Telnet サーバーの IP アドレスとポート (デフォルト 23) の両方をホスト・オンデマンド・セッションに構成できるため、ポートとして設定できます。幾万ものユーザーをサポートするこれらの多重 Telnet サーバー構成に必要なのは、1 台のホスト・オンデマンド・サーバーだけです。

このサポートにより、TN3270E サーバーとして活動する IBM 2216 は端末エミュレーション・アプレットをキャッシュに入れ、要求に応じてそれをクライアント・ブラウザーに提供します。アプレットは、最初にクライアントがそれを要求すると、Web サーバーから検索され、ホスト・オンデマンド・キャッシュ・メモリーに

保管されます。このアプレットをそれ以降クライアントが要求すると、キャッシュから直接サービスされ、Web サーバーから検索を追加して行う必要がなくなります。

クライアント・ブラウザーからのホスト・オンデマンドの使用の詳細については、*eNetwork Host On-Demand Version 3.0 Administrator's Guide*、IBM 資料番号 SC31-8627 の 『Understanding the Host On-Demand Clients』 というタイトルの章を参照してください。

注: ホスト・オンデマンド・クライアント・キャッシュと Web サーバー・キャッシュ・フィーチャーは 1 つの構成で共存できません。

この章では、ホスト・オンデマンド・クライアント・キャッシュ・フィーチャーの構成方法、およびホスト・オンデマンド・クライアント・キャッシュ監視コマンドの使用法について説明します。この章には、次の内容が記載されています。

ホスト・オンデマンド・クライアント・キャッシュの構成

ホスト・オンデマンド・クライアント・キャッシュは、ネットワーク・ディスパッチャーと一緒に使用することが必要があります。ホスト・オンデマンド・クライアント・キャッシュを使用する前に、次を行う必要があります。

1. `talk 6` で `Config>` プロンプトから **feature ndr** コマンドを使用して、ネットワーク・ディスパッチャーにアクセスする。
2. 実行プログラムを使用可能にする。
3. クラスターを追加する。
4. 次のポートを追加する。
   - ポート 80 をクラスターに追加し、それを hod client cache モードに設定する。ポート 80 は、インターネットの標準 HTTP プロトコル・ポートです。
   - ポート 8999 をクラスターに追加し、ポート番号以外のすべてのパラメーターについてデフォルト値を受け入れる。クライアントはポート 8999 を使用して、ホスト・オンデマンド・サーバーに保管されている group/user/session プロファイルと通信します。
   - It is assumed that ホスト・オンデマンド・サーバー管理者はホスト・オンデマンド・サーバーを、この IBM 2216 を経由せずに直接アクセスし、クライアントがアクセスできるのは構成済みポートだけであるため、システムはネットワーク・ディスパッチャーの設計によるセキュリティー上の利点を得ることができます。しかし、このことが制限し過ぎる場合には、ポート 8989 をクラスターに追加し、パラメーターのデフォルト値を受け入れます。

5. 1 つだけホスト・オンデマンド・サーバーを追加する。例外的な管理理由からホスト・オンデマンド・サーバーを追加して必要とする場合には、162 から始まるすべてのステップを繰り返して、固有なクラスターとしてサーバーを追加します。サーバーは、ポート 80、8999、および 8989 (使用されている場合) のそれぞれに追加する必要があります。
6. また、ルーターが TN3270E サーバーになる必要がある場合には、105ページの『第8章 ネットワーク・ディスパッチャー・フィーチャーの使用』 の手順に従って、クラスター・アドレスの下で Telnet ポート (23) を構成して、TN3270E サーバーをそのポートに追加する。ホスト・オンデマンド・サーバー管理者が、この代替 Telnet アドレスを使用するためにホスト・オンデマンド・サーバーを同時に構成することも必要となります。

これで、構成および監視コマンドを使用してホスト・オンデマンド・クライアント・キャッシュ環境を変更できるようになります。

注: Talk 6 で行ったネットワーク・ディスパッチャーの変更は現行の実行環境を変更しますが、ホスト・オンデマンド・クライアント・キャッシュの変更は、Talk 6 で **activate** コマンドを使用するか、Talk 5 のフィーチャー HOD クライアント・キャッシュを使用して明示的に活動化しない限り、現行の実行環境には影響を与えません。ただし、例外として、HTTP プロキシーのクラスター / ポートを Talk 6 のフィーチャー NDR を使用して除去した場合は、現行の実行環境のホスト・オンデマンド・クライアント・キャッシュ用の HTTP プロキシーも除去されます。

例:

```
Config>f ndr
NDR Config>enable executor
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.10
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Cluster 113.3.1.10 has been added.
Fincount has been set to 4000 for cluster 113.3.1.10
Fintimeout has been set to 30 for cluster 113.3.1.10
Staletimer has been set to 1500 for cluster 113.3.1.10
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]? 80
Port type (tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 extcache=4 hod client cache=5) [0]? 5
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
URL mask to identify Java applet [*.jar]?
      Default expiration time for Java applet
              (1-10080 minutes or 0 for no expiration) [60]?
Do you want to add a URL mask? [No]:

The Host On-Demand Client Cache partition has been successfully created.
Requested port has been added to cluster 113.3.1.10
Port Mode has been set to hod for port 80 in cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
Port Type has been set to Both for port 80 in cluster 113.3.1.10
NDR Config>exit
```

注: この例は部分的なもので、固有なポート・モードとコンソール・メニューを使用して HOD クライアント・キャッシュ・ポート (80) の追加を示すだけです。構成の残りは、105ページの『第8章 ネットワーク・ディスパッチャー・フィーチャーの使用』に表示された例に続きます。

次に、パラメーターの例とそれぞれの記述を示します。

cluster-address
クラスターの IP アドレスを指定します。

注: クラスター IP アドレスは、直前のホップ・ルーター (IP ルーター) と同じ論理サブネット上に存在するものと想定しています。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

FIN-count
実行プログラムが *FIN-timeout* または *Stale-timer* の経過後にネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に、FIN 状態にあることが必要な接続の数を指定します。

有効値 : 0 〜 65535

デフォルト値 : 4000

FIN-timeout
接続が FIN 状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みます。

有効値 : 0 〜 65535

デフォルト値 : 30

Stale-timer
接続が非活動状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから接続の情報の除去を試みます。

有効値 : 0 〜 65535

デフォルト値 : 1500

port#
このクラスターのプロトコルのポート番号を指定します。

有効値 : 1 〜 65535

デフォルト値 : 80

port-type
このポートでロード・バランスを取ることができる IP トラフィックのタイプを指定します。サポートされるタイプは、次のとおりです。

- 1 = TCP
- 2 = UDP
- 3 = 両方

有効値 : 1、2、3

デフォルト値 : 3

max-weight
このポート上のサーバーの最大重みを指定します。これは、実行プログラムが各サーバーに与える要求数の相違に影響します。

有効値 : 0 〜 100

デフォルト値 : 20

port-mode
ポートが、1 つのクライアントからのすべての要求を 1 つのサーバーに送る (stickyと呼ばれる) か、パッシブ ftp を使用する (pftp) か、外部スケーラブル・キャッシュ・アレイを送る (extcache) か、ホスト・オンデマンド・クライアント・キャッシュを使用するか、あるいはこのクラスターでは特定のプロトコルを使用しない (none) かを指定します。

有効値 : 0 、1、2、4、5。値は、それぞれ次のものを示します。

- 0 = none
- 1 = sticky
- 2 = pftp
- 4 = extcache
- 5 = hod client cache

デフォルト値 : 0

Default server TCP connection timeout
サーバー接続が満了する前の時間を指定します。

有効値 : 5 〜 240 秒

デフォルト値 : 120 秒

Default client TCP connection timeout
クライアント接続が満了する前の時間を指定します。

有効値 : 5 〜 240 秒

デフォルト値 : 120 秒

Do you want to modify the Host On-Demand Client Cache partition?
ホスト・オンデマンド・クライアント・キャッシュ区画の構成を変更できるようにします。

有効値 : Yes または No

デフォルト値: No

Maximum partition size
このホスト・オンデマンド・クライアント・キャッシュ区画に割り当てる最大メモリー量を指定します。この値が、現在利用可能なメモリーの量を超えている場合、この値は無視され、最大区画サイズは適用されません。

有効値 : 1 〜 4095 MB または 0 (最大値なし)

デフォルト値 : 0 (最大値なし)

URL mask to identify Java applets
Java アプレットを識別するのに使用する URL マスクを指定します。

有効値 : 任意の URL マスク

デフォルト値 : *.jar*

Default expiration time for Java applet

Java アプレットに適用されるデフォルトの有効期限時刻を指定します。

有効値 : 1 ～ 10080 分、または有効期限がない場合は 0

デフォルト値 : 60

Do you want to add a URL mask?

新しい URL マスクをホスト・オンデマンド・クライアント・キャッシュに追加するかどうかを指定します。URL マスクは、その汎用リソース・ロケーター (URL) によって、個々のオブジェクトまたはオブジェクト・グループを包含または除外することができます。

注: このフィーチャーは、通常ホスト・オンデマンドと一緒に使用されませんが、完全を期してここで説明します。重要な 1 つの URL マスクがあります。これは、区画の一部として構成される Java アプレット・マスクです。このマスクは、通常構成が必要なただ 1 つのものです。したがって、add、delete、list、modify urlmask コマンドを使用しないことをお勧めします。

有効値 : Yes または No

デフォルト値: No

URL マークを指定するときは、ワイルドカード文字を使用できます。ワイルドカードを使えるのは、ホスト・オンデマンド・クライアント・キャッシュ用にネットワーク・ディスパッチャーを構成するとき、あるいは `HOD Client Cache` プロンプトから **add** または **modify url** コマンドを使用するときです。ワイルドカードとして使用できる文字は、* (アスタリスク) または # (番号記号) です。ワイルドカードは URL の一部としてどの位置にでも使用できます。

* は、URL の一部として、文字なし、または全文字を表します。

例: *abc.html は、次のような URL マスクをフィルターに掛けます。

```
abc.html
finabc.html
defchtjqsprabc.html
```

は、1 文字を表します。

例: ab#.html は、次のような URL マスクをフィルターに掛けます。

```
abc.html
abf.html
abo.html
```

ネットワーク・ディスパッチャーを使用して、ホスト・オンデマンド・クライアント・キャッシュ・フィーチャー用の初期クラスターとポートを構成することが必要です。クラスターとポートを追加し、*port mode* をキャッシュ・ポートとして構成した後は、`HOD Client Cache Config>` プロンプトでホスト・オンデマンド・クライアント・キャッシュ構成パラメーターを変更したり、表示したりすることができます。

ネットワーク・ディスパッチャーについては、132 ページを参照してください。

ホスト・オンデマンド・クライアント・キャッシュ環境へのアクセス

ホスト・オンデマンド・クライアント・キャッシュ構成環境にアクセスするには、Config> プロンプトで、コマンド **f hod client cache** を入力します。

```
Config> f h
HOD Client Cache Config>
```

ホスト・オンデマンド・クライアント・キャッシュ・コマンド

ここでは、ホスト・オンデマンド・クライアント・キャッシュ構成コマンドについて説明します。 表17 は、ホスト・オンデマンド・クライアント・キャッシュ構成コマンドを示しています。これらのコマンドは、ホスト・オンデマンド・クライアント・キャッシュ・フィーチャーのパラメーターを指定します。これらの変更をアクティブにするには、ルーターを再始動するか、または **activate** コマンドを使用します。

表 17. ホスト・オンデマンド・クライアント・キャッシュ構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Activate	最新の構成を使用して、ホスト・オンデマンド・クライアント・キャッシュ区画を活動化します。
Add	URL マスクを追加します。
Delete	URL マスクまたは区画を削除します。
List	ホスト・オンデマンド・クライアント・キャッシュ情報を表示します。
Modify	ホスト・オンデマンド・クライアント・キャッシュ情報を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxv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

最新の構成を使用して、**activate** コマンドは、ホスト・オンデマンド・クライアント・キャッシュ区画を初期設定するのに使用します。

構文:

activate

例:

```
HOD Client Cache Config>act ?
ACTIVATE ALL initializes the Host On-Demand Client Cache partition, using
the latest configuration.
```

Add

add コマンドは、URL マスクを追加するのに使用します。

注: このフィーチャーは、通常ホスト・オンデマンドと一緒に使用されません。

構文:

add urlmask

注: プロキシーおよび区画を追加するには、ネットワーク・ディスパッチャーを使用して **add port** または **set port** コマンドを実行しなければなりません。

Delete

delete コマンドは、URL マスクまたは区画を削除するのに使用します。

構文:

delete partition
urlmask

partition
ホスト・オンデマンド・クライアント・キャッシュ区画を削除します。

urlmask
ホスト・オンデマンド・クライアント・キャッシュから削除する URL マスクの名前

注: URL マスクは、通常 HOD クライアント・キャッシュで、追加または削除されません。

例:

```
HOD Client Cache Config>del part
The HOD Client Cache partition number has been deleted.
```

注: プロキシーを削除するには、ネットワーク・ディスパッチャー・フィーチャーを使用して関連のポートまたはクラスター (あるいは、その両方) を削除するか、あるいはポートのポート・モードをホスト・オンデマンド・クライアント・キャッシュ以外のものに変更しなければなりません。

List

list コマンドは、ホスト・オンデマンド・クライアント・キャッシュ情報を表示するのに使用します。

構文:

list all
external
partition
proxy
urlmask

all ホスト・オンデマンド・クライアント・キャッシュに定義された区画、すべてのポート、プロキシー、およびマスクを表示します。

external
外部キャッシュ制御マネージャーのための情報を表示します。

注: ECCM は、ホスト・オンデマンド・クライアント・キャッシュと一緒に通常使用されません。

partition
ホスト・オンデマンド・クライアント・キャッシュ区画を表示します。

proxy ホスト・オンデマンド・クライアント・キャッシュ・プロキシーを表示します。

urlmask
定義済みのホスト・オンデマンド・クライアント・キャッシュ URL マスクを表示します。

例: list all

```
HOD Client Cache Config>list all
Host On-Demand Client Cache Partition
    Cluster address 113.3.1.10, Port 80

1 Host On-Demand Client Cache partition defined.
```

例: list partition

```
HOD Client Cache Config>list pa
Host On-Demand Client Cache Partition
Maximum partition size    : Unlimited
URL mask to identify Java applets:   '*.jar'
      Default expiration time for Java applet:   60
Associated proxies (cluster port)  : (113.3.1.10 80)

1 Host On-Demand Client Cache partition defined.
```

例: list proxy

```
HOD Client Cache Config>li pro
    1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition
HTTP proxy number [1]? 1
HTTP Proxy 1
HOD Client Cache Partition
Cluster Address           : 113.3.1.10
Port Number               : 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
```

Modify

modify コマンドは、ホスト・オンデマンド・クライアント・キャッシュ構成情報を変更するのに使用します。

構文:

modify external
partition
proxy
urlmask

external
外部キャッシュ制御マネージャーの特性を変更します。

注: このフィーチャーは、通常ホスト・オンデマンドと一緒に使用されません。

partition
既存のホスト・オンデマンド・クライアント・キャッシュ区画の特性を変更します。

proxy 既存の HTTP プロキシーの特性を変更します。

urlmask
既存の URL マスクを変更します。

注: このフィーチャーは、通常ホスト・オンデマンドと一緒に使用されません。

例: modify partition

```
HOD Client Cache Config>modify partition
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]? 2000
URL mask to identify Java applet [*.jar]?
      Default expiration time for Java applet
              (1-10080 minutes or 0 for no expiration) [60]?
The Host On-Demand Client Cache partition has been modified.
```

例: modify proxy

```
HOD Client Cache Config>mod proxy
    1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition
HTTP proxy number [1]? 1
Default server TCP connection timeout (Range 5-240 seconds) [120]? 200
Default client TCP connection timeout (Range 5-240 seconds) [120]?
The HTTP proxy has been modified.
```

ホスト・オンデマンド・クライアント・キャッシュ監視環境へのアクセス

ホスト・オンデマンド・クライアント・キャッシュ監視環境にアクセスするには、t 5 Config プロンプトでコマンド **f hod client cache** を入力します。

```
+f h
```

ホスト・オンデマンド・クライアント・キャッシュ監視コマンド

表18 は、ホスト・オンデマンド・クライアント・キャッシュ監視コマンドを表示しています。

表 18. ホスト・オンデマンド・クライアント・キャッシュ監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Activate	最新の構成を使用して、ホスト・オンデマンド・クライアント・キャッシュ情報を活動化します。
Clear	ホスト・オンデマンド・クライアント・キャッシュ区画からすべてのオブジェクトをクリアするか、またはホスト・オンデマンド・クライアント・キャッシュ統計をクリアします。
Enable	ホスト・オンデマンド・クライアント・キャッシュ区画を使用可能にします。
Delete	ホスト・オンデマンド・クライアント・キャッシュ区画、プロキシー、または URL マスクを削除します。
Disable	ホスト・オンデマンド・クライアント・キャッシュ区画を使用不可にします。
List	ホスト・オンデマンド・クライアント・キャッシュ情報を表示します。
Modify	ホスト・オンデマンド・クライアント・キャッシュ情報を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxv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、ホスト・オンデマンド・クライアント・キャッシュ区画またはプロキシー。あるいは特定のプロキシーを起動するのに使用します。

構文:

activate all
external
partition
proxy

all ホスト・オンデマンド・クライアント・キャッシュ区画、すべての定義済みプロキシー、および定義済み外部キャッシュ制御マネージャーを活動化します。

external
外部キャッシュ制御マネージャーを活動化します。

partition
ホスト・オンデマンド・クライアント・キャッシュ区画を活動化します。

proxy ホスト・オンデマンド・クライアント・キャッシュ・プロキシーを活動化します。

例: activate all

```
HOD Client Cache>act all
The Host On-Demand Client Cache partition must be disabled to reactivate it.
Do you wish to continue? [No]: y
```

例: activate partition

```
HOD Client Cache>act pa
The Host On-Demand Client Cache partition must be disabled to reactivate it.
Do you wish to continue? [No]: y
Do you wish clear this partition? [No]: y
Do you wish to enable this partition? [Yes]: y
```

例: activate proxy

```
HOD Client Cache>activate pr
    1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition
Enter proxy number: [1]? 1
You are trying to activate an existing proxy.
Doing this will cause the proxy to be terminated before
being reactivated.
Do you wish to continue? [No]: y
```

Clear

clear コマンドは、ホスト・オンデマンド・クライアント・キャッシュ区画からすべてのオブジェクトをクリアしたり、統計をクリアするのに使用します。

注: 区画からオブジェクトをクリアしても、区画の統計はクリアされません。

構文:

clear partition
statistics

partition
区画からすべてのオブジェクトをクリアします。

statistics
区画の既存の統計をクリアします。

例: clear partition

```
HOD Client Cache>clear pa
HOD Client Cache partition must be disabled to clear its contents.
Do you wish to continue? [No]: y
Do you wish to enable this partition? [Yes]: y
```

Enable

enable コマンドは、ホスト・オンデマンド・クライアント・キャッシュ区画を使用可能にするのに使用します。

構文:

enable partition

例:

```
HOD Client Cache>enable partition
```

Delete

delete コマンドは、ホスト・オンデマンド・クライアント・キャッシュ区画を削除するのに使用します。

構文:

delete partition

partition
ホスト・オンデマンド・クライアント・キャッシュ区画を削除します。

例: delete partition

```
HOD Client Cache>delete partition
WARNING: This will delete partition and free all memory!
Do you wish to continue?  [No] : yes
HOD Client Cache>
```

Disable

disable コマンドは、ホスト・オンデマンド・クライアント・キャッシュ区画を使用不可にするのに使用します。

構文:

disable partition

例:

```
HOD Client Cache>disable partition
```

List

list コマンドは、ホスト・オンデマンド・クライアント・キャッシュ区画、すべてのポリシーおよびプロキシー、または指定されたポリシーまたはプロキシーのための情報を表示するのに使用します。

構文:

list all
delete
depend
external
item

partition
policy
proxy

all ホスト・オンデマンド・クライアント・キャッシュ区画、すべてのポリシー、およびすべてのプロキシーを表示します。

delete ホスト・オンデマンド・クライアント・キャッシュ区画から削除された最後の 100 項目を表示します。

depend
区画の依存関係テーブルを表示します。

external
外部キャッシュ制御マネージャーのための情報を表示します。

item ホスト・オンデマンド・クライアント・キャッシュ区画内の現在の項目を表示します。

partition
ホスト・オンデマンド・クライアント・キャッシュ情報を表示します。

policy ホスト・オンデマンド・クライアント・キャッシュ・ポリシー情報を表示します。

proxy ホスト・オンデマンド・クライアント・キャッシュ・プロキシー情報を表示します。

例: list all

```
HOD Client Cache>list all
HOD Client Cache Partition         Status: Enabled
     Cluster address: 113.3.1.10  Port 80
1 partition(s) active.
External Cache Manager Port: 83
         Connection timeout: 120 seconds
```

例: list delete

```
HOD Client Cache>list delete

Delete Table
URL string -- hit count
=======================
'/abc.html' -- 4
'/soccer.html' -- 2
'/tennis.html' -- 1
'/curling.html' -- 3
```

例: list item

```
HOD Client Cache>list item

Current number of items: 5
URL String -- hit count
=======================
'/' -- 2
'/file5k.html' -- 1
'/file4k.html' -- 1
'/file2k.html' -- 3
'/file1k.html' -- 1
```

例: list partition

```
HOD Client Cache>list partition
HOD Client Cache Partition         Status: Enabled
     Cluster address: 113.3.1.10, Port 80
Partition size: Current - 0 bytes  Highest - 0 bytes   Maximum - Unlimited
```

```
Number of objects: Current - 0  Highest - 0 Maximum - Unlimited
Maximum object size: Unlimited
HOD Client Cache purge interval: 600 minute(s)
Hit ratio: 0%
Total number of hits:  0
Cache Hit Bytes Served:  0
Breakdown of responses for the Cache Hits
 (note: this is based on whether the HTTP Proxy considered it a hit.
  So these count may not add up to the hit count above)
   Response 200(OK):                0
   Response 203(Non-Authoriative):  0
   Response 206(Partial Content):   0
   Response 300(Multiple Choices):  0
   Response 301(Moved Permanently): 0
   Response 304(Not Modified):      0
   Response 410(Gone):              0
Total number of misses:  0
Cache Miss Bytes Served:  0
Breakdown of responses for the Cache Misses
   Response 100 Range(Information):         0
   Response 200(OK):                        0
   Response 200 Range(Successful-not 200):  0
   Response 304(Not Modified):              0
   Response 300 Range(Redirection-not 304): 0
   Response 400 Range(Client Error):        0
   Response 500 Range(Server Error):        0
   Response other (not in the above):       0
Object Excluded (Object too large):        0
                (Object expired):          0
                (DONT CACHE header):       0
                (URL Mask excluded):       0
                (Image excluded):          0
                (Static object excluded):  0
                (Dynamic object excluded): 0
                (Cache disabled):          0
Total number of objects added via ECCM Interface: 0
Total number of objects not added via ECCM Interface but was attempted: 0
Total number of objects replaced via ECCM Interface: 0
```

例: list policy

```
HOD Client Cache>list policy
URL mask to identify Java Applets: *.jar
     Default lifetime: 60 minute(s)
```

例: list proxy

```
HOD Client Cache>list proxy
    1)   Cluster address 113.3.1.10, Port 80, HOD Client Cache Partition
Enter proxy number: [1]? 1
Proxy 1: assigned to the HOD Client Cache partition
Cluster address: 113.3.1.10     Port number: 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
Client connections: 0 current / 0 at highest point
Server connections: 0 current / 0 at highest point
Total cache hits: 0
Total cache misses: 0
Cache misses (object not in cache): 0
             (unsupported method):  0
             (can't send response): 0
             (non-cached request):  0
```

Modify

modify コマンドは、外部キャッシュ制御マネージャーを変更するのに使用します。

構文:

modify external

ホスト・オンデマンド・クライアント・キャッシュ動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

ホスト・オンデマンド・クライアント・キャッシュは、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、ホスト・オンデマンド・クライアント・キャッシュには適用できません。ホスト・オンデマンド・クライアント・キャッシュはフィーチャーで、インターフェースではありません。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、ホスト・オンデマンド・クライアント・キャッシュには適用できません。ホスト・オンデマンド・クライアント・キャッシュはフィーチャーで、インターフェースではありません。

GWCON (Talk 5) 構成要素リセット・コマンド

ホスト・オンデマンド・クライアント・キャッシュ (HOD) は、次のホスト・オンデマンド・クライアント・キャッシュ (HOD) 固有 GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature HOD, Activate All コマンド

説明: このコマンドは、ホスト・オンデマンド・クライアント・キャッシュ用のすべての SRAM を読み取り、現在の実行時環境を同一にします。

ネットワークへの影響:
現在アクティブであったすべてのプロキシーを終了します (すなわち、これらのプロキシーのすべての接続をダウンさせます)。外部キャッシュ制御マネージャーが稼働していた場合、装置は現在のポートの新しい接続の listen を停止します (すなわち、現在のポートへの接続がダウンしません)。

制限事項:
制限はありません。

すべてのホスト・オンデマンド・クライアント・キャッシュ・コマンドは、**GWCON, feature HOD, activate all** コマンドによってサポートされます。

GWCON, Feature HOD, Activate Partition コマンド

説明: このコマンドは、この区画用のすべての SRAM を読み取り、現在の実行時環境を同一にします。

ネットワークへの影響:
活動化されている区画がすでに存在する場合、この区画のすべてのプロキシーを終了します (すなわち、これらのプロキシーのすべての接続をダウンさせます)。

制限事項:

ホスト・オンデマンド・クライアント・キャッシュは、すでに活動化されていなければなりません (**CONFIG, feature HOD, activate** を参照)。

次の表では、**GWCON, feature HOD, activate partition** コマンドが起動されると活動化されるホスト・オンデマンド・クライアント・キャッシュの構成変更を要約します。

GWCON, feature HOD, activate partition コマンドによって変更が活動化されるコマンド
CONFIG, feature HOD, add URLMASK
CONFIG, feature HOD, delete PARTITION
CONFIG, feature HOD, delete URLMASK
CONFIG, feature HOD, modify PARTITION
CONFIG, feature HOD, modify PROXY
CONFIG, feature HOD, modify URLMASK

GWCON, Feature HOD, Activate Proxy コマンド

説明: このコマンドは、このプロキシー用のすべての SRAM を読み取り、プロキシー用の現在の実行時環境を同一にします。

ネットワークへの影響:

活動化されているプロキシーがすでに存在する場合、このプロキシーを最初に終了します (すなわち、これらのプロキシーのすべての接続をダウンさせます)。

制限事項:

- ホスト・オンデマンド・クライアント・キャッシュは、すでに活動化されていなければなりません (**CONFIG, feature HOD, activate** を参照)。

次の表では、**GWCON, feature HOD, activate proxy** コマンドが起動されると活動化されるホスト・オンデマンド・クライアント・キャッシュの構成変更を要約します。

GWCON, feature HOD, activate proxy コマンドによって変更が活動化されるコマンド
CONFIG, feature HOD, modify PROXY

GWCON, Feature HOD, Activate External Port コマンド

説明: このコマンドは、外部キャッシュ制御マネージャー用のすべての SRAM を読み取り、外部キャッシュ制御マネージャー用の現在の実行時環境を同一にします。

ネットワークへの影響:

外部キャッシュ制御マネージャーが稼働していた場合、装置は現在のポートの新しい接続の listen を停止します (すなわち、現在のポートへの接続がダウンしません)。

制限事項:

- ホスト・オンデマンド・クライアント・キャッシュは、すでに活動化されていなければなりません (**CONFIG, feature HOD, activate** コマンドを参照)

次の表では、**GWCON, feature HOD, activate external port** コマンドが起動されると活動化されないホスト・オンデマンド・クライアント・キャッシュ (HOD) の構成変更を要約します。

GWCON, feature HOD, activate external port コマンドによって変更が活動化されるコマンド
CONFIG, feature HOD, modify EXTERNAL

CONFIG (Talk 6) Activate コマンド

ホスト・オンデマンド・クライアント・キャッシュ (HOD) は、次の CONFIG (Talk 6) **activate** コマンドをサポートします。

CONFIG, Feature HOD, Activate コマンド

説明: 現在の SRAM に基づいて現在稼働しているホスト・オンデマンド・クライアント・キャッシュを動的に変更します。

ネットワークへの影響:
現在アクティブであったすべてのプロキシーを終了します (すなわち、これらのプロキシーのすべての接続をダウンさせます)。外部キャッシュ制御マネージャーが稼働していた場合、装置は現在のポートの新しい接続の listen を停止します (すなわち、現在のポートへの接続はダウンしません)。

制限事項:
なし

すべてのホスト・オンデマンド・クライアント・キャッシュ・コマンドは、**CONFIG, feature HOD, activate** コマンドによってサポートされます。

GWCON (Talk 5) 一時変更コマンド

ホスト・オンデマンド・クライアント・キャッシュ (HOD) は、装置の操作状態を一時変更する、次の GWCON コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行すると、行われません。

・コマンド
GWCON, feature HOD, modify external **注:** このコマンドは、外部キャッシュ制御マネージャー用の現在の実行時環境を変更します。外部キャッシュ制御マネージャーが稼働していた場合、装置は現在のポートの新しい接続の listen を停止します (すなわち、現在のポートへの接続がダウンしません)。
GWCON, feature HOD, delete partition **注:** このコマンドは、現在の実行時環境から区画を削除します。

第11章 Web サーバー・キャッシュの使用

この章では、2216 Web サーバー・キャッシュ・フィーチャーについて説明します。この章には、次の内容が記載されています。

- 『Web サーバー・キャッシュの概説』
- 184ページの『HTTP プロキシーの使用』
- 186ページの『スケーラブルな高可用性キャッシュ』
- 190ページの『外部キャッシュ制御マネージャーの概説』

Web サーバー・キャッシュの概説

Web サーバー・キャッシュは、頻繁に要求される Web ページを保管して、すばやく検索できるようにします。 Web サーバー・キャッシュは、要求頻度の高い項目をクライアントの近くに保持することにより、現在ファイル・サービスや通信の接続に使用されているサーバー資源を解放します。2216 Web サーバー・キャッシュは、Web ページへの高速アクセスを可能にし、ホスト通信のオーバーヘッドを軽減します。2216 Web サーバー・キャッシュは、次の機能を備えています。

- 静的な無保護 Web ページを保管する。
- HTTP クライアントとサーバーに、キャッシュへのアクセスを提供する。
- ユーザーがキャッシュ保管および無効化ポリシーを定義できるようにする。
- ネットワーク・ディスパッチャー機能を使用して、サーバー間のワーク ロードのバランスを取り、バックアップ・キャッシュ機能を提供する。
- 将来のサーバー指向キャッシュ機能のためのプラットフォームを提供する。

注: 1 つの構成内に、Web サーバー・キャッシュとホスト・オンデマンド・クライアント・キャッシュ・フィーチャーが共存することはできません。

TCP/IP 接続をサポートするすべての 2216 ネットワーク・インターフェースは、Web サーバー・キャッシュ、HTTP サーバー、およびクライアント間の接続をサポートします。

180ページの図10 は、Web サーバー・キャッシュが存在しない場合のネットワーク・ディスパッチャーの作動を示しています。

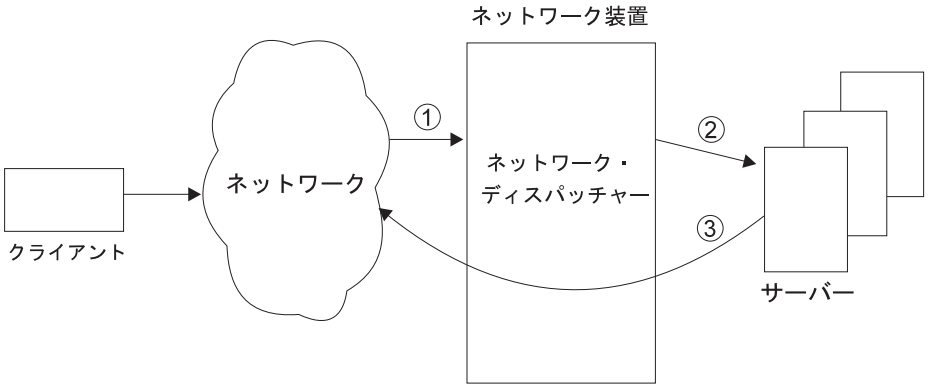


図 10. Web サーバー・キャッシュが存在しない場合のネットワーク・ディスパッチャー

1. クラスター・アドレスあてに要求が来ます。
2. ネットワーク・ディスパッチャーは、要求をサーバーに転送します。
3. サーバーは応答をクライアントに戻します。

図11 は、Web サーバー・キャッシュが存在し、要求されたページが現在キャッシュされていない場合のネットワーク・ディスパッチャーの作動を示しています。Web サーバー・キャッシュは、応答をキャッシュにロードします (ポリシーで可能な場合)。

HTTP プロキシーについては、184ページの『HTTP プロキシーの使用』を参照してください。

区画とは、キャッシュ・コア・メモリーの一部分です。各キャッシュ区画は、独立して構成されており、装置が複数のサイトをサポートできるようにします。

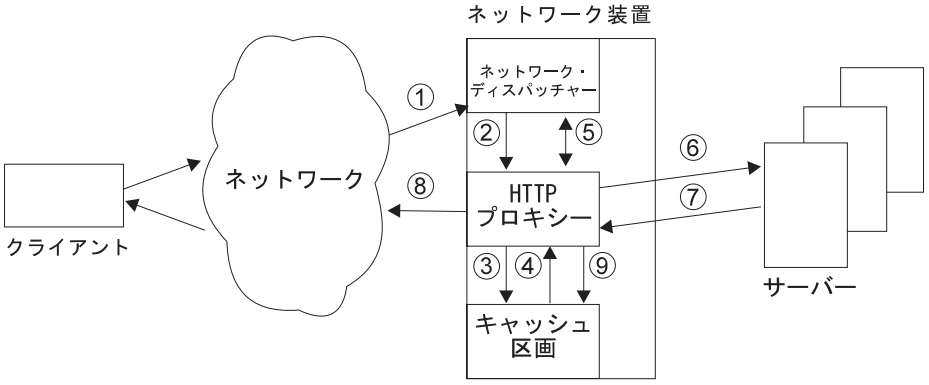


図 11. Web サーバー・キャッシュが存在し、キャッシュでヒットしない場合のネットワーク・ディスパッチャー

1. クラスター・アドレスに要求が入ります。
2. ネットワーク・ディスパッチャーは、要求を HTTP プロキシー (区画が使用可能にされた場合) に転送します。
3. HTTP プロキシーはキャッシュ区画を調べます。
4. HTTP プロキシーは、キャッシュ区画内で要求されたページを見つけることができません。

5. HTTP プロキシーは、ネットワーク・ディスパッチャーからサーバー情報を入手します (新しい接続に必要な場合)。
6. HTTP プロキシーは要求をサーバーに転送します。(TCP 接続の場合、発信元 IP アドレスは 2216 ネットワーク・インターフェースのアドレスです。着信先 IP アドレスは、サーバー・インターフェース IP アドレスです。)
7. サーバーは応答を HTTP プロキシーに戻します。
8. HTTP プロキシーは要求をクライアントに送信します。
9. HTTP プロキシーは応答をキャッシュ区画にロードします (ポリシーで可能な場合)。

サーバーあてのパケットの宛先アドレスがサーバー・アドレスであり、上記ステップ 6 に述べたとおり、クラスター・アドレスではないことを管理者が認識することが重要です。この問題は、Web サーバーをホストに構成するときに重要です。Web サーバーを特定の IP アドレスで listen するように構成した場合、この IP アドレスはサーバー・インターフェース IP アドレスでなければなりません。もっと一般的に、サーバー・インターフェースは、このインターフェースに割り当てられた一連の論理 IP アドレスをもちます。サーバー論理 IP アドレスを使用するように、ネットワーク・ディスパッチャー・クラスターを構成すると、この論理 IP アドレスで listen するように、対応する Web サーバーを構成する必要があります。したがって、1 つのホスト (サーバー) には、異なる論理 IP アドレスでそれぞれ listen する、いくつかの Web サーバーをもつ場合があります。ネットワーク・ディスパッチャーは、各 Web サーバー用に別個のクラスターを使用して構成できます。このようにして、1 つのホストは多くの Web サイト用に使用できます。また、別個のキャッシュ区画がそれぞれの Web サーバーように使用する必要になります。 Web サーバーが複製ホスト上にあるときは、複製ホスト数に Web サーバー数を掛け算して、使用されるサーバー・アドレス数を決めます。

さらに、クラスター・アドレス数は、各ホストのループバック・アドレスで別名で使用する必要があります。それによって、キャッシュ区画が使用不可である場合、ネットワーク・ディスパッチャーがシンプル・ポート・モードをゼロ (キャッシュしない)にフォールバックしたときに、Web サーバーは継続して到達可能です。フォールバック操作が保証されるのは、直接接続サーバーの場合だけです。その他の場合には、ルーティングが処理不能または不可能になります。

182ページの図12 は、Web サーバー・キャッシュが存在し、要求されたページが現在キャッシュされている場合のネットワーク・ディスパッチャーの作動を示しています。

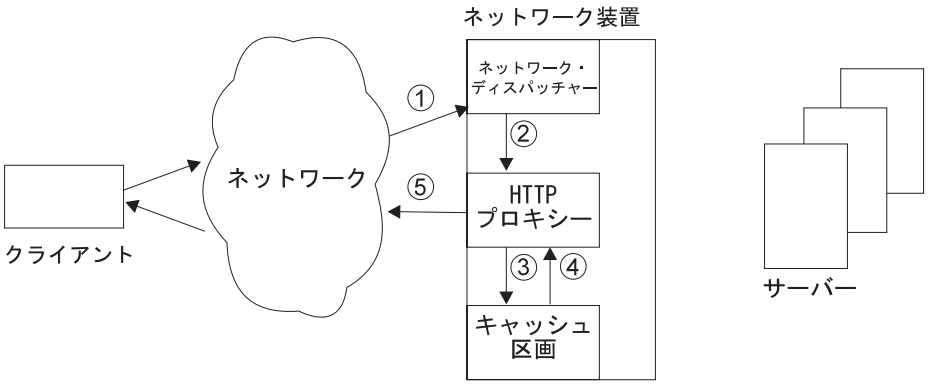


図 12. Web サーバー・キャッシュが存在し、キャッシュでヒットする場合のネットワーク・ディスパッチャー

1. クラスター・アドレスあてに要求が来ます。
2. ネットワーク・ディスパッチャーは要求を HTTP プロキシーに転送します。
3. HTTP プロキシーはキャッシュ区画を調べます。
4. HTTP プロキシーは、キャッシュ区画内で要求されたページを見つけます。
5. HTTP プロキシーは応答をクライアントに戻します。

キャッシュ

2216 Web サーバー・キャッシュは、次の機能を備えています。

Web ページのキャッシュ

2216 は、サーバーから要求されたオブジェクトをキャッシュに入れることができます。このキャッシュは、透過的キャッシュと呼ばれます。`talk 6` を使用すると、区画についての透過的キャッシュを使用可能にしたり、使用不可にしたりできます。

透過 (自動) キャッシュに代わるものとして、手動キャッシュがあります。この場合、外部エージェントはキャッシュ・マネージャーを使用して Web ページをキャッシュに入れます。外部制御 Web キャッシュについては、190ページの『外部キャッシュ制御マネージャーの概説』を参照してください。

キャッシュに入れられた失効オブジェクトは、自動的に削除されます。2216 Web サーバー・キャッシュは、HTTP 1.0 および 1.1 サーバーとクライアントをサポートします。

柔軟なキャッシュ・ポリシー

ユーザーが、さまざまなクラスの Web オブジェクト (イメージ、非イメージ静的ページ、動的ページ) をキャッシュするかどうかを指定できるようにします。オブジェクトおよびキャッシュ区画の最大サイズも指定できます。さらに、URL マスクを指定して、特定のクラスの Web オブジェクトをユーザー環境に明示的に組み込む、または除外する (該当する方) こともできます。

透過的キャッシュ・ポリシーのフロー・チャート

1. キャッシュが使用可能にされ、透過的キャッシュが使用可能にされていますか?

- いいえ - オブジェクトはキャッシュされません。
- はい - 2 のステップに進んでください。

2. オブジェクト・サイズは最大オブジェクト・サイズ以内ですか?
   - いいえ - オブジェクトはキャッシュされません。
   - はい - 3 のステップに進んでください。
3. オブジェクトは有効期限切れになっていますか?
   - いいえ - 4 のステップに進んでください。
   - はい - オブジェクトはキャッシュされません。
4. HTTP ヘッダーを使用することになっており、HTTP ヘッダーの 1 つが使用されましたか? **使用される HTTP ヘッダーは、DO または DONT 指示をもつキャッシュ制御ヘッダーです。**
   - いいえ - オブジェクトはキャッシュされません。
   - はい - HTTP ヘッダーが使用され、オブジェクトにキャッシュ制御ヘッダーが含まれていませんか? 5 のステップに進んでください。
5. HTTP ヘッダーは ″DO″ キャッシュを指示していますか?
   - いいえ - オブジェクトはキャッシュされません。
   - はい - 9 のステップに進んでください。
6. 除外マスクによって URL が除外されていますか?
   - はい - オブジェクトはキャッシュされません。
   - いいえ - 7 のステップに進んでください。
7. 包含マスクによって URL が組み込まれていますか?
   - はい - 9 のステップに進んでください。
   - いいえ - 8 のステップに進んでください。
8. オブジェクトはイメージ (.jpg または .gif) ですか?
   - いいえ - 9 のステップに進んでください。
   - はい - イメージはキャッシュ可能ですか?
     - はい - 184ページの11 のステップに進んでください。
     - いいえ - オブジェクトはキャッシュされません。
9. オブジェクトは静的非イメージですか?
   - いいえ - 10 のステップに進んでください。
   - はい - 静的非イメージ・オブジェクトはキャッシュ可能ですか?
     - はい - 184ページの11 のステップに進んでください。
     - いいえ - オブジェクトはキャッシュされません。
10. このオブジェクトは動的オブジェクトです。動的オブジェクトはキャッシュ可能ですか?
    - はい - 184ページの11 のステップに進んでください。
    - いいえ - オブジェクトはキャッシュされません。

11. 区画内にオブジェクトを入れる余地がありますか? **オブジェクトを入れる余地を作るために、最も古く使用されたオブジェクトが除去されます。**
    - いいえ - オブジェクトはキャッシュされません。
    - はい - オブジェクトはキャッシュされます。

複数の独立したキャッシュのサポート

最大 16 の区画をサポートし、1 台の 2216 が複数のクラスターに対して独立したキャッシュ・サービスを提供することができます。キャッシュ区画は完全に独立しています。各キャッシュ区画は、独自のコンテンツとポリシーを保持します。

全 TCP/IP サーバーとの接続

TCP/IP プロトコルをサポートするすべての 2216 ネットワーク・インターフェースを介してサーバーおよびクライアントと通信します。

バックエンド・サーバーの負荷平衡 (ネットワーク・ディスパッチャーを使用して)

ネットワーク・ディスパッチャーを使用してサーバーのグループを定義し、サーバー間のロード・バランスを取ることによって、キャッシュ内で見つからなかった Web ページの検索を高速化します。

バックアップ・キャッシュのサポート

ユーザーは 2 台目の 2216 をバックアップ・サーバー・キャッシュとして定義することができます。バックアップ・サーバー・キャッシュは、ネットワーク・ディスパッチャー高可用性機能を使用する ″コールド″ バックアップとして作動します。詳しくは、107ページの『ネットワーク・ディスパッチャーの高可用性』を参照してください。

注: バックアップ・サーバー・キャッシュは、起動時には空です。透過的キャッシュを使用する (たとえば、URL を求める要求) か、または外部キャッシュ制御マネージャー機能を使用してページを強制的にキャッシュに入れることにより、バックアップ・サーバー・キャッシュの中身を入れ直す必要があります。

HTTP プロキシーの使用

各 HTTP プロキシーは、キャッシュを実行するクラスター・アドレス / ポートを表します。複数の HTTP プロキシーが 1 つのキャッシュ区画を使用することも可能です。

HTTP プロキシーはクライアントから要求を受信し、キャッシュ区画から要求を満たそうと試みます。HTTP プロキシーが要求を満たせる場合は、クライアントに応答を戻します。HTTP プロキシーが要求を満たせない場合は、サーバーとの TCP 接続をオープンして要求を満たそうと試みます。サーバーが HTTP プロキシーの要求に応答した場合、HTTP はサーバーの応答をクライアントに転送します。HTTP プロキシーはクライアントからの応答をキャッシュする必要があるかどうかも調べます。応答をキャッシュする必要がある場合には、HTTP プロキシーは応答をキャッシュ区画に渡します。

HTTP プロキシーは、次のガイドラインに従って接続を処理します。

- HTTP プロキシーは、キャッシュからの GET および HEAD 方式についての要求だけを満たそうと試みます。その他の要求はすべて、クライアントからの TCP 接続と対になっているサーバーへの TCP 接続を介して、変更しないままサーバーに転送します。クライアントからの TCP 接続と対になっている TCP 接続が存在しない場合は、サーバーへの新規の TCP 接続をオープンし、クライアントへの TCP 接続と対にします。
- キャッシュ区画から満たすことができなかった GET および HEAD 方式要求はすべて、メッセージを変更しないまま、TCP 接続を介してサーバーに転送します。
- 応答はすべて、サーバーが送信したまま変更せずに、クライアントへの TCP 接続を介して、クライアントに戻します。
- GET 方式の応答だけキャッシュできます。その他の応答はすべてキャッシュ不能とみなされます。GET 応答は、応答の状況が「受け入れ可能」であり、GET 応答と区画のキャッシュ・ポリシーがキャッシュを許可している場合にだけ、キャッシュされます。
  - 次の状況コードを持つ応答だけがキャッシュされます。HTTP プロキシーは、HTTP ヘッダーでこの規則を無効にできません。

    状況コード

    - 200 (OK)
    - 203 (non-authoritative (不許可))
    - 300 (multiple-choice)
    - 301 (moved permanently (永久移動))
    - 410 (gone (除去))
- GET 要求に HTTP ヘッダーが使用されている場合、`If-Modified-Since` 要求ヘッダーだけを使用して、その要求を満たす項目がキャッシュ内に存在するかどうかを調べます。その他の条件付きヘッダーは使用されません。Web サーバー・キャッシュは、エンティティー・タグを使用して、キャッシュされたエンティティーを応答内に使用できるかを調べることはしません。
- 要求内の `Cache-Control` ヘッダー指示は無視されます。エンティティーがキャッシュ区画内に存在しない場合、要求はサーバーに渡されます。

  注: Web サーバー・キャッシュはサーバーの拡張なので、HTTP プロキシー・キャッシュのように `Cache-Control` ヘッダーを使用することはありません。
- 応答ではキャッシュ・ヘッダー指示 ″do″ および ″dont″ がサポートされます。その他の指示はすべて無視されます。″do″ および ″dont″ 指示は、エンティティーをキャッシュするのか、しないのかを Web サーバー・キャッシュに知らせるためにサーバーが使用できる新規の指示です。
- HTTP プロキシーは、キャッシュからの部分的 GET 要求は満たそうと試みますが、部分的 GET 応答はキャッシュしません。

  注: 部分的 GET 要求に含まれる範囲の数が 10 を超えている場合は、応答全体が戻されます。
- 着信要求はすべて同じサーバー・クラスターあてのはずなので、すべての HTTP メッセージの `Host` ヘッダーは無視されます。

- HTTP プロキシーは、持続 HTTP 接続をサポートします。

  注: 持続接続が HTTP 1.0 レベルのクライアントから着信し、応答をキャッシュから戻す場合、要求に基づいて Connection ヘッダーが付けられます。たとえば、クライアントが長期的接続を望む場合は、長期的接続を保持します。
- HTTP プロキシーは、Authorization ヘッダーを含む要求には、キャッシュを使用しません。そのような要求に対する応答はキャッシュしません。Proxy-Authorization ヘッダーを含む応答はキャッシュしません。
- HTTP プロキシーは、HTTP 接続上の要求または応答の解析で問題が生じた場合、HTTP 接続をトンネル伝送に切り替えることができます。トンネル伝送の動作は、すべてのメッセージの解析を停止し、クライアントからのすべての要求をサーバーに転送し、サーバーからのすべての応答をクライアントに転送します。
- キャッシュ区画が使用不可にされた場合、既存および新規の接続はすべてバックエンド・サーバーに直接転送されます。このフィーチャーを作動させるためには、105ページの『第8章 ネットワーク・ディスパッチャー・フィーチャーの使用』の手順 『ネットワーク・ディスパッチャー用のサーバーの構成』 に従ってください。
- キャッシュ区画が使用可能にされた場合、新規クライアント接続はすべてキャッシュによって処理されます。既存のクライアント接続は、引き続き要求をバックエンド・サーバーに直接転送します。

スケーラブルな高可用性キャッシュ

スケーラブルな高可用性キャッシュにより、接続された Web サーバー・キャッシュのグループは 1 つの大きなキャッシュとして機能することができます。1 つのグループ内のキャッシュの最大数は 16 です。1 つのキャッシュ・メンバーで障害が発生すると、すべてのキャッシュ機能が終了するのではなく、キャッシュに使用できるメモリーの総数が少なくなります。構成の例については、190ページの図17 を参照してください。

合計キャッシュ・スペースは、個々のキャッシュにより構成されます。キャッシュが機能しなくなると、着信ページは、作動している残りのキャッシュによって引き続きキャッシュされます。

着信 Web ページは、グループのキャッシュ内に保管されます。それらのページは、使用可能なキャッシュ間で等しく分配されます。グループ内の各キャッシュは、グループ内の到達可能なキャッシュの数とそれぞれの IP アドレスを追跡するテーブルを保持します。テーブルは、1 つのグループ内のすべてのキャッシュについて同じです。これらのテーブルをキャッシュ・アレイ・ルーチン・プロトコル (CARP) アルゴリズムと一緒に使用して、特定の URL をどのキャッシュが所有するかを判別します。テーブルの情報は、ネットワーク・ディスパッチャー装置から来るものと、HTTP アドバイザーを使用してグループ内の Web サーバー・キャッシュの状況を追跡しているキャッシュから間接的に来るものとがあります。次の図は、SHAC を使用して URL の位置を確認するための条件を示します。

187ページの図13 では、最初に要求を受け取ったキャッシュに入っているネットワーク・ディスパッチャーからの要求を示しています。

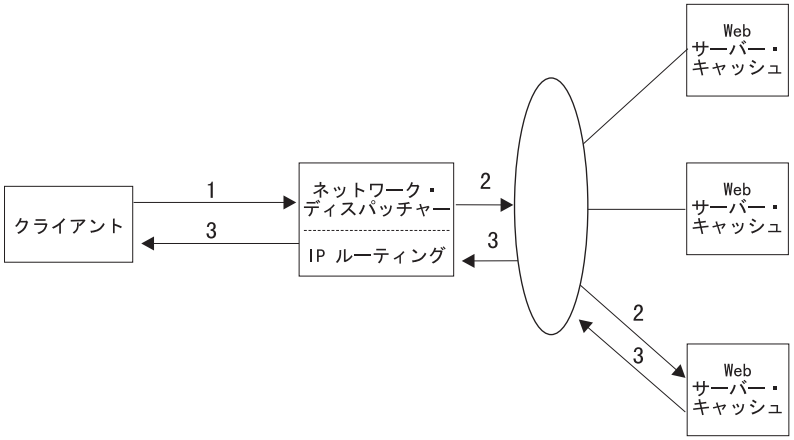


図 13. キャッシュ要求の検出

1. Web ページについての HTTP 要求が、クライアントからネットワーク・ディスパッチャーへ来ます。
2. この要求は、ネットワーク・ディスパッチャーにより、Web サーバー・キャッシュの 1 つに転送されます。キャッシュは、要求を受け取り、その要求に Web ページが含まれていることを検出します。
3. キャッシュは、ネットワーク・ディスパッチャーをう回して、Web ページをクライアントへ直接送信します。

図14 では、要求は、ネットワーク・ディスパッチャーから最初に要求を受け取ったキャッシュに入っておらず、CARP アルゴリズムは、別のキャッシュが URL を所有していることを示します。

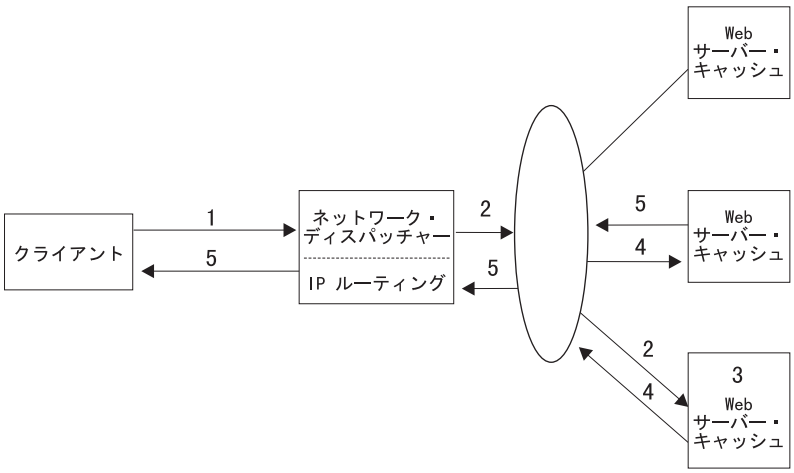


図 14. 責任を負うキャッシュへの要求の転送

1. Web ページについての HTTP 要求が、クライアントからネットワーク・ディスパッチャーへ来ます。
2. この要求は、ネットワーク・ディスパッチャーにより、Web サーバー・キャッシュの 1 つに転送されます。

3. キャッシュは、要求を受け取りますが、そのキャッシュ内では Web ページを検出できません。そこで、キャッシュはアルゴリズムを使用して、Web ページについて責任を負うキャッシュを見付けます。
4. 次に要求は、その Web ページについて責任を負うキャッシュに転送されます。
5. Web ページについて責任を負うキャッシュは要求を受け取り、Web ページを検出し、Webページをクライアントに送信します。

図15 では、要求は、ネットワーク・ディスパッチャーからその要求を受け取ったキャッシュに入っていませんが、CARP アルゴリズムは、そのキャッシュが URL の責任を負っていることを示します。

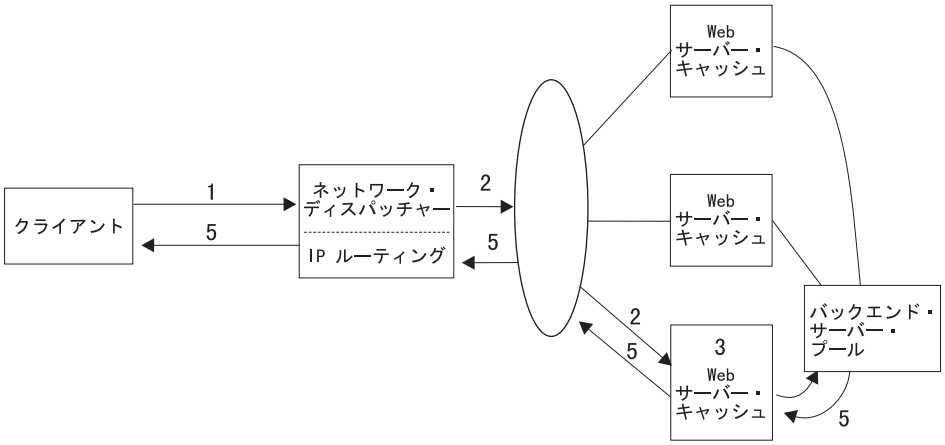


図 15. バックエンド・サーバーに転送される要求

1. Web ページについての HTTP 要求が、クライアントからネットワーク・ディスパッチャーへ来ます。
2. この要求は、ネットワーク・ディスパッチャーにより、Web サーバー・キャッシュの 1 つに転送されます。
3. キャッシュは、要求を受け取りますが、そのキャッシュ内では Web ページを検出できません。キャッシュはアルゴリズムを使用して、その Web ページについて責任があるか判別します。
4. キャッシュは、その要求をバックエンド・サーバーに送信します。
5. バックエンド・サーバーはその Web ページを検出します。すると、その Web ページは、そのページについて責任を負うキャッシュからクライアントへ戻されます。キャッシュがそのページをキャッシュに入れるよう構成されている場合には、そのページはキャッシュに入れられます。構成情報については、221ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。

189ページの図16 では、キャッシュ・グループ内のどのキャッシュにも入っていない要求を示しています。

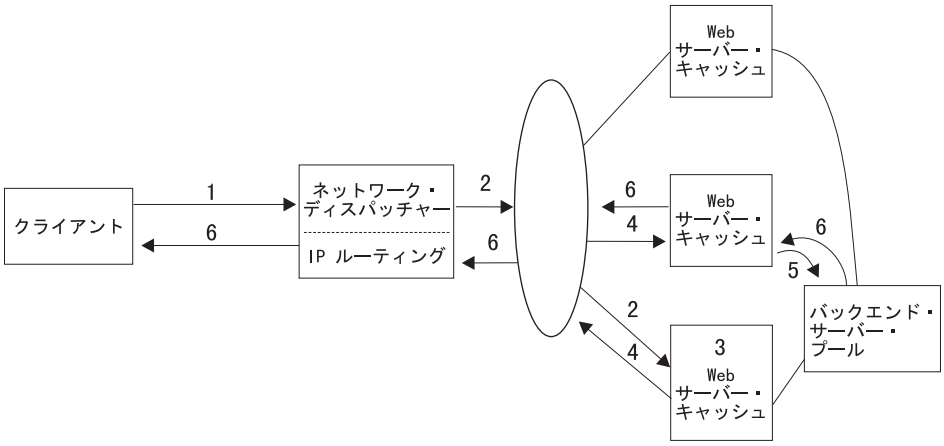


図 16. 責任を負うキャッシュへ転送されても検出されない要求

1. Web ページについての HTTP 要求が、クライアントからネットワーク・ディスパッチャーへ来ます。
2. この要求は、ネットワーク・ディスパッチャーにより、Web サーバー・キャッシュの 1 つに転送されます。
3. キャッシュは、要求を受け取りますが、そのキャッシュ内では Web ページを検出できません。そこで、キャッシュはアルゴリズムを使用して、Web ページについて責任を負うキャッシュを見付けます。次に要求は、その Web ページについて責任を負うキャッシュに転送されます。
4. Web ページについて責任を負うキャッシュは、要求を受け取りますが、その Web ページを検出できません。
5. Web ページについて責任を負うキャッシュは、要求をバックエンド・サーバー・プールへ送信します。
6. バックエンド・サーバーはその Web ページを検出します。すると、その Web ページは、そのページについて責任を負うキャッシュからクライアントへ戻されます。キャッシュがそのページをキャッシュに入れるよう構成されている場合には、そのページはキャッシュに入れられます。構成情報については、221ページの『第12章 Web サーバー・キャッシュの構成と監視』を参照してください。

注: 188ページの図15 および 図16では、グループ内のすべてのキャッシュは、プール内のすべてのバックエンド・サーバーに接続されて最高の信頼性が得られることがよく分かります。

190ページの図17 は、124ページの『スケーラブル高可用性キャッシュ (SHAC) でのネットワーク・ディスパッチャーの使用』、127ページの『第9章 ネットワーク・ディスパッチャー・フィーチャーの構成と監視』 および 221ページの『第12章 Web サーバー・キャッシュの構成と監視』と一緒に使用された詳細な構成パラメーターを示す、SHAC のテスト済みの例を示します。インターフェース・アドレス、内部アドレス、クラスター・アドレス、およびサーバー IP アドレスは、サブネット・マスクと一緒に示されています。キャッシュに必要なルーティング・コマンドおよび 113 リングに接続されたバックエンド・サーバーも示されています。

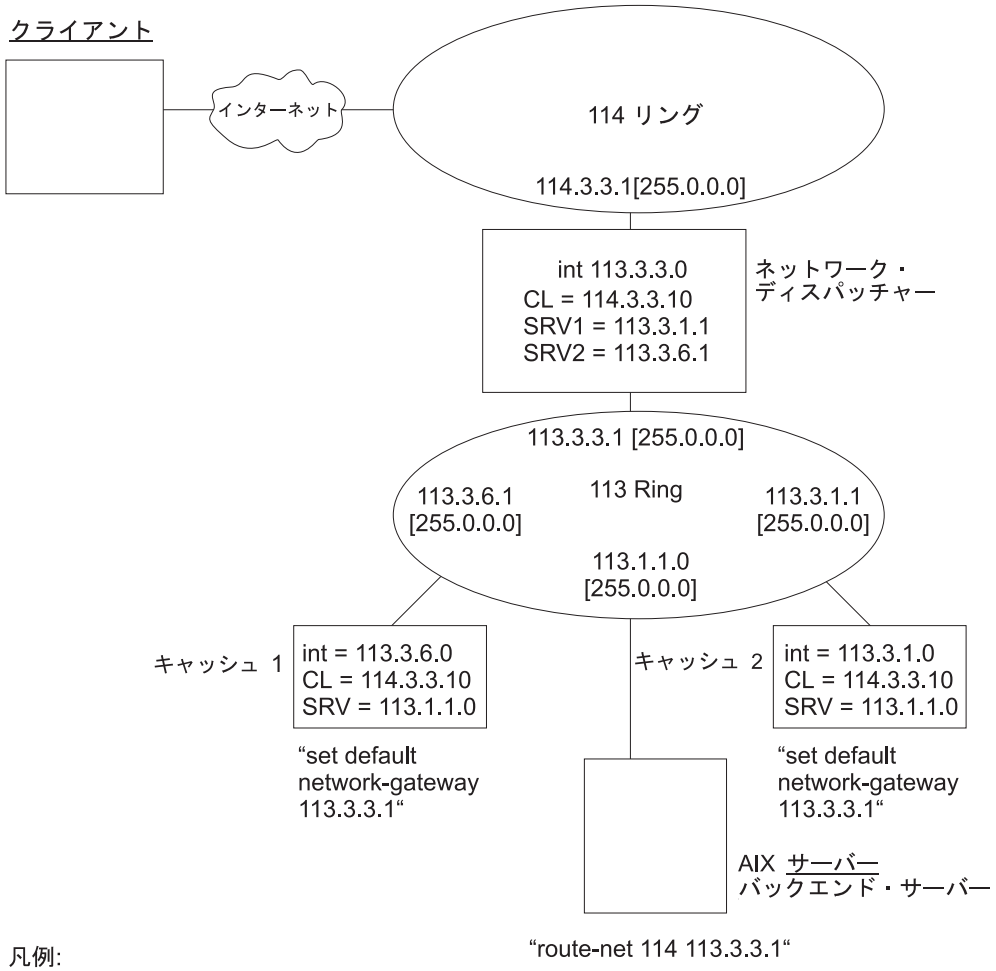


図 17. ネットワーク・ディスパッチャー、クライアント、およびバックエンド・サーバー付きの 2 つのキャッシュ

外部キャッシュ制御マネージャーの概説

外部キャッシュ制御マネージャーにより、Web サーバーは、Web サーバー・キャッシュおよびホスト・オンデマンド・クライアント・キャッシュを制御することができます。この制御は、外部キャッシュ制御マネージャー (ECCM) のためのユーザー定義ポートを介して行われます。ECCM は、接続を受け入れ、このポートを介して区画についてターゲットとされたコマンドを処理します。これらのコマンドは、外部キャッシュ制御プロトコル (ECCP) を使用します。ECCP は、ベクトル / サブベクトル形式を使用して、要求コマンドと応答コマンドを送信します。

複数のサブベクトルを付けることによって、1 つのコマンド・ベクトルで複数の機能を要求できます。各サブベクトルは、新しい機能を表します。コマンド・ベクトルは、キャッシュ区画で定義されているプロキシーのクラスター・アドレスおよびポートを指定することにより、コマンドが適用されるキャッシュ区画を示します。

ECCP によってサポートされる機能は、次のものです。

- キャッシュ区画との間でのオブジェクトの追加 / 削除
- キャッシュ区画の使用可 / 使用不可
- キャッシュ区画についてのポリシーの変更 / リスト
- キャッシュ区画についての統計のクリア / リスト
- キャッシュ区画の焦慮 (キャッシュ区画からのすべてのオブジェクトの除去)
- キャッシュ区画の照会 (特定のオブジェクトの検索)
- キャッシュ区画についての URL マスクの追加 / 削除 / リスト / クリア
- 依存関係テーブルの変更 / リスト
- 依存関係を使用したオブジェクトの無効化

依存関係テーブル

外部キャッシュ制御マネージャーにより、各キャッシュ区画について依存関係テーブルを作成することができます。このテーブルは、キャッシュ内で動的オブジェクトを扱う際に特に役立ちます。

注: 動的オブジェクトのキャッシュでは、これらのオブジェクトを構成している情報が変更されたときにオブジェクトが更新されることが必要です。

依存関係テーブルを構築する情報は、外部キャッシュ制御マネージャー・インターフェースを使用してキャッシュ区画に渡す必要があります。

依存関係テーブルにより、依存関係ストリングを一連の URL オブジェクト (キャッシュに入れられた Web ページ) に割り当てることができます。これらの依存関係は、外部キャッシュ制御マネージャー・インターフェースを使用して、Web サーバー・キャッシュ内の依存関係テーブルに保管されます。依存関係テーブルは、オブジェクトの発信元が変更されたときにこの依存関係をもつキャッシュ区画内のオブジェクトを無効化するのに使用されます。依存関係テーブルを使用しない場合には、削除するオブジェクトごとに別個の削除コマンドを送信する必要があります。

例: 次の 3 つのデータベースには、異なるオブジェクトが含まれています。

```
database1           database2           database3
---------           ---------           ---------
object_a            object_a            object_b
object_b            object_c            object_e
object_c            object_d
```

object_a から object_e までのすべてのページがキャッシュに入っているものと想定します。 database2 が変更された場合は、(キャッシュ制御マネージャー・インターフェースを介して) **invalid dependency database2** コマンドを送信できます。すると、Web サーバー・キャッシュは、キャッシュ区画から object_a、object_c、および object_d を削除します。

注: オブジェクトは、キャッシュ区画に入っていなくても依存関係テーブルに入れられます。

外部キャッシュ制御マネージャーの認証

外部キャッシュ制御マネージャーにより、ユーザー・アクセスを制御できます。この制御は、着信接続にユーザー ID とパスワードをもつよう要求することにより行

います。ユーザー ID とパスワードは、ログオン・ユーザー ID とパスワードに結び付いています。装置がパスワード保護されており、着信接続がユーザー ID とパスワードをもっていなかったり、あるいはユーザー ID とパスワードが無効である場合、認証エラー応答が戻され、接続はクローズされます。ユーザー ID とパスワードが正しければ、ユーザーはそのインターフェースを介してコマンドを送信できます。

セキュリティー

セキュリティーは、ECCP ユーザーを認証する仕組みを提供します。設定できる認証のタイプは、RADIUS、TACACS、local、none の 4 種類です。データの暗号化は用意されていません。どの認証メカニズムでも (ただし、none の場合は除く)、ユーザー ID および関連付けられたパスワードの両方が必要です。この情報は、認証ベクトルを使用して 2216 に渡されます。ユーザー ID およびパスワードは共に、1 〜 8 バイトの長さのものが可能です。外部キャッシュ制御接続で渡されるパスワードは、DES 暗号化を使用して暗号化する必要があります。暗号化に使用されるランダムの 8 バイト・シードも渡されます。暗号化のキーは、接続では渡されません。ポート値および TCP 値の設定については、231ページの『Modify』を参照してください。

注: ルーターがパスワード保護されていない場合、認証ベクトルは無視されます。

外部キャッシュ制御プロトコル

外部キャッシュ制御プロトコル (ECCP) により、バックエンド・サーバーは、ルーター・キャッシュを制御することができます。この制御により、キャッシュ性能は最大になります。

ECCP は、サーバーがキャッシュ・ポリシーの変更だけでなく、オブジェクトの追加や削除もできるように設計されたプロトコル・インターフェースです。

外部キャッシュ制御マネージャーは、接続を受け入れ、キャッシュ区画についてターゲットとされたコマンドを処理するよう、ルーター (Web サーバー・キャッシュまたはホスト・オンデマンド・クライアント・キャッシュ) で定義されます。

構成

外部キャッシュ制御マネージャーは、次のパラメーターで構成されます。

User-defined port:

外部キャッシュ制御マネージャーが接続を listen して受け入れるポート番号。0 が設定された場合、外部キャッシュ・マネージャーは使用不可と想定されます。

有効値 : 0 〜 65535

デフォルト値 : 0

Maximum TCP timeout value:

有効値 : 5 〜 240 秒

デフォルト値 : 120

Encryption Key:

Encryption Key (暗号化キー) は、ボックスがパスワード保護されている場合に使用されます。Encryption Key は、16 個の 16 進文字 (0 ～ 9、a ～ f、A ～ F) でなければなりません。

外部キャッシュ制御マネージャー機能の説明

ここでは、外部キャッシュ制御マネージャーの機能について説明します。

オブジェクトの追加

キャッシュ区画には HTTP 応答オブジェクトを追加できます。オブジェクト・データの形式は、HTTP 応答と同じでなければなりません。外部キャッシュ制御マネージャーは、応答のヘッダーを解析し、必要な情報を引き出します。すると、オブジェクトがキャッシュに追加されます。

Add Object と Add (Force) Object の違いは、Add (Force) Object では、DO または DONT を指定する Cache_Control ヘッダーはすべて無視される点です。オブジェクトをキャッシュに入れるかどうかを判別するのに HTTP プロキシーが使用するその他のヘッダーはすべて、今までどおりに使用されます。Add Object と Add (Force) Object の両方について、日付に関係なく、オブジェクトはキャッシュ区画内で置き換えられます。

オブジェクトの削除

キャッシュからオブジェクトを削除することができます。オブジェクトの URL を与えます。

依存関係テーブルの使用

キャッシュ区画の依存関係テーブルを変更、表示、および使用して、オブジェクトを無効化することができます。

依存関係テーブルを変更する (依存関係の追加または除去) 際には、依存関係と依存関係 URL の両方を与える必要があります。依存関係テーブルを変更する方法は、この他にも 2 とおりあります。 1 つはテーブル全体、依存関係全体 (つまり、依存関係を完全に除去する) 、または URL 依存関係 (つまり、すべての依存関係から URL 依存関係を除去する) をリセットする方法です。もう 1 つは、依存関係テーブル上で不要情報の収集を行う方法です。不要情報を収集することにより、キャッシュ内に依存関係 URL 付きのオブジェクトをもっていないすべての依存関係 URL が依存関係テーブルからクリアされます。

依存関係テーブル内の情報を表示する方法はいくつかあります。テーブル全体を取り出したり、所定の依存関係についての依存関係 URL をすべて取り出すことができます。また、与えられた依存関係 URL をもつすべての依存関係を取り出すこともできます。

オブジェクトは、依存関係テーブルを使用してキャッシュから除去 (無効化) することができます。依存関係を使用して、依存関係テーブルが検査されます。その依存関係の依存関係 URL がすべて、キャッシュ区画から除去されます。

区画の使用化 / 使用不可

この機能により、キャッシュ区画状態を変更できます。外部キャッシュ制御マネージャーを使用するためには、キャッシュ区画が正しい状態になっている必要があり

ます。すべてのオブジェクトをキャッシュ区画から除去するためには、キャッシュ区画が使用不可になっている必要があります。

ポリシーの使用

1 つの区画のポリシーを表示したり、変更することができます。各ポリシーごとに別個に行うこともできますが、1 つのグループとして行うこともできます。ポリシーを変更する際には、そのポリシーの正しいタイプのデータを渡す必要があります。ポリシーに基づくデータの形式については、195ページの『外部キャッシュ制御プロトコル (ECCP) ベクトルの形式』 (Policy コマンド・サブベクトルおよびポリシー応答サブベクトル) を参照してください。

区画の除去

この機能により、キャッシュ区画内のすべてのオブジェクトを除去することができます。キャッシュ区画を除去するためには、キャッシュ区画が使用不可の状態になっている必要があります。

オブジェクトの照会

この機能により、オブジェクトがキャッシュ区画内にあるかどうかを知ることができます。さらに、オブジェクトがキャッシュ区画内にあり、最後に変更された日付をもっている場合には、そのデータは戻されます。戻される日付の形式については、195ページの『外部キャッシュ制御プロトコル (ECCP) ベクトルの形式』 (照会応答サブベクトル) を参照してください。

統計の使用

この機能により、キャッシュ区画統計のリストとリセット (クリア) が可能になります。統計の形式については、195ページの『外部キャッシュ制御プロトコル (ECCP) ベクトルの形式』 (統計応答サブベクトル) を参照してください。

URL マスクの使用

この機能により、キャッシュ区画の URL マスクの表示と変更が可能になります。この機能を使用するときには、URL タイプの包含、除外、動的、またはホスト・オンデマンド・クライアント・キャッシュ・アプレットを指定する必要があります。URL タイプを 1 つ表示する必要があります。この機能は、複数の URL タイプについては働きません。

URL マスクを追加することはできます。URL マスクが包含、動的、またはホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクの場合は、存続時間を指定する必要があります。動的マスクを追加すると、現在の動的 URL マスクが変更され、ホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクを追加すると、現在のホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクが変更されます。URL マスクを削除することができます。この機能は、動的 URL マスクやホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクには無効です。特別なタイプの URL マスクをすべてリセットすることができます。動的 URL マスクをリセットすると、デフォルトの動的 URL マスクにリセットされ、ホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクをリセットすると、デフォルトのホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクにリセットされます。

注: 動的マスクは、Web サーバー・キャッシュ・イメージと一緒に使用され、ホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクはホスト・オンデマンド・クライアント・キャッシュ・フィーチャーをもつイメージと一緒に使用されます。

外部キャッシュ制御プロトコル (ECCP) ベクトルの形式

ECCP クライアントは、ベクトルの形式を使用してコマンドの送信と、応答の受信を行います。ボックスがパスワード保護されている場合は認証ベクトルが必要です。ボックスがパスワード保護されていない場合には、認証ベクトルは受信しても無視されます。

ベクトルの形式

ここでは、ベクトルのフィールド記述について説明します。

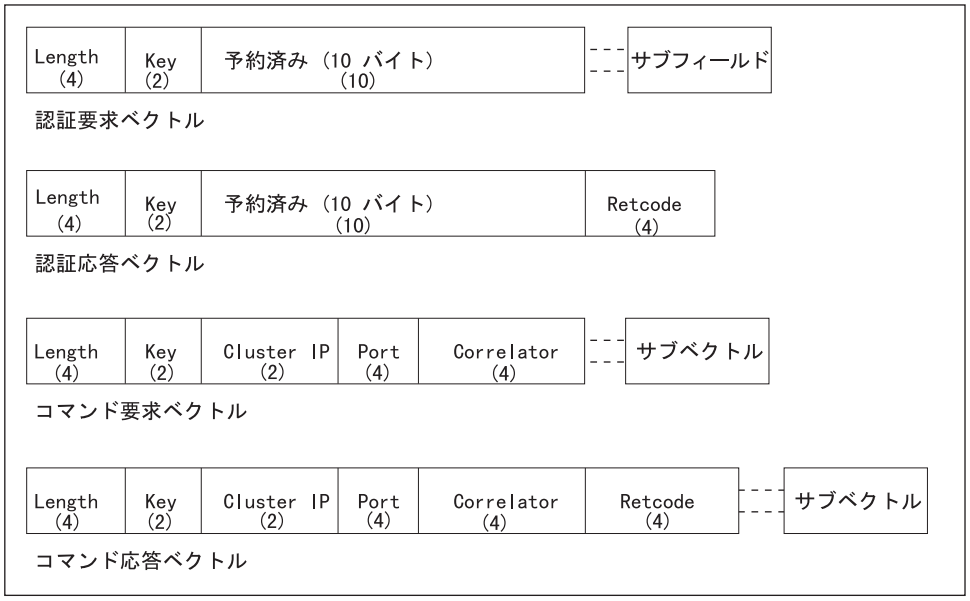


図 18. コマンド応答ベクトル

Length: ベクトル全体の長さをバイト単位で表す、符号なしの 32 ビット値。これには、フィールド length および key のほか、サブベクトルおよびサブフィールドも含まれます。受け入れ可能な範囲は、次のとおりです。

- 48 ～ 56 (認証要求ベクトル)
- 20 (認証応答ベクトル)
- 24 ～ 4GB-4 (コマンド要求ベクトル)
- 20 ～ 4GB-4 (コマンド応答ベクトル)

Key: 主要なベクトル・キーを表す、符号なし 16 ビット値。主要ベクトル・キーとは次のものです。

- 0x4A00 (認証要求ベクトル)
- 0x4A01 (認証応答ベクトル)
- 0x4B00 (コマンド要求ベクトル)
- 0x4B01 (コマンド応答ベクトル)

Cluster IP: ターゲット・キャッシュ区画に関連付けられたキャッシュ・クラスターの 32 ビットの IP アドレス。

Port: キャッシュ区画に関連付けられたキャッシュ・クラスターの 16 ビットのポート番号。

Correlator: コマンド応答をコマンド要求に関連付けるために ECCPクライアントが使用する符号なし 32 ビット値。

Retcode: 戻りコードを表す符号なし 32 ビット値。これは、応答ベクトル内にだけ存在します。

ベクトルには、1 つまたは複数のサブベクトルが含まれます。認証要求ベクトルには、name と password 両方のサブフィールドが必要です。コマンド要求ベクトルには、1 つまたは複数のコマンド・サブベクトルが含まれます。コマンド要求ベクトルに複数のサブベクトルが入っている場合には、コマンド応答ベクトル内に複数のサブベクトルが含まれます。重大エラーが発生すると、コマンド応答ベクトルの Retcode フィールドに反映されます。

認証要求ベクトル

ボックスがパスワード保護されている場合、認証要求ベクトルは、外部キャッシュ制御接続上の最初のベクトルでなければなりません。ボックスがパスワード保護されていない場合には、このベクトルは無視されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x4A00

6-15 Reserved

将来の使用に備えて予約済みです。

16 ～ (4n-1)
名前サブフィールド

4n ～ (4m-1)
パスワード・サブフィールド

コマンド要求ベクトル

コマンド要求ベクトルは、外部キャッシュ制御マネージャーにコマンドを送信します。ボックスがパスワード保護されている場合、外部キャッシュ制御マネージャーが最初に有効な認証要求ベクトルを受信してからでないと、コマンドは受け入れられません。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ。

4-5 Key

0x4B00

6-7 Port

ターゲット・キャッシュ区画と関連付けられたキャッシュ・クラスター (HTTP プロキシー) のポート番号

8-11 Cluster IP Address

ターゲット・キャッシュ区画と関連付けられたキャッシュ・クラスター (HTTP プロキシー) の IP アドレス

12-15 Correlator

相関係数 (correlator) は、コマンド応答をその対応するコマンド要求に関連付けるために使用されます。

16 ～ (4n-1)
サブベクトル

次のサブベクトルのうち 1 つまたは複数のものを付加できます。

- Add Object コマンド・サブベクトル (0x0100)
- Add Object (Force) コマンド・サブベクトル (0x0110)
- Delete Object コマンド・サブベクトル (0x0400)
- 依存関係コマンド・サブベクトル (0x0A00)
- Disable コマンド・サブベクトル (0x0300)
- Enable コマンド・サブベクトル (0x0200)
- Policy コマンド・サブベクトル (0x0500)
- Purge コマンド・サブベクトル (0x0600)
- Query コマンド・サブベクトル (0x0700)
- Statistics コマンド・サブベクトル (0x0800)
- URL マスク・コマンド・サブベクトル (0x900)

認証応答ベクトル

認証応答ベクトルは、認証要求ベクトルに応えて戻されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x4A01

6-15 Reserved

将来の使用に備えて予約済みです。

16-19 戻りコード

これは、ベクトルの戻りコードです。218ページの『戻りコード』を参照してください。

20 ～ (4n-1)
サブベクトル

現在、認証応答ベクトルにはベクトルはありません。

コマンド応答ベクトル

コマンド応答ベクトルは、コマンド要求ベクトルに応えて戻されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x4B01

6-7 Port

ターゲット・キャッシュ区画と関連付けられたキャッシュ・クラスター (HTTP プロキシー) のポート番号

8-11 Cluster IP Address

ターゲット・キャッシュ区画と関連付けられたキャッシュ・クラスター (HTTP プロキシー) のクラスター IP アドレス

12-15 Correlator

相関係数 (correlator) は、コマンド応答をその対応するコマンド要求に関連付けるために使用されます。

16-19 戻りコード

これは、ベクトルの戻りコードです。218ページの『戻りコード』を参照してください。

20 ～ (4n-1)

サブベクトル

次のサブベクトルのうちゼロ個またはそれ以上のものを付加できます。

- Add Object 応答サブベクトル (0x0101)
- Add Object (Force) 応答サブベクトル (0x0111)
- Delete Object 応答サブベクトル (0x0401)
- 依存関係応答サブベクトル (0x0A01)
- 使用不可応答サブベクトル (0x0301)
- 使用可能応答サブベクトル (0x0201)
- ポリシー応答サブベクトル (0x0501)
- 除去応答サブベクトル (0x0601)
- 照会応答サブベクトル (0x0701)
- 統計応答サブベクトル (0x0801)
- URL マスク応答サブベクトル (0x901)

サブベクトルの形式

ここでは、サブベクトルの形式について説明します。サブベクトルは、主要ベクトルと同じ基本形式に従います。

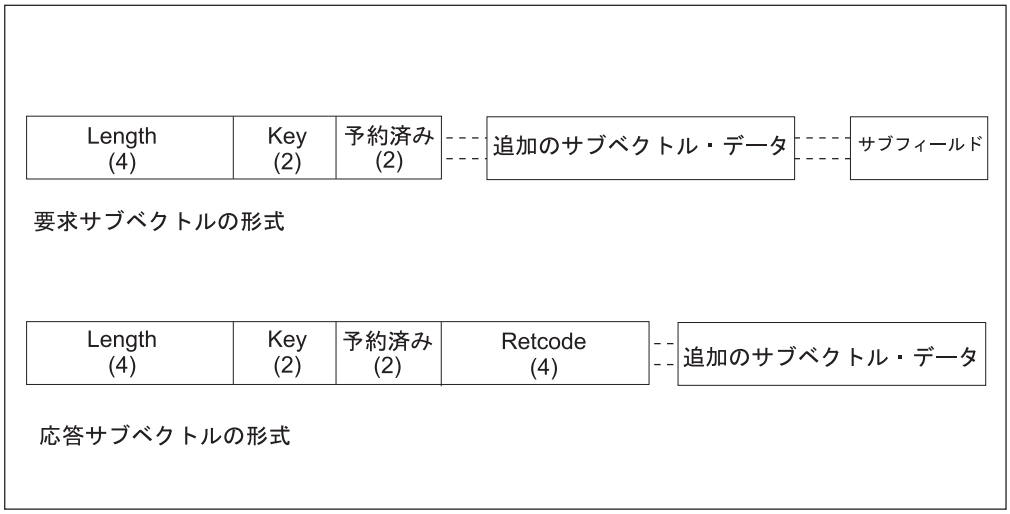


図 19. サブベクトルの形式

Length: サブベクトル全体の長さをバイト単位で表す、符号なしの 32 ビット値。これには、フィールド length および key のほか、サブフィールドも含まれます。受け入れ可能な範囲は 6-4GB です (上限については検査していません)。

Key: サブベクトル・キーを表す、符号なし 16 ビット値。要求サブベクトル・キーには、次のものが含まれます。

- 0x0100 (Web オブジェクトの追加)
- 0x0110 (Web オブジェクトの追加、cache control ヘッダーの無視)
- 0x0200 (区画上でのキャッシュの使用可能)
- 0x0300 (区画上でのキャッシュの使用不可)
- 0x0400 (Web オブジェクトの削除)
- 0x0500 (キャッシュ・ポリシーの変更またはリスト)
- 0x0600 (区画からのすべての Web オブジェクトの除去)
- 0x0700 (Web オブジェクトが区画に入っているかどうかの判別)
- 0x0800 (キャッシュ統計のリセットまたはリスト)
- 0x0900 (URL マスクの追加、削除、リスト)
- 0x0A00 (依存関係の追加、削除、リスト、リセット)

戻される応答サブベクトル・キーは、次のものです。

- 0x0101 (Web オブジェクトの追加)
- 0x0111 (Web オブジェクトの追加、cache control ヘッダーの無視)
- 0x0201 (区画上でのキャッシュの使用可能)
- 0x0301 (区画上でのキャッシュの使用不可)
- 0x0401 (Web オブジェクトの削除)
- 0x0501 (キャッシュ・ポリシーの変更またはリスト)
- 0x0601 (区画からのすべての Web オブジェクトの除去)
- 0x0701 (Web オブジェクトが区画に入っているかどうかの判別)
- 0x0801 (キャッシュ統計のリセットまたはリスト)

- 0x0901 (URL マスクの追加、削除、リスト)
- 0x0A01 (依存関係の追加、削除、リスト、リセット)

Reserved: 現在使用されていない 16 ビットのフィールド

Retcode: 要求サブベクトルの戻りコードを表す符号なし 32 ビット値。これは、応答サブベクトル内にだけ存在します。

Add Object コマンド・サブベクトル: Add Object コマンド・サブベクトルは、Web オブジェクトをキャッシュ区画に追加するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0100

6-7 Reserved

8 ～ (4n-1)
URL サブフィールド

4n ～ (4m-1)
オブジェクト・サブフィールド

Add Object (Force) コマンド・サブベクトル: Add (force) Object コマンド・サブベクトルは、Web オブジェクトをキャッシュ区画に追加するのに使用されます。これは、オブジェクトの Cache Control ヘッダーがどれも無視されるところが Add Object コマンド・サブベクトルと異なります。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0110

6-7 Reserved

8 ～ (4n-1)
URL サブフィールド

4n ～ (4m-1)
オブジェクト・サブフィールド

Delete Object コマンド・サブベクトル: Delete Object コマンド・サブベクトルは、Web オブジェクトをキャッシュ区画から削除するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0400

6-7 Reserved

8 〜 (4n-1)
URL サブフィールド

依存関係コマンド・サブベクトル: 依存関係コマンド・サブベクトルは、依存関係テーブルの変更 / 表示、あるいは依存関係テーブルを使用したオブジェクトの無効化を行うのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0A00

6-7 Reserved

8-9 Command

実行される依存関係コマンド

0x0001
依存関係テーブルの入手 (依存関係については「Dependency Type」を参照)

0x0002
依存関係テーブルへの新規依存関係 /依存関係 URL の追加

0x0003
依存関係テーブルからの依存関係 / 依存関係 URL の除去

0x0004
依存関係テーブル情報のリセット (依存関係については「Dependency Type」を参照)

0x0005
依存関係に基づくオブジェクトの無効化

0x0006
依存関係テーブルの不要情報収集

10-11 Dependency Type

dependency type フィールドは、変更されるデータを識別するのに使用されます。このデータは、識別されると、依存関係コマンドを使用して変更できます。

0x0000
依存関係タイプなし

0x0001
テーブル全体に対してコマンドを使用します。

- 上記コマンドが 0x0001 (入手) の場合 - テーブル全体を入手します。
- 上記コマンドが 0x0004 (リセット) の場合 - テーブル全体をクリアします。

0x0002

依存関係に基づいてコマンドを使用します。

- 上記コマンドが 0x0001 (入手) の場合 - 指定された依存関係についてすべての URL を入手します。
- 上記コマンドが 0x0004 (リセット) の場合 - テーブルから依存関係をクリアします。

0x0003

URL に基づいてコマンドを使用します。

- 上記コマンドが 0x0001 (入手) の場合 - 指定された依存関係 URL についてすべての依存関係を入手します。
- 上記コマンドが 0x0004 (リセット) の場合 - テーブルから依存関係 URL をクリアします。

12 ～ (4n-1)

ゼロ個またはそれ以上のサブフィールド。

依存関係サブフィールド
注: このサブフィールドは、両方のサブフィールドが必要とされる場合、最初になければなりません。これらの依存関係コマンド・タイプをもつ場合に必要です。

コマンド	依存関係タイプ
0x0001	0x0002
0x0002	0x0000
0x0003	0x0000
0x0004	0x0002
0x0005	0x0000

URL サブフィールド
注: このサブフィールドは、両方のサブフィールドが必要とされる場合、2 番目になければなりません。これらの依存関係コマンド・タイプをもつ場合に必要です。

コマンド	依存関係タイプ
0x0001	0x0003
0x0002	0x0000
0x0003	0x0000
0x0004	0x0003

Disable コマンド・サブベクトル: Disable コマンド・サブベクトルは、キャッシュ区画を使用不可にするのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0300

6-7 Reserved

Enable コマンド・サブベクトル: Enable コマンド・サブベクトルは、キャッシュ区画を使用可能にするのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0200

6-7 Reserved

Policy コマンド・サブベクトル: Policy コマンド・サブベクトルにより、キャッシュ区画を変更したり、キャッシュ区画内の情報を表示したりできます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0500

6-7 Reserved

8-9 Command

実行されるコマンド

0x0001
ポリシーの入手

0x0002
ポリシーの更新

10-11 Policy Type

Policy Type (ポリシーのタイプ) は、変更されるデータを識別するのに使用されます。このデータは、識別されると、Policy コマンドを使用して変更できます。

0x0001
透過的キャッシュ

0x0002
HTTP キャッシュ制御ヘッダー

0x0003
動的オブジェクトのキャッシュ

0x0004
イメージ・オブジェクト (″*.gif,″ ″*.jpg″) のキャッシュ

0x0005
静的オブジェクトのキャッシュ

0x0006
動的オブジェクトのデフォルトの存続時間

0x0007
イメージ・オブジェクトのデフォルトの存続時間

0x0008
静的オブジェクトのデフォルトの存続時間

0x0009
不要情報収集間の時間 (秒単位)

0x000A
最大区画サイズ (MB 単位)

0x000B
キャッシュ区画内のオブジェクトの最大数

0x000C
キャッシュ区画内のオブジェクトの最大サイズ

0xFFFF
すべてのポリシーについての操作

注: Command が get (0x0001) である場合、これはサブベクトルの終わりです。

12 ～ (4n-1)
上記の Policy Type に応じて、次のどれか 1 つです。

Policy Type = 0x0001、0x0002、0x0003、0x0004、または 0x0005 の場合は、次のものです。

12-13 設定値

- 0x0001 (使用可能)
- 0x0002 (使用不可)

14-15 Reserved

Policy Type = 0x0006、0x0007、または 0x0008 の場合は、次のものです。

12-15 オブジェクトの分単位の存続時間を表す値

範囲は 0 ～ 10080 で、0 は有効期限のないオブジェクトを表します。

Policy Type = 0x0009 の場合は、次のものです。

12-15 分単位のキャッシュ除去間隔を表す値

範囲は 0 ～ 720 で、0 は、不要情報収集を使用不可にすることを示します。

Policy Type = 0x000A の場合は、次のものです。

12-13 MB 単位の最大区画サイズを表す値。範囲は 0 ～ 4095 で、0 は無制限であることを示します。

注: 値は検証されません。

14-15 Reserved

Policy = 0x000B である場合は、次のものです。

12-15 オブジェクトの最大数を表す値

範囲は 0 ～ 100000 で、0 は無制限であることを示します。

注: 値は検証されません。

Policy = 0x000C である場合は、次のものです。

12-15 キャッシュ区画内のオブジェクトの最大サイズを表す値

範囲は 512 ～ 300000 で、0 を入力すると無制限であると指示されます。

注: 値は検証されません。

Policy = 0xFFFF である場合は、次のものです。

12-13 キャッシュは透過的である (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

14-15 HTTP Cache Control ヘッダー (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

16-17 キャッシュは動的である (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

18-19 キャッシュはイメージである (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

20-21 キャッシュは静的である (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

22-23 MB 単位の最大区画サイズを表す値。

範囲は 0 ～ 4095 で、0 は無制限であることを示します。

注: 値は検証されません。

24-27 オブジェクトの最大数を表す値

範囲は 0 ～ 1000000 で、0 は無制限であることを示します。

注: 値は検証されません。

28-31 1 つのキャッシュ区画内のオブジェクトの最大サイズを表す値

範囲は 512 ～ 3000000 で、0 を指定すると無制限であると指示されます。

注: 値は検証されません。

32-35 動的オブジェクトの分単位の存続時間を表す値

範囲は 0 ～ 10080 で、0 は有効期限のないオブジェクトを表します。

注: 値は検証されません。

36-39 イメージ・オブジェクトの分単位の存続時間を表す値

範囲は 0 ～ 10080 で、0 は無制限であることを示します。

注: 値は検証されません。

40-43 静的オブジェクトの分単位の存続時間を表す値

範囲は 0 ～ 10080 で、0 は無制限であることを示します。

注: 値は検証されません。

44-47 分単位のキャッシュ除去間隔を表す値

範囲は 0 ～ 720 で、0 は不要情報収集を使用可能にする必要があることを示します。

Purge コマンド・サブベクトル: Purge コマンド・サブベクトルは、キャッシュ区画からすべてのオブジェクトをクリアするのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0600

6-7 Reserved

Query コマンド・サブベクトル: Query コマンド・サブベクトルは、与えられた URL がキャッシュ区画内にあるかどうかを検査するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0700

6-7 Reserved

8 ～ (4n-1)
URL サブフィールド

Statistics コマンド・サブベクトル: 静的コマンド・サブベクトルは、キャッシュ区画の統計を入手 / リセットするのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0800

6-7 Reserved

8-9 Command

- 0x0001 - キャッシュ区画についての統計を入手します。
- 0x0004 - キャッシュ区画についての統計をリセットします。

10-11 Reserved

URL マスク・コマンド・サブベクトル: URL マスク・コマンド・サブベクトルは、1 つのキャッシュ区画と関連付けられた URL マスクをリスト / 変更するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0900

6-7 Reserved

8-9 Command

- 0x0001 - 現在定義済みの URL マスクを入手します (戻すマスクのタイプについては、次の URL Type を参照)。
- 0x0002 - 指定された URL マスクを追加します (追加されるマスクのタイプについては、次の URL Type を参照)。
- 0x0003 - 指定された URL マスクを削除します (削除されるマスクのタイプについては、次の URL Type を参照)。

  注: 動的 URL マスクまたはホスト・オンデマンド・クライアント・キャッシュ・アプレット・マスクの削除は、無効な機能です。
- 0x0004 - 次に指定された URL Type のすべての URL マスクをリセットします。

10-11 URL Type (URL のタイプ)

- 0x0001 - 包含
- 0x0002 - 除外
- 0x0003 - 動的
- 0x0004 - ホスト・オンデマンド・クライアント・キャッシュ・アプレット

12-15 Lifetime

範囲は 0 ～ 10080 で、0 は有効期限のないオブジェクトを表します。URL のタイプが包含 (0x0001)、動的 (0x0003)、またはホスト・オンデマンド・クライアント・キャッシュ・アプレット (0x0004) の場合は、追加 (0x0002) コマンドにだけ使用されます。

注: Command が GET (0x0001) または Clear (0x0004) である場合、これはサブベクトルの終わりです。

16 ～ (4n-1)
1 つの URL コマンド・サブベクトル

Add Object 応答サブベクトル: Add Object 応答サブベクトルは、Add Object (Force) コマンド・サブベクトルに応答するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0101

6-7 Reserved

8-11 戻りコード

218ページの『戻りコード』を参照してください。

Add (Force) 応答サブベクトル: Add (Force) 応答サブベクトルは、Add Object (Force) コマンド・サブベクトルに応答するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0111

6-7 Reserved

8-11 戻りコード

218ページの『戻りコード』を参照してください。

Delete Object 応答サブベクトル: Delete Object 応答サブベクトルは、Add Object (Force) コマンド・サブベクトルに応答するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0401

6-7 Reserved

8-11 戻りコード

218ページの『戻りコード』を参照してください。

依存関係コマンド・サブベクトル: 依存関係応答サブベクトルは、依存関係コマンド・サブベクトルに応答するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0A01

6-7 Reserved

8-11 戻りコード

218ページの『戻りコード』を参照してください。

12 ～ (4n-1)

ゼロ個またはそれ以上のサブフィールド。

依存関係サブフィールド
注: このサブフィールドは、依存関係に対応する URL サブコマンドの前になければなりません。これらの依存関係コマンド・タイプをもつ場合に、必要です。詳しくは、201ページの『依存関係コマンド・サブベクトル』を参照してください。

コマンド	依存関係タイプ	
0x0001	0x0001	注: 次の依存関係サブフィールドのすべての URL サブフィールドは、依存関係上の依存関係 URL です。
0x0001	0x0003	

URL サブフィールド
注: このサブフィールドは、両方のサブフィールドが必要とされる場合、2 番目になければなりません。これらの依存関係コマンド・タイプをもつ場合に必要です。

コマンド	依存関係タイプ	
0x0001	0x0001	注: URL サブフィールドの前の、依存関係サブフィールドは、依存関係に対応する URL を示します。
0x0001	0x0002	

使用不可応答サブベクトル: 使用不可応答サブベクトルは、Disable コマンド・サブベクトルに応答するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0301

6-7 Reserved

8-11 戻りコード

218ページの『戻りコード』を参照してください。

使用可能応答サブベクトル: 使用可能応答サブベクトルは、Enable コマンド・サブベクトルに応答するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0201

6-7 Reserved

8-11 戻りコード

218ページの『戻りコード』を参照してください。

ポリシー応答サブベクトル: ポリシー応答サブベクトルは、Policy コマンド・サブベクトルに応答するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0501

6-7 Reserved

8-11 戻りコード

218ページの『戻りコード』を参照してください。

Policy コマンド・サブベクトルが PUT (0x0002) であった場合、これはサブベクトルの終わりです。

12 ～ (4n-1)

Policy コマンド・サブベクトルからの Policy Type に応じて、次のどれか 1 つです。

Policy Type = 0x0001、0x0002、0x0003、0x0004、または 0x0005 の場合は、次のものです。

12-13 設定値

- 0x0001 (使用可能)
- 0x0002 (使用不可)

14-15 Reserved

Policy Type = 0x0006、0x0007、または 0x0008 の場合は、次のものです。

12-15 オブジェクトの分単位の存続時間を表す値

範囲は 0 ～ 10080 で、0 は有効期限のないオブジェクトを表します。

Policy Type = 0x0009 の場合は、次のものです。

12-15 分単位のキャッシュ除去間隔を表す値

範囲は 0 ～ 720 で、0 は、不要情報収集を使用不可にすることを示します。

Policy Type = 0x000A の場合は、次のものです。

12-13 MB 単位の最大区画サイズを表す値。範囲は 0 ～ 4095 で、0 は無制限であることを示します。

注: 値は検証されません。

14-15 Reserved

Policy = 0x000B である場合は、次のものです。

12-15 オブジェクトの最大数を表す値

範囲は 0 ～ 100000 で、0 は無制限であることを示します。

注: 値は検証されません。

Policy = 0x000C である場合は、次のものです。

12-15 キャッシュ区画内のオブジェクトの最大サイズを表す値

範囲は 512 ～ 300000 で、0 を入力すると無制限であると指示されます。

注: 値は検証されません。

Policy = 0xFFFF である場合は、次のものです。

12-13 キャッシュは透過的である (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

14-15 HTTP Cache Control ヘッダー (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

16-17 キャッシュは動的である (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

18-19 キャッシュはイメージである (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

20-21 キャッシュは静的である (設定値)
- 0x0001 (使用可能)
- 0x0002 (使用不可)

22-23 MB 単位の最大区画サイズを表す値

範囲は 0 ～ 4095 で、0 は無制限であることを示します。

注: 値は検証されません。

24-27 オブジェクトの最大数を表す値

範囲は 0 ～ 1000000 で、0 は無制限であることを示します。

注: 値は検証されません。

28-31 1 つのキャッシュ区画内のオブジェクトの最大サイズを表す値

範囲は 512 ～ 3000000 で、0 を指定すると無制限であると指示されます。

注: 値は検証されません。

32-35 動的オブジェクトの分単位の存続時間を表す値

範囲は 0 ～ 10080 で、0 は有効期限のないオブジェクトを表します。

注: 値は検証されません。

36-39 イメージ・オブジェクトの分単位の存続時間を表す値

範囲は 0 ～ 10080 で、0 は無制限であることを示します。

注: 値は検証されません。

40-43 静的オブジェクトの分単位の存続時間を表す値

範囲は 0 ～ 10080 で、0 は無制限であることを示します。

注: 値は検証されません。

44-47 分単位のキャッシュ除去間隔を表す値

範囲は 0 ～ 720 で、0 は、不要情報収集を使用不可にする必要があることを示します。

Purge 応答サブベクトル: Purge 応答サブベクトルは、Purge コマンド・サブベクトルに応答するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0601

6-7 Reserved

8-11 218ページの『戻りコード』を参照してください。

照会応答サブベクトル: 照会応答サブベクトルは、与えられた URL がキャッシュ区画内にあるかどうかを検査するのに使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0701

6-7 Reserved

8-11 戻りコード

218ページの『戻りコード』を参照してください。

注: 戻りコードが bad (0x00000000 ではない) である場合、これはサブベクトルの終わりです。

12-39 オブジェクトが最後に変更された GMT で表される時刻

注: このフィールドは、戻りコードが 0x00000000 でなかった場合、あるいはそれがキャッシュ区画で認識されない場合には、存在しません。

12-15 秒数

16-19 分数

20-23 時間数

24-27 1 月以降の月数 (0-11)

28-31 1900 年以降の年数

32-35 日曜日以降の日数 (0-6)

36-39 月間通算日

統計応答サブベクトル: 統計応答サブベクトルは、Statistics コマンド・サブベクトルに応答します。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の全長

4-5 Key

0x0801

6-7 Reserved

8-11 戻りコード

これは、サブベクトルの戻りコードです。

12-

12-15 キャッシュ区画内の現在のバイト数。この数は、エンティティーのバイト数にだけ影響し、ヘッダーまたは制御ブロックの使用量の保管に使用されるバイト数は含まれません。

16-19 キャッシュ区画内のバイト数についての高位の水準点

20-23 キャッシュ区画内の現在のオブジェクト数

24-27 キャッシュ区画内のオブジェクト数についての高位の水準点

28-31 キャッシュ区画内でオブジェクトが検出された回数の合計

32-35 キャッシュ区画内でオブジェクトが検出されなかった回数の合計

36-39 包含 URL マスクによって明示的にキャッシュ区画に追加されるオブジェクトの数

40-43 キャッシュがオフになったためにキャッシュ区画に追加されなかったオブジェクトの数

44-47 オブジェクトが大きすぎたためにキャッシュ区画に追加されなかったオブジェクトの数

48-51 HTTP 制御ヘッダーに DONT CACHE が指定されているためにキャッシュ区画に追加されなかったオブジェクトの数

52-55 URL マスクによって明示的に除外されたためにキャッシュ区画に追加されなかったオブジェクトの数

56-59 オブジェクトが失効していたためにキャッシュ区画に追加されなかったオブジェクトの数

60-63 イメージ・オブジェクトが明示的にキャッシュされなかったためにキャッシュ区画に追加されなかったオブジェクトの数

64-67 静的オブジェクトが明示的にキャッシュされなかったためにキャッシュ区画に追加されなかったオブジェクトの数

68-71 動的オブジェクトが明示的にキャッシュされなかったためにキャッシュ区画に追加されなかったオブジェクトの数

72-75 キャッシュがいっぱいになった、あるいはキャッシュ区画が Web サーバー・キャッシュで可能とされる総量を超えたために除去されるオブジェクトの数

76-79 オブジェクトの存続時間が満了したために除去されたオブジェクトの数

80-83 URL を与えるか、あるいは区画全体を除去することによって、明示的に除去されたオブジェクトの数

84-87 依存関係が無効化されたために除去されたオブジェクトの数

88-91 外部キャッシュ制御インターフェースが原因で区画から削除された項目数 (delete)

92-95 外部キャッシュ制御インターフェースを経由して区画に追加された項目数

96-99 外部キャッシュ制御インターフェースを経由して区画に追加されずに、そのインターフェースを経由して追加を試みられた項目数

100-103
外部キャッシュ制御インターフェースを経由して区画で置き換えられた項目数

104-107
キャッシュ・ヒットがあったときに戻された 200 (OK) の数

108-111
キャッシュ・ヒットがあったときに戻された 203 (Non_Authoritative) 応答数

112-115
キャッシュ・ヒットがあったときに戻された 206 (部分的内容) 応答数

116-119
キャッシュ・ヒットがあったときに戻された 300 (複数選択項目) 応答数

120-123
キャッシュ・ヒットがあったときに戻された 301 (永久に移動された) 応答数

124- 127
キャッシュ・ヒットがあったときに戻された 304 (変更されていない) 応答数

128-131
キャッシュ・ヒットがあったときに戻された 410 (Gone) 応答数

132-135
キャッシュ・ヒットがなかったときに戻された 100 range (通知) 応答数

136-139
キャッシュ・ヒットがなかったときに戻された 200 (OK) 応答数

140-143
キャッシュ・ヒットがなかったときに戻された 200 range (正常) 応答数 (200 応答を含まない)

144-147
キャッシュ・ヒットがなかったときに戻された 304 (変更されていない) 応答数

148-151
キャッシュ・ヒットがなかったときに戻された 300 range (Redirection) 応答数 (304 メッセージを含まない)

152-155
キャッシュ・ヒットがなかったときに戻された 400 range (クライアント・エラー) 応答数

156-159
キャッシュ・ヒットがなかったときに戻された 500 range (サーバー・エラー) 応答数

160-163
キャッシュ・ヒットがなかったときに戻された他の (上記のどれにも当てはまらない) 応答数

164-167
キャッシュ・ヒットが原因でサービスされたバイト数 (注: HTTP ヘッダーを含まない)

168-171
キャッシュ・ヒットがないためにサービスされたバイト数 (注: HTTP ヘッダーを含まない)

URL マスク応答サブベクトル: URL マスク応答サブベクトルは、URL Mask コマンド・サブベクトルに応答するために使用されます。

0-3 Length

フィールド length および key のほか、サブベクトルも含むベクトルのバイト単位の長さ

4-5 Key

0x0901

6-7 Reserved

8-11 戻りコード

これは、サブベクトルの戻りコードです。218ページの『戻りコード』を参照してください。

12 ～ (4n-1)
URL Mask コマンド・サブベクトルが GET (0x0001) であった場合は、ゼロ個またはそれ以上の URL サブベクトル

サブフィールドの形式

ここでは、サブフィールドのフィールド記述について説明します。

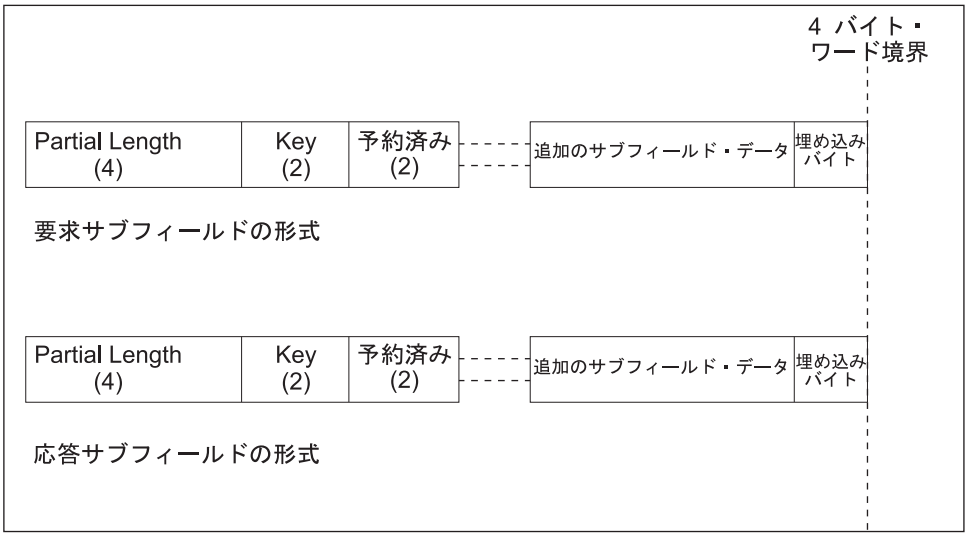


図 20. サブフィールドの形式

Partial Length: サブフィールド全体の長さをバイト単位で表す、符号なしの 32 ビット値。これには、フィールド length および key が含まれますが、埋め込みのバイト数は含まれません。サブフィールドは、4 バイト (ワード) 境界に位置合わせを行うために埋め込まれます。受け入れ可能な範囲は、6 ～ 4GB です。

Key: サブフィールド・キーを表す、符号なし 16 ビット値。コマンド・サブフィールド・キーには、次のものがあります。

- 0x0010 (プロトコル ″http:″ およびインターネット・リソース・アドレスを除いた URL。たとえば、URL ″http://192.9.200.50/file1.html″ は ″/file1.html″ として送信されます。)
- 0x0020 (HTTP 応答メッセージ形式の Web オブジェクト)
- 0x0030 (ECCP ユーザーの名前。このサブフィールドは、認証ベクトルの場合に必要です。)
- 0x0040 (ECCP ユーザーのパスワード。このサブフィールドは、認証ベクトルの場合に必要です。)
- 0x0050 (依存関係サブフィールド)

応答サブフィールド・キーは、次のものです。

- 0x0011 (プロトコル ″http:″ およびインターネット・リソース・アドレスを除いた URL)
- 0x0051 (依存関係サブフィールド)

Reserved: 現在使用されていない 16 ビットのフィールド

依存関係サブフィールド: URL マスク応答サブベクトルの依存関係サブフィールド。

0-3 Partial Length

図20 に示すサブフィールドのバイト単位の長さ

4-5 Key

0x0050 - 要求

0x0051 - 応答

6-7 Reserved

8 ～ (4n-1)
依存関係と埋め込みバイト数

依存関係は、長さが 1 ～ 50 でなければなりません。

名前サブフィールド: URL マスク応答サブベクトルの名前サブフィールド

0-3 Length

216ページの図20 に示すサブフィールドのバイト単位の長さ

4-5 Key

0x0030 - 要求

6-7 Reserved

8 ～ (4n-1)
名前と埋め込みバイト数

名前は、長さが 1 ～ 8 でなければなりません。

オブジェクト・サブフィールド: URL マスク応答サブベクトルのオブジェクト・サブフィールド

0-3 Length

216ページの図20 に示すサブフィールドのバイト単位の長さ

4-5 Key

0x0020 - 要求

6-7 Reserved

8 ～ (4n-1)
オブジェクトと埋め込みバイト数

オブジェクトは、HTTP 応答と同じ形式に設定する必要があります。これは、文字配列です。

パスワード要求サブフィールド: URL マスク応答サブベクトルのパスワード要求サブフィールド。

0-3 Length

216ページの図20 に示すサブフィールドのバイト単位の長さ

4-5 Key

0x0040

6-7 Reserved

8-15 暗号化で使用されるシード (8 バイトでなければなりません)

16 ～ (4n-1)
パスワードと埋め込みバイト数

パスワードは、長さが 1 ～ 8 で、暗号化されている必要があります。

URL 要求サブフィールド: URL マスク要求の URL 要求サブフィールド

0-3 Length

216ページの図20 に示すサブフィールドのバイト単位の長さ

4-5 Key

0x0010 - 要求

0x0011 - 応答

6-7 Reserved

8 ～ (4n-1)

URL または URL マスクおよび埋め込みバイト数

この URL または URL マスクは、文字配列です。この配列の長さは、1 ～ 255 でなければなりません。

戻りコード

応答ベクトル内の戻りコードのほかに、各応答サブベクトルごとに戻りコードを検査することが重要です。重大エラーが検出された場合には、応答ベクトルの戻りコードは、ゼロ以外の値に設定されます。重大エラーが検出された場合、コマンド・ベクトルからのすべてのコマンド・サブベクトルが対応する応答サブベクトルをもっていることもあれば、もっていないこともあります。

戻りコードと記述:

0000 0000: Operation was successful (操作は正常に行われた)
0001 0000: Object not found (オブジェクトが見つからない)
0002 0000: Cache partition is already enabled (キャッシュ区画はすでに使用可能になっている)
0003 0000: Cache partition is already disabled (キャッシュ区画はすでに使用不可になっている)
0004 0000: Cache partition is not enabled (キャッシュ区画は使用可能になっていない)
0005 0000: Cache partition is not defined (キャッシュ区画は定義されていない)
0006 0000: Cache partition is terminating (キャッシュ区画は終了中である)
0007 0000: URL subfield is required but not present (URL サブフィールドが必要であるが、存在しない)
0008 0000: Purge interval provided is not valid (与えられた除去間隔は無効である)
0009 0000: Unsupported Set value (サポートされない設定値)
000A 0000: Unsupported Command value (サポートされないコマンド値)
000B 0000: Unsupported Policy type value (サポートされないポリシー・タイプ値)
000C 0000: Unsupported URL type value (サポートされない URL タイプ値)
000D 0000: Unsupported vector key (サポートされないベクトル・キー)
000E 0000: Unsupported subvector key (サポートされないサブベクトル・キー)
000F 0000: Unable to parse object's headers (オブジェクトのヘッダーを解析できない)
0010 0000: Unable to obtain storage (記憶域を取得できない)
0011 0000: Object too large to add to partition (オブジェクトが大きすぎて区画に追加できない)
0012 0000: Vector format is not valid (ベクトルの形式が正しくない)
0013 0000: Object is not cachable (オブジェクトがキャッシュできない)
0014 0000: HTTP parse error detected (HTTP 解析エラーが検出された)

0015 0000: Object subfield is required but not present (オブジェクト・サブフィールドが必要であるが、存在しない)
0016 0000: Dependency subfield is not provided or invalid (依存関係サブフィールドが与えられていないか、正しくない)
0017 0000: Authentication Vector required (認証ベクトルが必要である)
0018 0000: Authentication Vector not required - therefore ignored (認証ベクトルは不要であるため、無視された)
0019 0000: Dependency was not in Dependency table (依存関係テーブルに依存関係が入っていない)
001A 0000: Dependency URL was not in Dependency table (依存関係テーブルに依存関係 URL が入っていない)
001B 0000: Unsupported Depend type (サポートされない依存タイプ)
001C 0000: Bad userid/password/permission for ECC (ECC のユーザー ID/ パスワード / 許可が正しくない)
001D 0000: Bad URL mask type for the image load on the box (ボックス上のイメージ・ロードの URL マスク・タイプが正しくない)
FF01 yyyy: Command failed. Last 2 bytes contain additional information. (コマンドが失敗した。最後の 2 バイトに追加情報が含まれている)

0101: Object was not found. (オブジェクトが見つからなかった)
0102: Object cannot be cached. (オブジェクトをキャッシュできない)
0103: Object already exists in partition. (オブジェクトはすでに区画内に存在する)
0104: Partition initialization failed, maximum number of partitions already active. (区画の初期設定が失敗した。最大数の区画はまだ活動状態である)
0105: Partition is active. (区画は活動状態である)
0106: Partition is not active. (区画が活動状態でない)
0107: The partition is in a pending state and cannot execute the command. Wait a few seconds and try the command again. (区画が保留状態で、コマンドを実行できない。数秒間待ってから、コマンドを再試行する)
0108: Partition is not defined. (区画が定義されていない)
0109: URL type is not supported. (URL タイプがサポートされていない)
010A: URL pointer is not valid. (URL ポインターが正しくない)
010B: Partition number is not valid. (区画番号が正しくない)
010C: Partition command is not supported. (区画コマンドがサポートされていない)
010D: Partition pointer is not valid. (区画ポインターが正しくない)
010E: Partition handle does not reference an active partition. (区画ハンドルが活動状態の区画を参照しない)
010F: Partition handle does not reference a valid partition. (区画ハンドルが有効な区画を参照しない)
0110: Policy pointer is required but not present. (ポリシー・ポインターが必要であるが、存在しない)
0111: Statistics pointer is required but not present. (静的ポインターが必要であるが、存在しない)
0112: Purge interval is too large. (除去間隔が大きすぎる)
0113: Dependency already has URL on it. (依存関係にはすでに URL が付いている)
0FFF: External cache control is not available. (外部キャッシュ制御が使用できない)

FFF9: Unable to acquire storage. (記憶域を獲得できない)
FFFA: Unable to acquire a partition handle. (区画ハンドルを獲得できない)
FFFB: Policy SRAM pointer is required but not present.
(ポリシー SRAM ポインターが必要であるが、存在しない)
FFFC: Partition SRAM pointer is required but not present.
(区画 SRAM ポインターが必要であるが、存在しない)
FFFD: Unable to allocate/initialize cache expiration interval.
(キャッシュ有効期限間隔の割り振り / 初期設定ができない)
FFFE: Unable to allocate/initialize cache partition.
(キャッシュ区画の割り振り / 初期設定ができない)
FFFF: Unable to allocate/initialize cache core.
(キャッシュ・コアの割り振り / 初期設定ができない)

第12章 Web サーバー・キャッシュの構成と監視

この章では、Web サーバー・キャッシュ・フィーチャーの構成方法、および Web サーバー・キャッシュ監視コマンドの使用法について説明します。この章には、次の内容が記載されています。

Web サーバー・キャッシュの構成

Web サーバー・キャッシュは、ネットワーク・ディスパッチャーと一緒に使用することが必要です。Web サーバー・キャッシュを初めて使用する前に、次を行う必要があります。

1. talk 6 で Config> プロンプトから **feature ndr** コマンドを使用して、ネットワーク・ディスパッチャーにアクセスする。
2. 実行プログラムを使用可能にする。
3. クラスターを追加する。
4. ポートを追加する。
5. 1 つまたは複数のサーバーを追加する。

これで、構成および監視コマンドを使用して Web サーバー・キャッシュ環境を変更できるようになります。

注: Talk 6 で行ったネットワーク・ディスパッチャーの変更は現行の実行環境を変更しますが、Web サーバー・キャッシュの変更は、Talk 6 で **activate** コマンドを使用するか、Talk 5 のフィーチャー Webc で明示的に活動化しない限り、現行の実行環境には影響を与えません。ただし、例外として、HTTP プロキシーのクラスター / ポートを Talk 6 のフィーチャー NDR を使用して除去した場合は、現行の実行環境の Web サーバー・キャッシュ用の HTTP プロキシーも除去されます。

例:

```
Config>f ndr
NDR Config>enable executor
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.10
FIN count [4000]?
FIN time out [30]?
FIN stale timer [1500]?
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.10
Fintimeout has been set to 30 for cluster 113.3.1.10
Staletimer has been set to 1500 for cluster 113.3.1.10
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]?
Port type (tcp=1, upd=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0]? 3
```

```
Do you want a new cache partition? [Yes]:
Enter cache partition [0]?
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
Maximum number of objects (1-100000 or 0 for no limit) [0]?
Maximum object size (512-300000 bytes or 0 for no limit) [0]?
Do you want the cache enabled upon reboot? [Yes]:

Default cache purge interval (1-720 minutes or 0 to disable) [10]
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
      Default expiration time for images
              (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
      Default expiration time for non-image static objects
              (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?
Cache dynamic objects? [No]:
Do you want to add a URL mask? [No]:

Cache partition number 1 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
NDR Config>add server
Cluster Address  [0.0.0.0] ? 113.3.1.10
Port number  [80] ? 80
Server Address  [0.0.0.0] ? 113.1.2.0
Server weight   [20] ?
Server state (down=0, up=1)  [1] ?
Server 113.1.2.0 has been added to the requested port(s) of cluster 113.3.1.10
Weight of server 113.1.2.0 has been set to 20 in port 80 of cluster 113.31.10
Server 113.1.2.0 has been set up.
NDR Config> exit
```

次に Web サーバー・キャッシュと説明に特有のパラメーターの例をリストします。

cluster-address

クラスター IP アドレスを指定します。

注: クラスター IP アドレスは、このクラスターにクラスター・アドレス公示を使用していない限り、直前のホップ・ルーター (IP ルーター) と同じ論理サブネット上に存在するものと想定しています。

有効値 : 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

FIN-count 実行プログラムが *FIN-timeout* または *Stale-timer* の経過後にネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みる前に、FIN 状態にあることが必要な接続の数を指定します。

有効値 : 0 ～ 65535

デフォルト値 : 4000

FIN-timeout 接続が FIN 状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから未使用接続情報の除去を試みます。

有効値 : 0 ～ 65535

デフォルト値 :30

Stale-timer 接続が非活動状態にある秒数を指定します。この時間の後、実行プログラムはネットワーク・ディスパッチャー・データベースから接続の情報の除去を試みます。

有効値 : 0 ～ 65535

デフォルト値 :1500

port# このクラスターのプロトコルのポート番号を指定します。

有効値 : 1 ～ 65535

デフォルト値 :80

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

- 1 = TCP
- 2 = UDP
- 3 = 両方

有効値 : 1、2、3

デフォルト値 : 3

max-weight このポート上のサーバーの最大重みを指定します。これは、実行プログラムが各サーバーに与える要求数の相違に影響します。

有効値 : 0 ～ 100

デフォルト値 :20

port-mode ポートが、1 つのクライアントからのすべての要求を 1 つのサーバーに送る (stickyと呼ばれる) か、パッシブ ftp を使用する (pftp) か、Web サーバー・キャッシュを使用する (cache) か、外部スケーラブル・キャッシュ・アレイを送る (extcache) か、あるいはこのクラスターでは特定のプロトコルを使用しない (none) かを指定します。

有効値 : 0 ～ 4。値は、それぞれ次のものを示します。

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

デフォルト値 : 0

Do you want a new cache partition?
既存のキャッシュ区画を使用するか、新しい区画を使用するかを指定します。

有効値 : Yes または No

デフォルト値 : Yes

Enter cache partition
使用する既存のキャッシュ区画の番号を指定します。

有効値 : 任意の既存のキャッシュ区画番号

デフォルト値 : 0

Default server TCP connection timeout
サーバー接続が満了する前の時間を指定します。

有効値 : 5 ～ 240 秒

デフォルト値 : 120 秒

Do you want to modify cache partition?
既存のキャッシュ区画の構成を変更することができます。

有効値 : Yes または No

デフォルト値: No

Default client TCP connection timeout
クライアント接続が満了する前の時間を指定します。

有効値 : 5 ～ 240 秒

デフォルト値 : 120 秒

Maximum partition size
このキャッシュ区画に割り当てる最大メモリー量を指定します。この値が、現在利用可能なメモリーの量を超えている場合、この値は無視され、最大区画サイズは適用されません。

有効値 : 1 ～ 4095 MB または 0 (最大値なし)

デフォルト値 : 0 (最大値なし)

Maximum number of objects
キャッシュ区画に保管できるオブジェクトの最大数を指定します。0 を入力すると、キャッシュ区画は、その区画用に利用可能なメモリーの量によってだけ制限されることになります。

有効値 : 1 ～ 100000 または 0 (制限なし)

デフォルト値 : 0 (制限なし)

Maximum object size
キャッシュに取り込むオブジェクトの最大サイズを指定します。この最大サイズを超えるオブジェクトは、キャッシュに取り込まれることはありません。キャッシュが作成された後で最大オブジェクト・サイズが変更された場合、すでにキャッシュ内にあるオブジェクトが一時的に、定義された最大値を超える可能性があります。

有効値 : 512 ～ 300000 バイト、または 0 (最大サイズなし)

デフォルト値 : 0 (最大サイズなし)

Do you want the cache enabled upon reboot?
キャッシュ区画を自動的に使用可能にするか、明示的なユーザー要求に基づいて使用可能にするかを指定します。即時使用可能化として設定されているキャッシュ区画は、2216 をリブートすると自動的に使用可能になります。即時使用可能化として設定されていないキャッシュ区画は、引き続き使用可能ですが、ユーザーが `talk 5` の Web サーバー・キャッシュ・コンソールから区画を使用可能にするまでは使用不可のままです。

有効値 : Yes または No

デフォルト値 : Yes

Default cache purge interval?
デフォルトのキャッシュ除去間隔を指定します。

有効値 : 1 ～ 720 分、または 0 (使用不可)

デフォルト値 : 10 分

Enable transparent caching?
オブジェクトがキャッシュ内に見つからない場合のサーバーの応答 (キャッシュ・ミス) を自動的にキャッシュするかどうかを指定します。もう1 つの方法は、ECCP を使用してキャッシュを操作するものです。

有効値 : Yes または No

デフォルト値 : Yes

Check cache control headers?
サーバーは、Web サーバー・キャッシュの応答がキャッシュするのに適格かどうかを指定することができます。

有効値 : Enabled または Disabled

デフォルト値 : Disabled

Cache images?
イメージ・ファイル (*.gif または *.jpg) をキャッシュするかどうかを指定します。

有効値 : Yes または No

デフォルト値 : Yes

イメージのデフォルト満了時間

有効値 : 1 ～ 10080 分、または 0 (なし)

デフォルト値 : 60 分

Cache non-image static objects?
非イメージの静的データ (*/cgi* を含まないファイル、および .jpg または .gif で終わっていないファイル) をキャッシュするかどうかを指定します。

有効値 : Yes または No

デフォルト値 : Yes

非イメージ・オブジェクトのデフォルト満了時間

有効値 : 1 ～ 10080 分、または 0 (なし)

デフォルト値 : 60 分

URL mask to identify dynamic objects
動的オブジェクトを識別するのに使用する URL マスクを指定します。

有効値 : 任意の URL マスク

デフォルト値 : */cgi**

Cache dynamic objects?

動的オブジェクトをキャッシュするかどうかを指定します。動的オブジェクトというのは、そのオブジェクトが要求されたときにサーバーによって作成され、データが変更されたかどうかに関係なく、新しい要求のたびに再作成されるオブジェクトをいいます。

有効値 : Yes または No

デフォルト値: No

Do you want to add a URL mask?

新しい URL マスクをキャッシュに追加するかどうかを指定します。URL マスクは、その汎用リソース・ロケーター (URL) によって、個々のオブジェクトまたはオブジェクト・グループを包含または除外することができます。

有効値 : i または e

デフォルト値 : i

URL マークを指定するときは、ワイルドカード文字を使用できます。ワイルドカードを使えるのは、Web サーバー・キャッシュ用にネットワーク・ディスパッチャーを構成するとき、あるいは `f webc` プロンプトから **add** または **modify url** コマンドを使用するときです。ワイルドカードとして使用できる文字は、* (アスタリスク) または # (番号記号) です。ワイルドカードは URLの一部としてどの位置にでも使用できます。

* は、URL の一部としての、文字数ゼロを含む、任意の文字数を表します。

例: *abc.html は、次のような URL マスクをフィルターに掛けます。

```
abc.html
finabc.html
defchtjqsprabc.html
```

は、1 文字を表します。

例: ab#.html は、次のような URL マスクをフィルターに掛けます。

```
abc.html
abf.html
abo.html
```

次の例は、ポート・モード 3 (cache=3) が選択され、新規のキャッシュ区画が追加されない場合に適用されます。

```
NDR Config>add port
Cluster Address  [0.0.0.0] ? 113.3.1.11
Port number  [80] ?
Max. weight (0-100)  [20] ?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4)  [0] ? 3
Do you want a new cache partition?  [Yes] :  n
Enter cache partition  [0] ? 0
Maximum TCP segment size  (Range 512-32768 bytes)  [4096] ?
Default server TCP connection timeout (Range 5-240 seconds) [120] ?
Default client TCP connection timeout (Range 5-240 seconds)  [120] ?
Do you want to modify cache partition [0]?  No :
Requested port has been added to cluster 113.3.1.11
Maxweight has been set to 20 for port 80 in cluster 113.3.1.11
```

注: 次の例は、ポート・モード 3 (cache=3) が選択され、新規のキャッシュ区画が追加される場合に適用されます。

```
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]?
Port type (tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0]? 3
Do you want a new cache partition? [Yes]: y
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
Maximum number of objects (1-100000 or 0 for no limit) [0]?
Maximum object size (512-300000 bytes or 0 for no limit) [0]?
Do you want the cache enabled upon reboot? [Yes]:

Default cache purge interval (1-720 minutes or 0 to disable) [10]?
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
      Default expiration time for images
              (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
      Default expiration time for non-image static objects
              (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?
Cache dynamic objects? [No]:
Do you want to add a URL mask? [No]:

Cache partition number 0 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
Port Type has been set to Both for port 85 in cluster 113.3.1.10
NDR Config>
```

ネットワーク・ディスパッチャーを使用して、Web サーバー・キャッシュ・フィーチャー用の初期クラスターとポートを構成することが必要です。クラスターとポートを追加し、ポート・モードをキャッシュ・ポートとして構成した後は、WEBC Config> プロンプトで Web サーバー・キャッシュ構成パラメーターを変更したり、表示したりすることができます。

ネットワーク・ディスパッチャーについては、132 ページを参照してください。

Web サーバー・キャッシュ環境へのアクセス

Web サーバー・キャッシュ構成環境にアクセスするには、Config> プロンプトで、次のコマンドを入力します。

```
Config> feature webc
WEBC Config>
```

Web サーバー・キャッシュ・コマンド

ここでは、Web サーバー・キャッシュ構成コマンドについて説明します。表19 は、Web サーバー・キャッシュ構成コマンドを示しています。これらのコマンドは、Web サーバー・キャッシュ・フィーチャー・パラメーターを指定します。変更を活動化するには、ルーターをリスタートします。

表 19. Web サーバー・キャッシュ構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。

表 19. Web サーバー・キャッシュ構成コマンドの要約 (続き)

コマンド	機能
Activate	最新の構成を使用して、キャッシュ区画を活動化または再活動化します。
Add	URL マスクを追加します。
Delete	URL マスクまたは区画を削除します。
List	キャッシュ情報を表示します。
Modify	キャッシュ情報を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxv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、最新の構成を使用して、すべてのキャッシュ区画を初期設定するのに使用します。

構文:
activate

例:

```
WEBC Config>act ?
ACTIVATE all initializes cache partitions, using
the latest configuration.
```

Add

add コマンドは、URL マスクを追加するのに使用します。

構文:
add urlmask

例:

```
WEBC Config>add url
Partition number [0]?
New URL mask []? *newmask*
Include or Exclude from cache (i or e) [i]? i
Set default expiration time?  [No]:y
Default expiration time
        (1-10080 minutes or 0for no expiration) [0]?  20
The URL mask has been added to cache partition number 0.
```

注: プロキシーおよび区画を追加するには、ネットワーク・ディスパッチャーを使用して **add port** または **set port** コマンドを実行することが必要です。

partition number
追加される区画の区画番号。

有効値 : 任意の有効な区画番号

デフォルト値 : 0

new URL mask
追加される URL マスクの名前。

有効値 : 任意の有効な URL マスク

デフォルト値: なし

include or exclude from cache
URL をキャッシュに含めるか、キャッシュから除外するかを指定します。

有効値 : i または e

デフォルト値 : i

default expiration time
デフォルトの有効期限を分単位で指定します。ゼロは、有効期限時間がないことを示します。

有効値 : 0 〜 10080 分

デフォルト値 : 0 (有効期限なし)

Delete

delete コマンドは、URL マスクまたは区画を構成データベースから削除するのに使用します。

構文:

delete partition
urlmask

partition キャッシュから削除する区画の数

urlmask キャッシュから削除する URL マスクの名前

例:

```
WEBC Config>delete url
Partition number [0]? 0
URL masks defined : 5
     1: EXCLUDE '*index*'
     2: EXCLUDE '*comp*'
     3: INCLUDE '*tmp*'
        Default expiration time: 1 minutes
     4: INCLUDE '*stat*'
        Default expiration time: 5 minutes
     5: INCLUDE '*html*'
        Default expiration time: 1000 minutes (16 hrs 40 mins)
URL mask number [1]? 5
The URL mask for cache partition number 0 has been deleted.
```

注: 区画を削除する前にこの区画を使用してすべてのプロキシーを削除する必要があります。プロキシーを削除するには、ネットワーク・ディスパッチャー・フィーチャーを使用して関連のポートまたはクラスター (あるいは、その両方) を削除するか、あるいはポートのポート・モードをキャッシュ以外のものに変更することが必要です。

partition number
削除される区画の区画番号。

有効値 : 任意の有効な区画

デフォルト値 : 0

URL mask number
削除される URL マスクの番号。

有効値 : 任意の有効な URL マスク番号。

デフォルト値 : 1

List

list コマンドは、Web サーバー・キャッシュ情報を表示するのに使用します。

構文:

list all
external
partition
proxy
urlmask

all キャッシュに定義されたすべてのポート、区画、プロキシー、およびマスクを表示します。

external 外部キャッシュ制御マネージャーのための情報を表示します。

partition キャッシュ内の区画番号を表示します。

proxy キャッシュに定義されたプロキシーを表示します。

urlmask キャッシュに定義された URL マスクを表示します。

例: list all

```
WEBC Config>list all
Cache Partition 0
    Cluster address 113.3.1.10, Port 80

1 cache partition(s) defined.
```

例: list external

```
WEBC Config>list ext
External Cache manager : Enabled
Port number            : 82
TCP timeout            : 120 seconds
```

例: list partition

```
WEBC Config>list part
Cache Partition 0
Maximum partition size         : 1 MB
Maximum number of objects      : Unlimited
Maximum object size:           : Unlimited
Activate on reboot             : Enabled
Cache purge interval           : 10 minutes
Dynamic URL mask               : '*/cgi*' "
Transparent caching               : Enabled
Check cache control headers       : Disabled
Cache images                      : Disabled
Cache non-image static objects    : Enabled
      Default expiration time     : 60 minutes (1 hrs 0 mins)
Cache dynamic objects             : Disabled
Associated proxies (cluster port)  : (113.3.1.10 80)

1 cache partition(s) defined.
```

例: list url

```
WEBC Config>list url
Partition number [0]?
URL masks defined : 5
    1: EXCLUDE '*index*'
    2: EXCLUDE '*comp*'
    3: INCLUDE '*tmp*'
       Default expiration time: 1 minutes
    4: INCLUDE '*stat*'
       Default expiration time: 2 minutes
    5: INCLUDE '*html*'
       Default expiration time: 1000 minutes (16 hrs 40 mins)
```

Modify

modify コマンドは、Web サーバー・キャッシュ情報を変更するのに使用します。

構文:

modify external
partition
proxy
urlmask

external 外部キャッシュ制御マネージャーを変更できるようにします。

partition 区画を変更できるようにします。

proxy プロキシーを変更できるようにします。

urlmask URL マスクを変更できるようにします。

例: modify external

```
WEBC Config>mod ext
External cache manager port number(0 to disable) [82]?
TCP connection timeout (Range 5-240) seconds) [120]?  20
Do you want to modify the encryption key:? [No]?  Y
Encryption key should be 16 characters long.
Encryption key (16 characters) in Hex (0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex (0-9, a-f, A-F):
The external cache manager has been modified.
```

external cache manager port number
変更される外部キャッシュ制御マネージャーのポート番号を指定します。

有効値 : 0 ～ 255

デフォルト値 :82

TCP connection timeout
変更される外部キャッシュ制御マネージャーの TCP 接続を指定します。

有効値 : 5 ～ 240 秒

デフォルト値 : 120

do you want to modify the encryption key
暗号化キーを変更するかどうかを指定します。

有効値 : yes または no

デフォルト値: no

encryption key
変更したい外部キャッシュ制御マネージャーの暗号化キー。暗号化キーは、長さが 16文字で、16 進数で表す必要があります。

有効値 : 16 進数 (0 ～ 9、a ～ f、A ～ F)

デフォルト値: なし

例: modify partition

```
WEBC Config>modify partition
Partition number [0] ?
Maximum partition size (1-255 megabytes or 0 for no limit) [0]? 200
Maximum number of objects (1-100000 or 0 for no limit)[0]?  5000
Maximum object size (512-300000 bytes or 0 for no limit)[0]? 250000
Do you want the cache enabled upon reboot? [Yes]:
```

```
Default cache purge interval (1-720 minutes or 0 to disable) [10]? 20
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
      Default expiration time for images
              (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
      Default expiration time for non-image static objects
              (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?  *dyn*
Cache dynamic objects? [No]: y
Cache partition number 0 has been modified.
```

partition number
変更される区画の番号

有効値 : 任意の有効な区画番号

デフォルト値 : 0

maximum partition size
変更される区画の最大区画サイズ。ゼロは、無制限を示します。

有効値 : 1 〜 255 メガバイト。無制限の場合は 0。

デフォルト値 : 0

maximum number of objects
区画内で変更されるオブジェクトの最大数。ゼロは、無制限を示します。

有効値 : 0 〜 100000。無制限の場合は 0。

デフォルト値 : 0

maximum object size
区画内で変更されるオブジェクトの最大サイズ。ゼロは、無制限を示します。

有効値 : 512 〜 300000。無制限の場合は 0。

デフォルト値 : 0

do you want the cache enabled upon reboot
リブートの後でキャッシュを使用可能にするかどうかを指定します。

有効値 : yes または no

デフォルト値 : yes

default cache purge interval
デフォルトのキャッシュ除去間隔を指定します。ゼロの場合、デフォルトのキャッシュ除去間隔は使用不可になります。

有効値 : 1 〜 170 分。使用不可にする場合は 0。

デフォルト値 : 10

enable transparent caching
透過的キャッシュを使用可能にするかどうかを指定します。もう 1 つの方法は、ECCPを使用してキャッシュを操作することです。

有効値 : yes または no

デフォルト値 : yes

check cache control headers
Cache Control ヘッダーを検査するかどうかを指定します。

有効値 : yes または no

デフォルト値 : yes

cache images

イメージをキャッシュするかどうかを指定します。

有効値 : yes または no

デフォルト値 : yes

イメージのデフォルト満了時間

イメージのデフォルトの有効期限時間を指定します。無制限の場合はゼロです。

有効値 : 1 ～ 10080。無制限の場合は 0。

デフォルト値 : 60

cache non-image static objects

イメージ以外の静的オブジェクトをキャッシュに入れるかどうかを指定します。

デフォルト値 : yes

有効値 : yes または no

非イメージ・オブジェクトのデフォルト満了時間

イメージ以外の静的オブジェクトのデフォルトの有効期限時間を指定します。無制限の場合はゼロです。

有効値 : 1 ～ 10080。無制限の場合は 0。

デフォルト値 : 60

url mask to identify dynamic objects

動的オブジェクトを識別するのに使用する URL マスクを指定します。

有効値 : 任意の有効な URL マスク

デフォルト値 : */cgi*

cache dynamic objects

動的オブジェクトをキャッシュに入れるかどうかを指定します。

有効値 : yes または no

デフォルト値: no

例: modify url

```
WEBC Config>modify url
Partition number [0]?
URL masks defined : 5
    1: EXCLUDE '*index*'
    2: EXCLUDE '*comp*'
    3: INCLUDE '*tmp*'
       Default expiration time: 1 minutes
    4: INCLUDE '*stat*'
       Default expiration time: 2 minutes
    5: INCLUDE '*html*'
       Default expiration time: 1000 minutes (16 hrs 40 mins)
URL mask number  [1] ? 4
New URL mask *stat*?
Include or Exclude from cache (i or e) [i]?
```

```
Set default expiration time?  Yes :
Default expiration time
        (1-10080 minutes or 0 for no expiration) [2]?  5
URL mask number 4 has been modified.
```

partition number

変更される URL の区画番号を指定します。

有効値 : 任意の有効な区画番号

デフォルト値 : 0

url mask number

変更される URL マスクの URL マスク番号を指定します。

有効値 : 任意の有効な URL マスク番号

デフォルト値 : 1

new url mask *stat*

有効値 : yes

デフォルト値 : yes または no

include or exclude from cache

変更された URL をキャッシュに含めるか、除外するかを指定します。

有効値 : i または e

デフォルト値 : i

set default expiration time

デフォルトの有効期限時間を設定するかどうかを指定します。

有効値 : yes または no

デフォルト値 : yes

default expiration time

デフォルトの有効期限を分単位で指定します。ゼロは、有効期限がないことを示します。

有効値 : 1 ～ 10080 分。有効期限がない場合は 0。

デフォルト値 : 0

Web サーバー・キャッシュ監視環境へのアクセス

Web サーバー・キャッシュ監視環境にアクセスするには、`t 5` config プロンプトで **f webc** と入力します。

```
t 5>f webc
```

Web サーバー・キャッシュ監視コマンド

表20 は、Web サーバー・キャッシュ監視コマンドを示しています。すべてのコマンドは、稼働中のシステムに対して使用できますが、構成データベースを変更しません。**Activate** コマンドは、構成からの情報を使用します。

表 20. Web サーバー・キャッシュ監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Activate	最新の構成を使用して、キャッシュ区画を活動化または再活動化します。
Clear	区画または統計をクリアします。
Enable	区画を使用可能にします。
Delete	区画、プロキシー、または URL マスクを稼働中のシステムから削除します。
Disable	区画を使用不可にします。
List	キャッシュ情報を表示します。
Modify	キャッシュ情報を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxv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、すべての Web サーバー・キャッシュ区画、あるいは特定の区画またはプロキシーを活動化するのに使用します。

構文:

activate all | external | partition | proxy

all すべての定義済みキャッシュ区画を活動化または再活動化します。

external 外部キャッシュ制御マネージャーを活動化します。

partition キャッシュ内の区画を活動化または再活動化します。

proxy キャッシュ内のプロキシーを活動化または再活動化します。

例: activate all

```
WEBC>act all
Cache partitions, must be disabled to reactivate them.
Do you wish to continue? [No]: y
WEBC>
```

例: activate Proxy

```
WEBC>act pr

    1) Cluster address 113.3.1.10, Port 80, Cache partition 0
    2) Cluster address 113.3.1.10, Port 81, Cache partition 0
Enter proxy number:  1 ? 1
You are trying to activate an existing proxy.
Doing this will cause the proxy to be terminated before
being reactivated.
Do you wish to continue? [No]: yes
```

Clear

clear コマンドは、区画または統計をクリアするのに使用します。

注: 区画からオブジェクトをクリアしても、区画の統計はクリアされません。

構文:

clear partition
statistics

partition
区画からすべてのオブジェクトをクリアします。

statistics
区画の既存の統計をクリアします。

例:

```
WEBC>clear partition
Enter partition number: [0]?
Cache partition 0 must be disabled to clear its contents.
Do you wish to continue? [No]: yes
Do you wish to enable this partition? [Yes]: yes
```

partition number
クリアされる区画番号を指定します。

有効値 : 任意の有効な区画番号

デフォルト値 : 0

Enable

enable コマンドは、稼働中のシステムの区画を使用可能にするのに使用します。

構文:

enable partition

例:

```
WEBC>enable partition
Enter partition number: [0]?
```

partition number
使用可能にされる区画の区画番号

有効値 : 任意の有効な区画番号

デフォルト値 : 0

Delete

delete コマンドは、稼働中のシステムから区画を削除するのに使用します。この区画を使用しているすべてのプロキシーは、削除されます。プロキシーまたは区画のどちらの構成データベースにも変更は行われません。

構文:

delete partition

partition
キャッシュから区画を削除します。

例:

```
WEBC>delete partition
Enter partition number: [0]? 0
WARNING: This will delete partition 0 and free all memory!
Do you wish to continue?  [No] : yes
WEBC>
```

partition number

削除される区画番号を指定します。

有効値 : 任意の有効な区画番号

デフォルト値 : 0

Disable

disable コマンドは、稼働中のシステムの区画を使用不可にするのに使用します。

構文:

disable partition

partition

区画を使用不可にします。

例:

```
WEBC>disable partition
Enter partition number: [0]?
```

partition number

使用不可にされる区画の区画番号。

有効値 : 任意の有効な区画番号

デフォルト値 : 0

List

list コマンドは、すべての Web サーバー・キャッシュ、区画、ポリシー、またはプロキシーを表示するのに使用します。

構文:

list all
delete
depend
external
item
partition
policy
proxy

all キャッシュ内のすべての区画、ポリシー、およびプロキシーを表示します。

delete キャッシュ区画から削除された最後の 100 項目を表示します。

depend

区画の依存関係テーブルを表示します。

external

外部キャッシュ制御マネージャーのための情報を表示します。

item キャッシュ区画内の、現在時刻とヒット・カウントを表示します。

partition
キャッシュ内の区画情報を表示します。

policy キャッシュ内のポリシー情報を表示します。

proxy キャッシュ内のプロキシー情報を表示します。

例:

```
WEBC>list all
Cache Partition 0        Status: Enabled
     Cluster address: 113.3.1.10  Port 80
1 partition(s) active.
External Cache Manager Port: 82
         Connection Timeout: 120 seconds
```

例:

```
WEBC>list delete
Enter partition number: [0]? 0
Delete Table
URL String -- hit count
======================
'/abc.html' -- 4
'/soccer.html' -- 2
'/tennis.html' -- 1
'/curling.html' -- 3
```

例:

```
WEBC>list depend
Enter partition number: [0]?

Dependency table for Partition 0
------------------------------------
dep: tennis_info
   count of URLs: 2
   URLs:
         tennis_schedule.html
         tennis_roster.html
dep: soccer_info
   count of URLs: 2
   URLs:
         soccer_schedule.html
         soccer_roster.html
dep: roster
   count of URLs: 2
   URLs:
         soccer_roster.html
         tennis_roster.html
dep: schedule
   count of URLs: 2
   URLs:
         soccer_schedule.html
         tennis_schedule.html
```

例:

```
WEBC>list item
Enter partition number: [0]? 0
Current number of items: 5
URL String -- hit count
======================
'/' -- 2
'/file5k.html' -- 1
'/file4k.html' -- 1
'/file2k.html' -- 3
'/file1k.html' -- 1
```

例:

```
WEBC>li partition 0
Cache Partition 0        Status: Enabled
     Cluster address: 113.3.1.10, Port 80
```

```
     Cluster address: 113.3.1.10, Port 81
Partition size: Current - 0 bytes  Highest - 0 bytes  Maximum - Unlimited
Number of objects: Current - 0  Highest - 0  Maximum - Unlimited
Maximum object size: Unlimited
Cache purge interval: 10 minute(s)
Hit ratio: 0%
Total number of hits:  0
Cache Hit Bytes Served: 0
Breakdown of responses for the Cache Hits
 (note: this is based on whether the HTTP Proxy considered it a hit.
  So these counts may not add up to the hit count above)
   Response 200(OK):                        0
   Response 203(Non-Authoriative):  0
   Response 206(Partial Content):   0
   Response 300(Multiple Choices):  0
   Response 301(Moved Permanently): 0
   Response 304(Not Modified):              0
   Response 410(Gone):              0
Total number of misses:  0
Cache Miss Bytes Served:  0
Breakdown of responses for the Cache Misses
 (note: this is based on whether the HTTP Proxy got the response
  back through it. In the case of multiple boxes working together
  as a big cache these counts will not add up to the total misses
  if a handoff was done)
   Response 100 Range(Information):         0
   Response 200(OK):                        0
   Response 200 Range(Successful-not 200):  0
   Response 304(Not Modified):              0
   Response 300 Range(Redirection-not 304): 0
   Response 400 Range(Client Error):        0
   Response 500 Range(Server Error):        0
   Response other (not in above):           0
Object Excluded (Object too large):        0
                (Object expired):          0
                (DONT CACHE header):       0
                (URL Mask excluded):       0
                (Image excluded):          0
                (Static object excluded):  0
                (Dynamic object excluded): 0
                (Cache disabled):          0
Total number of objects added via ECCM Interface: 0
Total number of objects not added via ECCM Interface but was attempted: 0
Total number of objects replaced via ECCM Interface: 0
```

例:

```
WEBC>li pol
Enter partition number: [0]?
Transparent caching: Enabled
Cache Control Headers: Enabled
Cache images:                   Enabled
     Default lifetime: 0 minute(s)
Cache non-image static objects: Enabled
     Default lifetime: 0 minute(s)
Cache dynamic objects: Disabled
Dynamic URL mask: *dyn*
URL masks defined:
  1: EXCLUDE *index*
  2: EXCLUDE *comp*
  3: INCLUDE *tmp*
      Default expiration time: 1 minutes
  4: INCLUDE *stat*
      Default expiration time: 2 minutes
  5: INCLUDE *html*
      Default expiration time: 1000 minutes (16 hrs 40 mins)
```

例: スケーラブル高可用性キャッシュ (SHAC) アレイの一部であるプロキシー

```
WEBC>li pr
    WEBC>li pr
    1)   Cluster address 113.3.3.10, Port 80, Cache Partition 0
    2)   Cluster address 113.3.3.20, Port 80, Cache Partition 0
Enter proxy number: [1]? 1
Proxy 1: assigned to cache partition 0
Cluster address: 113.3.3.10     Port number: 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
```

```
Client connections: 0 current / 2 at highest point
Server connections: 0 current / 2 at highest point
Total cache hits: 0
Total cache misses: 649
Cache misses (object not in cache): 649
             (unsupported method):  0
             (can't send response): 0
             (non-cached request):  0
This Proxy is part of a cache group
  Source IP address for group is: 113.3.3.1
  There are currently 2 Cache(s) in this group
  Below are the Caches in the group:
  113.3.1.1
  113.3.6.1
```

例: SHAC アレイの一部でないプロキシー

```
WEBC>li pr
    1)   Cluster address 113.3.1.10, Port 80, Cache Partition 0
    2)   Cluster address 113.3.1.10, Port 81, Cache Partition 0
Enter proxy number:  [1]?
Proxy 1: assigned to cache partition 0
Cluster address: 113.3.1.10     Port number: 80
Server Connection Timeout: 240 seconds
Client Connection Timeout: 240 seconds
Client connections: 0 current / 0 at highest point
Server connections: 0 current / 0 at highest point
Total cache hits: 0
Total cache misses: 0
Cache misses (object not in cache): 0
             (unsupported method):  0
             (can't send response): 0
             (non-cached request):  0
             (invalidation):        0
```

Modify

modify コマンドは、外部キャッシュ制御マネージャーを変更するのに使用します。

構文:

modify external

例: modify external

```
WEBC Config>mod ext
External cache manager port number(0 to disable) [82]?
TCP connection timeout (Range 5-240) seconds) [120]?  20
Do you want to modify the encryption key:? [No]?  Y
Encryption key should be 16 characters long.
Encryption key (16 characters) in Hex (0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex (0-9, a-f, A-F):
```

external cache manager port number

TCP connection timeout

do you want to modify the encryption key

encryption key

Web サーバー・キャッシュ動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

Web サーバー・キャッシュは、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、Web サーバー・キャッシュには適用できません。Web サーバー・キャッシュはフィーチャーで、インターフェースではありません。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、Web サーバー・キャッシュには適用できません。Web サーバー・キャッシュはフィーチャーで、インターフェースではありません。

GWCON (Talk 5) 構成要素リセット・コマンド

Web サーバー・キャッシュは、次の Web サーバー・キャッシュ固有 GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature WEBC, Activate All コマンド

説明: このコマンドは、Web サーバー・キャッシュ用のすべての SRAM を読み取り、現在の実行時環境を同一にします。

ネットワークへの影響:

現在アクティブであったすべてのプロキシーを終了します (すなわち、これらのプロキシーのすべての接続をダウンさせます)。外部キャッシュ制御マネージャーが稼働していた場合、2216 は現在のポートの新しい接続の listen を停止します (すなわち、現在のポートへの接続がダウンしません)。

制限事項:

Web サーバー・キャッシュは、すでに活動化されていなければなりません (**CONFIG, feature webc, activate** を参照)。

すべての Web サーバー・キャッシュ・コマンドは、**GWCON, feature webc, activate all** コマンドによってサポートされます。

GWCON, Feature WEBC, Activate Partition コマンド

説明: このコマンドは、この区画用のすべての SRAM を読み取り、現在の実行時環境を同一にします。

ネットワークへの影響:

活動化されている区画がすでに存在する場合、この区画のすべてのプロキシーを終了します (すなわち、これらのプロキシーのすべての接続をダウンさせます)。

制限事項:

- Web サーバー・キャッシュは、すでに活動化されていなければなりません (**CONFIG, feature webc, activate** を参照)。

次の表では、**GWCON, feature webc, activate partition** コマンドが起動されると活動化される Web サーバー・キャッシュの構成変更を要約します。

GWCON, feature webc, activate partition コマンドによって変更が活動化されるコマンド

CONFIG, feature webc, add urlmask
CONFIG, feature webc, delete partition
CONFIG, feature webc, delete urlmask
CONFIG, feature webc, modify partition
CONFIG, feature webc, modify proxy
CONFIG, feature webc, modify urlmask

GWCON, Feature WEBC, Activate Proxy コマンド

説明: このコマンドは、このプロキシー用のすべての SRAM を読み取り、プロキシー用の現在の実行時環境を同一にします。

ネットワークへの影響:

活動化されているプロキシーがすでに存在する場合、このプロキシーを最初に終了します (すなわち、これらのプロキシーのすべての接続をダウンさせます)。

制限事項:

Web サーバー・キャッシュは、すでに活動化されていなければなりません (**CONFIG, feature webc, activate** を参照)。

次の表では、**GWCON, feature webc, activate proxy** コマンドが起動されると活動化される Web サーバー・キャッシュの構成変更を要約します。

GWCON, feature webc, activate proxy コマンドによって変更が活動化されるコマンド
CONFIG, feature webc, modify proxy

GWCON, Feature WEBC, Activate External Port コマンド

説明: このコマンドは、外部キャッシュ制御マネージャー用のすべての SRAM を読み取り、外部キャッシュ制御マネージャー用の現在の実行時環境を同一にします。

ネットワークへの影響:

外部キャッシュ制御マネージャーが稼働していた場合、2216 は現在のポートの新しい接続の listen を停止します (すなわち、現在のポートへの接続がダウンしません)。

制限事項:

Web サーバー・キャッシュは、すでに活動化されていなければなりません (**CONFIG, feature webc, activate** を参照)。

次の表では、**GWCON, feature webc, activate external port** コマンドが起動されると活動化される Web サーバー・キャッシュの構成変更を要約します。

GWCON, feature webc, activate external port コマンドによって変更が活動化されるコマンド
CONFIG, feature webc, modify external

CONFIG (Talk 6) Activate コマンド

Web サーバー・キャッシュは、次の CONFIG (Talk 6) **activate** コマンドをサポートします。

CONFIG, Feature WEBC, Activate コマンド

説明: 現在の SRAM に基づいて現在稼働している Web サーバー・キャッシュを動的に変更します。

ネットワークへの影響:
現在アクティブであったすべてのプロキシーを終了します (すなわち、これらのプロキシーのすべての接続をダウンさせます)。外部キャッシュ制御マネージャーが稼働していた場合、2216 は現在のポートの新しい接続の listen を停止します (すなわち、現在のポートへの接続がダウンしません)。

制限事項:
なし。

すべての Web サーバー・キャッシュ・コマンドは、**CONFIG, feature webc, activate** コマンドによってサポートされます。

GWCON (Talk 5) 一時変更コマンド

Web サーバー・キャッシュは、装置の操作状態を一時変更する、次の GWCON コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行すると、行われません。

コマンド
GWCON, feature webc, modify external **注:** このコマンドは、外部キャッシュ制御マネージャー用の現在の実行時環境を変更します。外部キャッシュ制御マネージャーが稼働していた場合、2216 は現在のポートの新しい接続の listen を停止します (すなわち、現在のポートへの接続がダウンしません)。
GWCON, feature webc, delete partition **注:** このコマンドは、現在の実行時環境から区画を削除します。

第13章 コード化サブシステムの構成と監視

コード化サブシステム (ES) ではデータ圧縮機能と暗号化機能が一緒にまとめられています。ES は、インターフェースまたはプロトコル用のコード化ソフトウェア装置にアクセスできるようになっており、リンクが圧縮または暗号化できるように活動化されると必ず自動的に活動化されます。ソフトウェア装置は、圧縮および暗号化を実行する作動可能なソフトウェアで構成されます。圧縮および暗号アルゴリズムは、ルーターのプロセッサーで実行されます。ソフトウェア装置を使用するのにデフォルトの構成を変更する必要はありません。

注: PPP またはフレーム・リレーを介した圧縮セッションの構成に関する手順については 253ページの『第14章 データ圧縮の構成と監視』を、PPP またはフレーム・リレーを介した暗号化セッションの構成に関する手順については 297ページの『第17章 暗号化プロトコルの使用および構成』を、さらに IPSec セッションの構成に関する手順については 419ページの『第22章 IP セキュリティーの構成と監視』を、それぞれ参照してください。

監視 (talk 5) プロンプトから **feature es** と入力すると、ES 活動を監視することができます。

ES 構成パラメーターを使用して、ES ソフトウェア装置が使用するメモリーの量を制限することができます。デフォルトの構成では、ES は、必要な量のメモリーを入手できます。メモリーの使用量を制限するためには、構成プロセス (Talk 6) の **feature es** の下で **set** コマンドを使用してください。

この章は、次のセクションで構成されています。

コード化サブシステムの構成

ES 構成パラメーターにより、一度にソフトウェア・コード化装置を使用する圧縮および暗号化セッションの数を制御する方法が用意されます。ソフトウェア・コード化装置は、基本的に、ルーターのプロセッサーで実行される圧縮および暗号化ライブラリーの集合です。セッションは、圧縮または暗号化を使用するよう構成されている特定のインターフェースを介した全二重接続で構成されます。

一般的に、データ・コード化は、プロセッサー主体の操作です。ソフトウェア・コード化セッションの数を制限することにより、ルーターのパフォーマンスに対するデータ・コード化の影響を一定の程度まで制御することができます。たとえば、ルーターに、圧縮用に構成されたダイヤルイン・インターフェースが 20 あり、一度に 11 以上のインターフェースを圧縮するとルーターのパフォーマンスに悪影響が出ることが確認されている場合には、圧縮セッションの最大数を 10 に設定してください。こうすると、20 個のインターフェースのうちの 10 個が圧縮を使用できます。

ソフトウェア・コード化装置のメモリー要件も、セッションの数を制限する理由になる場合があります。各ソフトウェア圧縮セッションは、約 30 KB のルーター・メモリーを使用し、暗号化セッションは約 2 KB のルーター・メモリーを使用します。ES が使用するメモリー量が多すぎると、他の機能がメモリー制約を受け、ルーターのパフォーマンスに悪影響が出る場合があります。詳しくは、256ページの『考慮事項』を参照してください。

セッションの数を提示するか、値*unlimited*、*default* のどれかまたは数値を指定すると、ES セッションの最小数または最大数を設定できます。値 *unlimited* および *default* は同じ意味をもっています。これらの値により、ルーターは、メモリーが使いきるまで、暗号化または圧縮のために活動化されたセッションをすべてサポートすることができます。

注: ES 構成パラメーター (talk 6) はどれも、動的に再構成できません。パラメーター値を変更した後で活動化するには、ルーターを再ロードする必要があります。

Config プロセス (talk 6) で、`Config>` プロンプトに **feature es** と入力して、ES 構成コマンドにアクセスしてください。`ES Config>` プロンプトが表示されます。表 21 に、コマンドを示します。

表 21. ES 構成コマンド

コマンド	アクション
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
List	圧縮および暗号化セッションの現行の設定値を表示します。
Set	すべてのインターフェースで使用可能な暗号化および圧縮セッションの最大数を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

List

list コマンドは、圧縮および暗号化セッションの現行の設定値を表示するのに使用します。

構文:

list

例:

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

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

Set

set コマンドは、データの暗号化または圧縮セッションの最大数を設定するのに使用します。

構文:

set

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

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

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

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

注: 文字 sw は、ソフトウェアの省略形です。

software minimum compression-sessions *n, unlimited, or default*
インターフェースで使用可能な圧縮セッションの最小数を設定します。ルーターは、これだけの数のセッションが常に使用可能であるように予約しています。

デフォルト値 : 0

有効値 : 0 ～ *unlimited*; あるいは *default*

software maximum compression-sessions *n, unlimited, or default*
インターフェースで使用可能な圧縮セッションの最大数を設定します。これだけの数のセッションが活動化されていると、新たにセッションを活動化することはできません。

デフォルト値 : 0

有効値 : 0 ～ *unlimited*; あるいは *default*

software minimum encryption-sessions *n, unlimited, or default*
インターフェースで使用可能な暗号化セッションの最小数を設定します。ルーターは、これだけの数のセッションが常に使用可能であるように予約しています。

デフォルト値 : 0

有効値 : 0 ～ *unlimited*; あるいは *default*

software maximum encryption-sessions *n, unlimited, or default*
インターフェースで使用可能な暗号化セッションの最大数を設定します。これだけの数のセッションが活動化されていると、新たにセッションを活動化することはできません。

デフォルト値 : 0

有効値 : 0 ～ *unlimited*; あるいは *default*

コード化サブシステムの監視

監視プロセスで、+ プロンプトで **feature es** コマンドを入力して ES 監視コマンドにアクセスします。ES Monitor> プロンプトが表示されます。表22 は、使用可能なコマンドを示しています。

表 22. ES 監視コマンド

コマンド	アクション
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
List	ES ポート、回線、装置、構成、状況、または要約を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

List

list コマンドは、ES に関する情報を表示するのに使用します。ポート、装置、および状況が含まれる **list** コマンドの出力例については、**list summary** コマンドを参照してください。

構文:

list ports
circuits
devices
config
status
summary

ports **list ports** コマンドは、コード化システムの潜在的なクライアントによって作成されたコード化ポートを表示します。ポートは、ES を使用するよう構成されているコード化システムとクライアントとの間に連係を確立します。たとえば、PPP インターフェース Net 1 を介して圧縮または暗号化が構成されている場合、ポートはそのインターフェースと関連付けられています。QLen フィールドに、そのポートと関連付けられたすべての回線についての未処理の圧縮または暗号化要求の合計が示されます。特定のインターフェースを介して構成された PPP などのクライアントは、データの特定バッファーをコード化用に指定するときに ES に対して要求を提示します。

ポートでなにも待ち行列化されていない場合には、Status フィールドに *Idle* と示され、要求が処理中であるか、ポートで待ち行列化されている場合には *Busy* または *Waiting* と示されます。

circuits

list circuits コマンドは、コード化システムのクライアントによって定義されている回線を表示します。各回線は、全二重接続に対応しています。一方のエンドポイントで暗号化または圧縮された日付は、他方のエンドポイントで暗号化解除または解凍されます。

特に指定のない限り、活動状態の回線だけが表示されます。活動状態の回線と非活動状態の回線を両方とも含めるには、コマンド **list circuits all** を使用します。

検出された回線ごとに、ポートとユーザーが、**list ports** コマンドの場合と同様に表示されます。さらに、2 行の情報が表示されます。アウトバウンド回線用の Tx 行と、インバウンド回線用の Rx 行です。回線 ID は、クライアントによって提供される任意の数値であるため、クライアントは作成する各回線にタグを付けることができます。フレーム・リレーの場合には、この数値は、関連付けられたフレーム・リレー・データ・リンク回線 (DLCI) の ID に対応します。ポイントツーポイント・リンクが作成する回線は 1 つだけで、この回線は、必ず、数値 *1* で識別されます。

さらに、次の項目が表示されます。

Dev これは、そのストリームにサービスを行っているコード化装置を表す数値です。コード化が CPU を活動化するソフトウェアによって行われている場合には 1 であり、圧縮 / 暗号化アダプターによって行われている場合には 2 です。

Cmpr このフィールドは、そのストリームについて活動状態の圧縮または解凍アルゴリズムを表示します。それが *LZC* であれば、STAC-LZC 圧縮が使用されます。*MPPC* であれば、Microsoft® PPC が使用されます。ストリームがステートレス・モードで作動している場合は、アルゴリズムの名前にアスタリスク (*) が付いています。ステートレス・モードとは、データ・パケットが処理された後、そのパケットのヒストリーが保持されていないモードです。これに対し、連続モードでは、次のパケットを扱うために、1 つのパケットを処理した後そのヒストリーが保持されます。たとえば、連続圧縮の際に、エンコーダーは、現在のパケットをさらに効率よく圧縮するために、前のパケットから収集した情報のキャッシュを保持します。

Encr このフィールドには、使用中の暗号化または暗号アルゴリズムが表示されます。標準 DES の場合は *DES* であり、トリプル DES の場合は *3DES*、また、RSA の RC4 アルゴリズムが使用される場合には *RC4* が表示されます。ストリームがステートレス・モードで作動している場合は、名前にアスタリスク (*) が付いています。このことは、RC4 の場合には重要ですが、DES/3DES の場合にはあまり意味をもちません。示される名前は、クライアントが使用するカプセル化形式ではなく、採用された基本暗号アルゴリズムと対応していることに注意してください。たとえば、PPP は、2 つのサポート方式をサポートしています。DESE (RFC 1969) は DES で暗号化し、MPPE (Microsoft 非標準) は RC4 を使用します。

QLen このパラメーターは、コード化または復号されるのを待っているストリームの待ち行列に収められている未処理パケットの数を示します。この数値は、処理のために実際に ES に対して実行依頼されたパケットだけを反映するものであることに注意してください。クライアントの中には、独自の待ち行列を保持し、これらのプライベート待ち行列からコード化システムに一度に数個のパケットしか送らないクライアントもあります。

Status

ストリームの状況を即時に指示します。すべてのストリームが待ち状況をもち、使用中であるように見えるものがないこともよくあります。使用中状況を認知するには、処理サイクル内のかなり幅の狭い時間帯で待ち行列活動を捕える必要があります。次に、考えられる状態を示します。

Idle このストリーム上には待ち行列になっているパケットがない

Busy システムは、現在、このストリーム上でパケットを処理中である (待ち行列の先頭にある項目がその時点でコード化エンジンを通り抜けようとしていることを意味します)

Waiting

要求は保留中であるが、そのストリームからのものはなにも、現在、処理が行われていない

devices

list devices コマンドは、システムが使用できるようになっているコード化装置を表示します。コード化装置は、通常、圧縮 / 暗号化アダプターをいいます。ハードウェア・アクセラレーターが使用可能でない場合に使用されるソフトウェアは、バーチャル装置として実装されるもので、このリストでも、*Host Software* 装置として示されます。このコマンドには、**list devices** と **list device n** の 2 とおりの形式があります。最初の形式では、システムが認識したすべての装置の簡単な要約リストが作成されます。2 つ目の形式では、特定の装置 n (n は装置番号です) の詳細リストが作成されます。unit 1 は、バーチャル・コード化装置であるホスト・ソフトウェアを表し、unit 2 は圧縮 / 暗号化アダプターを表します。番号 n の代わりにアスタリスク (*) を使用することもできますが、その場合、両方の装置についてリストが作成されます。

config **list config** コマンドは、現行の構成パラメーターを表示します。これらのパラメーターは、ルーターの再ロード時に不揮発性メモリーから読み取られたものです。表示される情報は、構成 (Talk 6) **list config** コマンドによって表示されるものと同じです。

status **list status** コマンドは、コード化システム状況を表示します。この状況は、グローバル状況フラグといくつかの各種システム統計で構成されます。次に、**list status** コマンドによって表示されるフィールドの記述を示します。

Last Error

コード化システムの任意のクライアントに最後に戻されたエラー・コード。これは、デバッグのためのものであり、保守担当者が使用するものです。

Internal Condition flags

このフィールドには、次のリストに定義されているとおり、特定の内部状態が示されます。

Ready システムはアップであり、作動可能です。これは通常の状態です。

Not Working
コード化システムは、なんらかの内部エラーにより作動不能です。

No Devices Available
コード化を行うのに使用できる装置がないことを示します。ハードウェア・ベースのエンコーダーが存在しない場合、コード化は内部ソフトウェアによって行われるため、この状態が発生することはありません。

Out of Memory
システムは、メモリーを割り振ろうとしましたが、失敗しました。この状態は、ルーターの RAM の容量が不足しており、コード化システムに悪影響が出ていることを示します。

Number of Ports
このフィールドは、ES 内に自力でポートを設定したクライアントの数が示されます。ポートの定義については、**list ports** コマンドを参照してください。

Number of Circuits
回線の定義については、**list circuits** コマンドを参照してください。

Global Request pool size
割り振り済みおよび空いている要求バッファーの数。コード化されるパケットごとに、1 つの要求バッファーがほとんど全部使用されます。空いているバッファーの数が割り振り済みのバッファーの数より小さい場合には、コード化が進行中です。

Total # of Requests processed
この値は、コード化エンジンによって処理されたバッファーの総数を示します。この数値は、最後のルーターが再ロード後でシステムのすべてのクライアントによって圧縮または暗号化されたパケットの総数とほぼ同じです。

summary
このコマンドは、システムの要約を表示します。これは、コマンド **list status**、**list devices**、および **list ports** からの出力を結合する複合コマンドです。

例:

```
list summary

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

Last Error:                             14 (Stream not active)

Internal Condition flags:               0x00000001   -->
                                         Ready

Number of Ports:                        2

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



 Encoding System Devices
 Encoding System Devices
```

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


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

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

コード化サブシステム動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

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

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、コード化サブシステムには適用できません。ES 構成パラメーターは、ブート時に ES に割り振られるメモリーの大きさを決めます。このメモリーはインターフェースに関連付けられておりません。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、コード化サブシステムには適用できません。ES 構成パラメーターは、ブート時に ES に割り振られるメモリーの大きさを決めます。このメモリーはインターフェースに関連付けられておりません。

非動的再構成可能コマンド

コード化サブシステムは、どの構成パラメーターについても動的変更をサポートしません。

第14章 データ圧縮の構成と監視

この章では、フレーム・リレーおよび PPP インターフェースを介した 2216 上のデータ圧縮について説明します。この章には、次の内容が記載されています。

- 『データ圧縮の概説』
- 『データ圧縮の概念』
- 258ページの『PPP リンク上でのデータ圧縮の構成と監視』
- 261ページの『フレーム・リレー・リンクのデータ圧縮の構成と監視』

データ圧縮は、フレーム・リレーおよび PPP インターフェースでサポートされます。

データ圧縮の概説

データ圧縮は、装置上のネットワーク・インターフェースの有効帯域幅を増やす手段を提供します。主として低速の WAN リンクで使用することを目的としています。

装置上のデータ圧縮は、PPP およびフレーム・リレー・インターフェースでサポートされます。

- PPP インターフェースの場合、圧縮はインターネット技術特別調査委員会の RFC 1962 に定義されている圧縮制御プロトコル (CCP) に準拠して実現されています。CCP は、圧縮の使用を交渉する基礎になる機構と、複数の可能な圧縮プロトコルの中から選択する手段を提供します。

  この装置は、2 種類の圧縮プロトコルを提供します。すなわち、RFC 1974 に定義されている Stac-LZS と、RFC 2118 に記述されている Microsoft ポイントツーポイント圧縮プロトコル (MPPC) です。これらは両方とも Stac Electronics によって提供される圧縮アルゴリズムに基づいています。
- フレーム・リレー・インターフェースの場合、圧縮は、フレーム・リレー・フォーラム技術委員会によって作成された FRF.9、*Data Compression over Frame Relay Implementation Agreement* に準拠して実現されています。FRF.9 は、データ圧縮プロトコル (DCP) を記述し (PPP の CCP をモデルにしています)、同様に、各種の圧縮アルゴリズムおよびオプションをネゴシエーションする手段を提供しています。装置は DCP『モード 1』ネゴシエーションをサポートします。FRF.9 には、より汎用化された『モード 2』も記述されていますが、これはサポートされません。圧縮そのものは、PPP Stac-LZS プロトコルで使用されるのと同じ圧縮エンジンを使用して行われます。

データ圧縮の概念

装置上のデータ圧縮は、リンク上の利用可能な帯域幅をより効率的に使用して、ネットワーク・リンクのスループットを高める手段を提供します。その基本原理は簡単です。つまり、リンクを流れるデータをできるだけコンパクトな形にすることにより、速度が一定のリンク上で転送にかかる時間をできるだけ少なくすることです。

データ圧縮は、ネットワーク・モデルのさまざまなレイヤーで実行できます。たとえば、あるアプリケーションがネットワーク上の別の場所にあるピア・アプリケーションにデータを転送する前に圧縮する、あるいは 2 つのノード間でビット列の受け渡しだけを行っているデータ・リンク・レイヤーで装置が圧縮するといったことが可能です。この圧縮の方法とその効率は、さまざまなファクターによって決まります。このファクターとしては、圧縮を実行するネットワーク・レイヤー、圧縮機能と解凍機能が持っている圧縮されるデータに対する知識、選択された圧縮アルゴリズム、および圧縮される実際のデータなどが含まれます。通常は、最良の圧縮を達成できるのは、アプリケーション・レイヤーです。たとえば、ファイル転送アプリケーションは、圧縮する前にデータ・ファイル全体を入手できるので、ファイルに対して各種の圧縮アルゴリズムを試し、その特定ファイルのデータに最適なアルゴリズムを見つけることができます。しかし、これはその 1 つのタイプのアプリケーションの圧縮としては優れた方法かもしれませんが、ネットワーク上を流れる大量のトラフィックの圧縮の一般的問題の解決にはあまり役に立ちません。現在、ほとんどのネットワーク・アプリケーションは、データを生成する時点では圧縮を行っていないからです。

装置での圧縮は、これよりはるかに低いネットワーク・レイヤー、つまりデータ・リンク・レイヤーで行われます。装置内で、リンクを介して転送される個々のパケットが圧縮されます。圧縮はパケットが装置を通過するときにリアルタイムで行われます。送信側は転送する直前にパケットを圧縮し、受信側は受信すると同時にパケットを解凍します。この操作は、高位レイヤーのネットワーク・プロトコルには透過的です。

データ圧縮の基本

データ圧縮機能は、データ内の『冗長』情報を認識し、できるだけ冗長度の少ない別のデータ・セットを生成します。『冗長』情報とは、現在利用可能なデータに基づいて導出することができ、再作成が可能な情報のことを言います。たとえば、圧縮機能はデータ・ストリーム内の反復文字パターンを認識し、これらの反復パターンを、そのパターンを表す短いコード・シーケンスで置き換えます。圧縮機能と解凍機能でこれらのコード・シーケンスに関する認識が一致している限り、必ず解凍機能は圧縮されたデータから元のデータを再作成することができます。

元のデータ内のシーケンスを、圧縮された出力の対応するシーケンスにマッピングしたものを、一般に***データ・ディクショナリー*** と呼んでいます。これらのディクショナリーは、静的に定義すること (圧縮機能と解凍機能が利用できる経験に基づく情報) も、動的に生成すること (通常は、圧縮する情報に基づく) もできます。静的ディクショナリーは、処理されるデータが限定された既知の性質を持っており、汎用圧縮機能を使用してもあまり効率的ではない環境に最適です。ほとんどの圧縮システム (装置上の圧縮機能も含む) は、動的ディクショナリーを使用しています。2216 上のデータ・ディクショナリーは、現在処理中のパケットと以前に処理されたパケットについての知識に基づいていますが、他のレイヤーで圧縮が行われるときに存在するデータ・ストリームを『見通す』機能は備えていません。データ・ディクショナリーが動的に生成され、以前に処理されたデータにのみ基づくシステムは、***ヒストリー*** とも呼ばれます。この章の残りの部分ではヒストリーとデータ・ディクショナリーという用語を同義の用語として使用しますが、他の環境では、ヒストリーは特定の形のデータ・ディクショナリーを表すことを理解しておくことが必要です。

装置は動的ディクショナリーを使用し、圧縮機能と解凍機能はそれぞれのディクショナリーを同期に保つ必要があるということは、データ圧縮は 2 つのエンドポイント間で受け渡されるデータ・ストリームに作用するものであることを意味しています。つまり、ルーター上の圧縮は接続指向のプロセスであり、接続のエンドポイントは、圧縮機能と解凍機能そのものです。ストリーム上で圧縮が開始されると、両端はそれぞれのデータ・ディクショナリーを事前設定された開始状態にリセットし、データを受信するとその状態を更新します。

各パケットごとに個別に圧縮を実行し、各パケットを処理する前にヒストリーをリセットすることも可能です。しかし通常は、パケットとパケットの間ではデータ・ディクショナリーはリセットされません。これは、ヒストリーは現行パケットの内容だけでなく、以前に処理されたパケットの内容にも基づくことを意味しています。これにより、圧縮機能が冗長度を除去するために探索するデータの量が増えるので、通常は全体的な圧縮効率が上がります。一例として、あるホストが IP を使用して別のホストに 『PING』 している場合を考えてみます。一連のパケットが送信されますが、通常、各パケットは直前に送信されたパケットとほぼ同じです。圧縮機能は、最初のパケットの圧縮ではあまり効率を上げることができないかもしれませんが、後続のパケットがそれぞれ直前に送信されたものに非常によく似ていることを認識し、それらのパケットでは非常に高率で圧縮されたバージョンを生成できるようになります。

圧縮機能と解凍機能のヒストリーは、各パケットを受信するたびに変更されるので、圧縮機構はパケットの損失、破壊、または配列変更を検知できます。装置で採用されている圧縮プロトコルには、シグナル機構が組み込まれており、これにより圧縮機能と解凍機能が同期が失われたのを検出し、相互に再同期できるようになっています (たとえば、伝送エラーのためにパケットが損失した場合などに必要になります)。これは通常、各パケットにシーケンス番号を含め、解凍機能がこの番号をチェックして、すべてのパケットを順序通りに受信していることを確認する方法で行われます。エラーを検出すると、自身を事前設定された開始状態にリセットし、圧縮機能にも同様にリセットするようにシグナルし、圧縮機能自体がリセットしたことを知らせる確認応答を待ちます (着信した圧縮パケットを廃棄して)。

リンクでの圧縮は一般的に、リンク上の両方向のデータに対して実行されます。通常は、256ページの図21 に示すように、接続の各端に圧縮機能と解凍機能の両方があり、接続の他端の相手と通信します。出力 (圧縮) 側は、入力 (解凍) 側から独立して作動します。リンクの各方向でまったく異なる圧縮アルゴリズムを使用することも可能です。リンク・接続が確立されると、そのリンクの圧縮制御プロトコルが相手側とネゴシエーションし、その接続で使用する圧縮アルゴリズム (1 つまたは複数) を決めます。2 つの端が、使用する圧縮プロトコルについて合意できない場合には、圧縮は行われず、リンクは通常どおりに作動します (つまり、パケットは圧縮されない形で転送されます)。

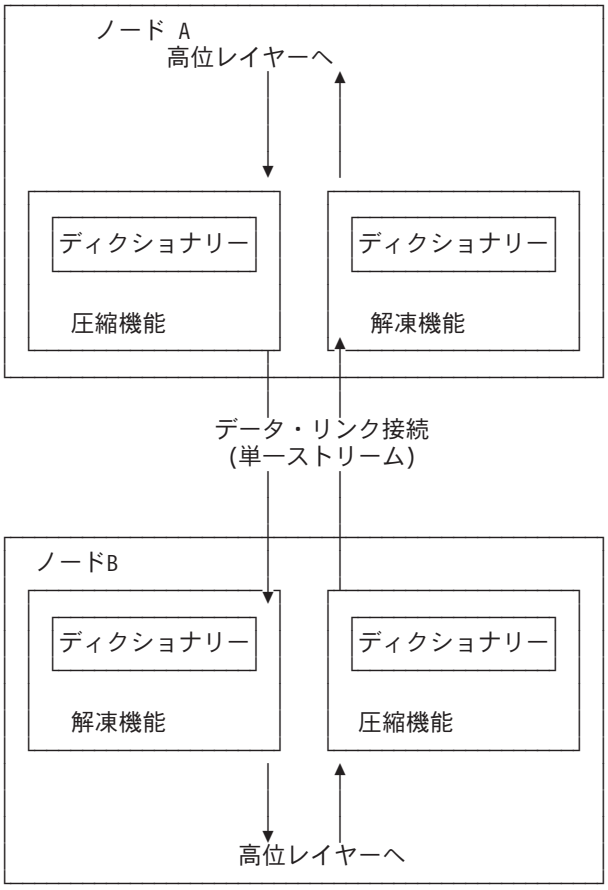


図 21. データ・ディクショナリーを使用した双方向データ圧縮の例

ストリームというのは、実際には、リンクの一端の特定の圧縮プロセスとリンクの他端の対応する解凍プロセス間の接続を表しているので、単なる 2 つのノード間の『接続』ではなく、より具体的な意味をもっています。精巧な圧縮プロトコルは、2 つのホスト間のデータ・フローを複数のストリームに分割し、個々のストリームを独立して圧縮することも可能です。たとえば、PPP の CCP は、単一の PPP リンク上で複数のヒストリーを使用することをネゴシエーションできます。ただし、ルーターはこれをサポートしていません。

考慮事項

データ圧縮を使用するか、しないかの選択は、必ずしも容易ではありません。接続上の圧縮を使用可能にする前に、いくつかの要因を考慮する必要があります。

CPU 負荷

データ圧縮は、演算に負担のかかる手順です。圧縮するデータの量が増えるほど (単位時間当り)、装置のプロセッサーにかかる負荷が大きくなります。負荷が大きくなり過ぎると、圧縮が行われる装置だけでなく、すべてのネットワーク・インターフェース上の装置の性能が低下します。

実際上は、装置には複数のプロセッサーが搭載されており、非対称マルチプロセッシングが使用されているので (たとえば、メイン・プロセッサーと直列式で操作するリンク入出力処理装置)、プロセッサーの負荷への影響は、必ずしも簡単に測定で

きるわけではありません。圧縮操作はパケットの転送とオーバーラップしている部分があるので、この負荷は事実上まったく透過的であり、問題がない場合もあります。しかし、装置のプロセッサーに過剰な負担をかけ、性能を低下させる可能性もあります。

おおまかな原則として、圧縮を使用可能にするのは、低速の WAN リンク、つまり速度が約 64 KBPS (標準的な ISDN ダイヤル・リンクの速度) までのリンクにだけ限るべきです。すべてのリンク上の圧縮されるデータの総帯域幅は、1 秒につき数百 KBPS に限定する必要があると考えられます。ISDN 1 次群速度アダプターのすべてのチャネルで圧縮を実行するのは賢明でありません。

コード化サブシステム・パラメーターは、同時に圧縮を実行できる接続の数を制限できるようにします。これを使用すると、実際に圧縮を実行する台数より多くのインターフェースに対して、圧縮を使用可能に設定することができます。活動圧縮接続数の限界に達すると、少なくとも既存の圧縮リンクが切断されるまでは、追加の接続は圧縮の使用をネゴシエーションしなくなるだけです。

メモリーの使用量

圧縮を構成するときに考慮しなければならない問題の 1 つは、メモリー所要量です。圧縮および解凍ヒストリーは、限られた装置資源であるメモリーをかなり使用します。たとえば、Stac-LZS アルゴリズムでは、圧縮ヒストリーに約 16 KB、解凍ヒストリーに約 8 KB 必要です。これらのヒストリーは、確立される各接続ごとに存在しなければならない (圧縮ヒストリーは、相手側ルーターの対応する解凍ヒストリーと同期される) ので、この問題は一層大きくなります。PPP リンクの場合、これは圧縮ヒストリーが 1 つと解凍ヒストリーが 1 つを意味しています (リンク上のデータ圧縮が双方向で実行されているものと想定した場合)。フレーム・リレー・リンクの場合は、このようなヒストリーが多数必要になる可能性があります (確立される各バーチャル・コネクション (DLCI) ごとに 1 組)。

装置はブート時に、多圧縮ヒストリーと解凍ヒストリーのプールを作成します。これらは常に対にして、***圧縮セッション*** として割り振られます (セッションは、1 つの圧縮ヒストリーと 1 つの解凍ヒストリーを単に結合したものです) 。技術的には、圧縮と解凍は独立した機能ですが、実際上は、圧縮はいつも双方向で実行されるのが一般的なので、運用を簡単にするために、メモリーの管理と構成は、個々のヒストリーではなく、セッションを対象にして行われます。各種圧縮アルゴリズムの圧縮および解凍のためのメモリー要件はそれぞれ異なるため、セッションのサイズは、最悪の場合に備えて約 30 KB に決められています。圧縮セッションのプールは、コード化サブシステム・フィーチャーに設定されているとおりに構成されます。詳しくは、245ページの『第13章 コード化サブシステムの構成と監視』を参照してください。

装置がリンク上で圧縮接続の確立を試みる際には、必ず割り振られたセッションのプールから 1 つのセッションを確保することから始めます。利用可能なセッションがない場合には、その接続では圧縮は行われません。ルーターは、後でセッションが利用可能になった時点で、その接続での圧縮の開始を試みることもできます。

割り振られる圧縮セッションの数は、構成可能なパラメーターです。割り振られるセッション数の設定値は、使用されるメモリーの量と、圧縮を使用して同時に操作できる接続の最大数の両方を制限します。同時に操作する圧縮接続の数を制限することは、CPU の負荷問題を制御するのに役立つ 1 つの手段となります。

データの内容

ある接続の圧縮を使用可能にする前に、その接続で転送されるデータの実際の性質を考慮することが必要です。圧縮は、データのタイプによって効果がさまざまです。ほぼ同一の情報が多数含まれているパケット (たとえば、IP『PING』によって生成される 1 組のパケット) は、一般的に非常によく圧縮されます。リンクを通る標準的なランダム・テキストおよび 2 進データの圧縮比率は 1.5:1 〜 3:1 程度です。まったく圧縮されないデータもあります。特に、すでに圧縮されているデータは、さらに圧縮されることはほとんどありません。実際には、以前に圧縮されたデータが圧縮エンジンを通過するときに拡張されることさえあります。

ある接続を通るデータのほとんどが圧縮データから成ることが前もって分かっている場合には、その接続では圧縮を使用可能にしないことをお勧めします。これに該当する例としては、主として FTP ファイル・アーカイブ・サイトとしてセットアップされたホストへの接続があります。この場合、転送に使用されるファイルはすべて圧縮した形でホストに保管されています。

リンク・レイヤーの圧縮

考慮が必要な最後のファクターは、2 つのホスト間のネットワーク・リンクの性質です。圧縮は、装置のハードウェア・インターフェースよりも下位レイヤーで実行することもできます。特に最新モデムの多くは、ハードウェアとファームウェアにデータ圧縮機構が組み込まれています。下位レイヤー (装置の外部) のリンクで圧縮が行われる場合には、そのインターフェースの装置ではデータ圧縮を使用可能にしないのが最善です。前にも述べたように、すでに圧縮されたデータ・ストリームを圧縮しても、通常は無効であり、実際には性能がいくぶん低下することもあります。ルーターの方がリンク・ハードウェアよりはるかに圧縮効率が高いと確信できる特別な理由がない限り、圧縮はリンク・ハードウェアに任せるのが最良です。

PPP リンク上でのデータ圧縮の構成と監視

2216 は、PPP 圧縮制御プロトコル (CCP) を使用して、リンク上での圧縮の使用をネゴシエーションします。CCP は、特定の圧縮プロトコル (リンクの各方向に異なるプロトコルを使用することも可能です) および各種のプロトコル特有のオプションの使用をネゴシエーションするための汎用機構を提供します。このソフトウェアは Stac-LZS および MPPC プロトコルをサポートするので、2 つのノード間でデータ圧縮のネゴシエーションを正常に行うためには、相手側でも少なくともこれらのアルゴリズムの 1 つがサポートされることが必要です。圧縮が機能するためには、2 つのノード間でアルゴリズム特有のオプションについて合意することも必要です。

PPP リンク上のデータ圧縮の構成

PPP リンク上のデータ圧縮を構成するには、次のようにします。

1. **enable ccp** コマンドを使用して、リンク上の CCP プロトコルを使用可能にする。これにより、リンクは他のノードと圧縮をネゴシエーションできるようになります。ネゴシエーションには、使用する圧縮アルゴリズム特有のオプションが含まれます。
2. **set ccp algorithms** コマンドを使用して、ネゴシエーションできる圧縮アルゴリズムを選択する。

3. **set ccp options** コマンドを使用して、各圧縮アルゴリズムのネゴシエーション可能パラメーターを設定する。

list ccp コマンドを使用すると、現行の圧縮構成を表示することができます。

表23 は、利用可能なコマンドを示し、図22 は、PPP リンク上の圧縮の構成例を示しています。これらのコマンドについての詳しい説明は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の ‘ポイントツーポイント構成コマンド’ の項を参照してください。

表 23. PPP データ圧縮構成コマンド

データ圧縮コマンド	アクション
disable ccp	データ圧縮を使用不可にします。
enable ccp	データ圧縮を使用可能にします。
set ccp options	圧縮アルゴリズムのオプションを設定します。
set ccp algorithms	圧縮アルゴリズムの優先順位付けされたリストを指定します。
list ccp	圧縮構成を表示します。

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

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

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

図 22. PPP リンク上の圧縮の構成例

注:

1. network コマンドは、PPP リンクのネットワーク・インターフェースを選択します。リンクが PPP ダイヤル回線の場合は、**encapsulator** コマンドを使用して、PPP 構成メニューにアクセスすることが必要です。
2. CCP を使用可能にしたが、リンクのアルゴリズムを設定しなかった場合、ソフトウェアは自動的にリンクがプロトコル STAC および MPPC を使用するように設定します (これは、コマンド **set ccp algorithms stac mppc** を入力した場合と同じです)。

   複数のアルゴリズムを設定する場合、アルゴリズムの設定順序によって、そのリンクのネゴシエーションの優先順位が決まります。

set ccp algorithms none を入力すると、ソフトウェアは自動的にリンク上の圧縮を使用不可にします。

MPPE が使用可能で、しかも CCP が使用可能であれば、MPPC は圧縮アルゴリズムです。

PPP リンク上でのデータ圧縮の監視

圧縮の監視は、他の PPP コンポーネントの監視と同様です。*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の ‘インターフェース監視プロセスへのアクセス’ の章で、PPP コンソール環境へのアクセス方法とコマンドの詳細について説明しています。表24 は、圧縮関連のコマンドを表示しています。図23 は、PPP インターフェースにリストされる圧縮の例です。

表 24. PPP データ圧縮監視コマンド

コマンド	機能
list control ccp	CCP 状態とネゴシエーション済みのオプションを表示します。
list ccp	CCP パケット統計を表示します。
list cdp または **list compression**	圧縮データグラム統計を表示します。

```
+ network 1
PPP > list control ccp

CCP State:                Open
Previous State:           Ack Sent
Time Since Change:        2 minutes and 52 seconds

Compressor:   STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ
MPPE:         Not negotiated

PPP > list ccp

CCP Statistic             In                        Out
-------------             --                        ---

Packets:                  2                         3
Octets:                   18                        27
Reset Reqs:               0                         0
Reset Acks:               0                         0
Prot Rejects:             1                         -

PPP > list cdp

Compression Statistic     In                        Out
---------------------     --                        ---

Packets:                  19541                     19542
Octets:                   2550673                   2740593
Compressed Octets:        821671                    899446
Incompressible Packets:   0                         0
Discarded Packets:        0                         -
Prot Rejects:             0                         -
Compression Ratios:       3.11                      3.24
```

図 23. PPP インターフェースの圧縮の監視

フレーム・リレー・リンクのデータ圧縮の構成と監視

グローバル圧縮パラメーターを構成し、インターフェース上の圧縮を使用可能にした後で、フレーム・リレー・インターフェース上の個々のサーキット (PVC) のパラメーターを設定する必要があります。インターフェースに定義されている各サーキットごとに圧縮を使用可能にすることができ、ネゴシエーションが正常に行われた各サーキットは、グローバル・プールから 1 つの圧縮セッションを使用します。インターフェース自体の圧縮を使用不可にすることもできます。これは、そのインターフェース上のどのサーキットも圧縮データ・トラフィックを伝送できなくなることを意味しています。

フレーム・リレー・リンクのデータ圧縮の構成

FR リンクのデータ圧縮を構成するには、次のようにします。

1. **enable compression** コマンドを使用して、インターフェースの圧縮を使用可能にする。これにより、リンクは他のノードと圧縮をネゴシエーションできるようになります。
2. **add permanent-virtual-circuit** コマンドを使用して、圧縮データを伝送する新規の PVC ごとに圧縮を使用可能にする。**change permanent-virtual-circuit** コマンドを使用すると、既存の PVC を変更できます。

現行の圧縮構成を表示したい場合は、**list lmi** または **list permanent-virtual-circuit** コマンドを使用します。

262ページの表25 は、フレーム・リレー・リンクの圧縮を構成するのに利用可能なコマンドを示しています。262ページの図24 は、フレーム・リレー・リンクの構成例を示しています。詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の“フレーム・リレー構成コマンド”の項を参照してください。

```
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Maximum number of run-time compression circuits (zero means no limit) [0]? 0
Do you want orphan PVCs to perform compression [Y]? n
The number of currently defined non-compression PVCs is 4
Would you like to change them all to compression PVCs [N]? y

FR Config> add perm

Circuit number [16]? 22
Committed Information Rate (CIR) in bps [65536]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []? cir22
Is circuit required for interface operation [N]?
Do you want to have data compression performed [Y]?

FR Config>list lmi

                        Frame Relay Configuration


  LMI enabled            =      No  LMI DLCI                      =       0
  LMI type               =    ANSI  LMI Orphans OK                =     Yes
  CLLM enabled           =      No  Timer Ty seconds              =      11

  Protocol broadcast     =     Yes  Congestion monitoring         =     Yes
  Emulate multicast      =     Yes  CIR monitoring                =      No
  Notify FECN source     =      No  Throttle transmit on FECN     =      No

  Data compression       =     Yes  Orphan compression            =      No
  Compression PVC limit  =    None  Number of compression PVCs    =       2

  PVCs P1 allowed        =      64  Interface down if no PVCs     =      No
  Timer T1 seconds       =      10  Counter N1 increments         =       6
  LMI N2 error threshold =       3  LMI N3 error threshold window =       4
  MIR % of CIR           =      25  IR % Increment                =      12
  IR % Decrement         =      25  DECnet length field           =      No
  Default CIR            =   65536  Default Burst Size            =   64000
  Default Excess Burst   =       0

FR Config>list perm

  Maximum PVCs allowable =      64
  Total PVCs configured  =       2

             Circuit                Circuit   Circuit     CIR    Burst  Excess
              Name                  Number     Type      in bps  Size   Burst
-------------------------------- ------- ----------- ------- ------- -----
 circ16                             16    @ Permanent   65536   64000       0
 cir22                              22    @ Permanent   65536   64000       0

* = circuit is required
# = circuit is required and belongs to a required PVC group
@ = circuit is data compression capable
```

図 24. フレーム・リレー・リンクの圧縮の構成例

表 25. データ圧縮構成コマンド

コマンド	アクション
add permanent-virtual-circuit #	インターフェース上に定義された特定の PVC 上のデータ圧縮を使用可能にするのに使用します。
change permanent-virtual-circuit #	特定の PVC がデータを圧縮するかどうかを変更するのに使用します。
disable compression	データ圧縮を使用不可にします。
enable compression	データ圧縮を使用可能にします。
list lmi	インターフェースの現行構成を表示します。

表 25. データ圧縮構成コマンド (続き)

コマンド	アクション
list permanent	サーキットに関する要約情報を表示します。

注: 孤立回線上の圧縮を使用可能にすると、装置上のネイティブ PVC が利用可能な圧縮セッションの数が減ります。

すでに圧縮が使用可能になっているフレーム・リレー・インターフェース上の圧縮を使用可能にすると、ソフトウェアは、下の例に示すように、圧縮パラメーターを変更したいかどうかを尋ねます。圧縮を使用不可にせずに、インターフェースの圧縮を変更することができます。

フレーム・リレー・インターフェース上での圧縮変更の例

```
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Data compression already enabled.
Do you wish to continue and change an interface parameter [Y]
Maximum number of run-time compression PVCs (zero means no limit) [0]? 32
Do you want orphan circuits to perform compression [Y]?
The number of currently defined circuits is 5
Change all of these circuits to perform compression?
```

フレーム・リレー・リンクのデータ圧縮の監視

圧縮の監視は、他のフレーム・リレー・コンポーネントの監視と同様です。*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の“フレーム・リレー監視コマンド”の章で、フレーム・リレー・コンソール環境へのアクセス方法とコマンドの詳細について説明しています。表26 は、圧縮関連のコマンドを示しています。『例 : フレーム・リレー・インターフェースまたはサーキット上の圧縮の監視』は、フレーム・リレー・インターフェースの圧縮のリスト例です。

表 26. フレーム・リレー・データ圧縮監視コマンド

コマンド	表示
list lmi	インターフェースの現在の状態を表示します。
list permanent	サーキットに関する要約情報を表示します。
list circuit	サーキットの現在の状態を表示します。

例 : フレーム・リレー・インターフェースまたはサーキット上の圧縮の監視

```
+ network 2
FR 2 > list lmi

Management Status:
  ------------------

    LMI enabled          =      No  LMI DLCI                   =       0
    LMI type             =    ANSI  LMI Orphans OK             =     Yes
    CLLM enabled         =      No

    Protocol broadcast   =     Yes  Congestion monitoring      =     Yes
    Emulate multicast    =     Yes  CIR monitoring             =      No
    Notify FECN source   =      No  Throttle transmit on FECN  =      No
    PVCs P1 allowed      =      64  Interface down if no PVCs  =      No
    Line speed (bps)     =   64000  Maximum frame size         =    2048
    Timer T1 seconds     =      10  Counter N1 increments      =       6
    LMI N2 threshold     =       3  LMI N3 threshold window    =       4
```

```
   MIR % of CIR         =      25  IR % Increment            =      12
   IR % Decrement       =      25  DECnet length field       =      No
   Default CIR          =   65536  Default Burst Size        =   64000
   Default Excess Burst =       0

   Current receive sequence  =       0
   Current transmit sequence =       0
   Total status enquiries    =       0  Total status responses   =       0
   Total sequence requests   =       0  Total responses          =       0

   Data compression enabled  =     Yes  Orphan Compression       =      No

   Compression PVC limit     =    None  Active compression PVCs  =       1

 PVC Status:
 -----------

   Total allowed  =      64  Total configured  =       1
   Total active   =       1  Total congested   =       0
   Total left net =       0  Total join net    =       0

FR 2 > list permanent

 Circuit                                    Orphan  Type/   Frames      Frames
 Number            Circuit Name             Circuit State Transmitted  Received
 ------- -------------------------------- ------- ----- ----------- --------

    16  circ16                              No   @ P/A        58364      58355
    22  circ22                              No   & P/A        58364      58355

   A - Active   I - Inactive   R - Removed   P - Permanent   C - Congested
   * - Required               # - Required and belongs to a PVC group
   @ - Data compression capable but not operational
   & - Data compression capable and operational
FR 2 > list circuit 22

 Circuit name = circ22

    Circuit state        =    Active  Circuit is orphan   =           No
    Frames transmitted   =     58391  Bytes transmitted   =      2676894
    Frames received      =     58383  Bytes received      =      2671009
    Total FECNs          =         0  Total BECNs         =            0
    Times congested      =         0  Times Inactive      =            0
    CIR in bits/second   =     65536  Potential Info Rate =        64000
    Committed Burst (Bc) =     64000  Excess Burst (Be)   =            0
    Minimum Info Rate    =     16000  Maximum Info Rate   =        64000
    Required             =        No  PVC group name      =   Unassigned

    Compression capable  =       Yes  Operational         =          Yes
    R-R's received       =         0  R-R's transmitted   =            0
    R-A's received       =         0  R-A's transmitted   =            0
    R-R mode discards    =         0  Enlarged frames     =            0
    Decompress discards  =         0  Compression errors  =            0
    Rcv error discards   =         0

    Compression ratio    =  1.00 to 1  Decompression ratio =    1.00 to 1

    Current number of xmit frames queued                  =            0
    Xmit frames dropped due to queue overflow             =            0
```

第15章 ローカルまたはリモート認証の使用

認証とは、ユーザー (または、エンティティー) が誰であるかを判別するプロセスです。 2216 上の PPP プロトコルに対するユーザー・アクセスを認証することは、PPP 認証プロトコルの PAP、MSCHAP、CHAP、および SPAP に関連しているので、ユーザー・プロファイル管理の柔軟性が増します。PAP、MSCHAP、CHAP、および SPAP の構成についての追加情報は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の 'PPP 認証プロトコル' の項を参照してください。

認証は、ローカルで構成することも、ユーザー構成を統合して構成する (ネットワーク上の認証サーバーを使用して、ネットワーク全体の認証要求に応じる) こともできます。IBM 2216 は、ローカルで維持される認証、および次の認証サーバー・プロトコルを実装します。

- Radius
- TACACS
- TACACS+

認証、許可、および会計 (AAA) セキュリティー

認証、許可、および会計 (AAA) セキュリティーは、サービスへのアクセスを制御できる構成可能なプロトコルです。ローカル認証またはリモート認証を実行するように AAA を構成できます。

3 つのタイプの機能のセキュリティー・プロトコルを構成できます。

- PPP リンク
- ログイン・ユーザー (Telnet / コンソール・ログイン)
- トンネル

構成は 1 次サーバーと 2 次サーバーを設定することによって行います。サーバー情報は、AAA 構成とは別に構成し、別に保管します。サーバー・プロファイルは、構成時に付けた名前を使用します。

どの環境でも、会計はローカルに行うことはできず、Radius または TACACS+ のどちらかでなければなりません。

許可は、ローカルで行うか、あるいは Radius または TACACS+ を使用するリモート認証を介して行うことしかできません。

AAA セキュリティーとは

AAA セキュリティーというのは、この装置のセキュリティー・システムの名前です。これには、次のものが含まれています。

認証 ユーザーを識別するプロセス。認証は、アクセスのために名前とパスワードを使用します。

許可 ユーザーのアクセスが許可されるサービスを決めるプロセス。

会計 ユーザーがセッションを開始または停止したときに記録するプロセス。サポートされる会計レコードには 2 つのタイプがあります。

開始レコード
サービスが開始されようとしていることを示します。

停止レコード
サービスが終了したことを示します。

PPP の使用

ポイントツーポイント・プロトコル (PPP) の場合、次の機能を構成できます。

- 認証
- 許可
- 会計

各機能は独自のセキュリティー・プロトコルを持つことができ、それぞれ独立して構成することができます。

- 認証プロトコルの設定値は、許可または会計には無効です。
- 許可プロトコルの設定値は、認証または会計には無効です。
- 会計プロトコルの設定は、認証または許可には影響を与えません。
- AAA をリモートに設定すると、認証はリモートに設定され、許可もリモートに設定され、会計もリモートに設定されます。
- AAA をローカルに設定すると、認証はローカルに設定され、許可もローカルに設定されます。認証または許可を使用不可にすることはできません。

この環境で使用する PPP 構成コマンドについての詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引きの* ポイントツーポイント構成コマンドの項を参照してください。

有効な PPP セキュリティー・プロトコル

有効な PPP セキュリティー・プロトコルは、次のとおりです。

認証方式
Local、RADIUS、TACACS+、TACACS

許可方式
Local、RADIUS、TACACS+

会計方式
RADIUS、TACACS+

表 27. PPP セキュリティー・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	無視
AAA をリモートに設定	リモート	リモート	リモート
AUTHENT をローカルに設定	ローカル	無視	無視
AUTHOR をローカルに設定	無視	ローカル	無視
AUTHENT をリモートに設定	リモート	無視	無視
AUTHOR をリモートに設定	無視	リモート	無視
ACCOUNTING をリモートに設定	無視	無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可

ログインの使用

AAA ログイン構成の場合、リモートまたはローカルを選択することができます。ローカル認証が必要な場合は、ローカル許可も使用する必要があります。リモート認証が選択されている場合には、リモート許可も使用する必要があります。会計はローカルではサポートされないので、認証と許可をローカルで行う場合は、会計を使用不可にする必要があります。

重要:

リモート認証サーバーが応答しない場合には、login-of-last-resort を使用可能にしたときにローカルのログインのユーザー ID とパスワードを使用することができます。これによって、リモート認証が期限切れになった場合、ローカルでログインを 1 回試行することができます。また、tech-support-bypass を使用可能にした場合、tech サポート id とパスワードを使用してログインして、要求を認証サーバーへは転送しません。

リモート認証を使用している場合特権レベルを指定することが重要です。ログイン・ユーザーは、正しいユーザー ID とパスワードを入力できますが、指定した特権なしでは、ユーザーはコンソールにアクセスできません。次の 3 つの特権レベルを設定できます。administrator、operator、および monitor。RADIUS の場合、SERVICE-TYPE 属性番号 6 を使用するかまたはベンダー属性番号 216 を追加します。特定の RADIUS 属性の詳細については、665ページの『付録. リモート AAA 属性』 を参照してください。

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

- AAA をローカルに設定すると、認証はローカルに設定され、許可もローカルに設定され、会計は使用不可に設定されます。
- AAA をリモートに設定すると、認証はリモートに設定され、許可もリモートに設定され、会計もリモートに設定されます。
- 認証プロトコルをローカルに設定すると、自動的に許可プロトコルを同じに設定し、会計を使用不可にします。
- 認証プロトコルをリモートに設定すると、許可プロトコルがローカルに設定されている場合にだけ、自動的に許可プロトコルを同じに設定し、会計プロトコルは無視します。
- 許可プロトコルをリモートに設定すると、認証プロトコルがローカルに設定されている場合にだけ、自動的に認証プロトコルを同じに設定し、会計プロトコルは無視します。
- 会計プロトコルをリモートに設定すると、認証プロトコルがローカルに設定されている場合にだけ、自動的に認証プロトコルを同じに設定し、許可がローカルに設定されている場合にだけ、自動的に許可プロトコルを同じに設定します。
- 会計プロトコルを使用不可に設定しても、認証または許可プロトコルには影響を与えません。
- 認証または許可を使用不可にすることはできません。

有効なログイン / 管理セキュリティー・プロトコル

有効なログイン / 管理セキュリティー・プロトコルは、次のとおりです。

認証 / 許可方式

Local、RADIUS、TACACS Plus

会計方式

RADIUS、TACACS Plus

表 28. ログイン・セキュリティー・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	使用不可
AAA をリモートに設定	リモート	リモート	リモート
AUTHENT をローカルに設定	ローカル	ローカル	使用不可
AUTHOR をローカルに設定	ローカル	ローカル	使用不可
AUTHENT をリモートに設定	リモート	ローカルの場合はリモート、その他の場合は無視	無視
AUTHOR をリモートに設定	ローカルの場合はリモート、その他の場合は無視	リモート	無視
ACCOUNTING をリモートに設定	ローカルの場合はリモート、その他の場合は無視	ローカルの場合はリモート、その他の場合は無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可

トンネルの使用

トンネル認証は、トンネル許可と同じに設定します。トンネル認証をローカルまたはリモートに設定した場合は、会計を使用可能にすることができます。トンネル認証サーバーと許可サーバーは同じでなければなりません。

また、会計のためのトンネル構成は IPSec トンネルにも適用されます。トンネル認証および許可は、IPSec トンネルには適用されません。AAA を使用して IPSec トンネルの認証または許可を行うことはできません。

有効なトンネル・セキュリティー・プロトコル

有効なトンネル・セキュリティー・プロトコルは、次のとおりです。

認証 / 許可方式

Local、RADIUS

会計方式

RADIUS、TACACS Plus

表 29. トンネル・セキュリティー・プロトコルの設定

アクション	認証	許可	会計
AAA をローカルに設定	ローカル	ローカル	無視
AAA をリモートに設定	リモート	リモート	リモート
AUTHENT をローカルに設定	ローカル	ローカル	無視

表 29. トンネル・セキュリティー・プロトコルの設定 (続き)

アクション	認証	許可	会計
Author をローカルに設定	ローカル	ローカル	無視
AUTHENT をリモートに設定	リモート	リモート	無視
AUTHOR をリモートに設定	リモート	リモート	無視
ACCOUNTING をリモートに設定	無視	無視	リモート
ACCOUNTING 使用不可	無視	無視	使用不可

パスワード規則

ローカル認証では、パスワードを使用してログイン・アクセスを制御することができます。次の規則のどれか、またはすべてに照らして、パスワードを検査することができます。

注: 次の規則は、PPP ユーザーのログインにだけ適用されるものであり、コンソール・ログインには適用されません。

- 長さが最小文字数である。必要な文字数を設定します。
- 少なくとも 1 字の英字が含まれている。
- 少なくとも 1 字の非英字が含まれている。
- 最初の位置に非数字がある。
- 最後の位置に非数字がある。
- 前のパスワードで使用されたのと同じ連続文字が 3 字しか含まれていない。
- 2 連続文字しか含まれていない。
- ユーザー ID がパスワードの一部として含まれていない。
- 直前の 3 つのパスワードのどれとも同じでない。
- 所定の日数の経過後に変更された。パスワードの変更の間隔の日数を設定します。
- 特定の回数のログイン失敗後にロック。失敗の回数を設定します。

認証サーバーとは

認証サーバー とは、ネットワークのユーザー ID とパスワードの妥当性を検査するネットワーク内のサーバーです。装置が認証サーバーを通して認証するように構成されている場合、装置は認証プロトコルからパケットを受信すると、ユーザー ID とパスワードをサーバーに渡して認証を依頼します。ユーザー ID とパスワードが正しい場合、サーバーは肯定応答します。その場合、装置は要求の発信元と通信することができます。装置から受け取ったユーザー ID とパスワードが見つからない場合、サーバーは装置に否定応答します。その場合、装置は認証要求を受け取ったセッションを拒否します。

SecurID サポート

2216 は、Security Dynamics ACE/サーバーで SecurID を使用するダイヤルイン・クライアントを認証することができます。このサポートは、ACE/サーバー上で TACACS、TACACS+、または RADIUS を使用して、クライアントを認証します。このダイヤルイン・クライアントの構成は、2216 の他のダイヤルイン・クライアントと同様に行います。

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

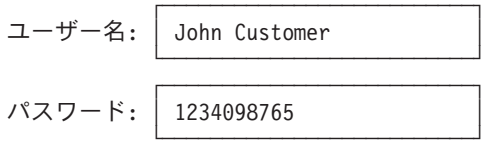


図 25. SecurID ユーザー名とパスコード

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

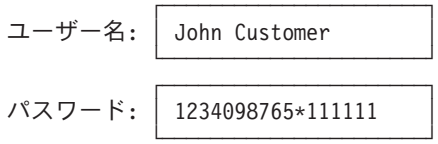


図 26. SecurID パスコードと次のトークン

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

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

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

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

SecurID の制約

次のような制限があります。

- Security Dynamics Inc. (SDI) および DES 暗号化はサポートされません。
- SecurID『New PIN』機能はサポートされません。

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

第16章 認証の構成

この章では、認証の構成コマンドおよびオペレーショナル・コマンドについて説明します。この章には、次の内容が記載されています。

- 『認証構成プロンプトへのアクセス』
- 『認証構成コマンド』
- 294ページの『認証 (AAA) 動的再構成サポート』

認証構成プロンプトへのアクセス

AAA Config> プロンプトにアクセスするには、次のようにします。

1. * プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **feature auth** を入力する。

認証構成コマンド

表30 には、AAA Config > プロンプトで使用できるコマンドのリストを示します。

表 30. 認証構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Disable	いろいろな AAA オプションを使用不可にします。
Enable	いろいろな AAA オプションを使用可能にします。
List	AAA 構成パラメーターを表示します。
Login	ログイン用の AAA を構成します。
Nets-info	ローカル PPP 認証に関する情報を表示します。
Password-rules	パスワード規則を構成します (使用可能または使用不可)。
PPP	PPP 用の AAA を構成します。
Servers	個々のリモート AAA サーバーを構成します。
Set	タイプに関係なく、認証パラメーターを構成します。
Tunnel	トンネル用に AAA を構成します。
User-profiles	ローカル PPP ユーザーを構成します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Disable

disable コマンドは、選択した会計オプションを使用不可にします。

構文:

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

accounting
AAA 会計を使用不可にすることを指定します。

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

login-last-resort
ログインの最終手段を使用不可にすることを指定します。

tech-support-bypass
tech サポート・バイパスを使用不可にすることを指定します。

unauthent-accounting
unauthent 会計を使用不可にすることを指定します。 PPP 認証を使用可能にすることによってユーザーを認証せずにアクティブになる PPP セッションは会計処理されません。開始レコードおよび停止レコードは転送されません。

Enable

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

構文:

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

accounting
AAA 会計を使用可能にすることを指定します。

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

login-last-resort
ログインの最終手段を使用可能にすることを指定します。認証情報をリモート認証サーバーに転送中にタイムアウトが発生した場合に、プロンプトが 1 回表示されてローカルに認証されたユーザーがログインできます。

tech-support-bypass
tech サポート・バイパスを使用可能にすることを指定します。

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

List

list コマンドは、AAA パラメーターを表示するのに使用します。

構文:

list	accounting
	all

authentication

authorization

config

options

リスト・コマンド出力の例

以下の例は、サポートされたリスト・コマンド・オプションの典型的な出力を示します。

```
AAA Config> list all
ppp AAA configuration...
 ppp authentication        : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 ppp authorization         : locallist
 ppp accounting            : Disabled
tunnel AAA configuration...
 tunnel authentication     : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 tunnel authorization      : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 tunnel accounting         : Disabled
login AAA configuration...
 login authentication      : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 login authorization       : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 login accounting          : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
```

```
AAA Config> list accounting all
accounting AAA configuration...
accounting ppp            : Disabled
accounting tunnel         : Disabled
accounting login          : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>


AAA Config> list accounting config
accounting ppp            : Disabled
accounting login          : Radius        serv01
accounting tunnel         : Disabled


AAA Config> list authentication all
authentication AAA configuration...
 authentication ppp        : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>
 authentication tunnel     : Radius        serv01
   authorizeAuthent          YES
   Primary server address    1.1.1.1
   Secondary server address  2.2.2.2
     Request tries           3
     Request interval        3
   Key for encryption        <notSet>


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

INBYTES              enabled
OUTBYTES             enabled
INPKTS               enabled
OUTPKTS              enabled
```

Login

login コマンドは、ログイン用の AAA を構成するのに使用します。

表31 は、**login** コマンドと共に使用できるサブコマンドを示しています。

表 31. ログイン・サブコマンド

コマンド	機能
Disable	ログインの会計を使用不可にします。
List	ログイン用の AAA 構成パラメーターを表示します。
Set	ログイン用の AAA 構成パラメーターを設定します。

Disable

login disable コマンドは、会計を使用不可にするのに使用します。

構文:

login disable accounting

List

login list は、AAA 構成パラメーターを表示するのに使用します。

構文:

login list all
accounting
authentication
authorization
config

Set

login set コマンドは、認証パラメーターを構成するのに使用します。

構文:

login set aaa
accounting
authentication
authorization

aaa *authtype*

認証、許可、および会計タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)

認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)

認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id

リモート・データベースの識別子を指定します。

accounting *authtype*

会計タイプを設定します。*Authtype* は、次のどれか 1 つです。

リモート (remote)

認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id

リモート・データベースの識別子を指定します。

authentication *authtype*
認証タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authorization *authtype*
許可タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

Nets-info

nets-info コマンドは、各 PPP インターフェースに現在構成されている PPP 認証プロトコルを表示します。

構文:

nets-info

Password-rules

password-rules コマンドは、パスワードを構成する (使用可能または使用不可) のに使用します。

表32 は、**password-rules** コマンドと共に使用できるサブコマンドを示しています。

表 32. ログイン・サブコマンド

コマンド	機能
Disable	パスワード規則を使用不可にします。
Enable	パスワード規則を使用可能にします。
List	パスワード規則の現在の状態 (使用可能または使用不可) を表示します。

Disable

password-rules disable コマンドは、任意のまたはすべてのパスワード規則を使用不可にするのに使用します。

構文:

password-rules disable

all

compare-ident-prev

change-days

first-non-numeric

ident-chars

last-non-numeric

minimum-length

one-alpha

one-nonalpha

prev-three

userid-contained

compare-ident-prev

前のユーザー識別とパスワード変更を要求しているユーザーとを比較します。

change-days

パスワード変更が必要になる前の最大日数

有効値 : 0 〜 360

デフォルト値 : 180

first_non-numeric

パスワードの先頭文字で、数字は使えません。

有効値 : 任意の非数字

デフォルト値 : なし

ident-chars

前のパスワードの同じ位置に使用された文字が 3 字より多く含まれていてはなりません。

last-non-numeric

パスワードの最後の文字は数字であってはなりません。

有効値 : 任意の非数字

デフォルト値 : なし

minimum-length

有効なパスワードに必要な最小文字数

有効値 : 1 〜 31

デフォルト値 : 8

maximum-length

パスワードに含めることができる最大文字数

有効値 : 1 〜 31

デフォルト値 : 8

one-alpha
パスワードの少なくとも 1 文字は英字でなければなりません。

one-nonalpha
パスワードの少なくとも 1 文字は数字でなければなりません。

prev-three
パスワードは、最後の 3 つのパスワードのどれとも同じであってはなりません。

userid-contained
ユーザー ID をパスワードの一部として含めることはできません。

Enable

password-rules enable コマンドは、任意のまたはすべてのパスワード規則を使用可能にするのに使用します。パスワード規則についての説明は、**disable** コマンドを参照してください。

構文:

password-rules enable all
compare-ident-prev
change-days
first-non-numeric
ident-chars
last-non-numeric
minimum-length
one-alpha
one-nonalpha
prev-three
userid-contained

List

password-rules list コマンドは、パスワード規則の現在の状態 (使用不可または使用可能) を表示するのに使用します。

構文:

password-rules list

PPP

ppp コマンドは、PPP 用の AAA を構成するのに使用します。

表33 は、**ppp** コマンドと共に使用できるサブコマンドを示しています。

表 33. PPP サブコマンド

コマンド	機能
Disable	PPP の会計を使用不可にします。
List	PPP 用の AAA 構成パラメーターを表示します。

表 33. PPP サブコマンド (続き)

コマンド	機能
Set	PPP 用の AAA 構成パラメーターを設定します。

Disable

ppp disable コマンドは、PPP の会計を使用不可にするのに使用します。

構文:

ppp disable accounting

List

ppp list コマンドは、PPP 用の AAA 構成パラメーターを表示するのに使用します。

構文:

ppp list all
accounting
authentication
authorization
config

Set

ppp set コマンドは、PPP 用の AAA 構成パラメーターを表示するのに使用します。

構文:

ppp set aaa
accounting
authentication
authorization

aaa *authtype*
認証、許可、および会計タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

accounting *authtype*
会計タイプを設定します。*Authtype* は、次のどれか 1 つです。

リモート (remote)
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authentication *authtype*
認証タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authorization *authtype*
許可タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

Servers

servers コマンドは、個々のリモート AAA サーバーを構成するのに使用します。

表34 は、**servers** コマンドと共に使用できるサブコマンドを示しています。

表 34. サーバー・サブコマンド

コマンド	機能
Add	リモート AAA サーバー・プロファイルを追加します。
Change	リモート・サーバー・プロファイルを変更します。
Delete	リモート・サーバー・プロファイルを削除します。
Lists	AAA サーバー・プロファイル情報を表示します。

Add

servers add コマンドは、リモート・サーバー・プロファイルを追加するのに使用します。

構文:

servers add name

radius 認証タイプを、Radius 認証サーバー・プロトコルを使用するように設定します。

以下のパラメーターの値を設定できます。

accounting-level

記録する会計情報のレベルを指定する。より高いレベルは、それより低い値のレベルでリストされたすべての情報を記録します。

範囲: 0 〜 10

デフォルト値 : 0

>0 次の情報の記録:

- INBYTES_AH
- OUTBYTES_AH
- INBYTES_ESP
- OUTBYTES_ESP

>1 次の情報の記録:

- INPKTS_AH
- OUTPKTS_AH
- INPKTS_ESP
- OUTPKTS_ESP

>2 次の情報の記録:

- INBYTES_BAD
- OUTBYTES_BAD
- INPKTS_BAD
- OUTPKTS_BAD

>3 次の情報の記録:

- INPKTS_BAD_AH
- OUTPKTS_BAD_AH
- INPKTS_BAD_ESP
- OUTPKTS_BAD_ESP

>4 次の情報の記録:

- INPKTS_BAD_AH_RPLY
- INPKTS_BAD_ESP_RPLY

accounting-port

RADIUS サーバー会計ポートを指定します。

範囲: 1 〜 10000

デフォルト値: 1646

authentication-port

RADIUS サーバー認証ポートを指定します。

範囲: 1 〜 1000

デフォルト値: 1645

author-authent
認証時に許可属性を転送するかどうかを指定します。

有効値 : yes、no

デフォルト値 : yes

account-for-packets
会計停止でのパケット・カウントを送信するかどうかを指定します。

有効値 : yes、no

デフォルト値 : yes

key-for-encryption:
暗号化キーを指定します。

有効値 : 最大 32 字の長さの任意の英数字列

デフォルト値 : なし。

primary-server-address:
1 次認証サーバーのアドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

retries

有効値 : 1 ～ 100

デフォルト値 : 3

retry-interval

有効値 : 1 ～ 60

デフォルト値 : 3

secondary-server-address:
2 次認証サーバーのアドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

tacacs
認証タイプを、TACACS 認証サーバー・プロトコルを使用するように設定します。

以下のパラメーターの値を設定できます。

primary-server-address:
1 次認証サーバーのアドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

retries

有効値 : 1 ～ 100

デフォルト値 : 3

retry-interval

有効値 : 1 〜 60

デフォルト値 : 3

secondary-server-address:

2 次認証サーバーのアドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

tacacsplus

認証タイプを、TACACS+ 認証サーバー・プロトコルを使用するように設定します。

以下のパラメーターの値を設定できます。

encryption:

暗号化を使用するかどうかを指定します。

有効値 : yes、no

デフォルト値 :

key-for-encryption:

使用する暗号化キーを指定します。

有効値 : 任意の 16 進値

デフォルト値 :

primary-server-address:

1 次認証サーバーのアドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

privilege-level

有効値 : 0 〜 15

デフォルト値 : 0

restarts

リスタートの回数を設定します。このパラメーターには、タイムアウトによるリスタートは含まれず、サーバーによって要求されたリスタートだけを対象にしています。

有効値 : 0 〜 3200

デフォルト値 : 0

time-to-connect

サーバーから認証を得るために許容される時間数

有効値 : 1 〜 60

デフォルト値 : 9

secondary-server-address:

2 次認証サーバーのアドレスを指定します。

有効値 : 任意の有効な IP アドレス

デフォルト値 : 0.0.0.0

Change

servers change コマンドは、リモート・サーバー・プロファイルを変更するのに使用します。リモート・サーバー・プロファイルの説明は、**add** コマンドの項を参照してください。

構文:

servers change	radius
	tacacs
	tacacsplus

リモート・サーバー・プロファイルの説明は、**servers add** コマンドの項を参照してください。

Delete

servers delete コマンドは、リモート・サーバー・プロファイルを削除するのに使用します。リモート・サーバー・プロファイルの説明は、**add** コマンドの項を参照してください。

構文:

servers delete	radius
	tacacs
	tacacsplus

リモート・サーバー・プロファイルの説明は、**servers add** コマンドの項を参照してください。

List

servers list コマンドは、AAA サーバー・プロファイル情報を表示するのに使用します。

構文:

servers list	all
	names
	profile

Set

set コマンドは、ログイン、PPP、および L2TP トンネルのパラメーターを設定するのに使用します。

構文:

set	aaa
	accounting

authentication

authorization

aaa *authtype*
認証、許可、および会計タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

accounting *authtype*
ログイン、PPP、およびトンネルの会計タイプを設定します。*Authtype* は、次のどれか 1 つです。

options
会計オプションを入力できるようにします。

bytes バイト・レベルで会計を行うことを指定します。

incoming
着信バイト数の会計を行うことを指定します。

enable
指定したオプションの会計を使用可能にします。

使用不可 (disable)
指定したオプションの会計を使用不可にします。

outgoing
発信バイト数の会計を行うことを指定します。

enable
指定したオプションの会計を使用可能にします。

使用不可 (disable)
指定したオプションの会計を使用不可にします。

packets
パケット・レベルで会計を行うことを指定します。

incoming
着信パケット数の会計を行うことを指定します。

enable
指定したオプションの会計を使用可能にします。

使用不可 (disable)
指定したオプションの会計を使用不可にします。

outgoing
発信パケット数の会計を行うことを指定します。

enable
指定したオプションの会計を使用可能にします。

使用不可 (disable)
指定したオプションの会計を使用不可にします。

リモート (remote)
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authentication *authtype*
ログイン、PPP、およびトンネルの認証タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authorization *authtype*
ログイン、PPP、およびトンネルの許可タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

Tunnel

tunnel コマンドは、L2TP トンネル用の AAA を構成するのに使用します。

表35 は、**tunnel** コマンドと共に使用できるサブコマンドを示しています。

表 35. トンネル・サブコマンド

コマンド	機能
Disable	L2TP トンネルの会計を使用不可にします。
List	L2TP トンネル用の AAA 構成パラメーターを表示します。
Set	L2TP トンネル用の AAA 構成パラメーターを設定します。

Disable

tunnel disable コマンドは、L2TP トンネルの会計を使用不可にするのに使用します。

構文:

tunnel disable accounting

List

tunnel list コマンドは、L2TP トンネル用の AAA を表示するのに使用します。

構文:

tunnel list all
accounting
authentication
authorization
config

Set

tunnel set コマンドは、L2TP トンネル用の AAA 構成パラメーターを設定するのに使用します。

構文:

tunnel set aaa
accounting
authentication
authorization

aaa *authtype*

認証、許可、および会計タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)

認証、許可、および会計タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)

認証、許可、および会計タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id

リモート・データベースの識別子を指定します。

accounting *authtype*
会計タイプを設定します。*Authtype* は、次のどれか 1 つです。

リモート (remote)
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authentication *authtype*
認証タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
認証タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
認証タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

authorization *authtype*
許可タイプを設定します。*Authtype* は、次のどれか 1 つです。

ローカル (local)
許可タイプを、ローカルで維持されているユーザー・データベースを使用するように設定します。

リモート (remote)
許可タイプを、リモート・ユーザー・データベースを使用するように設定します。

server id
リモート・データベースの識別子を指定します。

User-profiles

user-profiles コマンドは、`User profile config>` コマンド・プロンプトにアクセスするのに使用します。このプロンプトから、次のコマンドにアクセスできます。

表 36. ユーザー・プロファイル構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add	PPP ユーザー・プロファイルを追加します。
Change	PPP ユーザー・プロファイルを変更します。
Delete	PPP ユーザー・プロファイルを削除します。
Disable	PPP ユーザー・プロファイルを使用不可にします。
Enable	PPP ユーザー・プロファイルを使用可能にします。
List	PPP ユーザー・プロファイル情報を表示します。
Report	PPP ユーザー・プロファイル・レポートを生成します。
Reset-user	PPP ユーザー・プロファイルをリセットします。

表 36. ユーザー・プロファイル構成コマンド (続き)

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

Add

user profiles add コマンドは、リモート・ルーターのユーザー・プロファイルをローカル PPP ユーザー・データベースに追加したり、IP ネットワークを通したルーターへのトンネル・ピア間アクセスを指定するのに使用します。

構文:

add ppp-user

tunnel

ppp-user

リモート・ルーターのユーザー・プロファイルを、ローカル PPP ユーザー・データベースに追加します。最大 500 のユーザーを追加できます。構成している装置に接続できる各リモート・ルーターまたは DIALS クライアントの PPP ユーザーを追加します。

コマンド構文およびオプションについては、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*の “CONFIG プロセス (CONFIG - Talk 6) およびコマンド” の章の Add の項を参照してください。

例:

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

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

User 'pppusr01' has been added
```

例:

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

                    PPP user name: tunusr01
```

```
                    Endpoint: 1.1.1.1
                            Hostname: host01

        User 'tunusr01' has been added
```

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

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

例:

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

       Tunnel name: tunnel02
          Endpoint: 2.2.2.22
```

Change

change コマンドは、ユーザー・プロファイルを変更するのに使用します。

構文:

change	ppp-user
	tunnel

Delete

delete コマンドは、ユーザー・プロファイルを削除するのに使用します。

構文:

delete	ppp-user
	tunnel

Disable

disable コマンドは、ユーザー・プロファイルを使用不可にするのに使用します。

構文:

disable	*name*

Enable

enable コマンドは、ユーザー・プロファイルを使用可能にするのに使用します。

構文:

enable	*name*

List

list コマンドは、ユーザー・プロファイル情報を表示するのに使用します。

構文:

list ppp-user

tunnel

```
User profile config> list ppp-user
List  (Name, Verb, User, Addr, Encr, zdump): [Verb]
     PPP user name: ppp01
            Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
1 record displayed.
```

List リスト情報にアクセスする方法を指定します。

有効値 : name、verb、user、addr、encr、zdump

デフォルト値 : verb

PPP user name
ユーザー名を表示します。

Expiry
有効期限を表示します。

User IP address
ユーザー IP アドレスを表示します。

Encryption
暗号化が使用可能か使用不可かを表示します。

Status
状態が使用可能か使用不可かを表示します。

Login attempts
ユーザーがログインを試行した回数を表示します。

Login failures
ログインに失敗した試行回数を表示します。

Report

report コマンドは、PPP ユーザー・プロファイル・レポートを生成するのに使用します。

構文:

report addresses

all

callback

dump

encrypt

name

password

time

user

```
User profile config> report addresses
PPP user name      User IP address
-----------------  ------------------
ppp01              Interface Default
1 record displayed.
User profile config> report all
     PPP user name: ppp01
             Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
            Status: Enabled
    Login Attempts: 0
    Login Failures: 0
1 record displayed.
User profile config> report callback
PPP user name      Callback type        Phone Number
-----------------  -------------------  --------------------
ppp01
1 record displayed.
User profile config> report dump
Enter user name:  []? user01
User profile config> report encrypt
PPP user name      Encryption
-----------------  ---------------
ppp01              Not Enabled
1 record displayed.
User profile config> report name
PPP user name
-----------------
ppp01
1 record displayed.
User profile config> report password
PPP user name      Expiry        Grace
-----------------  ------------  ------
ppp01              <unlimited>
1 record displayed.
User profile config> report time
PPP user name      Time allotted
-----------------  -------------------
ppp01
1 record displayed.
User profile config> report user
Enter user name:  []? login01
     PPP user name: login01
             Expiry: <unlimited>
   User IP address: Interface Default
        Encryption: Not Enabled
```

Reset-user

reset-user コマンドは、ユーザー・プロファイルをリセットするのに使用します。

構文:

reset-user *name*

認証 (AAA) 動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

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

GWCON (Talk 5) Activate Interface

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

GWCON (Talk 5) Reset Interface

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

CONFIG (Talk 6) 即時変更コマンド

AAA は、装置の操作状態を即時に変更する、次の CONFIG コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行する場合には、保管されて保存されます。

コマンド
CONFIG, add ppp-user
CONFIG, feature authentication, enable login-last-resort
CONFIG, feature authentication, disable login-last-resort **注:** 次に続くログインに有効です。
CONFIG, feature authentication, enable tech-support-bypass
CONFIG, feature authentication, disable tech-support-bypass **注:** 次に続くログインに有効です。
CONFIG, feature authentication, enable unauthent-accounting
CONFIG, feature authentication, disable unauthent-accounting

非動的再構成可能コマンド

次の表には、動的に変更できない AAA 構成コマンドを記載します。これらのコマンドを活動化するには、装置を再ロードしたり、リスタートする必要があります。

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

第17章 暗号化プロトコルの使用および構成

暗号化の目的は、プライバシーを保証するために、データを読み取り不能な形にして転送することです。***暗号化された*** データは、元のデータを入手するためには、暗号化解除する必要があります。

2216 は、次のものをサポートしています。

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

暗号化制御プロトコルを使用した PPP の暗号化

暗号化制御プロトコル (ECP) は、PPP プロトコルを使用したポイントツーポイント・リンク通信で、ルーターが暗号化の使用を交渉するのに使用します。暗号化制御プロトコルは、PPP リンク上で使用する暗号化および暗号化解除アルゴリズムをネゴシエーションするための汎用機構を提供します。PPP リンクの各方向でそれぞれ異なる暗号アルゴリズムを交渉することも可能です。

暗号化と暗号化解除の方式を***暗号アルゴリズム*** と言います。暗号アルゴリズムは、キーを使用して、暗号化と暗号化解除を制御します。圧縮とは異なり、ルーターはリンクの両方向で暗号化を行います。一方向だけの暗号化はセキュリティー上の危険があるからです。ECP が両方向の暗号アルゴリズムをネゴシエーションできない場合、リンクは終了します。

PPP の ECP 暗号化の構成

データ・リンク・レイヤーで暗号化を使用するように装置を構成するには、次の手順で行います。

1. リモート装置およびローカル PPP インターフェースの暗号化キーを設定する。

   リモート装置の暗号化キーは、`Config >` プロンプトで **add ppp-user** コマンドを使用して設定します。コマンド構文およびオプションについては、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の “CONFIG プロセスの構成” の章の **Add** コマンドの項を参照してください。

   ローカル PPP インターフェースの暗号化キーは、**enable ecp** コマンドを使用して設定します (*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の talk 6 `PPP Config>` **enable** コマンドの項を参照してください)。
2. `PPP Config>` プロンプトで **enable ecp** コマンドを使用して、個々の PPP リンクが暗号化制御プロトコル (ECP) を使用するように構成する。
3. PAP、CHAP、または SPAP を使用可能にする。

暗号化を使用不可にする、ユーザーの暗号化キーを変更する、暗号化の状態を表示する、あるいは暗号化を要求するときに装置が使用する名前を設定するといったことも可能です。詳しくは、次を参照してください。

- 暗号化を使用不可にする方法については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の PPP Config> **disable ecp** コマンドの項を参照してください。
- リモート・ユーザーの暗号化キーおよびパスワードを変更する方法については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の Config> **change ppp-user** コマンドの項を参照してください。
- 暗号化の状況をリストする方法については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の PPP Config> **list ecp** コマンドの項を参照してください。
- 装置の名前を設定する方法については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の PPP Config> **set name** コマンドの項を参照してください。

PPP の ECP 暗号化の監視

インターフェース上の各種の暗号化設定を監視するには、次のようにします。

1. **talk 5** コマンドを使用して、監視プロンプトにアクセスする。
2. **network** コマンドを使用して、監視したいインターフェースを選択する。このコマンドを入力すると、PPP n> プロンプトが表示されます。ここで、*n* は、ネットワーク番号を表します。 **network** コマンドの使用に関する手順については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*の 『ポイントツーポイント・プロトコル・インターフェースの構成および監視』の章を参照してください。

このプロンプトから、次のことが行えます。

- 暗号化の現行状態、最新の暗号化の交渉、暗号化状態変更以降の経過時間、および暗号化機能によって使用されているアルゴリズムをリストする。(*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*の **list control ecp** コマンドの項を参照してください。)
- インターフェースで送受信された暗号化制御パケットを表示する。(*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の **list ecp** コマンドの項を参照してください。)
- インターフェースで送信または受信された、暗号化されたデータ・パケットを表示する。(*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の **list edp** コマンドの項を参照してください。)

Microsoft ポイントツーポイント暗号化 (MPPE)

Microsoft ポイントツーポイント暗号化 (MPPE) は、Microsoft ダイヤルアップ・ネットワーキング (DUN) クライアントと呼ばれる Windows ワークステーションが、それ自体と 2216 の間で PPP リンクを介して転送するデータを暗号化する手段を提供します。MPPE は、ルーターからルーターへ PPP リンクを介して転送されるデータを暗号化するのにも使用できます。MPPE は常に両方向でネゴシエーションされます。

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

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

MPPE の構成

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

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

MPPE を使用不可にしたり、MPPE オプションを表示することもできます。

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

MPPE の監視

298ページの『PPP の ECP 暗号化の監視』の説明に従って、`PPP>` プロンプトを立ち上げます。MPPE データ統計を見るには **list mppe** コマンドを使用し、MPPE 状況を見るには **list control ccp** コマンドを使用します。これらのコマンドの出力の例は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の 『ポイントツーポイント・プロトコル・インターフェースの構成および監視』 の章に示されています。

フレーム・リレー・インターフェース上の暗号化の構成

注: フレーム・リレーは、専有の暗号化方式を使用します。

データ暗号化は、暗号化が使用可能にされているすべてのインターフェースでサポートされます。暗号化が使用可能にされているインターフェース上の個々の回線を、必要に応じて、暗号化を実行する、または実行しないとして個別に構成することができます。

フレーム・リレー・リンク上で暗号化を使用するように装置を構成するには、以下の手順で行います。

1. **talk 6** コマンドを使用して、フレーム・リレー構成プロンプトにアクセスする。
2. **net** # コマンドを使用して、暗号化を可能にしたいフレーム・リレー・インターフェースを選択する。
3. **enable encryption** コマンドを使用して、フレーム・リレー・インターフェース上の暗号化を使用可能にする。 *Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*の「フレーム・リレー構成コマンド」の項を参照してください。
4. **add permanent-virtual-circuit** コマンドを使用して、暗号化が可能なパーマネント・バーチャル・サーキットを追加し、各 PVC ごとに暗号化キーを定義する。*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*の「フレーム・リレー構成コマンド」の項を参照してください。
5. 構成する各暗号化可能インターフェースごとに、ステップ 1 〜 4 を繰り返す。

注: FR パーマネント・バーチャル・サーキットの暗号化が使用可能にされている場合、バーチャル・サーキットの反対側の装置との暗号化のネゴシエーションが正常に行われない限り、データは回線上に流れません。暗号化キーを入力するためには PVC を構成する必要があるので、暗号化は孤立回線に対してはサポートされません。

インターフェースの暗号化を使用不可にする、PVC の暗号化の設定値を変更する、あるいは暗号化の状態を表示することもできます。詳しくは、次の個所を参照してください。

- インターフェースの暗号化を使用不可にする場合は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* のフレーム・リレー構成 **disable encryption** コマンドの項を参照してください。
- PVC の暗号化の設定を変更する場合は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引きの* フレーム・リレー構成 **change permanent-virtual-circuit** コマンドの項を参照してください。
- 暗号化の状態をリストする場合は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き の* フレーム・リレー構成 **list all**、**list lmi**、および **list permanent-virtual-circuit** コマンドの項を参照してください。

フレーム・リレー・インターフェース上の暗号化の監視

インターフェース上の各種の暗号化設定を監視するには、次のようにします。

1. **talk 5** コマンドを使用して、監視プロンプトにアクセスする。

2. **network** # コマンドを使用して、監視したいインターフェースを選択する。このコマンドを使用すると、FR *x*> プロンプトが表示されます。

このプロンプトから、インターフェース、PVC、または回線の暗号化の現行状態をリストすることができます。*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*のフレーム・リレー監視 **list** コマンドの項を参照してください。

第18章 サービス品質 (QoS) の構成と監視

この章では、装置内の LAN および ELAN インターフェースのサービス品質 (QoS) の構成コマンドおよびオペレーショナル・コマンドについて説明します。この章には、次の内容が記載されています。

サービス品質 (QoS) の概説

この QoS フィーチャーは、LAN エミュレーションのデータ・ダイレクト VCC の ATM QoS 機能の利点を活用したものです。このサポートは『LAN エミュレーションの構成可能 QoS』と呼ばれています。このフィーチャーの主要な属性と利点は、次のとおりです。

- LE クライアントは、そのデータ・ダイレクト VCC 用に構成された QoS パラメーターを使用します。
- QoS パラメーターは、次のように構成することができます。
  - LE クライアント
  - ATM インターフェース
- 構成された QoS パラメーター・セットは、ATM フォーラム UNI 3.0/3.1 信号に使用されます。これらのパラメーターには、ピーク・セル速度、持続セル速度、QoS クラス、および最大バースト・サイズが含まれます。
- LE クライアントが、サポートできないトラフィック・パラメーターをもつ VCC を受け入れる / 確立するのを防止するために、VCC 当りの最大予約帯域幅を構成することができます。
- QoS ネゴシエーション・メカニズムにより、参加している LE クライアントは相互の QoS パラメーターを知ることができます。データ・ダイレクト VCC は、ネゴシエーションされたパラメーターを使用して設定されます。

QoS の利点

- LE クライアント、ATM インターフェース、またはエミュレートされた LAN に対して QoS を使用すると、LANE データ・ダイレクト VCC は、次のような利点が得られます。
  - ある LE クライアントに必要な QoS が、ELAN 上の他のクライアントに必要な QoS と異なっている場合、その LE クライアントに QoS を構成することができます。たとえば、LE クライアントがファイル・サーバーとして作動し

ている場合、ファイル・サーバーとの間でやり取りされるすべてのトラフィックに対して適切な QoS パラメーターを構成したい場合があります。

– エミュレートされた LAN 内のすべてのトラフィックに適用する QoS を指定したい場合は、その ELAN に QoS を構成することができます。たとえば、SNA トラフィックを伝送する ELAN に対して QoS パラメーターを構成することによって、その ELAN に優先順位を与えるとことができます。

– ある ATM インターフェース上のすべての LE クライアントが同一の 1 組のパラメーターを使用するようにしたい場合、その ATM インターフェースに QoS を構成することができます。たとえば、ある ATM インターフェースが 25 Mbps で接続されている場合、155-Mbps インターフェースとは異なる適切なパラメーターを構成できます。

QoS 構成パラメーター

ここでは、QoS の構成に使用される 9 つのパラメーターについて説明します。次の 6 つのパラメーターは、LE クライアント、ATM インターフェース、およびエミュレートされた LAN に対して構成することができます。

1. max-reserved-bandwidth
2. traffic-type
3. peak-cell-rate
4. sustained-cell-rate
5. max-burst-size
6. qos-class

次の 2 つのパラメーターは、エミュレートされた LAN および LE クライアントに対して構成することができます。

1. *validate-pcr-of-best-effort-vccs*
2. *negotiate-qos*

accept-qos-parms-from-lecs パラメーターは、LE クライアントに対してだけ構成できます。

最初の 6 つのパラメーターは、LE クライアントによって確立されるデータ・ダイレクト VCC のトラフィック特性を制御します。最初のパラメーターは LE クライアントが受信したコールにも適用されます。次の特性は、LE クライアントによって確立されるすべてのデータ・ダイレクト VCC に関連するものです。

- ベストエフォート・トラフィック用の帯域幅は予約されません。
- トラフィック・パラメーターは順方向と逆方向の両方に適用されます。
- 予約帯域幅接続がトラフィック・パラメーターまたは QoS クラスが原因でリジェクトされた場合、そのコールは、構成されたピーク・セル速度を使用して、ベストエフォート・コネクションとして再試行されます (VCC が解放された理由は、解放時の原因コードまたは復旧完了メッセージを使用して判別します) 。
- best-effort 接続がピーク・セル速度が原因でリジェクトされた場合、そのコールは、より低い PCR を使用して自動的に再試行されることがあります。再試行は、次の条件下で行われます。

1. リジェクトされた PCR が 100 Mbps を超えている場合、コールは 100 Mbps の PCR で再試行されます。
2. そうでない場合、リジェクトされた PCR が 25 Mbps を超えている場合には、コールは 25 Mbps の PCR で再試行されます。

最大予約帯域幅 (max-reserved-bandwidth)

データ・ダイレクト VCC に対して許容される最大予約帯域幅。このパラメーターは、LE クライアントが受信するデータ・ダイレクト VCC のコールと、LE クライアントが発信するデータ・ダイレクト VCC のコールの両方に適用されます。着信コールの場合、このパラメーターはデータ・ダイレクト VCC の最大許容 SCR を定義します。着信コールに SCR が指定されていない場合には、このパラメーターは予約帯域幅をもつデータ・ダイレクト VCC の最大許容 PCR を定義します。

受信したコールのトラフィック・パラメーターがこれより高い速度に指定されている場合、そのコールは解放されます。着信コールに SCR が指定されている場合、そのコールは PCR または最大バースト・サイズが原因でリジェクトされることはありません。このパラメーターによる制約は BEST_EFFORT 接続には適用されません。発信コールの場合、このパラメーターは、データ・ダイレクト VCC 用に要求できる予約帯域幅の上限を設定します。したがって、トラフィック・タイプ (traffic-type) および持続セル速度 (sustained-cell-rate) パラメーターは、このパラメーターに依存します。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

0

トラフィック・タイプ (traffic-type)

データ・ダイレクト VCC のトラフィック・タイプ。QoS パラメーターがネゴシエーションされない場合、このパラメーターは LE クライアントからの発信コールのタイプを指定します。QoS パラメーターがネゴシエーションされる場合には、このパラメーターは、データ・ダイレクト VCC のトラフィック特性を指定します。QoS パラメーターがネゴシエーションされるときには、発信元またはターゲット LEC のどちらかの LEC が予約帯域幅接続を望み、両方の LEC が予約帯域幅接続をサポートしている場合 (つまり、max-reserved-bandwidth > 0) には、2 つの LEC 間で予約帯域幅データ・ダイレクト VCC の確立が試みられます。そうでない場合は、データ・ダイレクト VCC は best-effort 続になります。依存関係: 最大予約帯域幅 (max-reserved-bandwidth)

有効値:

best_effort または reserved_bandwidth

デフォルト値:

best_effort

ピーク・セル速度 (peak-cell-rate)

データ・ダイレクト VCC のピーク・セル速度。QoS パラメーターがネゴシエーションされない場合、このパラメーターは LE クライアントが発信するデータ・ダイレクト VCC のコールの PCR トラフィック・パラメーターを指定します。QoS パ

ラメーターがネゴシエーションされる場合には、このパラメーターは、データ・ダイレクト VCC の PCR トラフィック・パラメーターを指定します。ネゴシエーションされたベストエフォート VCC では、 2 つの LEC の PCR の最小値が使用されます。

予約帯域幅がネゴシエーションされ、一方の LE クライアントだけが予約帯域幅接続を要求している場合、その LEC の PCR がデータ・ダイレクト VCC に使用され、ローカル ATM 装置の回線速度による上限が適用されます。両方の LE クライアントだけが予約帯域幅接続を要求している場合には、LE クライアント の PCR の最大値がデータ・ダイレクト VCC に使用され、ローカル ATM 装置の回線速度による上限が適用されます。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

LEC ATM 装置の回線速度 (Kbps)

持続セル速度 (sustained-cell-rate)

データ・ダイレクト VCC の持続セル速度。QoS パラメーターがネゴシエーションされない場合、このパラメーターは LE クライアントが発信するデータ・ダイレクト VCC のコールの SCR トラフィック・パラメーターを指定します。QoS パラメーターがネゴシエーションされる場合は、このパラメーターは、データ・ダイレクト VCC の SCR トラフィック・パラメーターを指定します。

予約帯域幅がネゴシエーションされ、一方の LE クライアントだけが予約帯域幅接続を要求している場合、その LEC の SCR がデータ・ダイレクト VCC に使用されます (他方の LEC の max-reserved-bandwidth パラメーターによる上限が適用されます)。両方の LE クライアントが予約帯域幅接続を要求している場合には、LE クライアントの SCR の最大値がデータ・ダイレクト VCC に使用されます (両方の LEC の max-reserved-bandwidth パラメーターによる上限が適用されます)。どちらの場合も (ネゴシエーションまたは非ネゴシエーション)、シグナルされる SCR がシグナルされる PCR に等しい場合には、コールは PCR だけを用いてシグナルされます。

依存関係: 最大予約帯域幅 (max-reserved-bandwidth)、トラフィック・タイプ (traffic-type)、およびピーク・セル速度 (peak-cell-rate)。このパラメーターは、トラフィック・タイプが RESERVED_BANDWIDTH の場合にだけ適用されます。

有効値:

0 から最大予約帯域幅とピーク・セル速度の最小値までの範囲内の整数値 (Kbps)

デフォルト値

なし

最大バースト・サイズ (max-burst-size)

データ・ダイレクト VCC の最大バースト・サイズ。QoS パラメーターがネゴシエーションされない場合、このパラメーターは LE クライアントが発信するデータ・ダイレクト VCC のコールの「最大バースト・サイズ」トラフィック・パラメータ

ーを指定します。QoS パラメーターがネゴシエーションされる場合には、このパラメーターは、データ・ダイレクト VCC の「最大バースト・サイズ」トラフィック・パラメーターを指定します。

予約帯域幅がネゴシエーションされ、一方の LE クライアントだけが予約帯域幅接続を要求している場合、その LEC の「最大バースト・サイズ」がデータ・ダイレクト VCC に使用されます。両方の LE クライアントが予約帯域幅接続を要求している場合には、LE クライアントの「最大バースト・サイズ」の最大値が、データ・ダイレクト VCC に使用されます。

どちらの場合も (ネゴシエーションまたは非ネゴシエーション)、SCR がシグナルされる場合にだけ、最大バースト・サイズがシグナルされます。このパラメーターはセル単位で表し、最大データ・フレーム・サイズ (LEC の C3 パラメーターで指定) の整数倍として構成しますが、1 が下限です。

依存関係: このパラメーターは、トラフィック・タイプが RESERVED_BANDWIDTH の場合にだけ適用されます。

有効値:
整数のフレーム数。0 より大きいことが必要です。

デフォルト値:
1 フレーム

QoS クラス (qos-class)

予約帯域幅のコールの QoS クラス。QoS パラメーターがネゴシエーションされない場合、このパラメーターは LE クライアントが発信する予約帯域幅データ・ダイレクト VCC のコールに使用される QoS クラスを指定します。QoS パラメーターがネゴシエーションされる場合には、このパラメーターは、データ・ダイレクト VCC の QoS クラスを指定します。QoS クラスが未指定の場合は、常にベストエフォート・コールが使用されます。 指定された QoS クラスは、セル損失比率やセル転送遅延など、ATM 性能パラメーターの目標値を定 義します。

UNI 仕様には、次のように記述されています。

指定 QoS クラス 1
現行のディジタル専用回線の効率に匹敵する効率を生成する必要がある。

指定 QoS クラス 2
電話会議およびマルチメディア・アプリケーションにおけるパケット化ビデオおよびオーディオ用

指定 QoS クラス 3
接続型プロトコル (フレーム・リレーなど) のインターオペレーションが目的

指定 QoS クラス 4
非接続型プロトコル (IP または SMDS など) のインターオペレーションが目的

LEC は、上記のすべての QoS クラスのコールを受け入れることができる必要があります。QoS パラメーターがネゴシエーションされる場合、2 つの LEC に構成されている QoS クラスが比較され、要件が厳しい方の QoS クラスが適用されます。

有効値:

0: 未指定 QoS クラスの場合

1: 指定 QoS クラス 1 の場合

2: 指定 QoS クラス 2 の場合

3: 指定 QoS クラス 3 の場合

4: 指定 QoS クラス 4 の場合

デフォルト値:

0 (未指定 QoS クラス)

ベストエフォート VCC の PCR の検証 (validate-pcr-of-best-effort-vccs)

ベストエフォート VCC のピーク・セル速度を検証するのに使用します。FALSE の場合、シグナルされた順方向 PCR に関係なく、ベストエフォート VCC は受け入れられます。TRUE の場合、シグナルされた順方向 PCR が、LE クライアント ATM 装置の回線速度を超えている場合、ベストエフォート VCC はリジェクトされます。逆方向 PCR が原因でコールがリジェクトされることはありません。シグナルされた逆方向 PCR は、回線速度を超えていない場合は、受け入れられます。そうでない場合は、コール側への伝送は回線速度で行われます。

注:

1. 順方向 PCR が回線速度を超えている ベストエフォート VCC を受け入れると、過度の再送のために性能が低下する可能性があります。しかし、このような VCC をリジェクトすると、インターオペラビリティーに問題が生じる可能性があります。
2. 利用不能な回線速度が原因でコールがリジェクトされたときに、コール側がより低速の PCR を用いて再試行する場合は、yes に設定しておくと便利です。

有効値:

yes、no

デフォルト値:

no

QoS ネゴシエーション (negotiate-qos)

データ・ダイレクト VCC の QoS パラメーターのネゴシエーションを使用可能にします。このパラメーターを使用可能にするのは、IBM MSS LES に接続する場合に限ります。このパラメーターを yes に設定すると、LE クライアントは、IBM トラフィック・パラメーター TLV を、LES に送信する LE_JOIN_REQUEST および LE_ARP_RESPONSE フレームに組み込みます。この TLV には、最大予約帯域幅、トラフィック・タイプ、ピーク・セル速度、持続セル速度、最大バースト・サイズ、および QoS クラスの値が含まれます。IBM トラフィック・パラメーター TLV は、LES が LE クライアントに戻す LE_ARP_RESPONSE にも組み込まれることがあります。

LE クライアントが受信した LE_ARP_RESPONSE に TLV が含まれていない場合は、ローカル構成パラメーターを使用してデータ・ダイレクト VCC を設定する必要があります。LE_ARP_RESPONSE に TLV が含まれている場合、LE クライアントは、データ・ダイレクト VCC をシグナルする前に、TLV の内容を対応するロー

カル値と比較して、両方のパーティーに受け入れられる『ネゴシエーションされた』または『最善の』パラメーター・セットを判別することが必要です。

有効値:

yes、no

デフォルト値:

no

LECS からの QoS パラメーター受け入れ (accept-qos-parms-from-lecs)

このパラメーターは、LE クライアントが LECS からの QoS パラメーターを受け入れ/リジェクトするように構成することができます。このパラメーターが yes の場合、LE クライアントは、LE_CONFIGURE_RESPONSE フレーム内の LE クライアントから入手した QoS パラメーターを使用することが必要です。つまり、LE クライアントからの QoS パラメーターが、ローカル構成 QoS パラメーターを上書きします。このパラメーターが no の場合、LE クライアントは、LE クライアントからの LE_CONFIGURE_RESPONSE フレームで受信した QoS パラメーターを無視します。

有効値:

yes、no

デフォルト値:

no

QoS 構成プロンプトへのアクセス

サービス品質 (QoS) 構成コマンドにアクセスするには、CONFIG プロセスから **feature** コマンドを入力します。**feature** と入力し、その後にフィーチャー番号 (6) または短縮名 (QOS) を入力します。たとえば、次のようになります。

```
Config> feature qos
Quality of Service - Configuration
QoS Config>
```

QoS Config> プロンプトにアクセスすると、LE クライアント、または ATM インターフェースのサービス品質 (QoS) を構成することができます。QoS Config> プロンプトで **exit** コマンドを入力すれば、いつでも Config> プロンプトに戻ることができます。

あるいは、次のようにエンティティーにアクセスすることにより、LE クライアント、または ATM インターフェースの QoS パラメーターを構成することもできます。

- LE クライアント
  1. Config> プロンプトで、**network** コマンドと LE クライアント・インターフェース番号を入力する。
  2. LE Client configuration> プロンプトで、**qos-configuration** と入力する。

     例:

     ```
     config> network 3
     Token Ring Forum Compliant LEC Config> qos-configuration
     LEC QoS Config>
     ```
- ATM インターフェース

サービス品質 (QoS) の構成

1. Config> プロンプトで、**network** コマンドと ATM インターフェース番号を入力して、ATM Config> プロンプトを表示する。
2. **interface** パラメーターを入力して、ATM Interface Config> プロンプトを表示する。
3. ATM InterfaceConfig> プロンプトで、**qos-configuration** と入力する。

   例:

```
config> network 0
ATM Config> interface
ATM Interface Config> qos-configuration
ATM-I/F 0 QoS>
```

サービス品質 (QoS) コマンド

ここでは、QoS 構成コマンドの要約を示します。次のコマンドを使用して、サービス品質 (QoS) を構成します。コマンドは QoS Config> プロンプトから入力します。

表 37. サービス品質 (QoS) 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
le-client	選択された LE クライアントの LE Client QoS configuration > プロンプトを表示します。
atm-interface	選択された ATM インターフェースの ATM Interface QoS configuration> プロンプトを表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

LE クライアント QoS 構成コマンド

ここでは、特定の LE クライアントの QoS を構成するためのコマンドの要約を示し、個々のコマンドについて説明します。

次のコマンドは LEC QoS config> プロンプトで使用します。

表 38. LE クライアントのサービス品質 (QoS) 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
List	LE クライアントの現行 QoS 構成を表示します。
Set	LE クライアントの QoS パラメーターを設定します。
Remove	LE クライアントの QoS 構成を除去します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

List

list コマンドは、この LE クライアントの QoS 構成を表示するのに使用します。QoS パラメーターは、少なくとも 1 つのパラメーターが特別に構成されている場合にだけ表示されます (例 1 を参照)。そうでない場合には、パラメーターは表示されません (例 2 を参照)。

構文:

list

例 1:

```
LEC QoS Config> list

           LE Client QoS Configuration for Data Direct VCCs
           ========================================
     (ATM interface number = 36,  LEC interface number = 40)

  Maximum Reserved Bandwidth for a Data-Direct VCC = 10000 Kbps
  Data-Direct VCC Type ........................... = Best-Effort
  Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
  Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
  Desired QoS Class of Reserved Connections ...... = 0
  Max Burst Size of Reserved Connections    ...... = 0 frames

  Validate Peak Rate of Best-Effort connections .. = No
  Enable QoS Parameter Negotiation ............... = Yes
  Accept QoS Parameters from LECS ................ = Yes

LEC QoS Config>
```

例 2:

```
LEC QoS Config> list

   QoS has not been configured for this LEC.
   Please use the SET option to configure QoS.

LEC QoS Config>
```

Set

set コマンドは、LE クライアントの QoS パラメーターを指定するのに使用します。

構文:

set accept-qos-parms-from-lecs
all-default-values
max-burst-size
max-reserved-bandwidth
negotiate-qos
peak-cell-rate
qos-class
sustained-cell-rate
traffic-type
validate-pcr-of-best-effort-vccs

accept-qos-parms-from-lecs

このオプションは、LE クライアントが LECS から TLV として受信した QoS パラメーターの受け入れ / リジェクトを使用可能 / 使用不可にするのに使用します。このパラメーターの詳しい説明は、309ページの『LECS からの QoS パラメーター受け入れ (accept-qos-parms-from-lecs)』を参照してください。

有効値:

yes、no

デフォルト値:

yes

例:

```
LEC QoS Config> se acc y
LEC QoS Config>
```

all-default-values

このオプションは、QoS パラメーターをデフォルト値に設定するのに使用します。下記の例には、デフォルト値も示されています。

例:

```
LEC QoS Config> set all-default-values
   Failed to locate existing QoS configuration record!
   Using a new set of default values ...
   Initializing all parameters to default values
   LEC QoS Config>  list

              LE Client QoS Configuration for Data Direct VCCs
              ========================================
         (ATM interface number = 0,  LEC interface number = 3)

     Maximum Reserved Bandwidth for a Data-Direct VCC = 0 Kbps
     Data-Direct VCC Type ........................... = Best-Effort
     Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
     Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
     Desired QoS Class of Reserved Connections ...... = 0
     Max Burst Size of Reserved Connections    ...... = 0 frames

     Validate Peak Rate of Best-Effort connections .. = No
     Enable QoS Parameter Negotiation ............... = No
     Accept QoS Parameters from LECS ................ = Yes

   LEC QoS Config>
```

max-burst-size

フレームの最大バースト・サイズを設定します。このパラメーターの詳しい説明は、306ページの『最大バースト・サイズ (max-burst-size)』を参照してください。

有効値:

整数のフレーム数。0 より大きいことが必要です。

デフォルト値:

1 フレーム

例:

```
 LEC QoS Config>  se ma
   Maximum Burst Size in Kbps [1]? 10000
   LEC QoS Config>
```

max-reserved-bandwidth

このオプションは、各データ・ダイレクト VCC に許容される最大予約帯域幅を設定するのに使用します。このパラメーターの詳しい説明は、305ページの『最大予約帯域幅 (max-reserved-bandwidth)』を参照してください。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

0

例:

```
LEC QoS Config> set max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]? 20000
LEC QoS Config>
```

negotiate-qos

このオプションは、QoS 交渉への LE クライアントの参加を使用可能/使用不可にするのに使用します。このパラメーターの詳しい説明は、308ページの『QoS ネゴシエーション (negotiate-qos)』を参照してください。

有効値:

yes、no

デフォルト値:

no

例:

```
LEC QoS Config> se neg y
LEC QoS Config>
```

peak-cell-rate

データ・ダイレクトのピーク・セル速度を設定します。このパラメーターの詳しい説明は、305ページの『ピーク・セル速度 (peak-cell-rate)』を参照してください。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

LEC ATM 装置の回線速度 (Kbps)

例:

```
LEC QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
LEC QoS Config>
```

qos-class

データ・ダイレクト VCC の QoS クラスを設定します。このパラメーターの詳しい説明は、307ページの『QoS クラス (qos-class)』を参照してください。

有効値:

0: 未指定 QoS クラスの場合

1: 指定 QoS クラス 1 の場合

2: 指定 QoS クラス 2 の場合

3: 指定 QoS クラス 3 の場合

4: 指定 QoS クラス 4 の場合

デフォルト値:

0 (未指定 QoS クラス)

例:

```
LEC QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
LEC QoS Config>
```

sustained-cell-rate

データ・ダイレクト VCC の持続セル速度を設定します。このパラメーターの詳しい説明は、306ページの『持続セル速度 (sustained-cell-rate)』を参照してください。

有効値:

0 から最大予約帯域幅とピーク・セル速度の最小値までの範囲内の整数値 (Kbps)

デフォルト値

なし

例:

```
LEC QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
LEC QoS Config>
```

traffic-type

データ・ダイレクト VCC のトラフィックを設定します。このパラメーターの詳しい説明は、305ページの『トラフィック・タイプ (traffic-type)』を参照してください。

有効値:

best effort または reserved bandwidth

デフォルト値:

best effort

例:

```
LEC QoS Config>set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved-Bandwidth
Data Direct VCC Type [0]? 1
Note: Peak Cell Rate has been reset to 1
      Sustained Cell Rate has been reset to 1
      Max Reserved Bandwidth has been reset to 1
      Please configure appropriate values.
LEC QoS Config>
```

validate-pcr-of-best-effort-vccs

このオプションは、この LE クライアントが受信したデータ・ダイレクト VCC のコールの「ピーク・セル速度」トラフィック・パラメーターを使用可能/使用不可にするのに使用します。このパラメーターの詳しい説明は、308ページの『ベストエフォート VCC の PCR の検証 (validate-pcr-of-best-effort-vccs)』を参照してください。

有効値:

yes、no

デフォルト値:

no

例:

```
LEC QoS Config> se val y
LEC QoS Config>
```

Remove

remove コマンドは、この LE クライアントの QoS 構成を除去するのに使用します。

構文:

remove

例:

```
LEC QoS Config> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the LEC QoS configuration be deleted? [No]: yes
Deleted QoS configuration successfully
LEC QoS Config>
```

ATM インターフェース QoS 構成コマンド

表 39. LE クライアントのサービス品質 (QoS) 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
List	現行の ATM インターフェース QoS 構成を表示します。
Set	ATM インターフェース QoS パラメーターを設定します。
Remove	ATM インターフェースの QoS 構成を除去します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

List

list コマンドは、この ATM インターフェースの QoS 構成を表示するのに使用します。QoS パラメーターは、少なくとも 1 つのパラメーターが構成されている場合にだけ表示されます (下の例を参照)。そうでない場合には、パラメーターは表示されません。

構文:

list

例:

```
ATM-I/F 0 QoS> list

          ATM Interface 'Quality of Service' Configuration
          ================================================
                    (ATM interface number = 0  )

     Maximum Reserved Bandwidth for a VCC = 15000 Kbps
     VCC Type ........................... = RESERVED-BANDWIDTH
     Peak Cell Rate ..................... = 20000 Kbps
     Sustained Cell Rate ................ = 5000 Kbps
     QoS Class .......................... = 4
     Maximum Burst Size ................. = 5 frames
   ATM-I/F 0 QoS>
```

Set

set コマンドは、ATM クライアントの QoS パラメーターを指定するのに使用します。

構文:

set max-burst-size
max-reserved-bandwidth
peak-cell-rate
qos-class
sustained-cell-rate
traffic-type

max-burst-size

フレームの最大バースト・サイズを設定します。このパラメーターの詳しい説明は、306ページの『最大バースト・サイズ (max-burst-size)』を参照してください。

有効値:

整数のフレーム数。0 より大きいことが必要です。

デフォルト値:

1 フレーム

例:

```
ATM-I/F 0 QoS Config> se ma
Maximum Burst Size in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

max-reserved-bandwidth

このオプションは、各データ・ダイレクト VCC に許容される最大予約帯域幅を設定するのに使用します。このパラメーターの詳しい説明は、305ページの『最大予約帯域幅 (max-reserved-bandwidth)』を参照してください。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

0

例:

```
ATM-I/F 0 QoS> se max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]?
15000
ATM-I/F 0 QoS>
```

peak-cell-rate

データ・ダイレクト VCC のピーク・セル速度を設定します。このパラメーターの詳しい説明は、305ページの『ピーク・セル速度 (peak-cell-rate)』を参照してください。

有効値:

0 ～ ATM 装置の回線速度の範囲の整数値 (Kbps)

デフォルト値:

LEC ATM 装置の回線速度 (Kbps)

例:

```
ATM-I/F 0 QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
ATM-I/F 0 QoS Config>
```

qos-class

データ・ダイレクト VCC の QoS クラスを設定します。このパラメーターの詳しい説明は、307ページの『QoS クラス (qos-class)』を参照してください。

有効値:

0: 未指定 QoS クラスの場合

1: 指定 QoS クラス 1 の場合

2: 指定 QoS クラス 2 の場合

3: 指定 QoS クラス 3 の場合

4: 指定 QoS クラス 4 の場合

デフォルト値:

0 (未指定 QoS クラス)

例:

```
ATM-I/F 0 QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]?  1
ATM-I/F 0 QoS Config>
```

sustained-cell-rate

データ・ダイレクト VCC の持続セル速度を設定します。このパラメーターの詳しい説明は、306ページの『持続セル速度 (sustained-cell-rate)』を参照してください。

有効値:

0 から最大予約帯域幅とピーク・セル速度の最小値までの範囲内の整数値 (Kbps)

デフォルト値

なし

例:

```
ATM-I/F 0 QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

traffic-type

データ・ダイレクト VCC のトラフィックを設定します。このパラメーターの詳しい説明は、305ページの『トラフィック・タイプ (traffic-type)』を参照してください。

有効値:

best_effort または reserved_bandwidth

デフォルト値:

best_effort

例:

```
ATM-I/F 0 QoS> set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved Bandwidth
Traffic Type of VCCs [1]? 0
ATM-I/F 0 QoS>
```

Remove

remove コマンドは、この ATM インターフェースの QoS 構成を除去するのに使用します。

構文:

remove

例:

```
ATM-I/F 0 QoS> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the ATM Interface QoS configuration be deleted? [No]: yes
Deleted QoS SRAM record successfully
ATM-I/F 0 QoS>
```

QoS 監視コマンドへのアクセス

サービス品質コマンドにアクセスするには、GWCON プロセスから **feature** コマンドを入力します。**feature** と入力し、その後にフィーチャー番号 (6) または短縮名 (QOS) を入力します。たとえば、次のようになります。

```
+feature qos
Quality of Service (QoS) - User Monitoring
QoS+
```

QoS 監視プロンプトにアクセスしたら、特定の LE クライアントを監視することを選択できます。QoS 監視プロンプトで exit コマンドを入力すれば、いつでも GWCON プロンプトに戻ることができます。

あるいは、次のようにして、LE クライアントの QoS 監視にアクセスすることもできます。

1. GWCON プロンプト (+) で、network コマンドと LE クライアントのインターフェース番号を入力する。
2. LE クライアント監視プロンプトで、**qos-information** と入力する。

   例:

```
+network 3
ATM Emulated LAN Monitoring
LEC+qos information
LE Client QoS Monitoring
LEC 3 QoS+
```

サービス品質監視コマンド

ここでは、QoS 監視コマンドの要約を示します。これらのコマンドは QoS+ プロンプトで入力します。

表 40. サービス品質 (QoS) 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
le-client	選択された LE クライアントの LE Client QoS console + プロンプトを表示します。

表 40. サービス品質 (QoS) 監視コマンドの要約 (続き)

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

LE クライアント QoS 監視コマンド

ここでは、LE クライアント QoS 監視コマンドの要約を示します。コマンドは LEC num QoS+ プロンプトから入力します。

表 41. LE クライアント QoS 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
List	現行の LE クライアント QoS 情報を表示します。オプションには、構成パラメーター、TLV、VCC、および統計が含まれます。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

List

list コマンドは、この LE クライアントの QoS 関連情報を表示するのに使用します。

構文:

list configuration-parameters
data-direct-VCCs (Detailed Information)
statistics
tlv-information
vcc-information

configuration-parameters

QoS 構成パラメーターを表示します。パラメーターは、LE クライアント、ATM インターフェース、または ELAN に対して構成できるので、これらのパラメーターは LE クライアントが使用する解決済みパラメーター・セットとともに表示されます。

le-client

SRAM レコードから入手された、この LE クライアントに構成されているパラメーター。SRAM レコードに無効なパラメーター・セットが入っている場合、この欄にはパラメーター値は表示されません。

ATM Interface

この LE クライアントが使用する ATM インターフェースに構成されているパラメーター。これらのパラメーターは、ローカル SRAM レコードから入手されます。SRAM レコードに無効なパラメーター・セットが入っている場合、この欄にはパラメーター値は表示されません。

From LECS
この LE クライアントが LE 構成サーバーから受信したパラメーター。パラメーターは、LE_CONFIGURE_RESPONSE 制御メッセージ内の個々の TLV として受信されます。

used データ・ダイレクト VCC に使用される解決済みトラフィック・パラメーター・セット。どのエンティティーにも QoS パラメーターが構成されていない場合、USED パラメーターはデフォルト・パラメーターを表します。少なくとも 1 つのエンティティーが構成されている場合は、次のように解決されます。

- LE クライアントまたは ATM インターフェースのどちらか一方にだけパラメーターが構成されており、accept-parms-from-lecs が FALSE であるか、LECS からパラメーターを受信しなかった場合は、構成された LE クライアントまたは ATM インターフェースのパラメーターが使用されます。
- LE クライアントと ATM インターフェースの両方にパラメーターが構成されている場合は、LE クライアントのパラメーターが使用されます。
- accept-parms-from-lecs が TRUE であり、LECS からパラメーターを受信した場合は、LE クライアントのパラメーター (または、LE クライアントが構成されていない場合は、デフォルト値) と LECS から受信したパラメーターが結合されて、304ページの『QoS 構成パラメーター』に記述されている最初の 6 つの QoS パラメーターの完全なセットが作成されます。
- 304ページの『QoS 構成パラメーター』に記述されている最初の 6 つの QoS パラメーター・セットに無効な組み合わせが含まれている場合、LECS からのパラメーターはリジェクトされます。2 つのフラグ negotiate-qos と validate-pcr-of-best-effort-vccs は、独立して検証されます。

例:

```
LEC 1 QoS+  list configuration parameters

               ATM LEC Configured QoS  Parameters
               ==================================

     QoS                                       |    LEC      ATM-IF    FROM
   PARAMETER                             USED  |    SRAM     SRAM      LECS
 ------------------------------------------------------------------------------
 Max Reserved Bandwidth (cells/sec) :    23584  |    23584        0      none
                       (Kbits/sec) :    10000  |    10000        0      none
 VCC Type ........................ :   ResvBW  |   ResvBW   BstEft         0
 Peak Cell Rate .....(cells/sec) :    18867  |    18867   365566    365566
                       (Kbits/sec) :     8000  |     8000   155000    155000
 Sustained Cell Rate ...(cells/sec) :    18867  |    18867   365566      none
                       (Kbits/sec) :     8000  |     8000   155000      none
 QoS Class ....................... :        4  |        4        0      none
 Max Burst Size .....(cells) :       95  |       95        0      none
                          (frames) :        1  |        1        0      none
 Validate PCR of Best-Effort VCCs . :       no  |       no      n/a      none
 Enable QoS Negotiation ..... :      yes  |      yes      n/a      none
 Accept QoS Parameters from LECS .. :      yes  |      yes      n/a       n/a
 ------------------------------------------------------------------------------
(BstEft = Best Effort, ResvBW = Reserved Bandwidth)
(n/a = not applicable, none = no value is specified)

LEC 1 QoS+
```

data-direct-vccs (Detailed Information)

このオプションは、この LE クライアントのデータ・ダイレクト VCC 情報を表示します。**list vcc-information** を使用した場合も、同様の情報が表示されます。

例:

```
LEC 1 QoS+ list data direct vccs

          LEC Data Direct VCCs - QoS Information
          ======================================

Conn Handle = 80, VPI = 0, VCI = 546
        Connection Type = RETRIED CONNECTION PARAMETERS
          TrafficType    = BEST EFFORT VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 58962 (25 Mbps)
          QoS Class      = 0
          Max Burst Size = 0

Conn Handle = 78, VPI = 0, VCI = 544
        Connection Type = PARAMETERS SET BY DESTINATION
          TrafficType    = RESERVED BANDWIDTH VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 16509 (7 Mbps)
          QoS Class      = 1
          Max Burst Size = 95

LEC 1 QoS+
```

statistics

以下の統計のカウンターが維持されています。

Successful QoS Connections

LE クライアントによって確立された RESERVED-BANDWIDTH コネクションの数

Successful Best-Effort Connections

LE クライアントによって確立された BEST-EFFORT コネクションの数

Failed QoS Connections

LE クライアントが行い、失敗した RESERVED-BANDWIDTH コネクション要求の数

Failed Best-Effort Connections

LE クライアントが行い、失敗した BEST-EFFORT コネクション要求の数

QoS Negotiation Applied

QoS ネゴシエーション拡張が適用された回数。パラメーターのネゴシエーションが行われるのは、LE クライアントが LE_ARP_RESPONSE 制御メッセージで宛先 LE クライアントのパラメーターを受信した場合です。

PCR Proposal (IBM) Applied

IBM ピーク・セル速度が適用された回数。この提示は、BEST-EFFORT コネクションで 100 Mbps または 155 Mbps でシグナルする場合は、特定の速度パラメーターを使用することをお勧めしています。これにより、参加している他の IBM プロダクト (たとえば、25-Mbps ATM アダプター) は、シグナルされたピーク・セル速度に基づいてコネクションをリジェクトすることができます。

QoS Connections Accepted
この LE クライアントによって受け入れられた RESERVED-BANDWIDTH コネクションの数

Best-Effort Connections Accepted
この LE クライアントによって受け入れられた BEST-EFFORT コネクションの数

QoS Connections Rejected
この LE クライアントが受信し、リジェクトした RESERVED-BANDWIDTH コネクション要求の数

Best-Effort Connections Rejected
この LE クライアントが受信し、リジェクトした BEST-EFFORT コネクション要求の数

Rejected due to PCR Validation
validate-pcr-of-best-effort-vccs パラメーターが TRUE の場合、ピーク・セル速度の検証が原因で LE クライアントによってリジェクトされた BEST-EFFORT コネクションの数

例:

```
LEC 1 QoS+  li stat

QoS Statistics: of Data Direct Calls Placed by the LEC
------------------------------------------------------
    Successful QoS Connections          = 0
    Successful Best-Effort Connections  = 1
    Failed QoS Connections              = 1
    Failed Best-Effort Connections      = 1
    Qos Negotiation Applied             = 0
    PCR Proposal (IBM) Applied          = 0

QoS Statistics: of Data Direct Calls Received by the LEC
--------------------------------------------------------
    QoS Connections Accepted            = 1
    Best-Effort Connections Accepted    = 0
    QoS Connections Rejected            = 0
    Best-Effort Connections Rejected    = 0
    Rejected due to PCR Validation      = 0

LEC 1 QoS+
```

tlv-information

この LE クライアントが LE サーバーに登録した IBM トラフィック情報 TLV を表示します。TLV が登録されるのは、LE クライアントが QoS ネゴシエーションに参加している場合だけです。

例:

```
LEC 1 QoS+ list tlv

  Traffic Info TLV of the LEC (registered with the LES)
  =====================================================
    TLV Type .........................= 268458498
    TLV Length .......................= 24
    TLV Value:
           Maximum Reserved Bandwidth = 23584 cells/sec (10 Mbps)
           Data Direct VCC Type...... = RESERVED BANDWIDTH VCC
           Data Direct VCC PCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC SCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC QoS Class  = 4
           Maximum Burst Size         = 95 cells (1 frames)

LEC 1 QoS+
```

vcc-information

LE クライアントのすべてのアクティブ VCC を表示します。この情報には、コネクションのトラフィック・パラメーターが入っています。

BEST-EFFORT コネクションの場合は、持続セル速度が表示されますが、これはピーク・セル速度、QoS クラス、および最大バースト・サイズが 0 として表示されるのと同じことです。

パラメーター記述子エントリーは、次のとおりです。

SrcParms
この LE クライアントによって確立されたコネクションのパラメーター

DestParms
この LE クライアントが受信したコネクションのパラメーター

NegoParms
QoS 交渉を使用して LE クライアントが確立したコネクションのパラメーター

RetryParms
少なくとも 1 回失敗した後で、この LE クライアントによって確立されたコネクションのパラメーター

例:

```
LEC 1 QoS+  li vcc

                          LEC VCC Table
                          =============

                                                                          Burst
Conn   Conn              Conn          VCC    PCR    SCR   QoS   Size    Parameters
Index  Handle VPI   VCI   Type  Status  Type  (kbps) (kbps) Class (cells) Descriptor
-------------------------------------------------------------------------------------
   2)     69    0   535  Cntrl  Ready  BstEft 155000 155000    0      0   SrcParms
   3)     71    0   537  Cntrl  Ready  BstEft      0      0    0      0   DestParms
   4)     72    0   538  Mcast  Ready  BstEft 155000 155000    0      0   SrcParms
   5)     74    0   540  Mcast  Ready  BstEft      0      0    0      0   DestParms
   6)     78    0   544  Data   Ready  ResvBW  25000   7000    1     95   DestParms

LEC 1 QoS+
```

QOS 動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

サービス品質 (QOS) は、CONFIG (Talk 6) **delete interface** コマンドをサポートしますが、次の考慮が必要です。

QOS は、特定の LEC または ATM インターフェース用に構成します。QOS の変更は、このコマンドをこの特定のインターフェースに出したときに有効になります。

GWCON (Talk 5) Activate Interface

サービス品質 (QOS) は、GWCON (Talk 5) **activate interface** コマンドをサポートしますが、次の考慮が必要です。

QOS は、特定の LEC または ATM インターフェース用に構成します。QOS の変更は、このコマンドをこの特定のインターフェースに出したときに有効になります。

サービス品質 (QoS) の構成

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

GWCON (Talk 5) Reset Interface

サービス品質 (QOS) は、GWCON (Talk 5) **reset interface** コマンドをサポートしますが、次の考慮が必要です。

QOS は、特定の LEC または ATM インターフェース用に構成します。QOS の変更は、このコマンドをこの特定のインターフェースに出したときに有効になります。

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

GWCON (Talk 5) 一時変更コマンド

サービス品質 (QOS) は、装置の操作状態を一時変更する、次の GWCON コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行すると、行われません。

Talk 5 でのすべての QOS 変更は、構成されているインターフェースにコマンドを出したときに操作上の変更を即時に有効にします。

第19章 ポリシー・フィーチャーの使用

この章では、QOS、セキュリティー、またはそれら両方に関する決定を行うためにポリシー・フィーチャーが他のルーター・ソフトウェア・コンポーネントとどのように対話するかについて説明します。ポリシー・フィーチャーに関連する概念および特定の構成コマンドについても説明します。ポリシー・フィーチャーにより、LDAP ディレクトリー・サーバーをポリシー情報の中央リポジトリーとして使用することができます。この章では、LDAP 機能を使用可能にするのに必要な概念および構成ステップについても説明しています。次のトピックでは、これらの概念、ルーターがポリシーを実施する方法について解説し、例も示します。

- 『ポリシーの概説』
- 334ページの『LDAP およびポリシー・データベースの対話』
- 338ページの『規則の生成』
- 339ページの『構成の例』

ポリシーの概説

ポリシー・フィーチャーにより、ネットワーク内での IPv4 トラフィックの管理が容易になります。ポリシーは、非常に単純なフィルター規則 (drop または pass) や、複合セキュリティーおよび QOS シナリオに合わせて構成することができます。ポリシーの組み合わせにより、ネットワーク内でポリシーが IPv4 トラフィックをどのように処理するかが決まります。

ポリシーの決定と実施

このルーター・ファミリーにポリシーを実装することにより、ポリシー決定の基礎およびそれらの実施手段が設定されます。これらの概念は、たいてい、ポリシー決定ポイント (PDP) およびポリシー実施ポイント (PEP) と呼ばれます。

ポリシー・データベースは、ルーターのメモリー内に収容されていますが、ローカル構成からロードされたポリシーと LDAP から読み取られたポリシーとのセットで構成されます。ポリシー・データベースは、次の条件のもとで構築されます。

- Device reload または restart
- **reset database** 監視コマンド
- 自動リフレッシュ
- SNMP 設定要求

ポリシー・データベースは PDP として機能するもので、ポリシー・フィーチャー関連コンポーネントがパケットを処理する方法を決定するポリシーのセットで構成されます。ポリシーの結果として (時刻などの情報、IP パケット情報、および識別などのプロトコル固有情報に基づいて) 決定が下されると、その決定は実施ポイント (PEP) に渡されて、アクションが実行されます。 326ページの図27 は、これらのコンポーネントの関係を示しています。

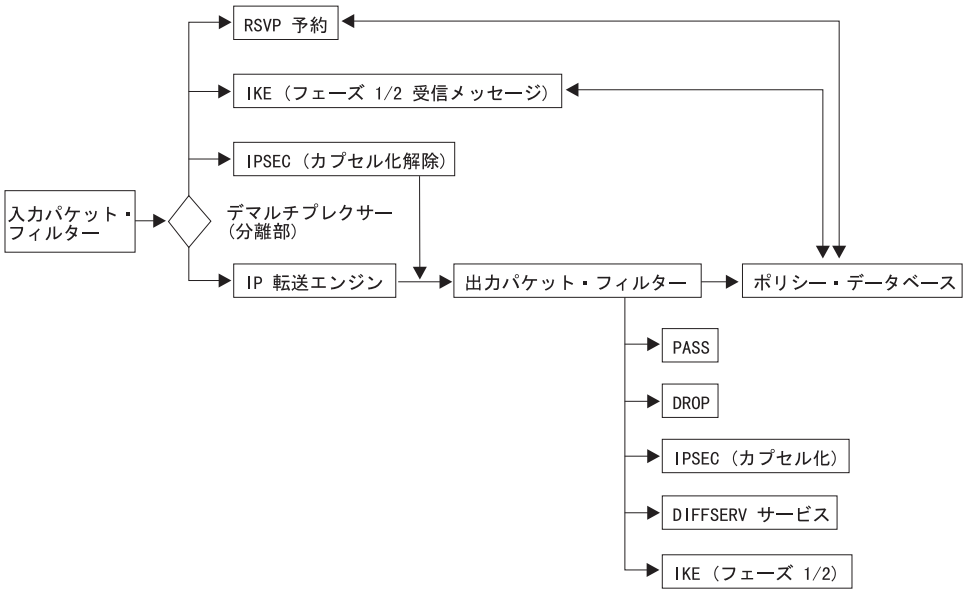


図 27. IP パケットの流れとポリシー・データベース

ポリシー決定とパケットの流れ

IP パケットが最初に、入力パケット・フィルターをパスしてからでないと、その他のアクションは一切行われません。入力パケット・フィルターに規則が存在していると、パケットに対してなんらかのアクションが行われます。パケットを除外するフィルター・マッチが存在したり、入力パケット・フィルターで一致が検出されないと、そのパケットはドロップされます。

パケットは入力パケット・フィルターをパスした場合は、分離フィルターに進み、これにより、パケットの着信先をローカルで決めるかどうかが検査されます。着信先がローカルで決められた場合は、パケットのタイプに応じて、他のモジュールにパスされます。これらのモジュールは、IPSec、IKE、RSVP、などです。
IPSec、IKE、または RSVP の場合にパケットの着信先がローカルで決められると、それらのモジュールは、どのアクションを取るべきかをポリシー・データベースに照会して判断できます。

パケットの着信先がローカルで決められない場合には、パケットは転送エンジンに与えられ、ルーティングが決定されます。ルーティングの決定によりパケットがドロップされないことになった場合 (ポリシー・ベースのルーティングの場合はパケットをドロップするよう決定される場合があります)、パケットは、出力パケット・フィルターに進みます。出力パケットにフィルター規則が存在する場合には、パケットはアドレス変換が実行される (NAT) 場合、パスされる場合、あるいはドロップされる場合があります。フィルター規則が存在しない場合、パケットはパスします。フィルター規則が存在するが、一致が見つからない場合には、パケットはドロップされます。パケットが出力パケット・フィルターをパスした場合、IP エンジンは、ポリシー・データベースに照会し、このパケットに対して他にアクションを実行すべきかどうかを判断します。

注: 入力および出力パケット・フィルターがインターフェース (複数の場合もあり) について使用可能になっており、ポリシー・データベースが制御することになっているパケットがこれらのインターフェースをパスすると予想される場合に

は、これらのパケットを含むフィルター規則が入力および出力パケット・フィルター内に存在している必要があります。そうすれば、ポリシー・データベースに照会が行われる前にそれらのパケットがドロップされることはありません。ポリシー・データベースに対して使用する 1 つの提示として、すべてのパス / ドロップ規則を設定し、パケット・フィルターを使用しないことです。

IP ポリシー照会

IP 転送エンジンがポリシー・データベースに照会すると、次のタイプの決定の組み合わせが戻されます。

- No match found-pass the packet (一致が見つからない - パケットをパスする)
- Match found-drop the packet (一致が検出された - パケットをドロップする)
- Match found-pass the packet (一致が検出された - パケットをパスする)
- Match found-secure the packet in IPSec manual tunnel x (一致が検出された - IPSec 手動トンネル x 内でパケットを保護する)
- Match found-secure the packet in IKE negotiated IPSec manual tunnel x (一致が検出された - IKE ネゴシエーション済み IPSec トンネル x 内でパケットを保護する)
- Match found-start ISAKMP negotiations for Phase 1 and 2, drop packet (一致が検出された - フェーズ 1 および 2 について ISAKMP ネゴシエーションを開始し、パケットをドロップする)
- Match found-provide DiffServ QOS x, secure packet with IPSec (一致が検出された - DiffServ QOS x を提供し、IPsec でパケットを保護する)

IPSec ポリシー照会

IPSec はパケットを受信したら、最初にそのパケットのカプセル化を解除し、次に、そのパケットが適切な IPSec トンネルに到着したかどうかを判断する (通常、適合検査といいます) 必要があります。この検査は、ポリシー・データベースに照会することによって行います。ポリシー・データベースは、この照会について次のタイプの判断を戻してきます。

- Conformancy check passed-forward the packet (適合検査にパスした - パケットを転送する)
- Conformancy check failed-drop the packet (適合検査に失敗した - パケットをドロップする)

IKE ポリシー判断

IKE がポリシー・データベースに照会すると、表42 に示されているフェーズ *1* IP ポリシー判断が戻されます。

表 42. IKE フェーズ 1 照会と返される判断

照会のタイプ	判断
Message 1 (Main Mode)	No match found, drop packet (一致が見つからない。パケットをドロップする)
Message 1 (Main Mode)	Match found, negotiate with Phase 1 policy x (一致が検出された。フェーズ 1 ポリシー x とネゴシエーションする)
Message 5 (Main Mode)	No match found, stop negotiations with peer, drop packet (一致が見つからない。ピアとのネゴシエーションを停止し、パケットをドロップする)

表 42. IKE フェーズ 1 照会と返される判断 (続き)

照会のタイプ	判断
Message 5 (Main Mode)	No match found, stop negotiations with peer, drop packet (一致が見つからない。ピアとのネゴシエーションを停止し、パケットをドロップする)
Message 5 (Main Mode)	Match found, policy x matched, finish Phase 1 (一致が検出された。ポリシー x は一致した。フェーズ 1 を終了する)
Message 5 (Main Mode)	Match found, policy y matched, stop current Phase 1 and initiate new Phase 1 with new policy (一致が検出された。ポリシー y は一致した。現在のフェーズ 1 を停止し、新規ポリシーで新たにフェーズ 1 を開始する)
Message 1 (Aggressive Mode)	No match found, drop packet (一致が見つからない。パケットをドロップする)
Message 1 (Aggressive Mode)	Match found, policy x matched (一致が検出された。ポリシー x は一致した)

IKE がポリシー・データベースに照会すると、表43 に示されているフェーズ *2* IP ポリシー判断が戻されます。

表 43. IKE フェーズ 2 照会と返される判断

照会のタイプ	判断
Message 2 (応答側)	No match found, drop packet (一致が見つからない。パケットをドロップする)
Message 2 (応答側)	Match found, negotiate with policy x (一致が検出された。ポリシー x とネゴシエーションする)

RSVP ポリシー判断

パケットが RSVP 制御メッセージである場合、RSVP はポリシー・データベースに照会し、予約を受け入れるか、拒否するかを判断します。予約を受け入れた場合には、RSVP は、ポリシーに基づいて、制限する予約の属性を判別します。ポリシー・データベース内のポリシーは、予約の期間、割り振るべき帯域幅の量、および保証最小遅延を制御できます。

ポリシー・オブジェクト

ポリシーはプロファイルで構成されます。これには、判断の基準となるパケットの属性のセット、パケットの属性がプロファイル内の属性と一致する場合に取るべきアクション、および判断が行われ、アクションが実施される妥当性期間が含まれています。これらの項目について、次のトピックでさらに詳しく解説していきます。

ポリシーを構成する各部分は、明確な名前をもつオブジェクトです。ポリシー・オブジェクトは互いに参照し、関連する一群の項目として 1 つのポリシーを構成します。構成情報を別個の明確なオブジェクトに分割することにより、それらの大部分を複数のポリシー定義にまたがって再利用することができるので、時間が節約でき、保守作業が軽減されます。個々のポリシー・オブジェクトについて、次のトピックで詳しく説明します。

ポリシー

ポリシー・オブジェクトは、検査を行う場合の条件と、チェックが適合した場合に実施すべきアクションについて記述します。ポリシーは、妥当性期間およびプロファイルに対して名前付きの参照を行います。ポリシーが有効であるためには、これらの参照は必須です。ポリシーは、IPSec 手動キー付きトンネル・オブジェクト、

IPSec アクション、ISAKMP アクション、RSVP アクション、または DiffServ アクションの複数のアクションに対して名前付きの参照を行う必要があります。有効は、次のものが有効です。

- IPSec 手動キー付きトンネル
- パケットをドロップするための IPSec アクション
- パケットをパスするための IPSec アクション (セキュリティーなし)
- パケットを保護するための IPSec アクション、ISAKMP アクション
- DiffServ アクション (ドロップ)
- IPSec 手動キー付きトンネルおよび DiffServ アクション (パス)
- パケットを保護するための IPSec アクション、ISAKMP アクション、DiffServ アクション (パス)
- RSVP アクション
- RSVP アクションおよび DiffServ アクション (パス)

注: 上記の組み合わせでは、IPSec 手動トンネルが IPSec アクション (IKE ネゴシエーション済み IPSec 手動トンネル) と同じポリシー定義に存在することはできず、RSVP アクションは、どのような種類の IPSec アクションとも関連付けてはなりません。パケットを保護するための IPSec アクションが 1 つのポリシーと関連付けられている場合には、ISAKMP アクションもそのポリシーと関連付ける必要があります。

各ポリシーには、優先順位番号もそれと関連付けられています (優先順位属性の数値が大きいほど、優先順位は高くなります)。優先順位により、このポリシーが別のポリシーよりも優先権をもつかどうかが決められます。一般的に、これを設定しなければならないのは、2 つまたはそれ以上のポリシーのプロファイルがなんらかの点で互いに対立している場合だけです。固有性の高いプロファイルをもつポリシーほど、優先順位を高くします。たとえば、あるポリシーがサブネット A からサブネット B へのトラフィックを IPSec (DES) で保護するよう指示し、別のポリシーがポイント a′ (サブネット A 内の特定のホスト) からサブネット B へのトラフィックを IPSec (3DES) で保護するよう指示するとします。固有性の高い方のポリシー (a′ から B) の優先順位を、A から B を指定されたポリシーよりも高くしてください。

初期優先順位の値 (5 またはそれ以上) に、後で対立するポリシーに備えて、追加の優先順位値を指定できるだけの数値を割り当てるようお勧めします。各ポリシーには使用可能な属性もあり、これにより、そのポリシーをポリシー・データベースにロードする際に使用可能にするかどうかが決まります。ポリシー・データベース検索中にポリシーの一致が検出されたが、そのポリシーが使用不可である場合には、その次に固有性の高いポリシーが実施されます。

check-consistency 監視コマンドを使用することによって、単一のポリシー内およびすべての定義済みポリシーの両方における整合性と競合を調べる検査を開始できます。このコマンドは、問題があっても解決を試みませんが、訂正処置を取ることができるように問題を識別します。コマンドの詳細については、391ページの『ポリシー監視コマンド』を参照してください。

プロファイル

プロファイルは、特定のポリシーを選択するのに使用する情報を判別します。プロファイルは、発信元アドレスおよび宛先アドレス情報、プロトコル情報、発信元および宛先のポート情報で構成されます。

注: ポリシーを IPSec/ISAKMP 用に定義するときには、セキュリティーを提供する各ゲートウェイがセキュリティー・アソシエーションを定義するポリシーをもっている必要があります。各ゲートウェイ上のプロファイルは、発信元と宛先との関連付けを行う必要があります。IPSec ポリシー用のプロファイルは、発信元アドレスをカプセル化されてトンネルに入れるトラフィックとして指定する必要があり、宛先アドレスはトンネルのリモート・エンドになければなりません。

プロファイルは、サービスのタイプ (TOS) バイトのほか、ingress および egress IP アドレスに基づいて選択することもできます。特に指定のない限り、任意の入力インターフェース上で受信されたパケットで、任意の出力インターフェースで出ていくパケットは、その他のセレクターに照らして突き合わせられます。場合によっては、パケットが着信する必要のあるインターフェースと、パケットが出ていく必要のあるインターフェースを正確に指定する柔軟性が必要となることがあります。これが必要な場合は、インターフェースの対オブジェクトを追加し、そのインターフェースの対オブジェクトのグループ名をプロファイルと関連付ける必要があります。インターフェースの対オブジェクトに同じ名前を付けて、1 つのグループに割り当てます。こうすることにより、そのような組み合わせ (IPaddrX に着信し、任意のインターフェースで出ていく任意のパケットまたは 任意のインターフェースに着信し、IPaddrX で出ていく任意のパケット) を指定することができます。これは、公衆インターフェースのために一般的なドロップ規則を定義する場合に特に役立ちます。

インターフェースのペア: 入力インターフェースと出力インターフェースを識別します。この選択を行うには、インターフェースの IP アドレスを指定してください。値 255.255.255.255 は、任意のインターフェースを暗黙指定します。

プロファイルを使用して IPSec/ISAKMP ポリシーを選択したい場合には、フェーズ 1 の間に送信されるローカル ID を指定するオプションと、フェーズ 1 ネゴシエーション時の受け入れ可能なリモート ID のリストが示されます。特に指定のない限り、ローカル ID は IPSec/IKE トラフィックのローカル・トンネル・エンドポイントであり、リモート ID リストは *Any* です。任意により、完全修飾ドメイン名 (FQDN)、ユーザー FQDN、およびキー ID を指定できます。通常、すべての ISAKMP フェーズ 1 ネゴシエーションは公衆認証または事前共用キーで認証されるため、これで十分です。ただし、ポリシーの宛先アドレスがワイルドカード指定になっているリモート・アクセス状態では、ネットワーク資源へのアクセスが許されているリモート・アクセス・ユーザーのリストを指定することをお勧めします。

これらのユーザーは、まだ、通常の ISAKMP 認証方式で認証されますが、ポリシー・データベースは、リモート・ピアによって送信されたローカル ID がポリシーのプロファイルのリモート・ユーザー・グループに指定された ID の 1 つと一致するようにすることにより、追加の認証ステップを実行します。公衆認証局 (CA) が一般に対する認証を管理しており、ネットワーク管理者がこれらのユーザーのうち特定のユーザー (たとえば、企業の従業員) だけにアクセス権をもたせたい場合に

は、これが必要です。リモート・ユーザー・グループは、同じグループに属すユーザーのリストで構成されます。これらのユーザーは、1 つまたは複数の *USER* を追加することによって入力されます。ユーザーのグループは、各ユーザーのグループ名を同じにすることができます。そうすると、任意により、このグループをプロファイルと関連付けることができます。

妥当性期間

妥当性期間は、ポリシーの寿命を、年、月、日数、および時間数で指定します。このような柔軟性により、ネットワーク管理者は、ポリシーが有効な期間を指定できます。たとえば、“常時” または “本年限り、1 月、2 月、3 月の間、月曜日から金曜日まで、午前 9 時から午後 5 時まで” という具合です。ポリシー・データベース内のポリシーが無効になると、次に固有性の高いポリシーが実施されます。したがって、月曜日から金曜日までの午前 9 時から午後 5 時までをサブネット A からサブネット B までのすべてのトラフィックを保護し、それ以外の時間はサブネット A からサブネット B までのすべてのトラフィックをドロップするよう指定するポリシーを定義することができます。この場合、最初のポリシー (Talk 5 **add policy** 監視コマンドを入力したときに指定されるもの) の方が高い優先順位をもっている必要があります。

DiffServ アクション

DiffServ アクションは、DiffServ アクションを指定するポリシーに一致するパケットに対して提供されるサービス品質を記述します。パケットをドロップするよう DiffServ アクションを構成することができます。DiffServ アクションを使用して、パケットを関連するサービス品質にマップすることもできます。割り当てられた帯域幅を、出力帯域幅のパーセントまたは Kbps 単位の絶対値として構成することができます。best effort/assured (AF)/best effort 待ち行列または premium (EF) 待ち行列が帯域幅割り当てを提供するかどうかを指定する必要があります。これらの待ち行列およびそれらの定義方法について詳しくは、455ページの『第23章 ディファレンシェーテッド・サービス・フィーチャーの使用』および 463ページの『第24章 ディファレンシェーテッド・サービス・フィーチャーの構成と監視』を参照してください。

DiffServ アクションは、egress インターフェースで送信される前に EF と AF トラフィック用の DS コード・ポイント (TOS バイト) にマークを付ける方法も指定します。EF と AF トラフィックは測定され、基準に合致しないトラフィックは規制されます。基準に合致しない EF トラフィックをドロップして、オプションとして、基準に合致しない AF トラフィックの DS バイトは、3 色マーカー (TCM) 方式を使用してマークを付け直します。パケットのマーク付け、測定、およびポリシングによって、DiffServ が使用可能なネットワークでのコア・ルーターは DS コード・ポイントに基づいてパケットを分類し、基準に合致しないトラフィックを最初にドロップすることによって輻輳を制御できます。このことは、スループットの向上を達成し、DiffServ が使用可能なネットワークでの優先トラフィックの遅延を短くするのに役立ちます。

RSVP アクション

RSVP アクションは、RSVP 予約が発生し、その予約要求がポリシーのプロファイルと一致した場合に RSVP の流れを許可するか、拒否するかを指定します。予約を許可したい場合には、RSVP アクションは、許される予約の期間、許される帯域幅、および任意により、DiffServ アクションへの参照も示します。DiffServ アクシ

ョンへの参照により、RSVP は、パケットがルーターを出る前に TOS バイトにマークを付ける方法を判別できます。これは、パケットが RSVP ネットワークから DiffServ ネットワークにパスする場合に役立ちます。RSVP は、QOS を RSVP 境界まで提供し、TOS バイトに適宜マークを付けることができるので、DiffServ ネットワークは正しい帯域幅を適用できます。

IPSec アクション

IPSec アクションは、drop (ドロップ)、pass (パス)、または secure (保護) アクションのいずれかを指定します。アクションが drop である場合は、このポリシーに一致するパケットはすべてドロップされます。アクションが保護のない pass であると、すべてのパケットはチェックなしでパスされます。アクションが保護付きの pass である場合、すべてのパケットは、このアクションによって指定されたセキュリティー・アソシエーションにより保護されます。IPSec アクションには、IPSec トンネルおよび IKE SA のトンネルのエンドポイントの IP アドレスを入れることができます。

SA の属性は、IPSec アクションが参照する IPSec 提示によって決定されます。IPSec アクションは複数の IPSec 提示を指定することができますが、それらの提示は、指定順に送信され、検査されます。1 つの IPSec アクションに複数の提示を入れておくと、受け入れ可能なセキュリティーのすべての組み合わせを構成に含めることができるので、VPN ゲートウェイ間の潜在的な構成の不一致の数が少なくなります。

IPSec 提示

IPSec 提示には、ESP または AH、あるいはその両方の変換を提示するかまたはフェーズ 2 ISAKMP ネゴシエーション中に検査するよう情報が含まれています。完全な転送セキュリティー (新しい Diffie Hellman 計算) が必要な場合、IPSec 提示が、使用すべき DH グループを識別します。IPSec 提示が参照する変換は、指定された順に送信または検査されます。リストの最初の ESP または AH 変換は、最も使用に適したものでなければなりません。リストに複数の変換がある場合、各変換は、一致がないかピアの変換のリストと比較されます。構成済みの変換がどれもピアのリストに一致しない場合、ネゴシエーションは失敗します。IPSec 提示により、AH と ESP 変換の組み合わせが表示されますが、有効な組み合わせは次のものだけです。

- AH だけのリスト (トンネル・モードまたはトランスポート・モード)
- ESP だけのリスト (トンネル・モードまたはトランスポート・モード)
- AH のリスト (トランスポート・モード) および ESP のリスト (トンネル・モード)

IPSec 変換

IPSec 変換の属性には、IPSec 暗号化および認証パラメーターに関する情報が含まれ、キーが更新される回数も指定します。変換は、AH (認証だけ) または ESP (暗号化または認証、あるいはその両方) のどちらかで、トンネル・モードまたはトランスポート・モードのどちらでも動作するよう構成できます。

ISAKMP アクション

ISAKMP アクションは、フェーズ 1 のキー管理情報を指定します。このアクションは、フェーズ 1 ネゴシエーションが main (メイン) モード (識別保護を提供しま

す) または aggressive (積極) モードのどちらで開始するかを指定します。フェーズ 1 セキュリティー・アソシエーションが装置開始時にネゴシエーションされるか、それともオンデマンドでネゴシエーションされるかも指定します。ISAKMP アクションは、1 つまたは複数の ISAKMP 提示も参照する必要があります。最初の参照は、最も受け入れ可能な ISAKMP 提示でなければなりません。

ISAKMP 提示

ISAKMP 提示は、フェーズ 1 セキュリティー・アソシエーションの暗号化および認証属性を指定します。キーの生成に使用する Diffie Hellman グループのほか、フェーズ 1 セキュリティー・アソシエーションの寿命も指定します。ISAKMP 提示で認証方式を選択する必要があります。それは、事前共用キー・モードでも認証モードでもかまいません。

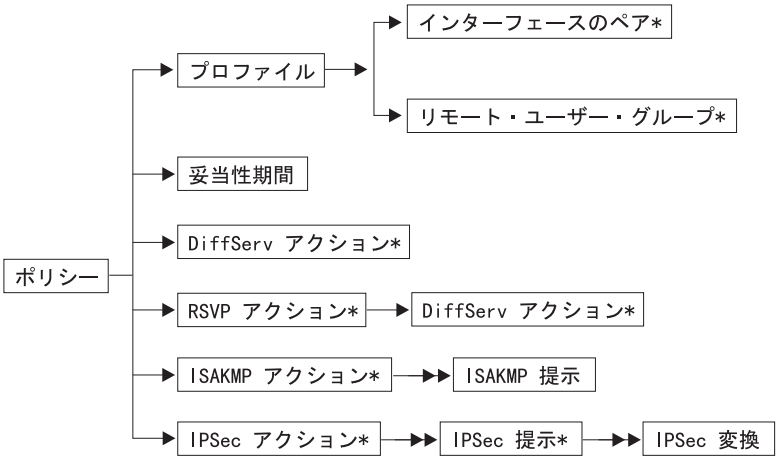
USER

認証方式として事前共用キーとの ISAKMP ネゴシエーションを使用するあらゆるポリシーについて USER を構成する必要があります。USER 構成は、ISAKMP ピアのために使用する事前共用キーを識別します。ユーザー・オブジェクトには、リモート ISAKMP ピアのための情報、つまり IP アドレス、FQDN、ユーザー FQDN またはキー ID のほか、ユーザーが認証に使用したいと考えている方式が含まれています。事前共用キー・モードまたは認証モードのどちらでも選択できます。事前共用キーを選択した場合は、事前共用キーを ASCII または 16 進数のどちらで入力する必要があるかと、そのキーの値を指定する必要があります。USER は、同じグループ名に割り当てることにより、1 つにまとめることができます。そうすると、任意により、このグループをポリシーのプロファイルと関連付けて、フェーズ 1 に対してさらに厳密なポリシー検索を実行できます。

IPSec 手動キー付きトンネル

IPSec 手動キー付きトンネルは、暗号化および認証パラメーターの静的構成です。トンネルに対してネゴシエーションは実行されないため、両方のピアがまったく同一の構成をもつ必要があります。キーは、この構成の一部として実際に入力されますが、トンネルの両側で一致する必要があります。このモードではネゴシエーションは実行されないため、キーは更新されません。 IPSec 手動キー付きトンネルについて詳しくは、401ページの『第21章 IP セキュリティーの使用』の IPSec フィーチャーの説明を参照してください。

334ページの図28 は、ポリシー構成オブジェクト間の関係を示しています。



注:

1. → は単一参照を示します。
2. →▶ は複数参照を示します。
3. * は任意選択の参照を示します。
4. ISAKMP/IPSec のセキュリティー・ポリシーでは、トラフィック・プロファイルが保護トンネルに入るトラフィックを定義します。

図 28. ポリシー構成オブジェクト間の関係

LDAP およびポリシー・データベースの対話

このルーターのファミリーにより、Lightweight Directory Access ProtocoL (LDAP) サーバーは、ポリシー情報のリポジトリー (ポリシー・データベース) になることができます。LDAP は、ディレクトリー・サーバーを検索し、変更できるようにするプロトコルです。LDAP は、X.500 標準の簡易バージョンです。ルーターは、ディレクトリー・サーバー内で情報を検索 (変更は行いません) するための機能をサポートします。ルーター内のポリシー検索エージェントは、その装置に使用する予定のディレクトリー・サーバー内のすべてのポリシー情報を検索します。LDAP バージョン 2 または 3 で作動する LDAP サーバーはすべてルーター内の設定で機能します。ローカルで保管された構成という従来方式に反してディレクトリー・サーバーを使用してポリシー情報を保管する一番の利点は、ある場所で変更を行い、拡張ネットワーク内のすべての装置に対してその変更を適用できることです。これには、公衆回線との境界にまたがった装置だけでなく、管理ドメイン内の装置が含まれます。

たとえば、ディレクトリーに収められている IPSec 変換定義をもっているものとします。DES から 3DES への暗号化のために法人ポリシーを変更したい場合は、通常、各ネットワーク境界を超えたあらゆる装置構成での変更が必要となります。ディレクトリーを使用してポリシーを展開する場合には、1 つの IPSec 変換を変更するだけで済みます。ネットワーク内のポリシーが使用可能になっている装置はすべて、データベースを再作成しなければならなくなります。別の例として、帯域幅の値を 40% から 45% の帯域幅に増やすよう、“GoldService” という名前の DiffServ アクションを変更する必要があるとします。LDAP サーバーおよびポリシー・インフラストラクチャーにより、これらのタイプの構成変更がさらにスケーラブルなものになるので、構成の不一致が少なくなります。

ネットワーク管理者であれば、毎日指定の時刻に自動的にデータベースを更新する機能を利用することもできます。このオプションは、ポリシー・フィーチャーの **set refresh** コマンドを入力して選択します。更新を使用可能にするかどうかを指定することができ、使用可能にする場合は、データベースが更新される時刻も指定できます。このオプションは、自動的に変更を行うのに役立ちます。たとえば、米国のマーケティング部門が日本の開発部門とインターネットを通じて話ができるように新しいポリシーを追加する必要があり、セキュリティー・ゲートウェイが SG1 および SG2 であるとします。SG1 および SG2 が自動更新について使用可能になっていれば、この情報をディレクトリーに入れるだけで、真夜中にそれらは自動的にこの変更を選び出します。

LDAP サーバーからポリシー情報を正常に読み取ると、この情報を装置上の永続的記憶域にキャッシュすることが必要となる場合があります。一度このことを行うと、キャッシュされた情報を常に読み取るようにすることができ、LDAP サーバーを調べるのに必要な時間がなくなります。更新を要求されたときに LDAP サーバーが使用できない場合ポリシー検索エンジンにキャッシュ・コピーを読み取らせることもできます。詳細については、391ページの『ポリシー監視コマンド』 での **cache-ldap-plcys** と **flush-cache** 監視コマンドおよび 386ページの『LDAP ポリシー・サーバー構成コマンド』 での **enable ldap** 監視コマンドを参照してください。

LDAP ポリシー検索エンジンにより、ポリシー・データベースの作成時に使用するセキュリティー・レベルを指定することができます。ポリシー・フィーチャーの **set default** コマンドを使用して、次のセキュリティー・オプションを定義します。オプションには、次のものがあります。

- 検索中にすべてのトラフィックをパスする (デフォルト)。
- LDAP ポリシー検索要求および結果*以外* のすべてのトラフィックをドロップする。
- IPSec によって保護される LDAP ポリシー検索要求および結果*以外* のすべてのトラフィックをドロップする。

場合によっては、最初の 2 つのオプションのどちらかで十分です。しかし、LDAP トラフィックが公衆インフラストラクチャーを通り抜ける場合は、3 番目のオプションを選択することにより情報を保護して認証する必要があります。これを行う場合は、フェーズ 1 およびフェーズ 2 認証および暗号化のオプションを選択する必要があります。トンネルのエンドポイント (1 次および 2 次 LDAP サーバー) の IP アドレスも入力する必要があります。このブートストラップ IKE/IPSec トンネルは、LDAP トラフィックが送信される前にネゴシエーションされます。このフィーチャーにより、336ページの図29に示されている構成を確立することができます。

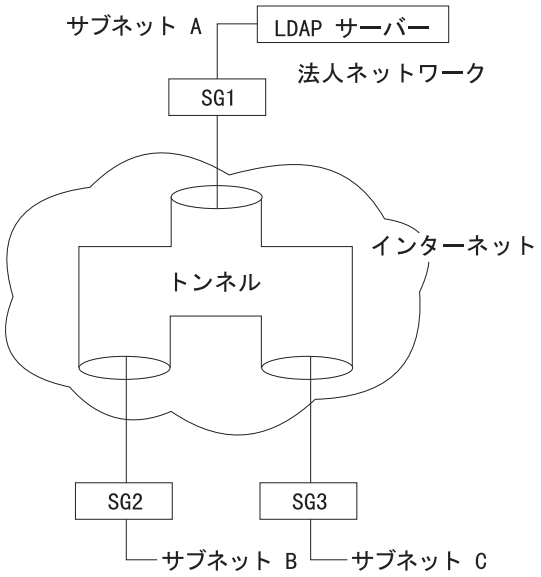


図 29. インターネットを流れるトラフィックの保護

この例は、法人ネットワーク内のサブネット A 上にある LDAP サーバーを示しています。SG1、SG2、および SG3 は、LDAP サーバーからそれぞれのポリシーを取り出します。SG2 および SG3 のポリシー検索は、インターネットを介して行われ、IPSec により保護されます。

ポリシー・データベースがディレクトリーからポリシーを取り出すのに必要な構成情報は、次のものです。

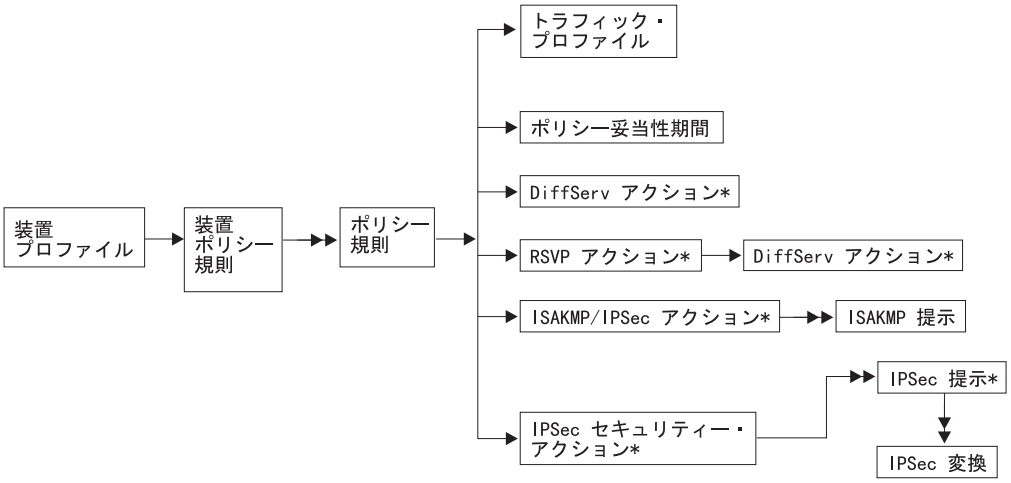
- 1 次サーバー IP アドレス (バックアップ用の 2 次サーバーも構成されます)
- サーバーが listen しているポート番号 (注 : SSL および TLS はサポートされません)
- ユーザー名およびパスワード情報 (必要な場合)
- このルーターまたはルーターのクラスの DeviceProfile オブジェクトの基本識別名
- デフォルト・ポリシー情報

この構成情報を入力した後で、次にポリシー・データベースが更新されると、ディレクトリー・サーバーにポリシー情報を求める信号の送信が試みられます。ポリシー・データベースでは、ローカルで構成されたポリシーと LDAP サーバーから読み取られた規則を組み合わせることができます。2 つの規則が対立していることが判明し、それらの優先順位が同じである場合には、ローカル構成から読み取られた規則が、ディレクトリー・サーバーから読み取られた規則に優先します。

ポリシー・スキーマ

LDAP スキーマは、ディレクトリー内の記入項目の内容を決定するクラス定義および属性定義を構成する規則と情報の集合です。一般的に、LDAP スキーマは、SNMP MIB と同様、ASN1 構文で作成されます。このルーターのファミリーがサポートするポリシー・スキーマは、IETF で行われている標準以前の作業を構成するものです。これは、IETF 内の IPSec and Policy Working Groups および DMTF 内の Policy Working Group で行われている標準追跡作業に基づいています。ポリシー・スキーマは、ルーター上のポリシー・フィーチャー内の既存の構成オブジェクトに

完全に一致しています。 **http://www.networking.ibm.com/support** という URL にアクセスすると、ポリシー・スキーマ定義ファイルおよび LDAP サーバー構成ファイルが見つかります。ご自分に必要なルーター・プロダクトを選択してから、*Downloads (ダウンロード)* リンクを選択してください。図30 は、ポリシー・スキーマの全体的な構造を示しています。



注:

1. →▶ は単一参照を示します。
2. →▶▶ は複数参照を示します。
3. * は任意選択の参照を示します。
4. ISAKMP/IPSec のセキュリティー・ポリシーでは、トラフィック・プロファイルが保護トンネルに入るトラフィックを定義します。

図 30. ポリシー・スキーマの構造

DeviceProfile および DevicePolicyRules は、ポリシー・スキーマの 2 つの主要オブジェクトです。これらにより、ポリシー検索エージェントは、その装置に必要なポリシーを見付けることができます。DeviceProfile には、装置の管理 IP アドレスに関する情報と必須 DevicePolicyRules 参照が含まれています。複数の装置を 1 つの DeviceProfile にまとめることもできますし、ネットワーク内の各装置がそれぞれ独自の DeviceProfile をもつこともできます。どちらを選択するかは、ネットワーク内の複数の装置が同じ規則の集合を取り出す必要があるかどうかで決めてください。一般的に、保護ゲートウェイの場合は、各ゲートウェイが異なるトンネルのエンドポイントをもっているため、これは当てはまりません。QOS 専用装置の場合は、1 つのグループのすべての装置が同じポリシーの集合を読み取ることが考えられます。

DevicePolicyRules オブジェクトは、その装置について取り出される DeviceProfile 内の値に基づいて取り出されます。DevicePolicyRules オブジェクトが取り出されていると、その装置の PolicyRules のリストを取り出すことができます。オブジェクトが見つからない場合や、オブジェクトについての整合性検査中にエラーが検出された場合には、検索は打ち切られ、そのエラーを識別する ELS (PLCY メッセージ) に対してメッセージが表示されます。エラーが発生すると、ネットワーク管理者は、次のどれか 1 つを構成して、エラーに対処します。

- ローカルで読み取られたポリシーをすべて削除し、drop or pass all (すべてドロップまたはパス) 規則に戻る
- ローカルで読み取られたポリシーを保持する。このオプションは、ポリシー・フィーチャーの **set default** コマンドを使用して指定してください。

どちらの場合も、検索は構成された再試行間隔で再試行されます。1 次 LDAP サーバーに連絡できない場合は、5 回の再試行の後で、2 次サーバーが試みられます。2 次サーバーに連絡できない場合は、5 回の再試行の後で、再度 1 次サーバーが試みられます。再試行間隔は、ポリシー・フィーチャーの **set ldap retry-interval** コマンドで指定することができます。ネットワーク待ち時間が原因で検索が失敗した場合は、ポリシー・フィーチャーの **set ldap search-timeout** コマンドを使用して、検索タイムアウトをデフォルトの 3 秒から変更できます。

規則の生成

希望するネットワークの動作を指定するポリシーを構成します。ルーターは、ポリシー情報を変換して規則の集合にまとめ、これをトラフィック・フローと比較します。これは、以前に、各トラフィック・パターンについてインバウンドおよびアウトバウンドのパケット・フィルターを定義することによって手動で行っている可能性があります。ポリシー・データベースを使用して、ポリシーを 1 つ構成するだけで済むので、これは必要なくなりました。

作業の大半は、ポリシー・データベースが作成されるたびに内部的に行われます。場合により、ルーターは 1 つのポリシーを直接 1 つの規則に変換します。ISAKMP/IPSec の場合、ルーターは、1 つのポリシーを 5 つの規則に変換します。トラフィックの方向 (着信と発信) や、IKE ネゴシエーションのフェーズ 1 およびフェーズ 2 で発生する制御の流れを説明するのに、5 つの規則が必要です。ポリシーと規則との関係は、次のようになっています。

1 つの DiffServ ポリシー → 1 つの DiffServ 規則

1 つの RSVP ポリシー → 1 つの RSVP 規則

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

例 : サブネット A からサブネット B へのトラフィックの保護。トンネルのエンドポイントは、SGa および SGb。

1. フェーズ 1 インバウンド (プロファイル = SGb から SGa、プロトコル UDP、発信元ポート 500、宛先ポート 500): この規則は、装置が ISAKMP 応答側として機能している場合にリモート ISAKMP からの着信フェーズ 1 ネゴシエーションをフィルターに掛けるのに必要です。
2. フェーズ 1 アウトバウンド (プロファイル = SGa から SGb、プロトコル UDP、送信元ポート 500、宛先ポート 500): この規則は、トラフィックが ISAKMP フェーズ 1 ネゴシエーションを開始する場合に必要なフェーズ 1 情報をフィルターに掛けるのに必要です。この場合、装置は ISAKMP 起動側として機能します。

3. フェーズ 2 インバウンド (プロファイル = SGb から SGa、プロトコル UDP、発信元ポート 500、宛先ポート 500): この規則は、リモート ISAKMP ピアからの着信フェーズ 2 トラフィックをフィルターするのに必要です。このトラフィックは、リモート・ピアがフェーズ 2 更新または初期ネゴシエーションを開始した結果です。ネゴシエーションは、必要であれば常にアウトバウンド・トラフィック (規則 5) が開始するため、フェーズ 2 アウトバウンド規則は不要です。
4. 保護トンネルへのトラフィック (プロファイル = サブネット A からサブネット B): この規則は、保護されていないトラフィックを保護トンネルに入れるのに必要です。セキュリティー・アソシエーションがネゴシエーションされていない場合は、フェーズ 1 規則も収集され、IKE はフェーズ 1 およびフェーズ 2 を開始します。SA が確立されていれば、この規則に適合するパケットは IPSec に与えられ、カプセル化され、伝送されます。
5. 保護トンネルからのトラフィック (プロファイル = サブネット B からサブネット A): この規則は、保護トンネルに着信しているはずのパケットが実際には保護トンネルに着信していないことを確認するのに必要です。パケットが IPSec によって暗号化解除されておらず、この規則が適用されると、そのパケットはドロップされます。この規則は、ネットワークにスプーフされるすべてのトラフィックを扱います。

1 つの IPSec 手動キー付きトンネル → 2 つの IPSec 規則

例 : サブネット A からサブネット B へのトラフィックの保護。トンネルのエンドポイントは、SGa および SGb。

1. 保護トンネルへのトラフィック (プロファイル = サブネット A からサブネット B): この規則は、保護されていないトラフィックを保護トンネルに入れるのに必要です。これは静的に構成されたトンネルであるため、常に使用可能であり、この規則に適合するパケットは、直接に IPSec に与えられて、カプセル化され、伝送されます。
2. 保護トンネルからのトラフィック (プロファイル = サブネット B からサブネット A): この規則は、保護トンネルに着信しているはずのパケットが実際には保護トンネルに着信していないことを確認するのに必要です。パケットが IPSec によって暗号化解除されておらず、この規則が適用されると、そのパケットはドロップされます。この規則は、ネットワークにスプーフされるすべてのトラフィックを扱います。

これらの規則は、ポリシー・フィーチャーの **list rule** コマンドを使用して表示できます。

構成の例

次の例は、ポリシー・フィーチャーを使用してネットワーク内にルーターを構成する方法を示しています。最初に、次のように、ポリシー・フィーチャーにアクセスします。

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

QOS 付きの IPSec/ISAKMP ポリシー

ポリシー情報は、2 つの方法のどちらでも入力できます。初め目の方法は、個々のポリシー・オブジェクトを定義してから、それらを 1 つにまとめる方法です。この方式を取るには、最初に IPSec 変換を定義してから、IPSec 提示 (これは、IPSec 変換を参照します) を定義します。次に、IPSec アクション (IPSec 提示を参照します) を定義するという具合に、ポリシーを完全に定義するまで続けます。図31 を参照として使用すると、この方式は、ポリシー・オブジェクトの右側で始まり、左側へ進みます。

2 つ目の方法は、もっと簡単ですが、最初に高水準ポリシーを定義し、プロンプトが出たら、順に個々のポリシー・オブジェクトの定義を入力する方法です。図31 の後に構成手順例を示します。この例では、図の中の値に対応する値を使用しています。ここでは、左から右の方式を取っており、**add policy** コマンドから始まります。

必要に合うオブジェクトが以前に定義されている場合は、新しい定義を作成せずにそれを再利用できます。たとえば、以前のポリシーについて allTheTime の妥当性期間が設定されている場合、それを再利用できます。次の手順はプロセス全体を示していますが、以前に定義されたポリシー情報の再利用を例示するものではありません。以前に定義された情報の例については、349ページの『IPSec/ISAKMP 専用ポリシー』を参照してください。

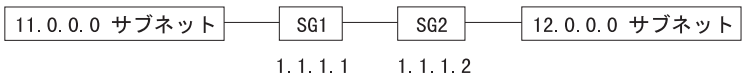


図 31. QOS 付きの IPSec/ISAKMP 構成

以下に記載されているポリシー構成のシナリオは、SG1 の全体像からとったものです。ポリシー・ステートメントは、次のとおりです。

トンネルのエンドポイントを SG1 および SG2 としてサブネット 11 からサブネット 12 までのトラフィックを保護し、DiffServ GoldService を使用してこのトンネル内のトラフィックに QOS を提供します。

1. ポリシーを追加する。

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

2. プロファイルは構成されていないため、新たに定義する必要があります。

```
List of Profiles:
0: New Profile

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

3. 新しいプロファイル定義。この場合、問題のトラフィックはサブネット 11 からサブネット 12 へのものです。

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

```
Enter IPV4 Destination Mask [255.0.0.0]?

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

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


Here is the Profile you specified...


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

4. プロファイル定義で終了し、ポリシー構成メニューに戻る。

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

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

5. 妥当性期間は設定されていないため、新たに定義する必要があります。

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

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

6. 妥当性期間設定の質問。この例では、妥当性期間は、1999 年の毎月、月曜日から金曜日までの午前 9 時から午後 5 時までです。

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

Here is the Policy Validity Profile you specified...

Validity Name   = MonToFri-9am:5pm-1999
        Duration  = 19990101000000 : 19991231000000
```

```
Months    = ALL
Days      = MON TUE WED THU FRI
Hours     = 09:00:00 : 17:00:00
Is this correct? [Yes]:
```

7. 妥当性期間定義で終了し、ポリシー構成メニューに戻る。

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

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

8. トンネルのエンドポイントは常に異なるため、必ず、新しい IPSec アクションを定義する必要があります。ただし、同じ 2 つのゲートウェイ間にトンネルが複数個存在する場合と、トンネルのエンドポイントが認識されていないワイルドカード指定のリモート・アクセス構成内の場合は例外です。

```
IPSEC Actions:
0: New IPSEC Action

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

9. IPSec アクション・メニュー

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

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

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

10. IPsec 提示は定義されていないため、新たに定義する必要があります。いったん IPsec 提示を定義すれば、複数の IPsec アクションで再利用できることに注意してください。

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

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

11. IPSec 提示構成

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

12. ESP 変換は構成されていないため、新たに定義する必要があります。いったん ESP 変換が定義されれば、あらゆる IPsec 提示で再利用できます。

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

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

13. IPSec 変換構成

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

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

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

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

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

Here is the IPSec transform you specified...

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

14. IPSec 提示メニューに戻る。

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

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

Here is the IPSec proposal you specified...

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

15. IPSec アクション・メニューに戻る。

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

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

```
Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPSec Action you specified...

IPSECAction Name = secure11NetTo12Net
Tunnel Start:End         =        1.1.1.1 : 1.1.1.2
Tunnel In Tunnel         =             No
Min Percent of SA Life   =             75
Refresh Threshold        =             85 %
Autostart                =             No
DF Bit                   =           COPY
Replay Prevention        =       Disabled
IPSEC Proposals:
genP2Proposal
Is this correct? [Yes]:
```

16. ポリシー・メニューに戻る。

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

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

17. 保護 IPSec アクション・タイプを指定してあるため、フェーズ 1 ネゴシエーションについて ISAKMP アクションを識別する必要があります。なにも定義されていないので、新しいものを入力してください。ほとんどの場合、すべてのセキュリティー・ポリシーに 1 つの ISAKMP アクションと提示で十分です。

```
ISAKMP Actions:
0: New ISAKMP Action

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

18. ISAKMP アクション構成

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

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

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

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

19. ISAKMP 提示は構成されていないため、新たに作成する必要があります。

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

20. ISAKMP 提示構成

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

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

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

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

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

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

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

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

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


Here is the ISAKMP Proposal you specified...

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

21. ISAKMP アクション構成に戻る。

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

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

Here is the ISAKMP Action you specified...

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

22. ポリシー構成に戻る。

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

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

23. DiffServ GoldService アクションを定義する。

```
DiffServ Actions:
0: New DiffServ Action

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

24. DiffServ アクション構成

    DiffServ アクションが assured (確実) 待ち行列を対象にするものである場合には、次のようになります。

```
Enter a Name (1-29 characters) for this DiffServ Action [AF11]? GoldService
Enter the permission level for packets matching this DiffServ
Action (1. Permit, 2. Deny) [2]? 1
List of DiffServ Queues:
   1) Premium
```

```
   2) Assured/BE
Enter the Queue Number(1-2) for outgoing packets matching
this DiffServ Action [2]?
How do you want to specify the bandwidth allocated to this service?
Enter absolute kbps(1) or percentage of output bandwidth(2) [2]?
Enter the percentage of output bandwidth allocated to this service [10]? 20

List of Assured Forwarding Class:
  1) AF11 Class DS Byte
  2) AF21 Class DS Byte
  3) AF31 Class DS BYte
  4) AF41 Class DS Byte
  5) New Class DS Byte

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

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

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

Here is the DiffServ Action you specified...

DiffServ Name   = GoldService                    Type =Permit

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

Is this correct? [Yes]:
```

DiffServ アクションが premium 待ち行列に対するものである場合には、次のようになります。

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

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

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

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


Here is the DiffServ Action you specified...


DiffServ Name   = ExpService                    Type =Permit
```

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

25. ポリシー構成に戻る。

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

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

Here is the Policy you specified...

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

26. DiffServ または IPSec が使用可能でない場合は、ポリシーが実施できるようになる前に DiffServ または IPSec (DiffServ フィーチャーまたは IPSec フィーチャー)、あるいはその両方を使用可能にする必要があるという警告が示されます。

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

27. このプロセスの最後のステップは、リモート ISAKMP ピアについて USER プロファイル定義を追加することです。このステップは、ISAKMP ネゴシエーションがピアを公衆認証で認証することである場合は不要です。ただし、上記の例では、認証方式として事前共用キーを選んでいるため、ユーザーを識別し、ピアが使用すると予想している事前共用キーを入力する必要があります。

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

Here is the User Information you specified...

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

28. ポリシー構成のステップはこれで完了です。DiffServ、IPSec、あるいは任意のネットワークまたは IP 構成を構成したい場合には、その構成を済ませてからでないと、IPSec トンネルは機能しません。次のリスト・コマンドの例は、完

了したばかりの構成を示しています。これらの変更を活動化するには、装置を再ロードするか、あるいはポリシー・フィーチャーの **reset database** 監視コマンドを入力してください。

```
Policy config>list all

Configured Policies....

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

Configured Profiles....

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

Configured Validity Periods

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

Configured DiffServ Actions....

DiffServ Name   = GoldService                    Type =Permit

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

Configured IPSEC Actions....

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

Configured IPSEC Proposals....

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

Configured IPSEC Transforms....

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

```
--More--

Configured ISAKMP Actions....

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

Configured ISAKMP Proposals....
Name = genP1Proposal
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB
--More--

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

Configured Manual IPSEC Tunnels....

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

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

IPSec/ISAKMP 専用ポリシー

構成手順の例が、図32 の後に示してありますが、この例では図中の値に対応する値を使用し、左から右方式を採用しています。以前の手順で作成した情報を再利用することにより、以前の手順例での作成方法を示しています。

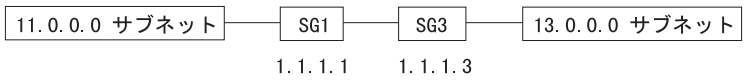


図 32. IPSec の構成と以前の定義の再利用

以下に記載されているポリシー構成のシナリオは、SG1 の全体像からとったものです。このシナリオのポリシー・ステートメントは、次のとおりです。

トンネルのエンドポイントを SG1 および SG3 としてサブネット 11 からサブネット 13 までのトラフィック (TCP トラフィックだけ) を保護し、QOS は提供しません。

1. ポリシーを追加する。

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

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

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

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

Here is the Profile you specified...

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

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

2. 妥当性期間を再利用する。

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

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

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

Select the Security Action type (1-2) [2]?
Should the traffic flow into a secure tunnel or in the clear:
     1) Clear
     2) Secure Tunnel
 [2]?
Enter Tunnel Start Point IPV4 Address
```

```
 [11.0.0.5]? 1.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 1.1.1.3
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

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

3. 以前に定義された構成からの IPSec 提示を再利用する。

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

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


Here is the IPSec Action you specified...


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

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

4. 以前の構成からの ISAKMP アクションを再利用する。

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

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

Here is the Policy you specified...

Policy Name     = examplePolicySecure11to13
State:Priority =Enabled    : 10
Profile        =trafficFrom11NetTo13Net
```

```
Valid Period   =MonToFri-9am:5pm-1999
IPSEC Action   =secure11To13
ISAKMP Action  =genPhase1Action
Is this correct? [Yes]:
```

全公衆トラフィックの除去 (フィルター規則)

このポリシー例は、IPSec を通じて保護されていないすべてのトラフィックをドロップする公衆インターフェースについての単純なドロップ規則の構成方法を示しています。この規則は汎用性が高いため、あらゆる規則の最低の優先順位を設定するもので **なければなりません**。

1. ポリシーを追加する。

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

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

2. 公衆インターフェース (1.1.1.1) で発着するすべてのトラフィックを含む新しいプロファイルを定義する。

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

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

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

3. 発信元および宛先 (あるいはそれら両方) の情報がワイルドカード指定になっているため、このトラフィックが着信または発信すると予想されるインターフェースを指定する必要があります。

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

4. 公衆インターフェースを介して発信されるトラフィックについてインターフェースのペアを追加する。

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

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

5. 公衆インターフェースを介して着信するトラフィックについて別のインターフェースのペアを追加する。このペアに、先のインターフェースの対と同じ名前を付けて、同じグループに割り当てます。

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

Number of Ifc Pair Group [1]?

Here is the Profile you specified...

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

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

6. all the time を指定する新しい妥当性期間を追加する。

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

Enter number of the validity period for this policy [1]? 0
Enter a Name (1-29 characters) for this Policy Valid Profile []? allTheTime
Enter the lifetime of this policy. Please input the
information in the following format:
                yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.
 [*]?
During which months should policies containing this profile
be valid.  Please input any sequence of months by typing in
```

```
the first three letters of each month with a space in between
each entry, or type ALL to signify year round.
 [ALL]?
During which days should policies containing this profile
be valid.  Please input any sequence of days by typing in
the first three letters of each day with a space in between
each entry, or type ALL to signify all week
 [ALL]?
Enter the starting time (hh:mm:ss or * denotes all day)
 [*]?

Here is the Policy Validity Profile you specified...

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

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

7. 全トラフィックをドロップする新しい IPsec アクション (フィルター・アクション) を追加する。

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

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

Here is the IPSec Action you specified...

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

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

Here is the Policy you specified...

Policy Name     = dropAllPublicTraffic
        State:Priority =Enabled    : 5
        Profile        =allPublicTraffic
        Valid Period   =allTheTime
```

```
        IPSEC Action   =dropTraffic
Is this correct? [Yes]:
```

LDAP ポリシー検索エンジンの構成と使用可能化

この例は、LDAP ポリシー検索エンジンを構成し、使用可能にする方法を示しています。この例では、LDAP ディレクトリーが 2 つ (1 次ディレクトリーと 2 次ディレクトリー) あり、それぞれ 11.0.0.2 および 13.0.0.1 という IP アドレスをもっています。これらのディレクトリーは、両方とも TCP ポート 389 で listen しているため、装置は、cn=router、パスワード myPassWord として LDAP サーバーまでバインドする必要があります。ルーターのポリシーのディレクトリー 3 の基本項目は cn=RouterDeviceProfile,o=ibm,c=us です。

注: 現在、1 次および 2 次両方の LDAP サーバーが同じポート上で listen しており、ルーターについて同じ認証証明をもつ必要があります。DeviceProfile は、両方のディレクトリー・サーバー内のルーターについて同じでなければなりません。

この例は、LDAP 通信が IPSec により保護されるデフォルト・ポリシーの設定方法も示しています。この例では、ISAKMP 認証については事前共用キーを、フェーズ 1 およびフェーズ 2 の認証および暗号化パラメーターについては SHA および 3DES を使用します。トンネルのスタートポイントは、LDAP ポリシー検索を実行する装置の場合は 1.1.1.4 で、トンネルのエンドポイントは、11.0.0.1 LDAP サーバーの場合は 1.1.1.1 、13.0.0.1 LDAP サーバーの場合は 1.1.1.3 です。

1. LDAP ポリシー検索エンジンを構成して使用可能にし、結果を表示する。

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

        Primary Server Address:               11.0.0.1
        Secondary Server Address:             13.0.0.1


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


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


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


        Search policies from LDAP Directory:  Enabled
```

2. デフォルト・ポリシーを設定する。

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

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

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

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

Enter phase 1 ISAKMP negotiation parameters:

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

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

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

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

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

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

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

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

Select the ESP Cipher Algorithm (1-4) [1]? 2
Tunnel Start IPV4 Address (Primary LDAP Server)
 [0.0.0.0]? 1.1.1.4
Tunnel End Point IPV4 Address (Primary LDAP Server)
 [0.0.0.0]? 1.1.1.1
Tunnel Start IPV4 Address (Secondary LDAP Server)
 [1.1.1.4]?
Tunnel End Point IPV4 Address (Secondary LDAP Server)
 [1.1.1.1]? 1.1.1.3
Policy config>list default-policy

Default Policy Rule:                  Drop All IP Traffic except secure LDAP
Default error handling procedure:     Reset Policy Database to Default Rule
```

```
Phase 1 ISAKMP negotiation parameters:
Diffie Hellman Group ID:               1
Hashing Algorithm:                     SHA
ISAKMP Cipher Algorithm:               ESP 3DES CBC
Per-shared key value:                  test

Phase 2 IPSEC negotiation parameters:
IPsec ESP Authentication Algorithm:    HMAC SHA
ESP Cipher Algorithm:                  3DES
Local Tunnel Addr (Primary Server):    1.1.1.4
Remote Tunnel Addr (Primary Server):   1.1.1.1
Local Tunnel Addr (Secondary Server):  1.1.1.4
Remote Tunnel Addr (Secondary Server): 1.1.1.3
```

この時点で、ポリシー・フィーチャーを使用してネットワーク内のルーターを管理する準備が整いました。プロファイル、提示、変換、およびアクションといった必要なポリシー・パラメーターの構成に使用されるコマンドについて詳しくは、365ページの『ポリシー構成コマンド』、386ページの『LDAP ポリシー・サーバー構成コマンド』、および 391ページの『ポリシー監視コマンド』を参照してください。

ポリシー・クィック構成例

ポリシー・フィーチャーで使用できる **qconfig** コマンドを使用すると、4 つのシナリオの中の 1 つの基づいたポリシーを迅速に追加できます。2、3 の簡単な質問があります。次に、応答に基づいて、ポリシー・オブジェクトが生成されます。**qconfig** コマンドは、事前定義のポリシー・テンプレートを利用して、尋ねられる構成の質問を最少にします。**qconfig** によってポリシー・オブジェクトを変更はできません。これは、ポリシーを迅速に追加する手段に過ぎません。このコマンドの詳細については、365ページの『ポリシー構成コマンド』を参照してください。

次の例は、この章で前に説明した IPSec/ISAKMP の例と同じものです。基本的には、その目標は、11.0.0.0 サブネットから SG1 と SG2 をもつ 12.0.0.0 サブネットへのトラフィックを保護し認証することです。加えて、これらのセキュリティー・ゲートウェイによって保護されるトラフィックには、QOS が提供される必要があります。この例では、その QOS は AF11 で、厳しいセキュリティーが選択されます。

```
Policy config>qconfig
Enter a Name (1-29 characters) for this Policy [policyQC_1]?
Please choose from one of the following Scenarios:

1: Branch Office Scenario
2: Remote Access User Scenario (IPSEC and L2TP)
3: Drop Traffic not matched on Untrusted Interface
4: Custom
Selection [1]?
Local Subnet (Base Address) [0.0.0.0]? 11.0.0.0
Local Subnet (Net Mask) [255.0.0.0]?
Local Tunnel Endpoint [11.0.0.5]? 1.1.1.1
Remote Subnet (Base Address) [0.0.0.0]? 12.0.0.0
Remote Subnet (Net Mask) [255.0.0.0]?
Remote Tunnel Endpoint [0.0.0.0]? 1.1.1.2
Configure Ports and Protocols? [No]:
1: Strong Security, 2: Very Strong Security, 3: Help [1]?
Authenticate Peer using 1:Pre-shared Key or 2:Certificate(RSA Signatures) [2]? 1
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (4 characters) in ascii:
Select from the following DiffServ Actions:
        0: Best Effort (No DiffServ)
```

```
        1: EF
        2: AF11
        3: AF21
        4: AF31
        5: AF41
        6: GoldService

Enter Selection [0]? 2
Configure advanced options? [No]:


Here is the information you entered...

Policy Name:  policyQC_1 (Branch Office Scenario)
Local Information:
------------------
            Subnet:  11.0.0.0/255.0.0.0
   Tunnel Endpoint:  1.1.1.1
        Port Range:  00000-65535

Remote Information:
-------------------
            Subnet:  12.0.0.0/255.0.0.0
   Tunnel Endpoint:  1.1.1.2
        Port Range:  00000-65535

Other Information:
------------------
          Protocol:  000-255
          Priority:  10
          Security:  Strong Security
        Encap Mode:  Tunnel
         Auth Mode:  Pre-Shared Key
   Validity Period:  allTheTime
   DiffServ Action:  AF11
Continue? [Yes]:
-----------------------------------------
```

Based on the input to these simple questions, the QCONFIG mechanism generated the following objects:

1.

```
Policy config>list policy by-name policyQC_1

Policy Name     = policyQC_1
        State:Priority =Enabled    : 10
        Profile        =policyQC_1
        Valid Period   =allTheTime
        IPSEC Action   =policyQC_1
        ISAKMP Action  =generalPhase1Action
        DiffServ Action=AF11
```

2.

```
Policy config>list ipsec-action by-name policyQC_1
IPSECAction Name = policyQC_1
        Tunnel Start:End         =        1.1.1.1 : 1.1.1.2
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =              1
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                strongP2EspProp
                strongP2EspAhProp
                veryStrongP2EspProp
                veryStrongP2EspAhProp
```

3.

```
Policy config>list profile by-name policyQC_1

Profile Name    = policyQC_1
        sAddr:Mask=       11.0.0.0 : 255.0.0.0       sPort=    0 : 65535
        dAddr:Mask=       12.0.0.0 : 255.0.0.0       dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
```

4.

```
Policy config>list user by-name
List of Users:
  num: User Info                          :Group Name
    1: 1.1.1.2                            :IKE-Peers
Enter the number of user [1]?
Name      = 1.1.1.2
        Type      = IPV4 Addr
        Group     =IKE-Peers
        Auth Mode =Pre-Shared Key
```

事前定義ポリシー・オブジェクト

次のポリシー・オブジェクトは、ユーザーのために事前に定義されています。これらのオブジェクトは、もっとも典型的な構成を表し、多くのポリシー構成で使用できるように意図されています。**qconfig** コマンドと一緒に、これらの事前定義ポリシー・オブジェクト定義は、ネットワーク構成にポリシーを追加する簡単な方法となります。事前定義テンプレートを変更することも削除することもできません。オブジェクトを変更したい場合には、新しい名前を指定して、**copy** コマンドを使用してこのオブジェクトをコピーする必要があります。一度これを行っておくと、コピーを変更できます。新しいリリースまたはコードの PTF バージョンにアップグレードし、テンプレートに変更があった場合には、ポリシー・フィーチャー **refresh-templates** 構成コマンドを使用して最新のテンプレートを入手する必要があります。このようにしなければ、元の定義が使用され続けます。

次の事前定義オブジェクトがポリシー・フィーチャーのためにあります。

妥当性期間

次の妥当性期間は、事前に定義されます。

```
Validity Name   = allTheTime
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day

Validity Name   = allTheTimeMonThruFri
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = All Day

Validity Name   = 9to5MonThruFri
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 09:00:00 : 17:00:00

Validity Name   = 5to9MonThruFri
```

```
        Duration  = Forever
        Months    = ALL
        Days      = MON TUE WED THU FRI
        Hours     = 17:00:00 : 09:00:00
```

DiffServ アクション

次の DiffServ アクション・オブジェクトは、事前に定義されます。

```
DiffServ Name   = EF                              Type =Permit
        DS mask:modify =xFC:xB8
        Queue:BwShare  =Premium    : 19 %
        Token Rate:    = 0 bytes/sec
        Token Bucket:  = 0 bytes

DiffServ Name   = AF11                             Type =Permit
        DS mask:modify =xFC:x28
        Queue:BwShare  =Assured    : 15 %
        No Policing Selected

DiffServ Name   = AF21                             Type =Permit
        DS mask:modify =xFC:x48
        Queue:BwShare  =Assured    : 10 %
        No Policing Selected

DiffServ Name   = AF31                             Type =Permit
        DS mask:modify =xFC:x68
        Queue:BwShare  =Assured    : 10 %
        No Policing Selected

DiffServ Name   = AF41                             Type =Permit
        DS mask:modify =xFC:x88
        Queue:BwShare  =Assured    : 5 %
```

IPSec アクション

次の IPSec アクションは、事前に定義されます。

```
IPSECAction Name = ipsecDropTraffic
        Action   = Drop

IPSECAction Name = ipsecPassTrafficClear
        Action   = Clear
```

IKE フェーズ 2 に関する IPSec 提示

IKE フェーズ 2 に関する IPSec 提示オブジェクトは、事前に定義されます。

```
Name  = strongP2EspProp
        Pfs   = N
        ESP Transforms:
                espTunnelMD5andDES
                espTunnelSHAandDES

Name  = strongP2EspAhProp
        Pfs   = N
        AH Transforms:
                ahTunnelMD5
                ahTunnelSHA
        ESP Transforms:
                espTunnelDES

Name  = veryStrongP2EspProp
        Pfs   = N
        ESP Transforms:
                espTunnelSHAand3DES
                espTunnelMD5and3DES

Name  = veryStrongP2EspAhProp
```

```
        Pfs   = N
        AH Transforms:
                ahTunnelSHA
                ahTunnelMD5
        ESP Transforms:
                espTunnel3DES

Name  = veryStrongP2EspPropPFS
        Pfs   = Y     DHGrp= 1
        ESP Transforms:
                espTunnelSHAand3DES
                espTunnelMD5and3DES

Name  = strongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportMD5andDES
                espTransportSHAandDES

Name  = strongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportMD5
                ahTransportSHA
        ESP Transforms:
                espTransportDES

Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = strongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportMD5
                ahTransportSHA
        ESP Transforms:
                espTransportDES

Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
                espTransport3DES

Name  = veryStrongP2EspPropXport
        Pfs   = N
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropXport
        Pfs   = N
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
```

```
                espTransport3DES

Name  = veryStrongP2EspPropPFSXport
        Pfs   = Y     DHGrp= 1
        ESP Transforms:
                espTransportSHAand3DES
                espTransportMD5and3DES

Name  = veryStrongP2EspAhPropPFSXport
        Pfs   = Y     DHGrp= 1
        AH Transforms:
                ahTransportSHA
                ahTransportMD5
        ESP Transforms:
                espTransport3DES
```

IPSec 変換

次の IPSec 変換オブジェクトは、事前に定義されます。

```
Transform Name  = ahTransportMD5
        Type =AH    Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =None

Transform Name  = ahTransportSHA
        Type =AH    Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =None

Transform Name  = ahTunnelMD5
        Type =AH    Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =None

Transform Name  = ahTunnelSHA
        Type =AH    Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =None

Transform Name  = espTunnelMD5andDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =DES

Transform Name  = espTunnelSHAandDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES

Transform Name  = espTunnelMD5and3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =3DES

Transform Name  = espTunnelSHAand3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES

Transform Name  = espTunnelDES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =DES

Transform Name  = espTunnel3DES
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =3DES

Transform Name  = espTransportMD5andDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =DES

Transform Name  = espTransportSHAandDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES
```

```
Transform Name  = espTransportMD5and3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =MD5   Encr =3DES

Transform Name  = espTransportSHAand3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =3DES

Transform Name  = espTransportDES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =DES

Transform Name  = espTransport3DES
        Type =ESP   Mode =Transport  LifeSize=   50000 LifeTime=    3600
        Auth =None  Encr =3DES
```

ISAKMP アクション

次の ISAKMP アクション・オブジェクトは、事前に定義されます。

```
ISAKMP Name     = generalPhase1Action
        Mode                    =            Main
        Min Percent of SA Life  =               1
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =              No
        ISAKMP Proposals:
                veryStrongP1PropRSACert
                strongP1PropRSACert
                veryStrongP1PropSharedKey
                strongP1PropSharedKey
```

ISAKMP 提示

次の ISAKMP 提示オブジェクトは、事前に定義されます。

```
Name = strongP1PropSharedKey
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC

Name = strongP1PropRSACert
        AuthMethod = Certificate (RSA SIG)
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC

Name = veryStrongP1PropSharedKey
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB

Name = veryStrongP1PropRSACert
        AuthMethod = Certificate (RSA SIG)
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = SHA
        Encr Algo  = 3DES CB
```

第20章 ポリシー・フィーチャーの構成と監視

この章では、ネットワーク内でルーター装置を構成し、操作するためにポリシー・フィーチャーが提供する LDAP およびポリシー・コマンドについて説明します。この章には、次の内容が記載されています。

- 『ポリシー構成プロンプトへのアクセス』
- 『ポリシー構成コマンド』
- 386ページの『LDAP ポリシー・サーバー構成コマンド』
- 391ページの『ポリシー監視プロンプトへのアクセス』
- 391ページの『ポリシー監視コマンド』
- 397ページの『ポリシー動的再構成サポート』

ポリシー構成プロンプトへのアクセス

ポリシー構成コマンドを入力するには、次のようにします。

1. OPCON (*) プロンプトで **talk 6** と入力する。
2. `Config>` プロンプトで **feature policy** と入力する。

`Policy config>` プロンプトが表示されます。これで、ポリシー構成コマンドを入力できます。

ポリシー構成コマンド

これらのコマンドを使用すると、ポリシーに含める情報を構成できます。 表44 はポリシー構成コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて詳しく説明します。これらのコマンドは、`Policy config>` プロンプトで入力します。コマンドとオプションを 1 行に入力することもできますが、コマンドだけを入力して、プロンプトに応答することもできます。有効なコマンド・オプションを見るためには、オプションの代わりに疑問符を付けてコマンドを入力してください。

表 44. ポリシー構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxvページの『ヘルプの入手』を参照してください。
Add	ポリシーの作成に使用される情報を追加します。
Change	ポリシーを構成する情報を変更します。
Copy	1 つのポリシーから別のポリシーへ情報をコピーします。
Delete	ポリシーから情報を削除します。
Disable	ポリシーを使用不可にします。
Enable	ポリシーを使用可能にします。
List	ポリシー内の情報を表示します。
Qconfig	事前定義テンプレートに基づいたポリシーを追加できます。
refresh-templates	特定のプラットフォームで実行しているコードのバージョンの最新のテンプレートを導入したり、除去できます。これによって、各種ソフトウェア・リリースや PTF レベル間での変更がより容易になり、そのようにする決定を簡素化します。

表 44. ポリシー構成コマンド (続き)

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

Add

add コマンドは、ポリシーに情報を追加するのに使用します。

構文 : add
- diffserv-action
- interface-pair
- ipsec-action
- ipsec-manual-tunn
- ipsec-proposal
- ipsec-transform
- isakmp-action
- isakmp-proposal
- policy
- profile
- rsvp-action
- user
- validity-period

diffserv-action

適用する DiffServ-action 選択項目に関する情報を入力するようプロンプト指示します。詳細については、455ページの『第23章 ディファレンシェーテッド・サービス・フィーチャーの使用』 および 463ページの『第24章 ディファレンシェーテッド・サービス・フィーチャーの構成と監視』 を参照してください。

name ポリシーの DiffServ アクションの固有な名前

permission level

この DiffServ アクションに適合するパケットをルーターが転送するかどうかを指定します。

1 許可

2 拒否

デフォルト値 : 2

queue number

この DiffServ アクションに適合する発信パケットが入れられる待ち行列。

1 特別 (EF)

2 確実 (AF)/Best Effort

デフォルト値 : 2

bwshare type
帯域幅共用割り当てのタイプ

1 絶対値 (Kbps 単位)

2 パーセント (合計出力帯域幅の)

デフォルト値 : 2

bwshare
このサービスに割り振られた帯域幅 (Kbps 単位または出力帯域幅のパーセント)

確実転送

Assured forwarding class
この DiffServ アクションに適合する発信パケットの確実転送クラスを指定します。

1 AF1 クラス DS バイト

2 AF2 クラス DS バイト

3 AF3 クラス DS バイト

4 AF4 クラス DS バイト

5 新しいクラス

Assured forwarding policing type
この DiffServ アクションに適合する発信パケットの AF ポリシングのタイプを指定します。

1 単一レート、color-blind TCM

2 単一レート、color-aware TCM

3 2 レート、color-blind TCM

4 2 レート、color-aware TCM

5 なし

単一レート TCM パラメーター

Committed information rate (CIR)
コミット情報レートを指定します。

Committed burst size (CBS)
コミット・バースト・サイズを指定します。

Excess burst size (EBS)
超過バースト・サイズを指定します。

注:

1. 秒当たりの IP パケット数についてバイト単位で CIR を指定します。これには、IP ヘッダーが含まれますが、リンク固有ヘッダーは含まれません。
2. バイト単位で CBS と EBS を指定します。これらの値は、少なくともこれらのいずれかをゼロより大きくするように構成する必要がありま

す。CBS または EBS の値がゼロより大きいとき、ストリーム内で使用できる最大の IP パケットのサイズより大きいか等しくすることをお勧めします。

2 レート TCM パラメーター

Committed information rate (CIR)
コミット情報レートを指定します。

Committed burst size (CBS)
コミット・バースト・サイズを指定します。

Peak information rate (PIR)
ピーク情報レートを指定します。

Peak burst size (PBS)
ピーク・バースト・サイズを指定します。

注:

1. 秒当たりの IP パケット数についてバイト単位で CIR と PIR を指定します。これには、IP ヘッダーが含まれますが、リンク固有ヘッダーは含まれません。PIR 値は、CIR に等しいか CIR より大きくする必要があります。
2. バイト単位で CBS と PBS を指定します。両方とも、ストリーム内で使用できる最大の IP パケットのサイズより大きいか等しい値に構成する必要があります。

Expedited Forwarding

transmitted ds-byte mask
優先転送の場合の送信済み ds バイトに適用されるマスク。この値は、パケットを送信するときに変更しなければならないパケットの DS バイトのビットを指示します。このバイトの任意の位置にゼロが入っていると、そのビットは変更してはならないことが暗黙指定されます。

デフォルト値: 00 (ビットは変更しない)

transmitted ds-byte modify value
パケットに適用すべき IP DS (TOS) バイトのマーク付けが、この装置によって転送されます。マスクにゼロが入っていると、対応するビットは変更されないことが暗黙指定されます。1 の場合、マーク・バイト内のビット値によってそのビットにマーク付けることが暗黙指定されます。演算は newTOSByte = (Mask^ & receivedTOSByte) | (Mask&Mark) です。^ ^ ^ は、ビット・ベースの補数 (Mask:Mark) です。

例 :

```
11111101:00000001
```

この例を使用すると、受信した値 0x07 は値 0x03 と一緒に送信されます。

デフォルト値 : X'00' (ビットは変更しない)

EF policing type
優先転送のポリス構成タイプを指定します。

1 Default config

token rate および token bucket size の各パラメーターは、帯域幅パラメーター構成から計算されます。

2 Custom config

Token Rate:
トークンの補充レート

Token Bucket Size:
トークンのバケット・サイズ

注:

1. 秒当たりの IP パケット数についてバイト単位でトークン・レートを指定します。これには、IP ヘッダーが含まれますが、リンク固有ヘッダーは含まれません。
2. バイト単位でトークンのバケット・サイズを指定します。この値は、ゼロより大きく、ストリームで最大の IP パケットのサイズより大きいかまたは等しくする必要があります。

interface-pair

インターフェースの対は、プロファイルを、特定のインターフェースまたはインターフェースの集合と関連付けます。デフォルトで、プロファイル・オブジェクトは、インターフェースへのポリシーの適用を制限しません。必要な場合は、インターフェースのペアを追加すると制限することができます。インターフェースの対は、トラフィックが着信するインターフェースの IP アドレスと、トラフィックが発信するインターフェースの IP アドレスを指定します。

次の例は、いずれかのインターフェースに着信し、公衆インターフェースから発信する (あるいは、その逆の場合もあり) トラフィックを表す、同じ名前の 2 つのインターフェースの対を示します。

```
1) Group Name: inOutPublic
        In:Out=255.255.255.255 : 1.1.1.1
        In:Out=1.1.1.1 : 255.255.255.255
```

Name インターフェースの対の名前

Ingress interface
入力インターフェースの IPv4 アドレス

デフォルト値 : 255.255.255.255 (任意)

Egress interface
出力インターフェースの IPv4 アドレス

デフォルト値 : 255.255.255.255 (任意)

IPSec-action

フェーズ 2 トンネルをセットアップするための情報を入力するようプロンプト指示します。

Name IPSec アクションの名前。

Action type
このアクションが含まれるポリシーのプロファイルに適合するパケットに適用されるアクション

1 Block (ブロック・コネクション)

2 Permit (このアクションに適合するパケットを許可します)。IPSec 提示が存在しない場合は、パケットをパスします。IPSec 提示が存在する場合は、パケットに IPSec セキュリティー処理を適用します。

デフォルト値 : 2

次のオプションは、アクション・タイプとして pass を指定した場合にだけ使用可能です。

Traffic flow type
トラフィック・フローのタイプ (保護トンネルまたはクリア内)

1 Clear

2 Secure Tunnel

デフォルト値 : 2

次のオプションは、トラフィック・フローを secure (保護) と指定した場合にだけ使用可能です。

Tunnel start point
トンネル・スタートポイントの IPv4 アドレス

Tunnel end point
トンネル・エンドポイントの IPv4 アドレス。(リモート・アクセスの場合は 0.0.0.0)

デフォルト値 : 0.0.0.0

Tunnel-in-tunnel
このトンネルによって保護されているトラフィックを、この装置上に構成されている別のポリシーでさらに保護するかどうかを指定します。

有効なオプション : Yes または No

デフォルト値 : No

Percentage of SA lifesize/lifetime to accept
SA 寿命サイズ / 存続時間の (パーセントとしての) 最小 SA 寿命サイズ / 存続時間。これより小さい値で受信された SA 寿命サイズ / 存続時間は受け入れられません。

デフォルト値 : 75

SA refresh threshold
SA が自動的に更新される SA 存続時間または寿命サイズ値へのパーセント。

デフォルト値 : 85

DF-Bit-Setting
オリジナルのパケットから Don't Fragment ビットをコピーする (Copy) かどうか、また、トンネル・モードで実行している場合は

IPSec パケットの外側のヘッダーにそのビットをセットする (Set) かクリアする (Clear) かを指定します。

1 Copy

2 Set

3 Clear

デフォルト値 : 1

Replay-Prevention
IPSec が受信した IPSec パケットについて再生 (replay) の防止を実施するかどうかを指定します。このモードでは、IPSec により、順序番号は有効であり、1 回しか受信されません。

1 Enable

2 Disable

デフォルト値 : 2

Negotiate SA Automatically
フェーズ 2 SA をシステムの初期設定時に自動的にネゴシエーションするかどうかを指定します。

Yes または No

デフォルト値 : No

IPSec proposal
フェーズ 2 の間に送信または検査される IPSec 提示の名前 (提示は最大 5 つまで指定できます)。指定する順序により、それぞれの優先順位が決められます。最初は 1 で、これが最高の優先順位です。

IPSec-manual-tunn
フェーズ 2 トンネルを手動でセットアップするための情報を入力するようプロンプト指示します。

Tunnel name
IPSec 手動トンネルの名前

Tunnel lifetime
トンネル存続時間 (分単位)

デフォルト値 : 46080

Encapsulation mode
使用するカプセル化モード

tunn トンネル・モード

trans トランスポート・モード

デフォルト値 : tunn

Policy 使用するトンネル・ポリシーのタイプ

AH 認証ヘッダー (Authentication Header)

ESP セキュリティー・ペイロードのカプセル化 (Encapsulating Security Payload)

AH-ESP
アウトバウンド・パケットの場合に、認証の前に暗号化が実行されることを指定します。

ESP-AH
アウトバウンド・パケットの場合に、暗号化の前に認証が実行されることを指定します。

デフォルト : AH-ESP

Local IP address
発信元 IPv4 アドレス

デフォルト値 : 11.0.0.5

Local encryption SPI
発信元セキュリティー・パラメーター・インデックス値

デフォルト値 : 256

Local encryption algorithm
発信元暗号アルゴリズム

Null 暗号化なし

CDMF 商用データ・マスキング機能 (Commercial Data Masking Facility)

DES-CBC
データ暗号化規格および暗号化ブロック・チェーン (Data Encryption Standard and Cipher Block Chaining)

3DES トリプル・データ暗号化規格 (Triple Data Encryption Standard)

デフォルト値 : DES-CBC

Local encryption key
16 文字のキー

Padding
ローカル暗号化のための追加埋め込み

デフォルト値 : 0

Local ESP authentication
ローカル ESP 認証を使用するかどうかを指定します。

Yes または No

デフォルト値 : Yes

Remote IP address
宛先 IPv4 アドレス

デフォルト値 : 0.0.0.0

Remote encryption SPI
宛先セキュリティー・パラメーター・インデックス値

デフォルト値 : 256

Remote encryption algorithm
宛先暗号アルゴリズム

Null 暗号化なし

CDMF 商用データ・マスキング機能 (Commercial Data Masking Facility)

DES-CBC
データ暗号化規格および暗号化ブロック・チェーン (Data Encryption Standard and Cipher Block Chaining)

3DES トリプル・データ暗号化規格 (Triple Data Encryption Standard)

デフォルト値 : DES-CBC

Remote encryption key
16 文字のキー

Verify remote encryption padding.
リモート暗号化埋め込みを検証するかどうかを指定します。

Yes または No

デフォルト値 : No

Remote ESP authentication
リモート ESP 認証を使用するかどうかを指定します。

Yes または No

デフォルト値 : Yes

DF bit
Don't Fragment ビットを処理する方法を指定します。

Copy DF ビットをコピーします。

Set DF ビットをオンにセットします。

Clear DF ビットをオフにセットします。

デフォルト値 : COPY

Enable tunnel
トンネルの作成時にトンネルを使用可能にするかどうかを指定します。

Yes または No

デフォルト値 : Yes

IPSec-proposal
IPSec 提示を作成するための情報を入力するようプロンプト指示します。

IPSec proposal name
IPSec 提示の名前

Perfect forward secrecy
以前に悪用されてしまったキーから現在のキーを誰にも判別できないようにするために、IKE を使用するかどうかを指定します。

Yes または No

デフォルト値 : No

Diffie Hellman Group ID
Diffie Hellman グループのタイプ

1 Diffie Hellman Group 1

2 Diffie Hellman Group 2

デフォルト値 : 1

AH transform
この提示のための AH 変換の名前 (変換は最大 5 つまで指定できます)。指定する順序により、それぞれの優先順位が決められます。最初は 1 で、これが最高の優先順位です。

ESP transform
この提示のための ESP 変換の名前 (提示は最大 5 つまで指定できます)。指定する順序により、それぞれの優先順位が決められます。最初は 1 で、これが最高の優先順位です。

IPSec-transform
IPSec 変換に関する情報を入力するようプロンプト指示します。

IPSec transform name
IPSec 変換の名前

Protocol ID
使用するセキュリティー・プロトコル

1 IPSec-AH

2 IPSec-ESP

デフォルト値 : 1

AH Authentication Algorithm
使用する AH 確認アルゴリズム

1 HMAC-MD5

2 HMAC-SHA

デフォルト値 : 1

Encapsulation mode
使用するカプセル化モード

1 Tunnel

2 Transport

デフォルト値 : 1

ESP Authentication Algorithm
使用する ESP 確認アルゴリズム

0 なし

1 HMAC-MD5

2 HMAC-SHA

デフォルト値 : 2

ESP cipher algorithm
使用する ESP 暗号アルゴリズム

1 ESP DES

2 ESP 3DES

3 ESP CDMF

4 ESP NULL (暗号化なし)

デフォルト値 : 1

SA lifesize
この提示についての SA の寿命サイズ (Kb 単位)

デフォルト値 : 50000

SA lifetime
この提示についての SA の存続時間 (秒単位)

デフォルト値 : 3600

ISAKMP-Action
適用する ISAKMP アクションに関する情報を入力するようプロンプト指示します。

Name ISAKMP アクションの名前

Exchange mode
フェーズ 1 ネゴシエーションの交換モードのタイプ

1 Main

2 Aggressive

デフォルト値 : 1

Percentage of Minimum SA lifesize/lifetime
SA 寿命サイズ / 存続時間の (パーセントとしての) 最小 SA 寿命サイズ / 存続時間。これより小さい値をもつ SA 寿命サイズ / 存続時間は受け入れられません。

デフォルト値 : 75

ISAKMP 接続の寿命サイズ
フェーズ 1 接続の寿命サイズ (Kb 単位)。フェーズ 1 接続が満了

すると、次にフェーズ 2 SA の更新が必要になったときは、フェーズ 1 が完全に再度ネゴシエーションしてからでないと、フェーズ 25 は開始できません。

デフォルト値 : 5000

ISAKMP connection lifetime
フェーズ 1 接続の存続時間 (秒単位)。フェーズ 1 接続が満了すると、次にフェーズ 2 の更新が必要になったときに、フェーズ 1 は完全に初めから開始します。

デフォルト値 : 5000

Negotiate SA automatically
SA をシステムの初期設定時に自動的にネゴシエーションするかどうかを指定します。

Yes または No

デフォルト値 : No

ISAKMP proposal
フェーズ 2 即時モード時に送信または検査される ISAKMP 提示の名前 (提示は最大 5 つまで指定できます)。指定する順序により、それぞれの優先順位が決められます。最初は 1 で、これが最高の優先順位です。

ISAKMP-Proposal
ISAKMP ネゴシエーションで使用される ISAKMP 提示情報を入力するようプロンプト指示します。

ISAKMP proposal name
ISAKMP 提示の名前

Authentication method
ISAKMP フェーズ 1 ネゴシエーション中に使用する認証のタイプ

1 Pre-Shared Key (事前共用キー)

2 RSA SIG (認証モード)

デフォルト値 : 1

Hash algorithm
フェーズ 1 ネゴシエーション時に使用するハッシュ・アルゴリズムのタイプ

1 MD5

2 SHA

デフォルト値 : 1

Cipher algorithm
フェーズ 1 ネゴシエーション時に使用する暗号アルゴリズムのタイプ

1 DES

2 3DES

デフォルト値 : 1

Diffie Hellman Group ID
フェーズ 1 ネゴシエーション時に使用する Diffie Hellman グループのタイプ

1 Diffie Hellman Group 1

2 Diffie Hellman Group 2

デフォルト値 : 1

SA lifesize
この提示についての SA の寿命サイズ (Kb 単位)

デフォルト値 : 50000

SA lifetime
この提示についての SA の存続時間 (秒単位)

デフォルト値 : 5000

Policy ポリシー構成に関する情報を入力するようプロンプト指示します。この情報とは、Profile name (必須)、RSVP name (任意指定)、DiffServ name (任意指定)、IPSec name (任意指定)、ISAKMP name (任意指定)、および Validity Period Profile (任意指定) です。ポリシーが有効であるためには、DiffServ、IPSec、ISAKMP、または RSVP のどれかを指定する必要があります。

デフォルト値 : Valid all the time

Name ポリシー構成の名前

Priority
このポリシーの、他のポリシーに対する相対的優先順位 (数値が大きいほど、優先順位は高くなります)。これは、1 つのパケットに複数のポリシーが適用される場合に対立を解決するために使用されます。

デフォルト値 : 5

Profile
このポリシーのために使用する、以前に構成済みのデータ・トラフィック・プロファイルの名前

Validity period
このポリシーのために使用する、以前に構成済みの妥当性期間の名前

IPSec action
このポリシーで IPSec アクションを実行しようとする場合は、このポリシーのために使用する、以前に構成済みの IPSec アクションの名前。保護 IPSec アクションを指定する場合は、ISAKMP アクションも指定する必要があります。

ISAKMP action
このポリシーのために使用する、以前に構成済みの ISAKMP アクションの名前。ISAKMP アクションを指定する場合は、IPSec アクションも指定する必要があります。

Diffserv action
DiffServ アクションをこのポリシーにマップしたい場合は、以前に構成済みの DiffServ アクションの名前

RSVP action
このポリシーが実施する RSVP アクションの名前

Profile
アクションを実行するポリシー・プロファイルについてのセレクター (条件) の集合を定義するための情報を入力するようプロンプト指示します。

name ポリシー・プロファイルの名前

ipv4-src-address-format
IPv4 発信元アドレスの形式 (range, netmask, single address)

ipv4-src-address
IPv4 発信元アドレス (アドレス形式が *range* の場合は低位のアドレス)

デフォルト値 : 0.0.0.0

ipv4-src-mask
IPv4 発信元アドレス (アドレス形式が *range* の場合は高位のアドレス)

デフォルト値 : 255.0.0.0

ipv4-dest-address-format
IPv4 宛先アドレスの形式 (range, netmask, single address)

ipv4-dest-address
IPv4 宛先アドレス (アドレス形式が *range* の場合は低位のアドレス)。

デフォルト値 : 0.0.0.0

ipv4-dest-mask
IPv4 宛先マスク (アドレス形式が *range* の場合は高位のアドレス)。

デフォルト値 : 255.0.0.0

protocol-id
フィルターするプロトコル ID

1 TCP

2 UDP

3 全プロトコル

4 範囲の指定

デフォルト値 : 3

src-port-start
発信元ポート番号範囲の最初のポート番号

デフォルト値 : 0

src-port-end
発信元ポート番号範囲の最後のポート番号

デフォルト値 : 65535

dest-port-start
宛先ポート番号範囲の最初のポート番号

デフォルト値 : 0

dest-port-end
宛先ポート番号範囲の最後のポート番号

デフォルト値 : 65535

src-id-type
発信元 ID タイプ。これは、リモートへ送信されます。この値は、ISAKMP フェーズ 1 ネゴシエーション時に必要な ISAKMP 情報がポリシーに含まれているかどうかを判別するのに使用されます。これは、ISAKMP パケットの識別ペイロード内の情報と比較されます。この情報は、リモート・ピアが IP アドレス以外の値をもつ装置を識別しなければならない場合に必要となります。

1 ローカル・トンネル・エンドポイント

2 ホスト完全修飾ドメイン名

3 ユーザー完全修飾ドメイン名

4 キー ID

any-user-access
プロファイル定義内の任意のユーザーについてアクセスを許可します。No を指定すると、このプロファイルについてのリモート・ユーザー・グループの名前を入力するようプロンプト指示されます。この属性は、リモート・アクセス・ピアのアクセスを特定のポリシーに制限したい場合にだけ必要です。

Yes または No

デフォルト値 : Yes

Received DS byte mask
着信パケットの DS (TOS) バイトに適用する 8 ビットのマスク

デフォルト値 : 0

Received DS byte match
Received DS (TOS) バイト・マスク値をもつ着信 TOS バイトを AND 結合した結果と比較される 8 ビットのパターン

デフォルト値 : 0

Interface pairs
このポリシーがトラフィック・フローを特定のインターフェースに制限しなければならない場合は、これは、インターフェースの対グループの名前です。

RSVP-Action

適用する RSVP アクションに関する情報を入力するようプロンプト指示します。

Name RSVP アクションの名前

Permission

このアクションに適合する RSVP セッションについての許可レベルを指定します。

1 Permit

2 Deny

デフォルト値 : 2

Max token rate

RSVP が個々のフローのために割り振る帯域幅の最大量 (Kbps 単位)

デフォルト値 : 100

Max duration

フローが継続できる分単位の最大時間 (0 は forever (永久) を暗黙指定します)

デフォルト値 : 600

RSVP-to-DS

このアクションに適合する RSVP フローを構成済みの DiffServ アクションにマップするかどうかを指定します。RSVP は、DiffServ アクションからの情報を使用して、次の DiffServ の使用可能な上流装置のために TOS バイトにマークを付けます。これは、パケットが RSVP の使用可能なネットワークを出て DiffServ の使用可能なネットワークに入るネットワーク内で使用するためです。

Yes または No

デフォルト値 : No

USER リモート IKE ピア用のユーザー・プロファイル定義についての情報を要求してプロンプト指示します。この情報には、フェーズ 1 ネゴシエーション中にピアが自分を識別する方法、このピア用に使用する認証方法、および認証メカニズムが事前共用キーである場合には、使用するキー値が含まれます。事前共用キーを使用する場合、ID タイプおよび名前に事前共用キーを関連付けるためにユーザーを定義する**必要があります**。このコマンドは、特定ユーザーのフェーズ 1 ネゴシエーションで使用されるキーを設定します。このキーは、提示者のためにメッセージ 1 と 5 で、応答者のためメッセージ 2 と 6 で使用されます。

Identification

ユーザーの識別。メイン・モード認証の場合、ユーザーの識別タイプは、IP アドレスで**なければなりません**。アグレッシブ・モード認証の場合、識別タイプはその他のタイプのいずれかにする必要があります。この理由は、メイン・モードでは ID はメッセージ 5 および 6 までは交換されず、これは事前共用キーには遅過ぎるため、唯

一のルックアップ・メカニズムは IKE ピアの IP アドレスを使用することになります。アグレッシブ・モードでは、ID はメッセージ 1 および 2 で交換されるため、事前共用キーのルックアップは ID タイプおよび対応する値を使用して行うことができます。

1 IP アドレス

2 完全修飾ドメイン名

3 ユーザー完全修飾ドメイン名

4 キー ID (任意のストリング)

デフォルト値 : 1

Group このユーザーを入れるグループの名前

デフォルト値 : なし

認証 ピアで使用する認証方式

1 事前共用キー

1 ASCII 形式のキー

有効な値: 2 to 128 桁の偶数桁数の文字

2 16 進形式のキー

有効な値: 2 to 128 桁の偶数桁数の 16 進数

2 公用証明。

デフォルト値 : 1

VALIDITY-PERIOD

ポリシーが有効な期間に関する情報を入力するようプロンプト指示し、ポリシー・プロファイルを作成します。

Name 妥当性期間プロファイルの名前

yyyymmddhhmmss:yyyymmddhhmmss

この妥当性期間プロファイルが入っているポリシーが有効である期間

例:

```
19980101000000:19981231000000
```

Months

この妥当性期間プロファイルが入っているポリシーが有効である月。各月の最初の 3 文字 (たとえば、jan または dec) を使用し、各月をスペースで区切ることにより、任意の順序で月を指定することができます。all を指定すると、一年のすべての月を意味することができます。

Days この妥当性期間プロファイルが入っているポリシーが有効である日付。各曜日の最初の 3 文字 (たとえば、mon または fri) を使用し、各曜日をスペースで区切ることにより、任意の順序で日付を指定することができます。all と入力すると、一週間の毎日を指定することができます。

Starting time
この妥当性期間プロファイルが入っているポリシーが有効である時刻。これは、形式 hh:mm:ss で指定するか、あるいはポリシーを一日中有効にしたい場合は * を指定してください。

デフォルト値 : *

Ending time
この妥当性期間プロファイルが入っているポリシーの妥当性が満了する時刻。これは、形式 hh:mm:ss で指定してください。

デフォルト値 : なし

Change

change コマンドは、ポリシー・オブジェクト内の情報を変更するのに使用します。使用可能なオブジェクトについては、**add** コマンドの説明を参照してください。

Copy

copy コマンドは、1 つのポリシー・オブジェクトから別のポリシー・オブジェクトへ情報をコピーするのに使用します。使用可能なオブジェクトについては、**add** コマンドの説明を参照してください。(interface-pair、manual tunnel、および user の各オプションは、**copy** コマンドには使用できません。)

Delete

delete コマンドは、ポリシー・オブジェクトから情報を削除するのに使用します。使用可能なオブジェクトについては、**add** コマンドの説明を参照してください。

Disable

disable コマンドは、ポリシー構成を使用不可にするのに使用します。

構文 : disable policy

Policy 使用不可にするポリシー構成の名前を入力するようプロンプト指示します。

Enable

enable コマンドは、ポリシー構成を使用可能にするのに使用します。

構文 : enable policy

Policy 使用可能にするポリシー構成の名前を入力するようプロンプト指示します。

List

list コマンドは、ポリシー構成情報の一部またはすべてを表示するのに使用します。

構文 : list all
default-policy
ldap
refresh

All すべてのポリシー構成情報を表示します。

Default-policy
デフォルト・ポリシーの名前を表示します。

LDAP 定義済みの LDAP 構成の名前を表示します。

Refresh
ポリシー更新状況 (Enable または Disable) および更新間隔時間を表示します。

Qconfig

qconfig コマンドを使用して、ネットワーク装置用にセキュリティー・ポリシーを迅速に作成します。短いリストから構成シナリオを選択すると、このコマンドによって、ユーザーの選択に基づいた簡潔な一連の簡単な質問が表示されます。次に、事前定義のシナリオ関連テンプレート (互換ポリシー・オプションの全セット) を使用してポリシー全体を作成します。これによって、ポリシーの細部を指定する必要がなくなり、ポリシーの構成に要する時間と間違いの可能性を減らします。

このコマンドは、カスタム・シナリオを除くすべてのシナリオのセキュリティー・レベルを指定します。

構文: qconfig *policy-name*
シナリオ

policy-name
ポリシーに割り当てる名前 (最大 29 文字) を指定します。

デフォルト値: システム生成の固有名

scenario
ポリシーを作成するシナリオを指定します。

デフォルト値 : なし

1 ブランチ・オフィス・シナリオ

この選択によって、ローカル・サブネットを保護している 2 つのセキュリティー・ゲートウェイ間の保護接続用のポリシー・オプションを指定できます。

オプションには、次のものがあります。

Local IP Subnet

Local IP Tunnel Endpoint

Remote IP Subnet

Remote IP Tunnel Endpoint

Ports and Protocols

Security Level

1: Strong Security。このオプションは、セキュリティー、パフォーマンス、および柔軟性が必要な場合に選択します。これは、SHA および MD5 の認証アルゴリズムと DES および 3DES の暗号化アルゴリズムの組み合わせを含む、一連の提

示 (PFS のない) を折衝します。強い提示は最初に折衝され、次により強い提示が折衝されますが、パフォーマンスを下げないようにします。

2: Very Strong Security。このオプションは、最高レベルのセキュリティーが必要な場合に、選択します。これは、SHA および MD5 の認証アルゴリズムと 3DES 暗号化アルゴリズムの組み合わせを含む、小さい一連の提示 (PFS、Grp 1 をもつ) を折衝します。

認証方式

1: 事前共用キー - ASCII キー

2: 証明 (RSA 署名) - ローカル ID

DiffServe アクション

0: Best Effort (DiffServ なし)

1: EF

2: AF11

3: AF21

4: AF31

5: AF41

ほかにローカルで構成された DiffServ アクションがあれば、このリストに表示されます。

妥当性期間

1. 1: allTheTime
2. 2: allTheTimeMonThruFri
3. 3: 9to5MonThruFri
4. 4: 5to9MonThruFri

ほかにローカルで構成された妥当性期間があれば、このリストに表示されます。

ポリシーの優先順位

2 **リモート・アクセス・ユーザー・シナリオ (IPSec および L2TP)。**

この選択によって、1 つのセキュリティー・ゲートウェイとリモート・アクセス・ユーザーとの間の保護接続用のポリシー・オプションを指定できます。このシナリオは、リモート・アクセス・クライアントにはトランスポート・モードで IPSec の 1 番上で L2TP を実行できる機能があることを想定します。

L2TP は、リモート・アクセス・クライアントの公用 IP アドレスとセキュリティー・ゲートウェイの公用 IP アドレスとの間のポイントツーポイント接続を設定します。UDP は、トランスポート・レイヤー接続を提供し、ソースと宛先のポートは 1701 です。セキュリティー・ゲートウェイ機能を実行するルーター上の fixed-udp-source-port 用に L2TP を構成することが重要です。IPSec は、これらのポートやプロトコル上での L2TP 接続の保護を行います。

一度構成シナリオを完了すると、事前共用キーを使用して認証される人についてポリシー・フィーチャーにユーザーを追加する必要があります。証明認証の場合、ルーターに PKI パラメーターを構成し、該当する証明が必ずロードされるようにする必要があります。

オプションには、次のものがあります。

保護インターフェースの IP アドレス

通常、これは、ローカル IP トンネル・エンドポイントと同じ値です。これは、パケットが保護されて送受信されるインターフェースの IP アドレスを表します。

セキュリティー・レベル

1: Strong Security

2: Very Strong Security

DiffServe アクション

0: Best Effort (DiffServ なし)

1: EF

2: AF11

3: AF21

4: AF31

5: AF41

ほかにローカルで構成された DiffServ アクションがあれば、このリストに表示されます。

妥当性期間

1. 1: allTheTime
2. 2: allTheTimeMonThruFri
3. 3: 9to5MonThruFri
4. 4: 5to9MonThruFri

ほかにローカルで構成された妥当性期間があれば、このリストに表示されます。

ポリシーの優先順位

3 非トラステッド・インターフェースで適合しないトラフィックをドロップします。装置がファイアウォールとして機能する構成の場合に、このシナリオが必要となります。多くのネットワーク構成では、ファイアウォールがセキュリティー・ゲートウェイの前面にあり、ドロップ規則は必要ありません。ドロップ規則を必要とする場合には、このシナリオを選択します。

オプションには、次のものがあります。

非トラステッド・インターフェースの IP アドレス

これは、不要なパケットをドロップするインターフェースの IP アドレスです。通常、これは公用または非トラステッド・ネットワークへの接続の IP アドレスです。

4 **カスタム・シナリオ**

この選択によって、**qconfig** を使用してポリシーを定義する際にもっとも大きな柔軟性が得られます。カプセル化モード (Tunnel または Transport のいずれか) を選択するようにプロンプト指示が出ます。tunnel モードを選択すると、ブランチ・オフィス・シナリオの場合と同じ質問が出されます。transport モードを選択すると、ローカルおよびリモートのサブネットに関する質問を除いて、これらは適用されないため、ブランチ・オフィス・シナリオの場合の質問が出されます。

LDAP ポリシー・サーバー構成コマンド

LDAP ポリシー・サーバー構成コマンドは、ポリシー情報を取り出すために LDAP サーバー・オプションを指定できるようにします。表45 は LDAP 構成コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて詳しく説明します。これらのコマンドは、`Policy config>` プロンプトで入力します。コマンドとオプションを 1 行に入力することもできますが、コマンドだけを入力して、プロンプトに応答することもできます。有効なコマンド・オプションを見るためには、オプションの代わりに疑問符を付けてコマンドを入力してください。

表 45. LDAP 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Disable ldap	LDAP 構成オプションを使用不可にします。
Enable ldap	LDAP 構成オプションを使用可能にします。
Set ldap	LDAP 構成オプションを指定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Disable LDAP

disable ldap コマンドは、ディレクトリー内の LDAP ポリシー検索機能を使用不可にしたり、LDAP サーバーからキャッシュしたポリシーを永久的記憶域に読み込みをできないようにするのに使用します。

構文 : disable ldap cached-search
policy-search

cached-search
LDAP がキャッシュしたポリシーをサーバーから永久的記憶域への読み込みをできないようにします。

policy-search
LDAP がディレクトリー内でポリシー検索機能を実行できないようにします。

Enable LDAP

enable ldap コマンドは、ディレクトリー内の LDAP ポリシー検索機能を使用可能にしたり、LDAP サーバーからキャッシュしたポリシーを永久的記憶域に読み込みをできるようにするのに使用します。

構文 : enable ldap cached-search
policy-search

cached-search
LDAP が、ディレクトリー内のポリシー検索機能を実行したり、LDAP サーバーからキャッシュしたポリシーを永久的記憶域に読み込みをできるようにします。

policy-search オプションを使用不可にしたときに、この cached-search オプションを使用可能にする場合には、ポリシー検索エンジンだけがローカル・キャッシュからポリシーを読み取ります。cached-search オプションと policy-search オプションの両方を使用可能にする場合に、ポリシー検索エンジンは、最初に LDAP サーバーからの読み込みを試みますが、この読み込みができない場合、キャッシュした LDAP ポリシー・オブジェクトから読み込みます。LDAP ポリシーをキャッシュする方法については、391ページの『ポリシー監視コマンド』 の **cache-ldap-polcys** コマンドを参照してください。

policy-search
LDAP がディレクトリー内でポリシー検索機能を実行できるようにします。

Set Default-Policy

set default-policy コマンドは、ポリシー・データベースの更新時に使用するポリシー・オプションを指定するのに使用します。このコマンドは、エラー処理オプションのほか、LDAP ポリシー・サーバーにアクセスするのに必要なデフォルト・セキュリティーを設定します。

構文 : set default-policy
default-error-handling
default-security

default-error-handling
ポリシー・データベースの更新時に使用するエラー処理オプションを指定します。

注: デフォルトのエラー処理設定は、ポリシー・データベースの再作成中にエラーが発生した場合に装置の動作を決定します。エラーが発生すると、装置がどのように動作するかについてのオプションが示されます。それらのオプションは、次のものです。

1. ポリシー・データベースをデフォルトのセキュリティーにリセットする。
2. LDAP から読み取った規則をフラッシュし、ローカル規則のほか、デフォルトのセキュリティーをロードする。

これらの設定は、ポリシー・データベースの作成エラーがあった場合に限り有効です。どちらのオプションも、エラーが発生すると、drop または pass というデフォルトのセキュリティーを継承します。オプション 2 を選択した場合、すべてのトラフィックはローカルに定義された

ポリシーに一致した場合を除き、ドロップされるか、パスされます。ポリシー・データベースが正常に作成された場合には、このオプションは使用されません。

default-security

ポリシー・データベースの更新時に使用するセキュリティー・オプションを指定します。

注: ポリシー・データベースが正常に作成されていれば、デフォルトの動作は pass として定義されます。これは、パケットがどのポリシー規則にも適合しない場合には、チェックなしでパスされることを意味します。基礎区に適合しないパケットをグローバルにあるいは一定のインターフェースについてだけドロップしたい場合は、そのようにポリシーを定義する必要があります。

1 全 IP トラフィックの受け入れと転送

2 LDAP トラフィックの許可、その他すべての IP トラフィックのドロップ

このオプションを選択すると、LDAP トラフィックの送受信が行われる装置でローカル IP アドレスを入力するようプロンプト指示されます。

3 LDAP トラフィックの許可と保護、その他すべての IP トラフィックのドロップ

このオプションを選択すると、次の情報を入力するようプロンプト指示されます。

DHGroupId

ISAKMP フェーズ 1 ネゴシエーション時に使用する Diffie-Hellman グループ ID

1 DH グループ 1

2 DH グループ 2

Phase1-Hash-Algorithm

フェーズ 1 ネゴシエーション時に使用するハッシュ・アルゴリズム。ハッシュ・アルゴリズムにより、フェーズ 1 メッセージの認証が与えられます。

1 MD5

2 SHA

Phase1-Cipher-Algorithm

フェーズ 1 ネゴシエーション時に使用する暗号アルゴリズム。暗号アルゴリズムは、フェーズ 1 ネゴシエーションに暗号化保護を提供します。

1 DES

2 3DES

Phase1-Authentication-Method

リモート・ピアで使用する認証方式。これは、リモート・ピ

アがネゴシエーションの相手として実際に正しい装置であるかどうかを ISAKMP が判別する方法を指定します。

1 Pre-Shared Key (事前共用キー)

2 認証 (RSA SIG)

Pre-Shared-Key-Value

事前共用キー・フェーズ 1 認証方式を指定した場合には、キー値を ASCII で入力するようプロンプト指示されます。

Phase2-ESP-Authentication-Algorithm

ESP は、デフォルトのセキュリティーについて許される唯一の IPSec プロトコルです。フェーズ 2 ISAKMP ネゴシエーション時に使用する確認アルゴリズムを入力するようプロンプト指示されます。

0 なし

1 HMAC-MD5

2 HMAC-SHA

Phase2-ESP-Cipher-Algorithm

ESP は、デフォルトのセキュリティーについて許される唯一の IPSec プロトコルです。フェーズ 2 ISAKMP ネゴシエーション時に使用する暗号アルゴリズムを入力するようプロンプト指示されます。

1 ESP DES

2 ESP 3DES

3 ESP CDMF

4 ESP NULL

Primary-Tunnel-Start

装置と、1 次 LDAP サーバーを保護するセキュリティー・ゲートウェイとの間で IKE および IPSec トラフィックに使用される装置での IP アドレス。

Primary-Tunnel-End

IKE および IPSec トラフィックに使用される 1 次 LDAP サーバーを保護するリモート・セキュリティー・ゲートウェイでの IP アドレス。

Secondary-Tunnel-Start

装置と、2 次 LDAP サーバーを保護するセキュリティー・ゲートウェイとの間で IKE および IPSec トラフィックに使用される装置での IP アドレス。

Secondary-Tunnel-End

IKE および IPSec トラフィックに使用される 2 次 LDAP サーバーを保護するリモート・セキュリティー・ゲートウェイでの IP アドレス。

Set LDAP

set ldap コマンドは、LDAP 操作パラメーターを構成するのに使用します。

構文 : set ldap

- anonymous-bind
  - yes
  - no
- bind-name <*name*>
- bind-pw <*pw*>
- policy-base <*string*>
- primary <*ip-address*>
- secondary <*ip-address*>
- version <*value*>

anonymous-bind [Yes or No]

LDAP ディレクトリーに匿名でバインドしたいか、それとも自分で指定したバインド名とバインド・パスワードを使用してバインドしたいかを指定します。

デフォルト値 : Yes

bind-name <*name*>

LDAP サーバーの検索が実行できるようになる前にそのサーバーにバインドするのに必要な情報を入力するようプロンプト指示します。*name* パラメーターは、ルーターが自らを識別するのに使用する識別名を指定します。このパラメーターを入力しない場合、バインドは、匿名要求として出されます。

bind-pw <*pw*>

LDAP サーバーの検索が実行できるようになる前にそのサーバーにバインドするのに必要な情報を入力するようプロンプト指示します。*pw* パラメーターは、識別名に関連するパスワードです。このパラメーターを入力しない場合、バインドは、匿名要求として出されます。

policy-base <*string*>

ルーターの SRAM および LDAP サーバー内のポリシーの検索範囲を定義するのに使用される文字ストリングを入力するようプロンプト指示します。たとえば、このオプションを使用して、ルーター A だけに適用されるポリシー、NHD 用のポリシー、または IBM-US 用のポリシーを戻すことができます。policy-base は、LDAP サーバー内の DeviceProfile オブジェクトの識別名です。

primary <*ip-address*>

ポリシーの取り出し元となる LDAP サーバーの IPv4 アドレスを入力するようプロンプト指示します。

secondary <*ip-address*>

デフォルト・サーバーに届かない場合に使用されるバックアップ LDAP サーバーの IPv4 アドレスを入力するようプロンプト指示します。

version <*value*>

LDAP サーバーがサポートする LDAP バージョン番号を入力するようプロンプト指示します。

デフォルト値 : 2 (許容値は 2 または 3 だけです。)

Set Refresh

set refresh コマンドは、毎日 1 回のポリシー・データベースの自動更新を使用可能または使用不可にするのに使用します。これを使用可能すると、ポリシー・データベースは、毎日 1 回指定の時刻に自動的に更新します。このことにより、ネットワーク内のすべてのポリシー使用可能ルーターは、LDAP ディレクトリー内で発生したあらゆるポリシー変更を自動的に受け入れることができます。このパラメーターをリセットするには、ポリシー・フィーチャーの Talk 5 **reset refresh** コマンドを使用します。

構文 : set refresh

enabled

yes

no

<*time*>

enabled [yes or no]
自動更新を実行するかどうかを指定します。

<*time*> enabled yes が指定された場合に、更新が発生する時刻 (24 時制形式) を指定します。

ポリシー監視プロンプトへのアクセス

ポリシー・フィーチャーのポリシー・コンソール部分により、ポリシー・データベース内のポリシーを表示したり、個々のポリシーを使用可能または使用不可することができます。ポリシー監視環境にアクセスするには、OPCON プロンプト (*) で **talk 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで以下のコマンドを入力します。

```
+ feature policy
Policy>
```

ポリシー監視コマンド

これらのコマンドにより、ポリシー・データベースで定義されているポリシーを表示したり、個々のポリシーを使用可能または使用不可することができます。 392ページの表46 はポリシー監視コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて詳しく説明します。コマンドは、`Policy console` プロンプトで入力します。コマンドとオプションを 1 行に入力することもできますが、コマンドだけを入力して、プロンプトに応答することもできます。有効なコマンド・オプションを見るためには、オプションの代わりに疑問符を付けてコマンドを入力してください。

ポリシー監視コマンド (Talk 5)

表 46. ポリシー監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Cache-ldap-plcys	LDAP サーバーからルーターの永久的な構成記憶域に読み込まれた最新のポリシー情報のコピーを保管します。
Check-consistency	個々のポリシー内およびすべての構成済みポリシー間での整合性を検査します。
Disable	ポリシー・データベースにロードされているポリシーを使用不可にします。
Enable	ポリシー・データベースにロードされているポリシーを使用可能にします。
Flush-cache	キャッシュしたポリシー情報をルーターの永久的構成記憶域から消去します。
Reset	ポリシー関連の基準を更新またはリセットします。
Search	LDAP クライアントとサーバー間のアクティビティーをテストまたはデバッグします。
Status	ポリシー・データベースに関する情報を表示します。
List	LDAP 構成および定義済みのポリシーに関する情報を表示します。
Test	ポリシー・エンジンに照会し、選択された規則を取り出します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Cache-LDAP-Plcys

cache-ldap-plcys コマンドは、LDAP サーバーからルーターの永久的構成記憶域に読み込まれた最新のポリシー情報のコピーを保管するために使用します。これによって、既存のキャッシュしたポリシー情報があれば永久的記憶域から除去します。

構文: cache-policy

注: 2212 および 2216 のプラットフォームで、このコマンドを入力すると、Talk 6 **write** コマンドを実行した場合と同様に、ルーター構成全体も書き込まれます。

Check-Consistency

check-consistency コマンドは、個々のポリシー (内部的) で、および重複した定義のあるポリシー間 (外部的) で構成されたオプション間の発生の可能性のある不整合を検査するために使用します。そのあと、矛盾があればそれを解消するために訂正処置を取ることができます。

内部的な 不整合は、単一のポリシー内のアクション・オブジェクト間に存在するもので、たとえば、Deny の DiffServ アクション・タイプをもつポリシーが Permit の IPSec アクション・タイプをもつ場合です。*外部的な* 不整合は、重複するプロファイルをもつ別個のポリシー間で存在するもので、たとえば、1 つのポリシーが Block の DiffServ アクション・タイプをもち、もう 1 つのポリシーが Permit の IPSec アクション・タイプをもつ場合です。もう 1 つの例は、重複するポリシーが異なる IPSec アクション・タイプを指定する場合です。

構文: check-consistency

例:

ポリシーが以下のように構成されているものと想定します。

Policy Name: dsDown

Loaded from: Local

State: Enabled and Valid

Priority: 5

Hits: 0

Profile: DSUP

Validity: always

DiffServ: dsDown

RSVP: rsvpActUp

Policy Name: ManualTunnel

Loaded from: Local

State: Enabled and Valid

Priority: 5

Hits: 0

Profile: DSUP

Validity: always

Tunnel ID: 1

Policy Name: ike

Loaded from: Local

State: Enabled and Valid

Priority: 30

Hits: 0

Profile: DSUP

Validity: always

IPSec: ipsecUP

ISAKMP: generalPhase1Action

consistency-check コマンドの出力は、次のように表示されます。

```
Policy console>check-consistency
Checking for inconsistencies with a policy...
Rule dsDown contains two conflicting actions:
   RSVP Action is of type PERMIT
   DiffServ Action is of type BLOCK

Checking for inconsistencies among policies with overlapping profiles...
  Mismatching IPSec and DiffServ actions at Priority 181 between:
        Rule: ike.traffic     State: ENABLE  Prio: 5 IPSec Action: PERMIT
        Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK

   Two rules with IPSec actions:
        Rule: ike.traffic     State: ENABLE  Prio: 30 Action: PERMIT
        Rule: Man             State: ENABLE  Prio: 5 Action: PERMIT

   Two rules with IPSec actions:
        Rule: ike.inBoundTunnel State: ENABLE  Prio: 30 Action: PERMIT
        Rule: Man.inBoundTunnel State: ENABLE  Prio: 5 Action: PERMIT

   Two rules with IPSec actions:
        Rule: Man.inBoundTunnel State: ENABLE  Prio: 5 Action: PERMIT
        Rule: ike.inBoundTunnel State: ENABLE  Prio: 30 Action: PERMIT
```

```
 Two rules with IPSec actions:
      Rule: Man             State: ENABLE  Prio: 5 Action: PERMIT
      Rule: ike.traffic     State: ENABLE  Prio: 30 Action: PERMIT

Mismatching IPSec and DiffServ actions at Priority 5 between:
      Rule: Man             State: ENABLE  Prio: 5 IPSec Action: PERMIT
      Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK

Mismatching IPSec and DiffServ actions at Priority 5 between:
      Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK
      Rule: ike.traffic     State: ENABLE  Prio: 30 IPSec Action: PERMIT

Mismatching IPSec and DiffServ actions at Priority 5 between:
      Rule: dsDown          State: ENABLE  Prio: 5 DiffServ Action: BLOCK
      Rule: Man             State: ENABLE  Prio: 5 IPSec Action: PERMIT
```

Disable

disable コマンドは、ポリシー・データベースを使用不可にするのに使用します。使用不可にするポリシーの基準に適合するあらゆるデータ・パケットに、デフォルトの決定が適用されます。

構文 : disable *policy-name*

Enable

enable コマンドは、ポリシー・データベースを使用可能にするのに使用します。使用可能にするポリシーの基準に適合するあらゆるデータ・パケットでは、ポリシー用に構成された決定が適用されます。

構文 : enable *policy-name*

Flush-Cache

flush-cache コマンドは、LDAP サーバーから読み込まれたポリシー情報の最新のキャッシュしたコピーをルーターの永久的構成記憶域から消去するために使用します。

構文: flush-cache

Reset

reset コマンドは、ポリシー関連基準を更新またはリセットするのに使用します。

構文 : reset ldap-config
policy-database
refresh-time

ldap-config

(**set ldap** コマンドに指定されているとおりに) LDAP 構成を動的にロードしてメモリーに入れます。変更は、次の検索操作についてアクティブになります。このコマンドは、ポリシー・データベースのリセットも強制的に行い、ポリシー・データベース更新時刻を非活動化します。

policy-database

ポリシー・データベースを更新します。すべてのトンネル、フェーズ 1、およびフェーズ 2 SA を停止し、RSVP および DiffServ データ構造をリセットし、ポリシー・データベースをフラッシュします。すると、ポリシーは LDAP サーバーからロードされ、自動開始が行われます。データベースの再

作成時に、パケットはルーターへの着信または発信ができません。ただし、LDAP サーバーへ着信または発信するパケットは除きます。

refresh-time
ポリシー・データベースが毎日自動的に更新される時刻を設定します。更新時刻を使用不可にした場合、データベースは、ルーターがリブートまたはリスタートされるまで更新されません。

Search

search コマンドは、LDAP クライアントおよびサーバー間のアクティビティーをテストまたはデバッグするのに使用します。ディレクトリーに対して検索を実行し、その検索の結果を talk 5 に表示させることができます。

構文 : search *filter*
ipaddress

filter 検索操作についてフィルター値を指定します。

ipaddress
サーバーの IP アドレスを指定します。

Status

status コマンドは、ポリシー・データベースに関する情報を表示するのに使用します。

構文 : status

status 最新のポリシー・データベースの更新の結果、その更新以後の経過時間、次の更新がスケジュールされている時刻を表示します。

例:

```
Policy>status
Status of Last Search:       Failed
Time since last refresh:     4 seconds
Next Policy Refresh not scheduled
```

List

list コマンドは、LDAP 構成およびポリシーに関する情報を表示するのに使用します。

構文 : list default-policy
ldap
policy
refresh
rule
stats

default-policy
ポリシー・データベースの更新中に使用されるデフォルト・ポリシーを表示します。

ldap SRAM 内の LDAP 構成を表示します。

policy

basic ポリシー・コンポーネントを論理ポリシー名別に表示します。ポリシーを 1 つ選択することもできますが、すべてのポリシーを表示することもできます。リストは、ポリシーが Talk 6 での構成中に入力されたとおりにポリシーのコンポーネントの名前を示します。

complete
リスト・ポリシーの基本と同じことを行います。ただし、各論理ポリシーのすべてのパラメーター値の完全リストが示されます。

generated
list policy basic と同じことを行います。ただし、各論理ポリシーについて生成されたすべての規則名前が表示されます。

refresh
ポリシー更新状況 (Enable または Disable) および更新間隔時間を表示します。

rule 次のオプションにしたがって、生成された規則に関する情報を表示します。

basic 生成された規則をすべて表示します。リストから規則を選択することもできますし、すべての規則を表示することもできます。リストは、規則のコンポーネントの名前を表示します。コンポーネントには、次のものがあります。

policy name
loaded from (LDAP または local)
state
priority
number of hits
profile
validity (次のもので構成されるアクション・リストが後ろに続く)
IPSec (and、or)
ISAKMP (and、or)
DiffServ (and、or)
RSVP

complete
rule basic と同じことを行います。ただし、各コンポーネントのすべてのパラメーターの名前が表示されます。

stats 適合する規則および適合の数を表示します。1 つの規則が複数のアクションをもつことができ、すべてのアクションが適合するわけではないので、このオプションはその規則の適合したアクションと、その数も示します。

Test

test コマンドは、ポリシー・データベースの動作を検証するのに使用します。このコマンドにより、ポリシー・エンジンに照会し、適合する規則を取り出すセレクター・セットを入力することができます。発信元および宛先アドレス、発信元および宛先ポート、プロトコル ID、TOS 値を入力するようプロンプト指示されます。規則が適合すると、コマンドは、その規則の名前を返します。適合しない場合は、*No match found* と表示します。

構文 : test forwarder

ISAKMP

IPSec

RSVP

forwarder
IP 転送エンジンからのデータベース照会をシミュレートし、そのような照会の結果生じるポリシー判断を戻します。戻されるポリシーのタイプには、DiffServ 情報、IKE フェーズ 1 およびフェーズ 1 情報、さらに IPSec 手動トンネル ID が含まれます。

ISAKMP
フェーズ 1 ポリシー情報の IKE からのデータベース照会をシミュレートし、そのような照会の結果生じるポリシー判断を戻します。このオプションを使用する場合は、発信元および宛先アドレスをトンネルのエンドポイント IP アドレスに、プロトコルを 17 に、発信元および宛先ポートを 500 に設定する必要があります。

IPSec フェーズ 2 ポリシー情報の IKE からのデータベース照会をシミュレートし、そのような照会の結果生じるポリシー判断を戻します。このオプションを使用する場合は、発信元および宛先アドレスをトンネルのエンドポイント IP アドレスに、プロトコルを 17 に、発信元および宛先ポートを 500 に設定する必要があります。

RSVP RSVP からのデータベース照会をシミュレートし、そのような照会の結果生じる RSVP ポリシー判断を戻します。

ポリシー動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

ポリシー・フィーチャーは、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、ポリシー・フィーチャーには適用できません。ポリシー・フィーチャーの構成は、特定のインターフェースから独立している、IP トラフィックに適用される一連の規則とそれ以降のアクションを決めます。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、ポリシー・フィーチャーには適用できません。ポリシー・フィーチャーの構成は、特定のインターフェースから独立している、IP トラフィックに適用される一連の規則とそれ以降のアクションを決めます。

GWCON (Talk 5) 構成要素リセット・コマンド

ポリシー・フィーチャーは、次の Web サーバー・キャッシュ固有 GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature Policy, Reset, Database コマンド

説明: ポリシー・フィーチャーに構成されたすべてのポリシーは、ローカル構成から読み込まれます。LDAP 検索機能を使用可能にしていると、この装置のポリシーは LDAP サーバーから読み込まれます。DIFFSERV アクションなどのベースとなるポリシー・オブジェクトに変更が行われると、ポリシーによって使用される IPSec と IKE ポリシー・オブジェクトも、同様に構成から再ロードされます。

すべてのポリシーが読み込まれると、これらのポリシーから生成される規則の集合からポリシー・データベースが構築されます。ポリシーが読み込まれている間中、デフォルトのデータベースが、**feature policy, set default-policy** コマンドを使用して、Talk 6 に構成されたデフォルトの規則を用いて作成されます。

ネットワークへの影響:

ポリシー・データベースが構築されている間中、IPv4 ユニキャスト・トラフィックは、Talk 6 に構成されたデフォルトのポリシーに基づいて転送されます。デフォルトのポリシーは、すべてのトラフィックを通すか、2216 との間の LDAP トラフィックを除くすべてのトラフィックをドロップするか、または 2216 との間の、IPSec を使用して保護した LDAP トラフィックを除くすべてのトラフィックをドロップします。

制限事項:

なし。

次の表では、**GWCON, feature policy, reset, database** コマンドが起動されると活動化されるポリシー・フィーチャーの構成変更を要約します。

GWCON, feature policy, reset, database コマンドによって変更が活動化されるコマンド
CONFIG, feature policy, add, policy
CONFIG, feature policy, delete, policy
CONFIG, feature policy, change, policy
nCONFIG, feature policy, disable, policy
CONFIG, feature policy, enable, policy

GWCON, Feature Policy, Reset, LDAP コマンド

説明: ポリシー・フィーチャーの LDAP 構成パラメーターは更新されます。

ネットワークへの影響:

次回ポリシー・データベースを更新すると、新しい LDAP 構成パラメーターを使用してサーバーを検索するかどうか、検索する場合には、使用するパラメーターを決めます。

制限事項:

なし。

次の表では、**GWCON, feature policy, reset, ldap** コマンドが起動されると活動化されるポリシー・フィーチャーの構成変更を要約します。

GWCON, feature policy, reset, ldap コマンドによって変更が活動化されるコマンド
CONFIG, feature policy, set, ldap, anonymous-bind

CONFIG, feature policy, set, ldap, bind-name
CONFIG, feature policy, set, ldap, bind-pw
CONFIG, feature policy, set, ldap, policy-base
CONFIG, feature policy, set, ldap, port
CONFIG, feature policy, set, ldap, primary-server
CONFIG, feature policy, set, ldap, retry-interval
CONFIG, feature policy, set, ldap, search-timeout
CONFIG, feature policy, set, ldap, secondary-server
CONFIG, feature policy, set, ldap, version
CONFIG, feature policy, enable, ldap, cached-search
CONFIG, feature policy, enable, ldap, policy-search
CONFIG, feature policy, disable, ldap, cached-search
CONFIG, feature policy, disable, ldap, policy-search

GWCON, Feature Policy, Reset, Refresh

説明: ポリシー・データベース更新パラメーターは再ロードされます。更新パラメーターは、データベースを一日一度、また使用可能であれば、日中に更新するかどうかを決めます。

ネットワークへの影響:
ポリシー更新フィーチャーを使用可能にした場合、次に更新構成に指定したタイム・イベントが発生したときに、ポリシー・データベースは更新されます。**reset database** コマンドを手操作で実行するのと同じ効果があります。

制限事項:
なし。

次の表では、**GWCON, feature policy, reset, refresh** コマンドが起動されると活動化されるポリシー・フィーチャーの構成変更を要約します。

GWCON, feature policy, reset, refresh コマンドによって変更が活動化されるコマンド
CONFIG, feature policy, set, refresh

CONFIG (Talk 6) 即時変更コマンド

ポリシー・フィーチャーは、装置の操作状態を即時に変更する、次の CONFIG コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行する場合には、保管されて保存されます。

コマンド
CONFIG, feature policy, set, default-policy **注:** 次回ポリシー・データベースを更新すると、デフォルト・ポリシーの設定値は、更新期間中にまたポリシー・データベースの更新中に発生する可能性のあるエラー状態を処理するために使用されます。
CONFIG, feature policy, add, user

CONFIG, feature policy, change, user
注: ユーザーのために定義された事前共用キーは、装置をリスタートしたり、再ロードせずに、即時に使用できます。このユーザーがプロファイルのリモート・ユーザー・グループに関連付けられたグループの一部である場合には、このアソシエーションが行われる前にポリシー・データベースをリセットする必要があります。

第21章 IP セキュリティーの使用

この章では、IP セキュリティー・フィーチャーの使用法について説明します。この章には、次の内容が記載されています。

- 『IP セキュリティーの概説』
- 402ページの『IP セキュリティーの概念』
- 411ページの『インターネット・キー交換の使用』
- 414ページの『公開キー・インフラストラクチャーの使用』
- 418ページの『手動 IP セキュリティー (IPv4) の使用』
- 418ページの『手動 IP セキュリティー (IPv6) の使用』

IP セキュリティーの概説

ここでは、IPv4 および IPv6 両方の IP セキュリティー機能を概説します。

保護トンネルの使用

別のホスト、ルーター、またはファイアウォールに送信する IP パケットを保護するために、保護する必要のある各 IP ルート用に保護トンネルを構成することができます。IPSec トンネルは、ローカル・ルーターが保護 IP パケットを転送するための、リモート・ホスト、ルーター、またはファイアウォールへの両方向の論理接続です。保護トンネルは、発信元ホストおよび宛先ホストのアドレス、ポート番号、およびトンネル ID といったパラメーターで識別されます。

IPv4 では、ポリシー・データベース内でトンネル・ポリシーを構成することにより、ネゴシエーションされたトンネルを定義することができますが、434ページの『ルーター A のトンネルの構成』に示されているとおりに Talk 6 **add tunnel** コマンドを使用して手動トンネルを作成することもできます。IPv6 では、Talk 6 **add tunnel** コマンドを使用します。

保護 IPSec トンネルを確立するために、ポリシーは、特別な認証ヘッダーを付加する IP 認証ヘッダー (AH) 機能 (404ページの『IP 認証ヘッダー』を参照)、およびデータを暗号化する IP 暗号化セキュリティー・ペイロード (ESP) 機能 (405ページの『IP カプセル化セキュリティー・ペイロード』を参照) を指定できます。ポリシーは、次のセキュリティー処置のうちどれがパケットについて実装されるかを設定します。

- AH アルゴリズムと AH 認証キー (適宜、424ページの『アルゴリズムの構成』または 436ページの『アルゴリズムの構成』を参照してください。)
- ESP 暗号化アルゴリズムと ESP 暗号化および暗号化解除キー (適宜、424ページの『アルゴリズムの構成』または 436ページの『アルゴリズムの構成』を参照してください。)
- セキュリティー・パラメーター・インデックス (SPI) (406ページの『セキュリティー・アソシエーション』を参照してください。)

注: 各保護トンネルについて、送信側と受信側で同じオプションを選択する必要があります。

IP セキュリティーの概念

インターネット・プロトコル (IP) を使用して送信されるパケットは、2216 の IP セキュリティー・フィーチャーを使用して保護することができます。

セキュリティー (インターネット・プロトコルの RFC 2401 セキュリティー体系によって定義) には、次の機能が含まれます。

認証 受信したデータは送信されたデータと同じであること、および提示された送信側が確かに実際の送信側であることが分かっている。

保全性 データが変更されずに発信元から宛先に転送されることが保証される。

機密性 指定の受信側は何が送信されたのかを知っているが、当事者以外は何が送信されたのかを判別できない方法で通信する。

非否認 後で送信側がそのデータを送信したことを否定しても、受信側は送信側が確かに所定のデータを送信したことを証明できる方法で通信する。

注: 一部の国では、米国の輸出規制や暗号化パラメーターが表示されないなどの理由で、暗号化サポートが提供されない場合がありますが、ESP-NULL アルゴリズムは、どこでも利用可能です。ESP-NULL アルゴリズムの定義については、405ページの『ESP 暗号化アルゴリズム』を参照してください。

IP セキュリティーの用語

IPv4 に関連する IPSec トピックを説明するために、次の用語が使用されています。

認証ヘッダー (AH)
パケット・ヘッダー情報が入っているデータ域。これは、データ・オリジン認証のほか、データ保全性および再生保護を提供します。

証明書 ASN.1 コード化データ項目 (ITU X.509 標準による)。これは、エンド・エンティティーの ID をその公開キーにバインドします。(この場合、エンド・エンティティーは ISAKMP ネゴシエーション・エンティティーです。) エンド・エンティティーは、認証要求を実行依頼することによってその ID と公開キーを認証局 (CA) に登録する必要があります。CA は、その要求を検証し、署名して、エンティティーに対して発行します。ISAKMP は、フェーズ 1 処理時に公開キー認証を使用して、ルーター間のマスター・シークレット (暗号キー) をセットアップする初期メッセージ交換を認証します。

認証局 (CA)
ISAKMP を使用して保護ユーザー・データを交換するのにネットワーク・ユーザーが使用する必要のある “署名付きの” X.509 ディジタル証明書を発行する承認済み電気通信事業者。他の ISAKMP の使用可能なパーティーとの保護データ交換に参加するには、ルーターは、CA に登録し、認証で使用される X.509 ディジタル証明書を取得する必要があります。

注: ISAKMP 使用可能パーティーの現行リストを使用していることを確実にするために定期的に CA を使用して検査する必要があります。詳細については、421ページの『公開キー・インフラストラクチャー構成コマンド』 の PKI Talk 6 **load** コマンドを参照してください。

ディジタル署名
ユーザーのコード化 ID を含むデータ。これは、X.509 ディジタル証明書の一部となります。ユーザーは、フェーズ 1 ネゴシエーション時に証明書を交換して、互いに認証します。署名は、署名される入力データ域に対して公開キー操作を実行すると生成されます。

カプセル化セキュリティー・ペイロード (ESP)
データグラムの内容が受信側以外の人には判別できないようにするためにカプセル化し、暗号化できる IPSec 機能。これは、データ保全性と再生保護で構成されます。ESP は、データ起点認証も提供します。この機能は、次のモードで操作します。トランスポート・モードでは、元のデータグラムのペイロードだけが暗号化され、アドレス指定情報は無許可のパーティーから見えるままになっています。トンネル・モードでは、ヘッダーを含め、元のデータグラム全体が暗号化されます。これにより、重要なアドレス情報は隠されます。

インターネット・キー交換 (IKE)
ISAKMP および Oakley プロトコルに由来するプロトコル。これは、インターネット・コミュニティーが暗号キーの交換や、通信パーティーの認証を行うのに使用します。

ISAKMP
Internet Security Association and Key Management Protocol (インターネット・セキュリティー・アソシエーションおよびキー管理プロトコル)。この機能は、セキュリティー・アソシエーションを自動的にセットアップし、データ交換の期間中パケットの暗号キーを管理します。

管理情報ベース (MIB)
ルーターの操作に関する統計情報を要求した中央の承認済み電気通信事業者からの照会に対してルーターが送信するデータ・ブロック。電気通信事業者は、ネットワーク内で問題を検出し、責任を負うパーティーに連絡して、適切な処置を取らせることができます。

Oakley
ISAKMP が使用する暗号キー管理プロトコル

パーフェクト・フォワード・セクレシー (PFS)
フェーズ 2 ネゴシエーションにより各ネゴシエーションについて新しい暗号キー情報が引き出される場合に取得されるデータ・セキュリティーのレベル。ISAKMP は、パーティー間での公衆 Diffie Hellman 値の交換を使用可能にして、これを完成します。このセキュリティー・フィーチャーは、以前に悪用されたキーから現在の暗号キーを誰にも判別できないようにします。

フェーズ 1 ネゴシエーション
ISAKMP セキュリティー・アソシエーションおよび暗号キーを確立する、送信側と受信側との間の通信。フェーズ 2 ネゴシエーション時に交換される ISAKMP メッセージはこれによって保護されます。フェーズ 1 は、プロセッサー集約的なもので、通常、毎日または週単位の頻度で行われます。

フェーズ 2 ネゴシエーション
送信側と受信側との間で行われる ISAKMP メッセージの交換。このときに、ユーザー・データ交換を保護するセキュリティー・アソシエーションと

暗号化キーが交渉されます。これらのネゴシエーションは、通常、2、3 分に 1 回という頻度で発生するもので、ユーザーの介入なしに定期的に暗号化キーを更新するのに使用されます。

Proxy 別のネットワーク装置の代わりに動作するよう割り当てられているルーター。

公開キー・インフラストラクチャー (PKI)
CA がユーザーの ID をその公開キーとバインドするのに使用するフレームワーク。バインドされた公開キーは、そのセキュリティーが確実に行われる方法で配布されます。

高速モード
非 ISAKMP セキュリティー・アソシエーションのためのフェーズ 2 交渉を説明するのに使用する用語。

再生 データグラムを取り込むほか、その内容を判別しようと試みるか、またはそれを繰り返し再送することによってサービス拒否アタックをマウントするという動作。

セキュリティー・アソシエーション (SA)
データ・パケットに関する情報 (たとえば、その暗号アルゴリズムとキー情報、関与するパーティーの識別など) を結び付けるデータ域。

変換 認証および暗号化選択の構成に関する情報の名前をもつ集合。

IP 認証ヘッダー

認証ヘッダー (AH) は、RFC 2402 IP 認証ヘッダーに記載されています。このヘッダーには、IP データグラムの認証データが入っています。

交渉の行われた IPSec を使用する IPv4 の場合、データグラムに割り当てられたポリシーは、インターネット・キー交換 (IKE) プロトコルおよび公開キー / プライベート・キーのペアに依存する暗号認証機能を実装します。IPv4 手動トンネルおよび IPv6 の場合、送信側は、機密の認証キーに依存する暗号機能を使用します。どちらの場合も、暗号認証機能は、データグラムの内容に適用されます。AH を単独で指定することもできますが、ESP と一緒に指定することもできます。詳しくは、405ページの『AH および ESP の使用』を参照してください。

AH 認証アルゴリズム

AH トンネル・ポリシーを使用する保護トンネルは、次の認証アルゴリズムのうちの 1 つを使用する必要があります。

- 再生防止付き HMAC-MD5 IP 認証
- 再生防止付き HMAC-SHA-1 IP 認証

これらの AH アルゴリズムは、暗号ハッシュ (ハッシュ・メッセージ認証コード (省略形は HMAC)) を使用してキー付きメッセージ認証機能を任意指定の再生防止機能と結合します。再生防止機能は、AH に入っているシーケンス番号を使用して、パケットが以前に受信されていないかどうかを確認します。再生防止はサービスの拒否アタックから受信側を保護します。そこでは同じパケットが繰り返し送信されるので、ルーターは重複パケットの処理に忙殺されて、正当なトラフィックを処理できなくなります。認証コードは、秘密の暗号キーおよびデータに適用され、次に、機密キーの出力および最初のオペレーションの出力に適用されます。

HMAC-MD5 の場合のこの適用方法の例については、図33 を参照してください。

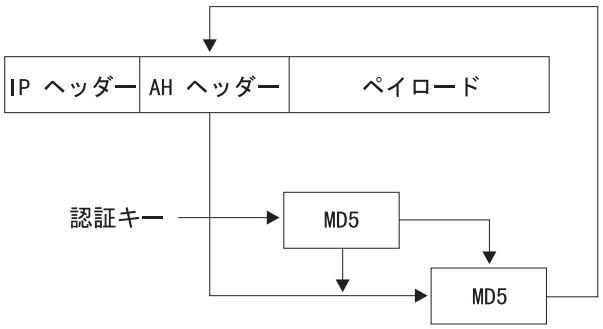


図 33. HMAC MD5 認証メッセージの作成

IP カプセル化セキュリティー・ペイロード

IP カプセル化セキュリティー・ペイロード (ESP) については、RFC 2406 IP カプセル化セキュリティー・ペイロードで説明しています。ESP は、IP パケットの一部または全部を暗号化して、認証 (任意選択) および保全性のほかに機密性を提供します。ただし、ESP NULL アルゴリズムを選択した場合、ESP は認証および保全性の検査だけを実行します。ESP を単独で指定することもできますが、AH と一緒に指定することもできます。詳しくは、『AH および ESP の使用』を参照してください。

ESP 認証アルゴリズム

ESP 認証に利用可能な認証アルゴリズムは、以前に 404ページの『AH 認証アルゴリズム』に示されたものと同じです。

ESP 暗号化アルゴリズム

ESP 暗号化ポリシーを使用している保護トンネルは、次の暗号化アルゴリズムまたは ESP-NULL アルゴリズムのどちらか 1 つを使用する必要があります。

- 暗号化ブロック・チェーン方式のデータ暗号化規格 (DES-CBC)
- 商業データ・マスキング・ファシリティー (CDMF)
- トリプル DES (3DES)

注: ESP 暗号化アルゴリズムは、ESP-NULL を除いて、米国の輸出規制の対象になっています。ご使用の 2216 で、これらのアルゴリズムの一部または全部を使用できない場合、これらのアルゴリズムの販売が禁止されている可能性があります。詳しくは、IBM 担当者にお尋ねください。

ESP-NULL 暗号化アルゴリズムは、クリアテキスト・データは暗号化せず、すべての国で利用可能です。このアルゴリズムにより可能になるのは、ESP 認証および保全性検査だけであり、暗号化は使用可能になりません。ESP-NULL を使用する場合は、ESP 確認アルゴリズムの 1 つを使用する***必要があります***。

AH および ESP の使用

保護トンネルは、AH、ESP、AH-ESP、または ESP-AH の認証 / 暗号化選択のどちらか 1 つを使用できます。AH と ESP を組み合わせたい場合は、次の記述が適用されます。

- ポリシー AH-ESP は、アウトバウンド・パケットは認証の前に暗号化を実行するよう指定します。この場合、宛先ルーターでは、最初に AH 認証機能が実行して、インバウンド・パケットを検査し、認証に合格したパケットだけが ESP に転送されて暗号解除されます。
- ポリシー ESP-AH は、アウトバウンド・パケットは暗号化の前に認証を実行するよう指定します。この場合、宛先ルーターでは、ESP 機能は最初にインバウンド・パケットを暗号解除し、正常に暗号解除されたパケットだけが AH 認証に転送されます。

セキュリティー・アソシエーション

セキュリティー・アソシエーション (SA) は、それによって伝送されるトラフィックへセキュリティー・サービスを提供するシンプレックス “接続” です。セキュリティー・サービスは、AH または ESP のどちらかを使用することにより SA に提供されますが、それらを両方使用した場合は提供されません。AH 保護および ESP 保護の両方がトラフィック・ストリームに適用される場合、そのトラフィック・ストリームに保護を提供するために SA が 2 つ (またはそれ以上) 作成されます。2 つのホスト間または 2 つのセキュリティー・ゲートウェイ間の一般的な双方向通信を保護するためには、SA が 2 つ (各方向に 1 つずつ) 必要です。

トンネル・モードとトランスポート・モード

動作モード (トンネルまたはトランスポート) により、IPSec が IP パケットをどのように扱うかが決まります。デフォルトはトンネル・モードで、ルーターがセキュリティー・ゲートウェイとして動作している場合は、トンネル・モードが必須です。このモードでは、データは、ネットワークを通るパスの単一セグメント上で保護されます。トランスポート・モードは、ルーターがホストとして動作している場合にだけ使用できます。このモードでは、データは、完全パスの終端間で保護されます。

AH と動作モード

トンネル・モードでは、AH は IP パケットの前に置かれ、新しい IP ヘッダーが作成されて AH の前に置かれます。トンネル伝送されるパケットの IP ヘッダー (内部ヘッダー) には、パケットの最終的な発信元と宛先のアドレスが入ります。新規 IP ヘッダー (外部ヘッダー) には、セキュリティー・ゲートウェイ (トンネルのエンドポイント) のアドレスを入れることができます。 AH は、新規 IP ヘッダー内の可変フィールドを除いて、新規 IP ヘッダーとトンネル伝送される IP パケットの両方を含めた新規パケット全体を保護します。

トランスポート・モードでは、AH は IP ヘッダーの後と高位レイヤー・プロトコル (TCP または UDP など) ヘッダーの前に挿入されます。このモードでは、AH は高位レイヤー・プロトコル・ヘッダーと IP パケットの内容を認証します。ただし、IP パケットの可変フィールド (たとえば、活動時間 [TTL]、チェックサム、フラグメント・フラグ、フラグメント・オフセット、およびサービス・タイプ [TOS] など) は除きます。

407ページの図34 は、AH 保護データグラムの形式を示しています。

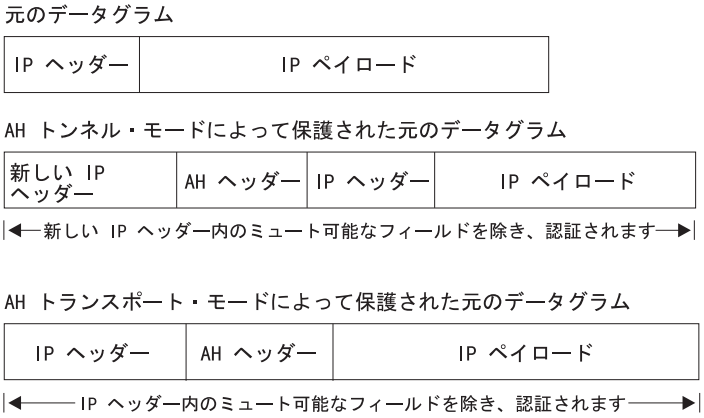


図 34. AH 保護データグラムの形式

ESP と動作モード

トンネル・モードでは、ペイロード・データには IP パケット全体が入れられ、新規の IP ヘッダーが作成されて ESP ヘッダーの前に置かれます。トンネル伝送されるパケットの IP ヘッダー (内部ヘッダー) には、パケットの最終的な発信元と宛先のアドレスが入り、新規の IP ヘッダー (外部ヘッダー) には、セキュリティー・ゲートウェイのアドレスが入ります。ESP は、トンネル伝送 IP パケットを暗号化します。ESP 認証を使用した場合は、ESP ヘッダー、トンネル伝送 IP パケット、および ESP トレーラーが認証されます。

トランスポート・モードでは、ペイロード・データには、高位レイヤー・プロトコル・データ (TCP または UDP データ) が入れられます。認証が使用されている場合には、ESP ヘッダー、高位レイヤー・プロトコル・データ、および ESP トレーラーが認証されます。

図35 は、ESP 保護データグラムの形式を示しています。

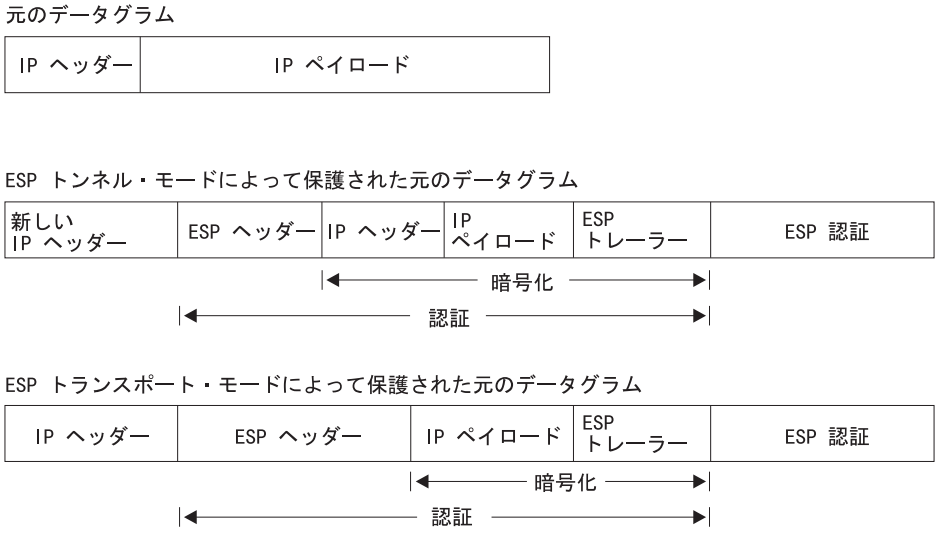
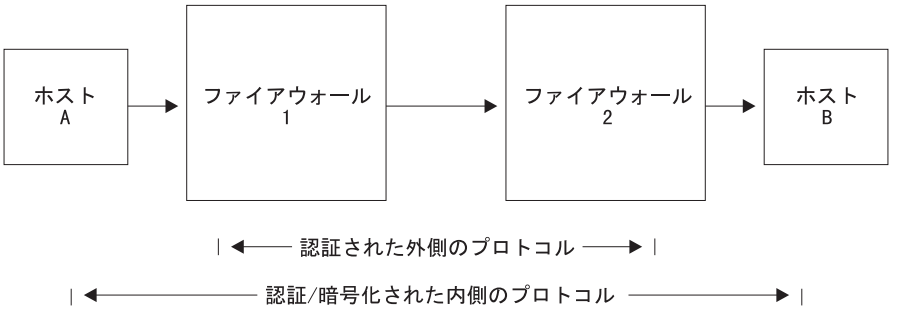


図 35. ESP 保護データグラムの形式

AH および ESP のネスト

あるプロトコルを、それ自身の別のインスタンス内またはもう一方のプロトコル内にネストすることができます。図36 は、ESP 保護データグラムを AH トンネル内でネストした場合の効果を示しています。



ホスト A は ESP トランスポートを使用します

IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証

ファイアウォール 1 は AH トンネルを使用し、新しい IP ヘッダーを追加します

新しい IP ヘッダー	AH ヘッダー	IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証

ファイアウォール 2 は AH トンネル・データグラムを受信し、
それを認証して、外側のヘッダーと AH ヘッダーを取り除きます

IP ヘッダー	ESP ヘッダー	IP ペイロード	ESP トレーラー	ESP 認証

図36. AH トンネル内での ESP のネスト

L2TP パケットでの IP セキュリティーの使用

IPv4 では、IPSec を使用して L2TP パケットを保護することもできます。UDP パケットの内側で L2TP フレームをカプセル化することにより L2TP トンネルを作成すると、発信元アドレスと宛先アドレスがトンネルのエンドポイントを定義する IP パケットの内側で UDP パケットをカプセル化することができます。そうすると、AH 、ESP、および ISAKMP プロトコルを IP パケットに適用できます。図37 は、インターネットを通じて伝送するための、PPP を含む IP がカプセル化された L2TP パケットとそのペイロード・プロトコルを示しています。

IP ヘッダー	UDP ヘッダー	L2TP ヘッダー	PPP ヘッダー	PPP ペイロード

これらのフィールドは IP パケット・ペイロードです

図37. IPSec 保護 L2TP パケット

トンネル内トンネル・モード

さらに強固なセキュリティーを得るためには、上記のセキュリティー・フィーチャーのほかに、トラフィック・ストリームのパケットを 2 度カプセル化し、最初にそれらを 1 つの IPSec トンネルを通じて送信し、次に別のトンネルを通じて送信します (トンネル内トンネル)。

注: ルーター内での複数の暗号化の使用 (両方のトンネルに対して暗号化を実行するときにトンネル内トンネル・モードを使用する) は、米国政府の輸出規制により制限されています。これは、厳格な輸出制御を受けているソフトウェア負荷 (128 ビット・キーおよびトリプル DES をサポートするソフトウェア負荷) でだけサポートされます。

IPv4 では、ポリシー・データベース内の規則が最初のトンネルについてのカプセル化 (内側) のためにパケットを指定し、そのパケットが送信される前に、規則はパケットを 2 度目のカプセル化 (外側) のために 2 番目のトンネルに送るようにします。IPv6 では、パケット・フィルター・アクセス制御規則が最初のトンネルについてのカプセル化 (内側) のためにパケットを識別し、そのパケットが送信される前に、規則はパケットを 2 回目のカプセル化 (外側) のために 2 番目のトンネルに送るようにします。

この 2 つの IPSec トンネルは 1 つのルーターから発しており、トンネルのリモート・エンドは、同じ物理位置にありますが、マシンは別個のマシンです。最初のトンネルのリモート・エンドは、保護ゲートウェイでもホストでも構いません。2 番目のトンネルのリモート・エンドは保護ゲートウェイ・ルーターでなければなりません。トンネルは、宛先がそれぞれ異なっているので、それぞれ異なるリモート IP アドレスを持っていなければなりません。トンネル内トンネルに使用されるトンネルは両方ともトンネル・モードに合わせて構成する必要があり、2 番目のトンネル上では追加の埋め込みはできません。

パケットは、2 度カプセル化された後で、2 番目 (外側) のトンネルを通じて送信されます。 2 番目のトンネルの終端で、外側のカプセル化が除去され、パケットは最初のトンネル・カプセル化機能によって作成されたヘッダーに基づいて、最初のトンネル (内側) に転送されます。このトンネルの終端で、最初のカプセル化が除去され、パケットはその最終宛先に転送されます。

パス最大伝送単位ディスカバリー

IPv4 と IPv6 の両方とも、2216 がセキュリティー・ゲートウェイとして働いている場合、IPSec はパス最大伝送単位 (PMTU) ディスカバリーをサポートします。PMTU ディスカバリーのサポートは、パケットを断片化できない場合にだけ必要になります。IPv4 では、Don’t Fragment (断片化不可 (DF)) ビットがセットされている場合にパケットを断片化できません。IPv6 では、中間ルーターでパケットを断片化することはできません。このような場合、パケットが保護トンネルの一端からほかの端までのパス内のリンク上に収まらないときは、『packet too big (パケットが大きすぎる)』という ICMP エラー・メッセージがパケットの発信元に送信されます。

ルーターはセキュリティー・ゲートウェイとして働いているので、エラー・パケットは、パケットの本当の発信元ではなく、発信側ルーターに戻されます。受信側ルーターは、報告された MTU を本当の発信元に正しく戻す必要があります。本当の発信元は、パケットが最終宛先に届くように、そのサイズを小さくすることができます。PMTU ディスカバリーのサポートについてはインターネット・プロトコルの RFC 2401 - セキュリティー体系に記述されています。

IPv4 では、トンネル伝送パケットの外側ヘッダー内の DF ビット設定のために次のオプションが用意されています。

1. 内部ヘッダーからコピーする
2. 常にセットする
3. 常にクリアする

上記オプションは、保護トンネル内トンネル・モードの構成時、たとえば、ポリシー・フィーチャー **add ipsec-manual-tunn** (IPv4) または Talk 6 **add tunnel** (IPv6) コマンドを使用している場合に使用できます。 DF ビットは、選択したオプションに応じて処理されます。ただし、次の条件の場合を除きます。

- トンネル MTU が最小 MTU に等しい場合
- 着信パケット・サイズが最小 MTU 以下の場合
- カプセル化パケット・サイズが最小 MTU より大きい場合

上記の場合、IPv4 では、構成に関係なく、DF ビットはセットされず、保護パケットは受信側へのパス上で、必要に応じて断片化されます。IPv6 では、パケットは、トンネルの PMTU に収まるように、セキュリティー・ゲートウェイを出るときに必要に応じて断片化されます。着信パケットはすでに最小 MTU 以下であり、発信元ホストはサイズをそれ以上縮小できないので、この特別処置が必要になります。断片化ができないと、このパケットは永久に最終宛先に到着しないことになります。

PMTU はネットワーク・トポロジーや構成の変更によって変更されることがあるので、PMTU 値を定期的に経時処理して、最大値にリセットすることが必要です。デフォルトの経時タイマー値は 10 分で、この設定は Talk 6 **set path** コマンドを使用して行います。経時パラメーターを 0 に設定すると、PMTU 経時は使用不可になります。

IP セキュリティー・トンネル付きのネットワーク・ダイアグラム

411ページの図38 は、ルーター A (IPSec 付き) をルーター B (IPSec のほか、IPv4 用のネットワーク・アドレス変換付き) へ接続する 2 つの IPSec トンネル付きのネットワーク例を示しています。

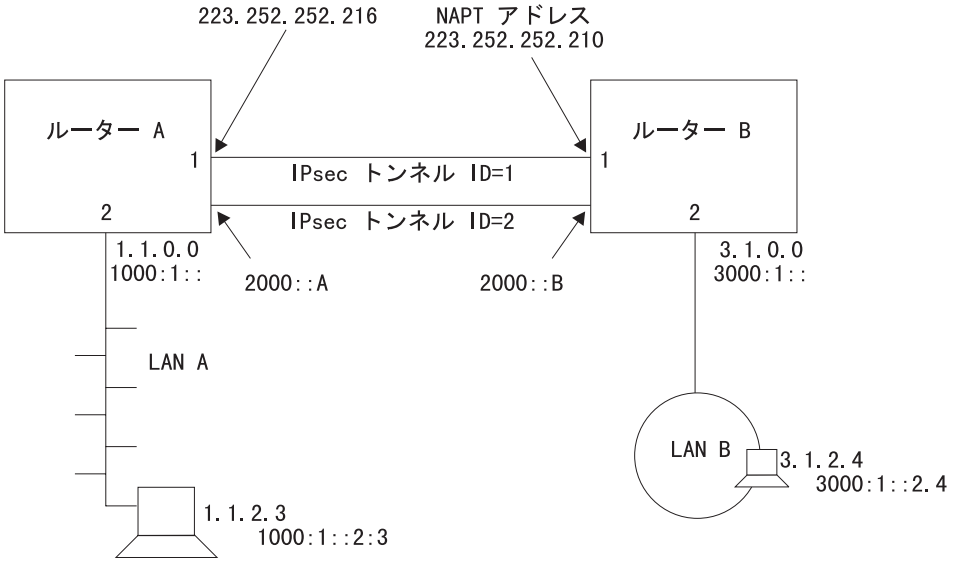


図 38. IPSec と NAT を備えたネットワーク

このネットワークでは、IPSec トンネル ID 1 をもつ IPSec トンネルが、ルーター A の IPv4 アドレス 223.252.252.216 からルーター B の IPv4 アドレス 223.252.252.210 に構成されています。ルーター A は IPSec 用に構成されています。ルーター B は、IPSec と NAT の両方用に構成されています。

このネットワークでも、IPSec トンネル ID 2 をもつ IPSec トンネルが、ルーター A の IPv6 アドレス 2000::A からルーター B の IPv6 アドレス 2000::B に構成されています。

IPv4 の場合、このネットワークを IKE 用に構成するには、419ページの『インターネット・キー交換の構成 (IPv4)』から始まるステップに従ってください。手動 IPSec の備わった IPv4 の場合は、434ページの『手動トンネルの構成 (IPv4)』から始まるステップに従ってください。 IPv6 の場合は、437ページの『手動トンネルの構成 (IPv6)』から始まるステップに従います。

注: ユーザーのネットワークで NAT を使用する計画がない場合は、ルーター B の構成の説明も通してお読みになると、IPSec トンネルの各端のパラメーターの関係をさらに深く理解することができます。

インターネット・キー交換の使用

ここでは、インターネット・キー交換 (IKE) を使用して、IPSec セキュリティー・アソシエーション (SA) の定義および作成を自動化する方法を説明します。IKE は、IETF (RFC 2409) によってサポートされている規格で、同一または異なるベンダーからの IPSec 使用可能製品がそれぞれのセキュリティー要件について通信するための標準的な仕組みを提供します。

IKE は、次のセキュリティー要件が適合するフレームワークを提供します。

リモート・ネゴシエーション・エンティティー (IKE ピア) の認証
IKE は、事前共用キーまたはディジタル証明書のどちらかを使用することに

より、エンティティーが主張するとおりのものであることを証明させることによってユーザーの通信相手であるエンティティーの識別を認証します。

両方のピアにおける同一キー入力資料の作成
Diffie-Hellman 公開キー / プライベート・キー機構を使用することにより、IKE は、公開キー・コンポーネントの交換および各ピア別の同一キーの独立生成に必要なものを提供します。

IPSec セキュリティー・アソシエーションのネゴシエーションのための保護の提供
次で説明する 2 段階のプロセスにより、IKE は、IPSec *tunnels* のネゴシエーションを保護するためだけに使用されるセキュリティー・アソシエーションの作成と、ユーザー・データを保護するために IPSec が使用するセキュリティー・アソシエーション の実際的なネゴシエーションおよび作成に必要なものを提供します。

インターネット・キー交換フェーズ

IKE は、フェーズ 1 およびフェーズ 2 という 2 つの異なるネゴシエーション交換を定義します。フェーズ 1 は、2 つの IKE ピア間に保護トンネルをセットアップするもので、これにより、それ以降の IPSec トンネル交渉について保護が提供されます。次のアクションは、フェーズ 1 中に示されている順序で発生します。

1. フェーズ 1 セキュリティー・アソシエーションの特性が、IKE ピアによってネゴシエーションされ、同意される。これらの特性には、*IKE 通信* を暗号化するのに使用される暗号化アルゴリズム、使用されるハッシュ・アルゴリズム、認証方式、およびキーを生成するときに使用される Diffie-Hellman グループが含まれます。
2. Diffie-Hellman キーが生成され、公衆部分は IKE ピアと交換される。これらのキーは、両方のフェーズ 1 認証を暗号化し、IPSec トンネルによって使用されるキーの生成も可能にする暗号化キーを生成するのに使用されます。
3. IKE ピアは、2 つのサポートされる方式、つまり事前共用キー・モードと署名モードのどちらかを使用して認証されます。

   事前共用キー・モードでは、両方の IKE ピアは、以前のオフライン・プロセスにより、キーを交換していました。これは、現在では、ピアを認証するためにフェーズ 1 の間に使用されています。事前共用キーは、ポリシー・フィーチャーの **add user** コマンドを使用して構成します。

   署名モードでは、フェーズ 1 メッセージのペイロードを暗号化したり、暗号化解除するのに使用されるキーを提供するために、署名付きの X.509 ディジタル証明書が使用されます。署名および検証が正しく実行されると、ピアは認証されます。署名モードおよび X.509 ディジタル証明書の使用について詳しくは、414 ページの『公開キー・インフラストラクチャーの使用』を参照してください。

フェーズ 1 交渉は、次の 2 つのモードのどちらかを使用して行われます。

- メイン・モード。このモードでは、フェーズ 1 ネゴシエーションを実行し、交渉中のピアの識別を暗号化するのに 6 つのメッセージが使用されます。
- 積極モード。このモードでは、フェーズ 1 ネゴシエーションを実行するのに 3 つのメッセージが使用されます。ピアは、最初の 2 つのメッセージで保護されていない識別を交換します。

IP セキュリティー・トンネルのネゴシエーション

このトピックに記載されている処理は、ルーターが、ポリシー・データベース内の規則で定義されている属性と一致する属性をもつパケットを送信する準備をするときに発生します。トンネルのネゴシエーションは、2 つの段階で発生します。フェーズ 1 では、送信側ルーターが 6 つのメッセージ交換の最初のメッセージを送信することによって通信を始めると、これにより、フェーズ 2 で使用される保護オプションが設定されます。受信側が応答し、送信側と受信側双方が ISAKMP セキュリティー・アソシエーション (SA) 特性や使用される認証および暗号化アルゴリズムをネゴシエーションして、互いの識別を認証します。フェーズ 2 の間に、双方は、合計 3 つのメッセージを交換して、双方間で送信される IP データグラムの保護に使用される SA およびキーをネゴシエーションします。フェーズ 1 は、次のように進みます。

1. メッセージ 1: 送信側は、通信アクティビティーが発生する方法、つまり、認証方式 (たとえば、ディジタル署名)、認証アルゴリズム (たとえば、HMAC-MD5)、および使用する暗号化アルゴリズム (たとえば、DES-CBC) を提示します。
2. メッセージ 2: 受信側は、サポートするセキュリティー・オプション (存在する場合) を送信側に示します。
3. メッセージ 3: 送信側は、その Diffie Hellman 公開値のほか、作成される暗号化キーの元になるランダム値を送信します。
4. メッセージ 4: 受信側は、その独自の Diffie Hellman 公開値のほか、作成される暗号化キーの元になるランダム値を送信します。この時点で、送信側と受信側は、公開キーとプライベート・キーおよび ISAKMP メッセージ交換で使用されるキー関連情報を作成します。
5. メッセージ 5: 送信側は、ディジタル署名を送信します。承認済みの認証局 (CA) によって署名された X.509 ディジタル証明書を含める場合があります。送信側が有効な証明書を含めない場合には、受信側は、LDAP プロトコルを使用して、承認済み CA または保護 DNS サーバー、以前に使用された証明をそれぞれの ID 値にマップする保護ローカル・キャッシュのどれかから証明を取得する必要があります。あるいは、送信側に証明を要求することもできます。この要求があった場合、送信側は、即時にそれを送信しなければなりません。
6. メッセージ 6: 送信側のディジタル署名を検証した後で、受信側は、自身に関する同じ種類の情報を送信側に送信します。

この時点で、送信側と受信側は、互いにそれぞれを認証し合い、SA の特性に関して同意し、ISAKMP SA を扱うためにキーおよびキー関連情報を引き出しています。これで、双方とも、フェーズ 2 に入って、非 ISAKMP SA およびキーをネゴシエーションします。これらは、送信側と受信側との間で交換される IP データグラムを保護するのに使用されます。フェーズ 2 は、次のように進みます。

1. メッセージ 1: 送信側は、AH または ESP アルゴリズム選択を送信することによって非 ISAKMP SA を提示します。これには、他のセキュリティー関連情報も含めます。
2. メッセージ 2: 受信側は、選択した提示を送信側に示します。これには、セキュリティー関連情報も含めます。
3. メッセージ 3: 送信側は、ネゴシエーションされたセキュリティー・プロトコルを使用して、さきに進む用意が整っていることを受信側に示すために、いくつか

の項目のハッシュ・レコードを送信します。受信側がこの情報を検証すると、リンクは完成し、送信側と受信側は保護されたデータ・ストリームの交換を始めます。

公開キー・インフラストラクチャーの使用

ここでは、公開キー・インフラストラクチャー (PKI) の使用方法について説明します。IKE は、PKI を使用して、IKE エンティティーを認証するために公開キー署名モードをサポートします。このリリースでは事前共用キー・モードをサポートしていますが、このモードでは PKI サポートは必要ないので、固有の不都合な点が含まれています。認証のためには、それぞれのピアの事前共用キーを使用して各 IKE エンティティーを構成する必要があります。このため、IKE 操作のスケーラビリティーは大きく制限されます。公開キーに基づく署名または公衆暗号化モードの方が、はるかに高いスケーラビリティーが提供されます。このリリースでは、IKE エンティティーを認証するために、署名モード IKE フェーズ 1 ネゴシエーションで X.509 ディジタル証明書が使用されます。

IKE ネゴシエーションに参加させたい各 IKE エンティティーごとに、そのユーザー・ポリシー・プロファイルを構成する際に ISAKMP ID フィールドに固有の値を指定することにより、識別を割り当てます。各 IKE エンティティーは、そのピアを使用してその識別を認証します。

PKI は、公開キー操作をサポートするよう、目下、定義し、開発しているところです。PKI では、X.509 ディジタル証明書が、エンティティーの公開キーをその主張する識別にバインドします。IKE エンティティーは、証明書に含まれている公開キーを取り出すことができます。そうすると、公開キー操作を実行して、IKE ネゴシエーションに参加しているピアの識別を認証することができます。公開キーは、IKE 署名モードに使用されます。このモードでは、署名者は、そのプライベート・キーを使用して、ディジタル署名に署名します。受信側は、証明書から署名者の公開キーを取り出し、それを使用して、署名を検証します。ディジタル証明書機能により、1つの IKE エンティティーが別の IKE エンティティーの識別を認証するための拡張が容易な方法が提供されます。

PKI の構成

このリリースでは、1 回のネゴシエーションの両方の IKE エンティティーが同じ CA を使用するものと想定しています。署名を使用して IKE ネゴシエーションを開始する前に、ルーターの PKI を構成する必要があります。ルーターのプライベート・キーおよびルーター証明を生成し、ルート CA の証明をダウンロードさせる必要もあります。次のステップで、PKI の構成方法を説明します。

1. キーのペアを生成し、その証明書を要求する。

   公開キー操作には 1 組みのキー・ペア (署名モードは、署名にはプライベート・キーを使用し、検証には公開キーを使用します) が必要であるため、ルーターのために 1 組みのキー・ペアを生成する必要があります。認証要求のためには、X.509 ディジタル証明書に入れるように、生成された公開キーを CA に送信する必要があります。ディジタル証明書に入っていると、ポテンシャル IKE ピアは、この公開キーを CA 発行の証明書から取り出すことができます。プライベート・キーは、ルーターに収められており、ルーター以外には機密にされます。

このバージョンでは、**certificate request** コマンドを出して、次のことを行うことができます。

a. 1 組みのキー・ペアを生成する。このキーの長さは、512、768、または 1024 ビットのどれかに指定できます。生成されたプライベート・キーは、キャッシュに入ったままです。

b. ユーザーが認証要求に組み込むために情報 (たとえば、IP アドレス形式のルーター ID、ドメイン名、または E メール名) を入力するよう要求する。

c. 生成された公開キーおよびユーザーが入力した情報が入っている (PKCS#10 形式の) 認証要求を作成する。

d. ホスト・マシンへ認証要求を TFTP する。

2. (ルーターの外側で) 証明書を発行する

   CA が PKCS#10 認証要求を受け取ります。CA は、手動でこの要求を検証し、証明書を発行できます。この証明書には、ルーター公開キーおよびユーザーが入力した情報が入っています。CA はそのプライベート・キーを使用して証明書に署名するため、これは、署名した CA をユーザーが信頼する限り、承認済みディジタル情報となります。これで、証明書は、IKE ネゴシエーションで使用できる状態になりました。(この処理は、ルーター操作の外側のことであり、本書ではこれ以上説明していません。)

3. ルーター証明書をダウンロードする

   CA が証明書を発行してあれば、PKI はそれをダウンロードしてルーターに入れることができます。 CA がこの証明書を公表する方法により、PKI は、TFTP または LDAP のどちらかを使用してダウンロードを行うことができます。

   ディジタル署名などの公開キー操作を実行するためには、ルーター証明書内のプライベート・キーと公開キーが一致する必要があることに注意してください。PKI が証明書をダウンロードしてルーターに入れるときには、公開キーを使用して生成されたプライベート・キーがルーター・キー・キャッシュに入っていなければなりません。ダウンロードされた証明書は、その一致するプライベート・キーがなくなった場合は役に立ちません。これは、ユーザーが認証要求を出してから証明書がダウンロードされるまで、ユーザーは、ルーターのリスタートまたは再ロード、キャッシュのクリア、新しい認証要求の発行を行っては**なりません**。これらのどの操作が行われても、ルーター実行キャッシュ内のプライベート・キーは破棄されます。

4. CA 証明書をダウンロードする

   IKE ピアの証明書を検証するためには、PKI はピアのルート CA 証明書を取得する必要があります。このリリースは、単一レベル CA 操作をサポートしており、そのことは、IKE エンティティーを同じ CA に割り当てる必要があることを意味します。各 IKE エンティティー (この場合は、各ルーター) は、ピアから受け取った証明書が有効であることを確認するために、(TFPT または LDAPのどちらかを使用して) CA の証明書をダウンロードする必要があります。

5. 証明書を保管し、再ロードする

   ユーザーは、ルーターが証明書、その一致するプライベート・キー、および CA の証明書を取得した後で、IKE ネゴシエーションを開始できます。証明書は一般時計に数か月間または数年間有効であるため、ルーターを再ロードまたはリスタートするたびに認証要求を発行してダウンロードを行わないで済むように、SRAM に証明書とプライベート・キーを保管する必要があります。このバージ

ョンでは、証明書とプライベート・キーを SRAM に保管したり、取り出したりできるように、**cert save** コマンドと **cert load** コマンドが用意されています。

ルーター証明書とプライベート・キーは、ペアとして処理する (たとえば、それらは、必ず、一緒に SRAM に保管したり、そこから取り出すなど) 必要があることに注意してください。

次の例に示されているように、Talk 6 コマンドを使用して、TFTP および LDAP 両方のサーバー情報を構成します。

例 : Add Server (T6)

```
Config>f ipsec
IP Security feature user configuration
IPsec config>pki
PKI config>add server
Name ? (max 65 chars) []? test
Enter server IP Address []? 8.8.8.8
Transport type (Choices: TFTP/LDAP)  [TFTP]?
PKI config>
```

例 : List Server Configuration (T6)

```
PKI config>li server

1)  Name: SERVER1
    Type: TFTP
    IP addr: 8.8.8.8


2)  Name: TEST
    Type: TFTP
    IP addr: 8.8.8.8
```

例 : List Root Certificate (T6)

```
PKI config>li cert

Root CA  certificate:
       SRAM    Name:   R1
       Subject Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
  Default Root Cert:   No

       SRAM    Name:   R2
       Subject Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
  Default Root Cert:   Yes



Router   Certificate:
       SRAM    Name:   B1
       Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
       Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   No

       SRAM    Name:   B2
       Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
       Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   Yes

       SRAM    Name:   B3
```

```
      Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
      Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:  1.1.1.1
         Key Usuage:  Sign & Encipherment
           Validity:  1998/10/29 -- 2001/10/29
      Default Cert:   No

      SRAM    Name:   YYY
      Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
      Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:  1.1.1.1
         Key Usuage:  Sign & Encipherment
           Validity:  1998/10/29 -- 2001/10/29
      Default Cert:   No
```

例 : Certificate Request (T5)

```
PKI Console>cert-req
Enter the following part for the subject name
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? IBM
   Organization Unit Name(Max 32 characters) []? NHD
   Common Name(Max 32 characters) []? router1
Key modulus size
 [512]?
Certificate subject-alt-name type:
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 12.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Memory transfer starting.
.Memory transfer completed - successfully.
Certificate request TFTP to remote host successfully.
Private Key Alias [ROUTER_KEY]? local
Generated private key LOCAL stored into cache
```

例 : List Router Certificate (T5)

```
PKI Console>li cert
Router   certificate
      Serial Number:   909343811
       Subject Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
       Issuer  Name:   /c=CA/o=Entrust Technologies/ou=PartnerCA
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29

Root CA  certificate
      Serial Number:   914034740
       Subject Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 -- 2018/12/19
```

例 : Cert Save (T5)

```
PKI Console>cert-save
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? yyy
Load as default router certificate at initialization?? [No]:
Private key YYY written into SRAM
Both Certificate and private key saved into SRAM successfully
PKI Console>
```

例 : Cert Load (T5)

```
PKI Console>cert-load
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
Name []? yyy
Box certificate and private key saved into cache successfully
PKI Console>
```

手動 IP セキュリティー (IPv4) の使用

2216 用に IPv4 に含まれている IP セキュリティー・フィーチャーは、ポリシー・フィーチャーおよび他の IPSec 関連プロセスと併用されると、認証、保全性、機密性、および非放棄 (non-repudiation) を提供します。IPSec を手動で設定するには、ポリシー・データベースに IPSec オプションのサブセットが入っているポリシーを事前に構成して、手動トンネルのプロファイルおよび妥当性期間を定義します。ポリシー使用可能ルーターが IPSec パケットを送信できる状態になったときにポリシーの内容に基づいて宛先ルーターを使用して IPSec オプションを動的にネゴシエーションして確立するように、データベース内に IPSec オプション (ポリシー) のフルセットを事前構成することもできます。手動トンネルを定義する場合は、424ページの『手動 IP セキュリティーの構成 (IPv4)』を参照してください。ポリシー・オプションの説明については、325ページの『第19章 ポリシー・フィーチャーの使用』を参照してください。

手動 IP セキュリティー (IPv6) の使用

2216 用の IPv6 に入っている IP セキュリティー・フィーチャーは、認証、保全性、および機密性を提供します。手動トンネルを定義する場合は、435ページの『手動 IP セキュリティー (IPv6) の構成』を参照してください。

第22章 IP セキュリティーの構成と監視

この章では、IP セキュリティーの構成および監視の方法、および IP セキュリティー監視コマンドの使用法について説明します。IPv4 の場合、325ページの『第19章 ポリシー・フィーチャーの使用』および 365ページの『第20章 ポリシー・フィーチャーの構成と監視』に、IP セキュリティー・ポリシーの構成と監視に関する付加情報が記載されています。この章には、次の内容が記載されています。

- 『インターネット・キー交換の構成 (IPv4)』
- 420ページの『公開キー・インフラストラクチャーの構成 (IPv4)』
- 420ページの『証明書の取得』
- 421ページの『公開キー・インフラストラクチャー構成コマンド』
- 424ページの『手動 IP セキュリティーの構成 (IPv4)』
- 425ページの『IP セキュリティー構成環境へのアクセス』
- 425ページの『手動 IP セキュリティー構成コマンド』
- 434ページの『手動トンネルの構成 (IPv4)』
- 435ページの『手動 IP セキュリティー (IPv6) の構成』
- 436ページの『IP セキュリティー構成環境へのアクセス』
- 437ページの『手動 IP セキュリティー構成コマンド』
- 437ページの『手動トンネルの構成 (IPv6)』
- 441ページの『手動 IP セキュリティー (IPv4) の監視』
- 452ページの『手動 IP セキュリティーの監視 (IPv6)』
- 452ページの『IP セキュリティー動的再構成サポート』

注: TN3270、APPN®-ISR、または APPN-HPR トラフィックを伝送するために IPSec トンネルを作成し、BRS を使用してそのトラフィックに優先順位を付ける計画の場合は、BRS の IPv4 優先順位ビット設定フィーチャーを使用することが必要です。詳しくは、10ページの『IP 保護トンネルおよび 2 次フラグメント内の SNA トラフィック用の IP バージョン 4 優先順位ビット処理の使用』を参照してください。

インターネット・キー交換の構成 (IPv4)

ここでは、インターネット・キー交換 (IKE) の構成方法について説明します。

IPSec トンネルを確立する前に、次のことを行う必要があります。

1. トンネルおよび結果として生じるアクション (ポリシー) を使用するパケットの属性を構成する。
2. 必要な暗号化オプションおよび認証オプションを構成する。

これらのタスクについて詳しくは、325ページの『第19章 ポリシー・フィーチャーの使用』、365ページの『第20章 ポリシー・フィーチャーの構成と監視』、および420ページの『公開キー・インフラストラクチャーの構成 (IPv4)』を参照してください。

公開キー・インフラストラクチャーの構成 (IPv4)

ここでは、公開キー・インフラストラクチャー (PKI) の構成方法について説明します。

IPSec トンネルを確立する前に、次のことを行う必要があります。

1. 公開 / プライベート暗号キーのペアを作成し、承認済み認証局 (CA) からディジタル証明書を取得する。詳しくは、『証明書の取得』を参照してください。
2. 構成しようとするポリシーをもつルーターに使用する IPSec アルゴリズム、SA、およびその他のオプションを決定する。詳しくは、413ページの『IP セキュリティー・トンネルのネゴシエーション』およびこれ以降のトピックを参照してください。
3. ポリシー・データベースを更新する。詳しくは、419ページの『インターネット・キー交換の構成 (IPv4)』、325ページの『第19章 ポリシー・フィーチャーの使用』、および 365ページの『第20章 ポリシー・フィーチャーの構成と監視』を参照してください。

証明書の取得

IPSec トンネルを確立する前に、414ページの『公開キー・インフラストラクチャーの使用』に記載されているとおりに、承認済み認証局 (CA) を選択して、それに登録する必要があります。CA は、署名付きの X.509 ディジタル証明書を戻します。この証明書により、ユーザーは、ネットワーク内の他のパーティーに対して自らを識別し、認証することができます。証明書は、コード化されたディジタル ID (署名) および公開 / プライベート暗号キーのペアで構成されます。次のことを行ってください。

1. CA を識別し、そのサーバー・アドレスを取得する。
2. 421ページの『公開キー・インフラストラクチャー構成コマンド』に記載されているとおりに PKI Talk 6 **add ldapserver** コマンドまたは **add tftpserver** コマンドを使用して、証明書リポジトリー取り出しオプションを構成する。
3. 443ページの『公開キー・インフラストラクチャー監視コマンド』に記載されているとおりに、PKI Talk 5 **certificate request** コマンドを使用して公開 / プライベート・キーのペアを作成する。この作成は、ルーター内でもリモートでも行えます。リモートの場合 (たとえば、バーチャル・プライベート・ネットワーク (VPN) 管理者として行動する場合がそうです) には、キーのペアを暗号化して、安全に送信してルーターに入れる必要があります。
4. 443ページの『公開キー・インフラストラクチャー監視コマンド』に記載されているとおりに、PKI Talk 5 **certificate request** コマンドを使用して、CA に対して初期認証要求を実行依頼する。要求は、E メールまたは FTP により、PKCS#10 メッセージに入れて送信されます。CA はこのキーのペアをバインドして証明書に入れ、CA のプライベート・キーを使用して署名し、中央 (LDAP または FTP) リポジトリーに保管するか、PKCS#7 メッセージに入れてユーザーに戻します。通常、証明書は、数か月間または数年間有効であり、更新されます。これにより、ネットワーク内のどのパーティーがまだ信頼できるかが識別されます。

5. 443ページの『公開キー・インフラストラクチャー監視コマンド』に記載されているとおりに、PKI Talk 5 **certificate save** コマンドを使用して、証明書をルーターの SRAM に入れて保管する。

注:

1. SRAM 内の認証レコードのリストを表示するためには、『公開キー・インフラストラクチャー構成コマンド』に記載されているとおりに PKI Talk 6 **list certificate** コマンドを使用します。
2. SRAM から認証レコードを削除するためには、『公開キー・インフラストラクチャー構成コマンド』に記載されているとおりに PKI Talk 6 **delete certificate** コマンドを使用します。
3. 将来の IPSec ネゴシエーション時に認証要求を再度実行依頼しなくて済むようにするためには、443ページの『公開キー・インフラストラクチャー監視コマンド』に記載されているとおりに PKI Talk 5 **certificate load** コマンドを使用して、受信した証明書をキャッシュにロードします。

公開キー・インフラストラクチャー構成コマンド

Add

PKI Talk 6 **add** コマンドは、証明書リポジトリー・サーバーとその位置を構成するのに使用します。

構文:

add server

server add (追加) 操作がサーバーを対象とするものであることを指示します。

例 1: サーバーの追加

```
PKI config>add server
Name ? (max 65 chars) []? myldap
Enter server IP Address []? 8.8.8.9
Transport type (Choices: TFTP/LDAP)  [TFTP]? ldap
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
LDAP version [2]?
Bind to the server anonymously? [No]:
Enter your bind DN: []? c=us o=ibm
Enter your bind PW: []? testldap
```

Change

PKI Talk 6 **change** コマンドは、証明書リポジトリー・サーバーとその位置を変更するのに使用します。

構文:

change server

server add (追加) 操作がサーバーを対象とするものであることを指示します。

例 1: サーバーの変更

```
PKI config>change server
Name []? myldap
Enter server IP Address []? 8.8.8.7
Server type will continue to be LDAP
```

```
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
LDAP version [2]?
Enter your bind DN: [c=us o=ibm]?
Enter your bind PW: [testldap]?
```

Delete

PKI Talk 6 **delete** コマンドは、認証レコードまたはプライベート・キー・レコードをルーターの SRAM から削除したり、サーバーを削除するのに使用します。

構文:

delete 証明書
private-key
server

certificate

delete (削除) 操作が 1 つまたは複数の認証レコードを対象とするものであることを指定します。

all すべての認証レコードを削除することを指定します。

id 削除される認証レコードの ID を指定します。

例 1: 証明書の削除

```
PKI config>delete certificate
Cert Name []? test
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Box Certificate [TEST] deleted successfully
Corresponding private Key [TEST] deleted successfully
```

例 2: プライベート・キーの削除

```
PKI config>delete private-keys
Private Key Name []? test
Private Key [TEST] deleted successfully
Corresponding box certificate [TEST] deleted successfully
```

例 3: サーバー・レコードの削除

```
PKI config>delete server
Name []? myldap
Server MYLDAP deleted successfully
```

private-key

delete (削除) 操作が 1 つまたは複数のプライベート・キー・レコードを対象とするものであることを指定します。

server delete (削除) 操作がサーバーを対象とするものであることを指示します。

List

PKI Talk 6 **list** コマンドは、to list certificate or key records in a router'sルーターの SRAM にある証明書やキー・レコードをリストしたり、証明書取り消しリスト (CRL--取り消された証明書をもつ ISAKMP 使用可能化パーティーのリスト) を表示するために使用します。現行の CRL を取得するためには、PKI Talk 6 **load** コマンドを使用します。

構文:

list certificates
crl
private-keys
servers

certificates
list (リスト) 操作が認証レコードを対象とするものであることを指定します。

crl list (リスト) 操作が証明書取り消しリストを対象とするものであることを指定します。

private-keys
list (リスト) 操作がプライベート・キー・レコードを対象とするものであることを指定します。

servers
list (リスト) 操作がサーバー・レコードを対象とするものであることを指定します。

例: 証明書のリスト

```
PKI config>list certificates

Root CA  certificate:
       SRAM    Name:   B
       Subject Name:   /c=US/o=ibm/ou=nhd
      Issuer   Name:   /c=US/o=ibm/ou=nhd
           Validity:   1998/12/19 2:2:21 -- 2018/12/19 2:32:21
  Default Root Cert:   Yes



Router   Certificate:
       SRAM    Name:   W
      Subject  Name:   /c=US/o=ibm/ou=nhd/cn=testip
      Issuer   Name:   /c=US/o=ibm/ou=nhd
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1999/1/19 23:24:27 -- 2002/1/19 23:54:27
       Default Cert:   No
```

例: crl のリスト

```
PKI config>list crl
```

例: プライベート・キーのリスト

```
PKI config>list private-keys
Private Keys In SRAM:

1) Name W
```

例: サーバー・レコードのリスト

```
PKI config>list servers
1)  Name: SERVER1
    Type: LDAP
    IP addr: 1.1.1.2
        LDAP search timeout (secs): 10
        LDAP retry interval (mins): 3
        LDAP server port number: 390
        LDAP version: 2
        Anonymous bind ?: y
```

```
2)  Name: TEST
    Type: TFTP
    IP addr: 8.8.8.8
```

Load

PKI Talk 6 **load** コマンドは、最新の証明書取り消しリスト (CRL) を CA から取り出すために使用します。リストのコピーの妥当性を確認するために定期的にかつ頻繁にこれを行う必要があります。認証の間、IPSec フィーチャーは、CRL の内容に基づいた証明書を検証します。

構文:

load crl

手動 IP セキュリティーの構成 (IPv4)

ここでは、IPv4 での手動 IPSec に使用できる構成オプションについて説明します。IPv4 には、すべての IPSec 機能が適用されます。

IPSec 手動トンネルを構成するには、次のステップを実行します。

1. IPSec トンネルを作成する。
2. IPSec をリセットする。
3. 手動トンネルのポリシー (プロファイル、妥当性、ポリシー) のポリシーを構成する。
4. ポリシーをリセットする。

アルゴリズムの構成

表47に示されているアルゴリズムを使用してトンネル・ポリシーを構成できます。

表 47. 各種のトンネル・ポリシーを使用して構成されたアルゴリズム

トンネル・ポリシー	アルゴリズム
AH、AH-ESP、または ESP-AH	• ローカル AH 認証アルゴリズム - 必須 • リモート AH 認証アルゴリズム - オプション
ESP、AH-ESP、または ESP-AH	• ローカル暗号アルゴリズム - 必須 • リモート暗号アルゴリズム - オプション • ローカル ESP 認証アルゴリズム - オプション • リモート ESP 認証アルゴリズム - オプション **注:** ソフトウェア・ロードに暗号化が含まれていない場合は、暗号化関連のパラメーターは表示されません。

トンネル・ポリシーは、アウトバウンド・パケットに対してはローカル・アルゴリズムを、インバウンド・パケットに対してはリモート・アルゴリズムを使用します。トンネルの手前の端にあるルーターのローカル・アルゴリズムは、トンネルの向こうの端にあるルーターのリモート・アルゴリズムと一致する必要があります。リモート・アルゴリズムの値の指定は任意であり、デフォルトとして、対応するローカル・アルゴリズムの値を取ります。ESP 認証は任意選択なので、ローカル認証アルゴリズムの選択は任意です。

暗号化キーの構成

構成するローカル・アルゴリズムごとに、リモート・ホスト内の対応するアルゴリズムのキーと同じキーを構成することも必要です。『手動 IP セキュリティー構成コマンド』の **add tunnel**コマンドについては、キーの説明を参照してください。

IP セキュリティー構成環境へのアクセス

IP セキュリティー構成環境にアクセスするには、OPCON (*) プロンプトで **t 6** と入力してから、Config> プロンプトで次の一連のコマンドを入力します。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPV4-IPsec config>
```

手動 IP セキュリティー構成コマンド

ここでは、IP セキュリティー構成コマンドについて説明します。これらのコマンドは、IPV4-IPsec config> プロンプトで入力します。

表 48. IP セキュリティー構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add tunnel	保護トンネルを追加します。
Change tunnel	保護トンネル構成パラメーター値を変更します。
Delete tunnel	保護トンネルを削除します。
Disable	安全な方法でのすべての IP セキュリティー処理 (パケット・フィルターに一致するパケットを廃棄する) を使用不可にする、非安全な方法でのすべての IP 処理 (パケット・フィルターに一致するパケットを通過させる) を使用不可にする、または保護トンネルを使用不可にします。
Enable	すべての IP セキュリティー処理を使用可能にするか、または保護トンネルを使用可能にします。
List	グローバル IP セキュリティー情報、または定義済みのトンネルに関する情報を表示します。
Set	各種の IPSec オプションを設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Add Tunnel

add tunnel コマンドは、IPSec トンネルを定義するためのパラメーターを追加するのに使用します。

構文:

add tunnel ...

tunnel-name

トンネルにラベルを付けるための任意指定パラメーター。これは 2216 内で固有でなければなりません。

有効値: 最大 15 文字。最初の字は文字でなければなりません。ブランクは使用できません。

デフォルト値 : なし

lifetime

トンネルが活動状態でいられる時間数 (分)。値 0 は、トンネルの存続時間は満了しないことを示します。

有効値: 0 ～ 525600 (0 = 満了しない、525600 = 365 日)

デフォルト値: 46080 (32 日)

encapsulation-mode

IP パケットをカプセル化する方法。トンネル・モードでは、IP パケット全体がカプセル化され、新規の IP ヘッダーが作成されます。トランスポート・モードでは、IP ヘッダーはカプセル化されません。保護トンネルの一端がルーターの場合は、インターネット技術特別委員会 (IETF) セキュリティー体系草案に準拠して、トンネル・モードを使用することが ***必要*** です。

有効値: トンネル (*TUNN*) またはトランスポート (*TRANS*)

デフォルト値: トンネル (*TUNN*)

tunnel-policy

トンネル・ポリシーを定義する 4 つの選択項目のうちの 1 つ。すなわち、IP 認証ヘッダー (AH)、IP カプセル化セキュリティー・ペイロード (ESP)、またはこれらのプロトコルの組み合わせ (AH-ESP および ESP-AH)。AH-ESP では、発信パケットで ESP 暗号化が最初に実行されます。ESP-AH では、発信パケットで AH 認証が最初に実行されます。一部のパラメーターは、ESP または AH のどちらかに固有です。暗号化パラメーターは、ESP、AH-ESP、または ESP-AH を選択した場合にだけ構成します。認証パラメーターは、AH、AH-ESP、または認証付き ESP を選択した場合にだけ構成します。

有効値: AH、ESP、AH-ESP、ESP-AH

デフォルト値: AH-ESP

local-IP-address

トンネルの手前の端の IP アドレス。

有効値: インターフェースに構成された、または 2216 の内部アドレスとして構成された、有効な IP アドレス。

デフォルト値: ルーターに構成された IP アドレスの 1 つ

local-spi

セキュリティー・アソシエーションとは、AH または ESP を使用して接続のトラフィックを保護する単方向セキュリティー接続です。セキュリティー・パラメーター・インデックス (SPI) は、この保護トンネルに対応する 2 つのセキュリティー・アソシエーション (インバウンドまたはアウトバウンド) の 1 つを固有に識別する任意の 32 ビット値です。このパラメーターは必須であり、トンネルのローカル側で受信されるインバウンド・パケットに対してこのトンネルで期待される SPI を識別します。この値は、同じローカル IP アドレスをもつ別のトンネルのローカル SPI と一致していてはなりません。トンネル・ポリシー (ESP、AH、AH-ESP、または ESP-AH)

に関係なく、1 つの IP 保護トンネルのインバウンド・トラフィックに対して 1 つだけローカル SPI を構成します。

有効値: 255 より大きい、任意の 32 ビット値

デフォルト値: 256

local-encryption-algorithm

ローカル・ルーターから送信されるアウトバウンド・パケットの ESP に使用される暗号アルゴリズム。ESP を構成する場合は必須です。一部の国では、米国の輸出規制のため、このアルゴリズムの一部または全部を使用できない場合があります。この暗号アルゴリズムは、リモート側の暗号アルゴリズムと一致していなければなりません。

ESP-NULL アルゴリズムは、ESP が暗号化を実行するのを防止します。このアルゴリズムは、すべての国で利用可能です。ESP-NULL を選択した場合は、認証アルゴリズム HMAC-MD5 または HMAC-SHA-1 を選択して、認証を活動化しておく必要があります。

有効値: DES-CBC、CDMF、3DES、または ESP-NULL

デフォルト値: DES-CBC

local-encryption-key

ローカル ESP 暗号アルゴリズムで使用される 1 つまたは複数のキー。これらは、保護トンネルの反対側に構成された対応するキーと一致していなければなりません。 ESP-NULL 暗号アルゴリズムを選択した場合は、このキーは構成しません。

有効値:

- DES-CBC の場合: 16 桁の 16 進文字 (0 〜 9、a 〜 f、A 〜 F)
- CDMF の場合: 16 桁の 16 進文字 (0 〜 9、a 〜 f、A 〜 F)
- 3DES の場合: どれも同じでない 3 つの別々のキー、それぞれ 16 桁の 16 進文字 (0 〜 9、a 〜 f、A 〜 F)

デフォルト値: なし

padding-for-local-encryption

アウトバウンド ESP パケットに追加される追加埋め込みのサイズ (バイト)。追加埋め込みは、暗号アルゴリズムの結果、暗号化されたパケットが元のパケットと同じサイズになる場合、暗号化される IP パケットのサイズを偽装するために使用できます。ESP 埋め込み値は 8 の倍数でなければなりません。

暗号アルゴリズムが ESP-NULL の場合は、埋め込みは必要ありません。ESP-NULL アルゴリズムは元のパケット・サイズに 1 バイトを追加するからです。ローカル暗号化の埋め込みを構成した場合、その値は無視されます。

有効値: 0 〜 120

デフォルト値: 0

local-ESP-authentication

ローカル ESP 認証を選択します (必要な場合)。暗号アルゴリズムが ESP-NULL の場合、認証の指定は必須です。

有効値: Yes または No

デフォルト値: Yes

local-authentication-algorithm

アウトバウンド・パケットで使用される認証アルゴリズム。ESP の場合、これは任意指定パラメーターで、ESP 認証を選択しない限り必要ではありません。AH、AH-ESP、または ESP-AH の場合、このパラメーターは必須です。使用する認証アルゴリズムは、IPSec トンネルの反対側で使用されるリモート認証アルゴリズムと一致していなければなりません。

有効値: HMAC-MD5 または HMAC-SHA

デフォルト値: HMAC-MD5

local-authentication-key

ローカル認証アルゴリズムで使用されるキー。これは、IPSec トンネルの反対側に構成される等価キーと一致していなければなりません。ポリシーが AH、AH-ESP、または ESP-AH の場合、またはポリシーが ESP でローカル ESP 認証アルゴリズムが構成されている場合には、このパラメーターは必須です。

有効値:

- HMAC-MD5 の場合: 32 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- HMAC-SHA の場合: 40 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)

デフォルト値: なし

remote-IP-address

トンネルのリモート側の IP アドレス。これは必須パラメーターです。

有効値: 有効な IP アドレス

デフォルト値: なし

remote-spi

セキュリティー・アソシエーションとは、AH または ESP を使用して接続のトラフィックを保護する単方向セキュリティー接続です。セキュリティー・パラメーター・インデックス (SPI) は、この保護トンネルに対応する 2 つのセキュリティー・アソシエーション (インバウンドまたはアウトバウンド) の 1 つを固有に識別する任意の 32 ビット値です。このパラメーターは必須であり、リモート・ホストあてのアウトバウンド・パケットの ESP または AH に期待される SPI を識別します。この値は、同じリモート IP アドレスをもつ別のトンネルのリモート SPI と一致していてはなりません。トンネル・ポリシー (ESP、AH、AH-ESP、または ESP-AH) に関係なく、1 つの IPSec トンネルのアウトバウンド・トラフィックに対して 1 つだけローカル SPI を構成します。

有効値: 255 より大きい、任意の 32 ビット値

デフォルト値: 256

remote-encryption-algorithm

リモート・ホストから受信するインバウンド・パケットで使用される暗号化解除アルゴリズム。これはローカル側の暗号アルゴリズムと一致していなければなりません。

ESP-NULL アルゴリズムは、ESP が暗号化を実行するのを防止します。ESP-NULL を選択した場合は、認証アルゴリズム HMAC-MD5 または HMAC-SHA-1 を選択して、認証を活動化しておく必要があります。

有効値: DES-CBC、CDMF、3DES、または ESP-NULL

デフォルト値: ローカル側の暗号アルゴリズムの値

remote-encryption-key

リモート側の ESP 暗号アルゴリズムで使用される 1 つまたは複数のキー。これらは、保護トンネルの反対側に構成された等価キーと一致していなければなりません。ESP-NULL 暗号アルゴリズムを選択した場合は、このキーは構成しません。

有効値:

- DES-CBC の場合: 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- CDMF の場合: 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- 3DES の場合: どれも一致しない 3 つの別々のキー、それぞれ 16 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)

デフォルト値: なし

verification-of-remote-encryption-padding

受信パケットの暗号化埋め込みのサイズを検査するかどうかを決めます。

有効値: Yes または No

デフォルト値: No

padding-for-remote-encryption

受信 ESP パケットに期待される追加埋め込みのサイズ (バイト)。このパラメーターは、*verification-of-remote-encryption-padding* の値が Yes の場合にだけ必須であり、有効です。ESP 埋め込み値は 8 の倍数でなければなりません。8 で割り切れない値が構成されている場合、その値は 8 で割り切れる次の値に切り上げられます。

有効値: 0 ～ 120

デフォルト値: 0

remote-ESP-authentication

インバウンド・パケットのリモート ESP 認証を選択します (必要な場合)。

有効値: Yes または No

デフォルト値: Yes

remote-authentication-algorithm

インバウンド・パケットに使用される認証アルゴリズム。ESP の場合、これは任意指定パラメーターで、ESP 認証を選択しない限り必要ではありません。AH または AH と ESP の組み合わせ (AH-ESP または ESP-AH) の場合、このパラメーターは必須です。使用する認証アルゴリズムは、IPSec トンネルの反対側で使用されるローカル認証アルゴリズムと一致していなければなりません。

有効値: HMAC-MD5 または HMAC-SHA

デフォルト値: HMAC-MD5

remote-authentication-key
リモート側の認証アルゴリズムで使用されるキー。これは、保護トンネルの反対側に構成された等価キーと一致していなければなりません。これは、AH、AH-ESP、ESP-AH、および ESP (リモート ESP 認証アルゴリズムが構成されている場合) で必須です。

有効値:
- HMAC-MD5 の場合: 32 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)
- HMAC-SHA の場合: 40 桁の 16 進文字 (0 ～ 9、a ～ f、A ～ F)

デフォルト値: なし

enable-replay-prevention
再生防止が使用可能かどうかを指定します。再生防止が使用可能の場合、IP セキュリティー・ヘッダー内のシーケンス番号を監視して、トンネルの受信側によって重複パケットが処理されるのを防止します。再生防止の使用はお勧めできません。送信側のシーケンス番号カウンターが限界に達すると、トンネル・セキュリティー・アソシエーションを非活動化しなければならないからです。この状態が起きた場合、手動で介入して、既存のセキュリティー・アソシエーションをリスタートするか、新規に作成することが必要になります。

再生防止が使用可能で、**reset ipSec** コマンドを使用して IPSec をリセットした場合は、必ず IPSec トンネルの反対側のルーター上の IPSec もリセットする必要があります。これは、トンネルの両側でシーケンス番号を再初期設定するために必要です。トンネルの一端で IPSec がリセットされ、他端はリセットされていない場合、トンネルの各端のルーターは、シーケンス番号ミスマッチによりパケットをドロップする可能性があります。

有効値: Yes または No

デフォルト値: No

DF-bit トンネル・モードの保護トンネルの外部ヘッダー内の断片化不可 (DF) ビットの扱いを指定します。パケットを断片化できないことを指定するために、IPv4 ヘッダー内にこのビットをセットすることができます。DF ビット・パラメーターは、着信パケット内の DF ビットの扱い方を 2216 に知らせます。すなわち、内部ヘッダー内に見つかった DF ビットを外部ヘッダーにコピーするか、外部ヘッダーにビットをセットするか、あるいは外部ヘッダー内のビットをクリアするかどうかを指示します。

DF ビットがセットされており、パケットを断片化できない場合、IPSec はパス MTU (PMTU) ディスカバリー機能を使用します。詳しくは、409ページの『パス最大伝送単位ディスカバリー』を参照してください。

有効値: Copy、Set、Clear

デフォルト値: Copy

enable-tunnel
このトンネルが使用可能かどうかを指定します。パケット・フィルターを構成して、この IPSec トンネルで使用するインターフェースを定義し、IP をリセットするか 2216 をリスタートするまでは、使用可能にされたトンネルはパケットをフィルターに掛けません。IP をリセットするには、**reset ip** コマンドを使用します。

有効値: Yes または No

デフォルト値: Yes

Change Tunnel

change tunnel コマンドは、**add tunnel** コマンドを使用して以前に構成した IPSec トンネル・パラメーターを変更するのに使用します。

構文:

change tunnel ...	変更できるパラメーターのリストについては、**add tunnel** コマンドの項を参照してください。

Delete Tunnel

Talk 6 **delete tunnel** コマンドは、IPSec トンネルを削除するのに使用します。

構文:

delete tunnel	*tunnel-id* *tunnel-name* all

tunnel-id

削除する IPSec トンネルの識別子を指定します。

有効値: 1 ～ 65535

デフォルト値: 1

tunnel-name

削除する IPSec トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all このインターフェース上のすべての IPSec トンネルを削除することを指定します。

Disable

disable コマンドは、IPSec トンネルを使用不可にするか、あるいはすべての IPSec トンネルを安全な方法 (IPSec フィルターに一致するパケットをドロップする) または無保護な方法 (IPSec フィルターに一致するパケットをパスさせる) で使用不可にするのに使用します。

構文:

disable	ipsec drop ipsec pass tunnel ...

ipsec drop

ルーター上の IP セキュリティーを安全な方法で使用不可にします。すべての IPSec トンネルが使用不可にされますが、パケット・フィルター規則の保護トンネル情報を使用して、IPSec トンネル・パケット・フィルターに一致するパケットを識別します。一致するパケットはドロップされます。

ipsec pass
ルーター上の IP セキュリティーを無保護な方法で使用不可にします。すべての IPSec トンネルが使用不可にされます。IPSec トンネル・パケット・フィルターに一致するパケットは、通常のトラフィックとして転送されます。

tunnel *tunnel-id tunnel-name* **all**
指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用不可にします。

tunnel-id
使用不可にする保護トンネルの識別子を指定します。

有効値: 1 ～ 65535

デフォルト値: 1

tunnel-name
使用不可にする保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all すべてのトンネル

Enable

enable コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを使用可能にするのに使用します。ルーター上の IPSec をグローバルに使用可能にしないと、個別に使用可能にされた IPSec トンネルは活動状態になりません。

構文:

enable ipsec
tunnel ...

ipsec ルーター全体の IP セキュリティーを使用可能にします。

tunnel *tunnel-id tunnel-name* **all**
指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用可能にします。

tunnel-id
使用可能にする保護トンネルの識別子を指定します。

有効値: 1 ～ 65535

デフォルト値: 1

tunnel-name
使用可能にする保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all すべてのトンネル

List

list コマンドは、現行の IP セキュリティー構成を表示するのに使用します。グローバル・トンネル (global tunnels) には、ルーター上のすべてのトンネル (活動および定義済みの両方) が含まれます。すべてのトンネル (all tunnels) には、このインターフェースに構成されたすべてのトンネル (活動および定義済みの両方) が含まれます。活動トンネル (active tunnels) は、現在活動状態のトンネルです。定義済みトンネル (defined tunnels) は、定義されているが活動状態ではないトンネルです。IPv4 の場合、ルーターの SRAM 内の選択された証明書も表示されます。

構文:

list ...

- all
- status
- tunnel
  - active *tunnel-id tunnel-name* all
  - defined *tunnel-id tunnel-name* all

例 1: すべての IPSec トンネルのリスト

```
IPsec config>list all

IPsec is ENABLED

IPsec Path MTU Aging Timer is 20 minutes

Defined Manual Tunnels:

   ID         Name         Local IP Addr   Remote IP Addr   Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
      1  test                    1.1.1.1          2.1.1.1  TUNN   Enabled
      2  test2                   1.1.1.1          1.1.1.3  TRANS  Enabled

Tunnel Cache:

 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
-----  ---------------  ---------------  -----  ------  ------------------
    2          1.1.1.1          1.1.1.3  TRANS  ESP     *****************
    1          1.1.1.1          2.1.1.1  TUNN   AH      *****************
```

例 2: ESP ポリシーと ESP-NULL アルゴリズムを使用する IPSec トンネルのリスト

```
IPsec config>li tun 1000

Tunnel  Name             Mode   Policy   Life   Replay  Rcv  IPsec  State
ID                                              Prev    Win  Vers
------  ---------------  -----  ------  ------  ------  ---  -----  --------
1000    t1000            TUNN   ESP      46080    No    ---   V2    Enabled

Handling of DF bit in outer header:  COPY

Local Information:

      IP Address: 10.11.12.10
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:  1234    Encryption Algorithm: NULL
                                 Extra Pad:   0
                                 ESP Authentication Algorithm: HMAC-MD5
Remote Information:

      IP Address: 10.11.12.11
  Authentication:  SPI: -----    Algorithm: ----------
      Encryption:  SPI:  1234    Encryption Algorithm: NULL
                                 Verify Pad?:  No
                                 ESP Authentication Algorithm: HMAC-MD5
```

Set

set コマンドは、トンネル PMTU 値を制御するのに使用します。

構文:

set path-mtu-age-timer

path-mtu-age-timer

2216 がトンネル PMTU 値を最大値に復元するまでに経過する時間 (分単位) を指定します。

デフォルト値: 10 (0 は使用不可 (disabled) を意味します)

手動トンネルの構成 (IPv4)

ここでは、411ページの図38 に示されているネットワークの手動 IPv4 トンネルの構成に関する情報を提供します。

ルーター A のトンネルの構成

次の例は、IPv4 を使用した、411ページの図38 に示されているネットワーク内のルーター A の IPSec 手動トンネルの構成方法を示しています。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPV4-IPsec config>add tunnel
Adding tunnel 1
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]?  AH
Local IP Address [1.1.1.1]? 223.252.252.216
Local Authentication SPI (256-65535)[256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 223.252.252.210
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set, or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-Ipsec config>
```

この例から分かるように、ユーザーが提供する必要があるパラメーターはプロンプトで指示されます。ESP、AH-ESP、または ESP-AH 保護トンネルの構成でも、同様のパラメーターが要求されます。

注: キーの値は、入力したときには表示されないので、この例には示されていません。 HMAC-MD5 認証のキーが表示されるとすれば、32 桁の 16 進文字で示されます。たとえば、キーは X'1234567890ABCDEF1234567890ABCDEF' といった値をもっています。

ルーター B のトンネルの構成

ルーター B 内に、ルーター A に構成したのと同じ IPSec 手動トンネル、つまり IPSec トンネル 1 を構成する必要があります。ルーター B 内のこのトンネルのローカル IP アドレスは 223.252.252.210 で、リモート IP アドレスは 223.252.252.216

です。その他のすべての IPSec トンネル・パラメーターは、ルーター A に構成されたパラメーターと一致していなければなりません。

例 : ESP を使用した IP セキュリティー・トンネルの手動による構成

トンネルがトンネル・モードにあり、トンネル・ポリシーが ESP である場合、DF ビットをセットするように求めるプロンプトが出ます。この例には、IPSec トンネルの構成だけを示します (パケット・フィルターの構成は示しません)。

```
IPV4-IPsec config>add tunnel
Adding tunnel 2
Tunnel Name (optional)? tunneltwo
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? [No]:
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0.0.0.0]?
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? [No]:
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>
```

例 : ESP および ESP-NULL を使用した IP セキュリティー・トンネルの手動による構成

認証が必要であることに注意してください。

```
IPV4-IPsec config>add tunnel
Adding tunnel 3
Tunnel Name (optional)? tunnel3
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]? 1234
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 10.11.12.11
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>
```

手動 IP セキュリティー (IPv6) の構成

ここでは、IPv6 での手動 IPSec に使用できる構成オプションについて説明します。IPv6 には、すべての IPSec 機能が適用されます。IPv6 用の IPSec を構成する場合は、IPSec 構成の質問が次のように変更されるので注意してください。

- アドレスは IPv6 アドレス形式で入力します (たとえば、8:0:9:8::1)。
- DF ビットの設定についての問い合わせはありません。

手動 IP セキュリティー (IPv6) の構成

IPSec 手動トンネルを構成するには、次のステップを実行します。
1. IPSec トンネルを作成する。
2. IPSec をリセットする。
3. フィルター規則を構成する。
4. IPV6 をリセットする。

アルゴリズムの構成

表49に示されているアルゴリズムを使用してトンネル・ポリシーを構成できます。

表 49. 各種のトンネル・ポリシーを使用して構成されたアルゴリズム

トンネル・ポリシー	アルゴリズム
AH、AH-ESP、または ESP-AH	• ローカル AH 認証アルゴリズム - 必須 • リモート AH 認証アルゴリズム - オプション
ESP、AH-ESP、または ESP-AH	• ローカル暗号アルゴリズム - 必須 • リモート暗号アルゴリズム - オプション • ローカル ESP 認証アルゴリズム - オプション • リモート ESP 認証アルゴリズム - オプション **注:** ソフトウェア・ロードに暗号化が含まれていない場合は、暗号化関連のパラメーターは表示されません。

トンネル・ポリシーは、アウトバウンド・パケットに対してはローカル・アルゴリズムを、インバウンド・パケットに対してはリモート・アルゴリズムを使用します。トンネルの手前の端にあるルーターのローカル・アルゴリズムは、トンネルの向こうの端にあるルーターのリモート・アルゴリズムと一致する必要があります。リモート・アルゴリズムの値の指定は任意であり、デフォルトとして、対応するローカル・アルゴリズムの値を取ります。ESP 認証は任意選択なので、ローカル認証アルゴリズムの選択は任意です。

暗号化キーの構成

構成するアルゴリズムごとに、リモート・ホスト内の対応するアルゴリズムのキーと同じキーを構成することも必要です。425ページの『手動 IP セキュリティー構成コマンド』の **add tunnel**コマンドについては、キーの説明を参照してください。

IP セキュリティー構成環境へのアクセス

IP セキュリティー構成環境にアクセスするには、OPCON (*) プロンプトで **t 6** と入力してから、Config> プロンプトで次の一連のコマンドを入力します。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-IPsec config>
```

手動 IP セキュリティー構成コマンド

IPv6 に使用可能な IP セキュリティー構成コマンドの説明は、425ページの『手動 IP セキュリティー構成コマンド』 を参照してください。IPv6 のコマンドは、特別に指示のない限り、IPv4 に使用されるものと同じです。コマンドは、IPV6-IPsec config> プロンプトで入力します。

手動トンネルの構成 (IPv6)

このトピックは、411ページの図38 のネットワーク例を見ながらお読みください。IPSec トンネル 1 のエンドポイントは、ルーター A のインターフェース 1 上にあります。ルーター A は、IPSec 用に構成します。次のステップに従って、ルーター A を構成します。

1. IPSec トンネルを作成する。
2. IPSec トンネルのエンドポイントであるルーター・インターフェース上に、1 つのアウトバウンド・パケット・フィルターを作成する。
3. パケット・フィルターのアクセス制御規則を作成する。
4. IPSec をリセットする。
5. IPv6 をリセットする。

ルーター A の IP セキュリティー・トンネルの作成

次の例は、ルーター A の IPsec トンネル 1 の作成方法を示しています。

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-IPsec config> add tunnel
IPsec Tunnel ID (1 - 65535) [1]
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]?  AH
Local IP Address [1000:1::1]? 2000::A
Local Authentication SPI (256-65535)[256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA)[HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

この例から分かるように、ユーザーが提供する必要があるパラメーターはプロンプトで指示されます。ESP、AH-ESP、または ESP-AH 保護トンネルの構成でも、同様のパラメーターが要求されます。

注: キーの値は、入力したときには表示されないので、この例には示されていません。 HMAC-MD5 認証のキーが表示されるとすれば、32 桁の 16 進文字で示されます。たとえば、キーは X'1234567890ABCDEF1234567890ABCDEF' のような値を持っています。

ルーター A のパケット・フィルターの構成

ルーター A の IPSec トンネルを作成した後で、IP パケット・フィルターを 1 つ設定する必要があります。次の例は、パケット・フィルター *out-router-A* の作成方法を示しています。IPv6 パケット・フィルターの構成およびアクセス制御規則について詳しくは、*プロトコルの構成と監視 解説書 第 1 巻* の IPv6 の使用の章の IPv6 フィルター機能および アクセス制御の個所を参照してください。

```
* talk 6
Config> Protocol IPv6
Internet protocol user configuration
IPv6 Config> set access-control on
IPv6 Config> add packet-filter
Packet-filter name [ ]? out-router-A
Filter incoming or outgoing traffic? [IN]? OUT
Which interface is this filter for [0]? 1
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config>
```

ルーター A のパケット・フィルター・アクセス制御規則の構成

次のステップは、パケット・フィルター・アクセス制御規則を構成することです。アウトバウンド・パケット・フィルター *out-router-A* に関するアクセス制御規則を 2 つ作成します。

アウトバウンド・パケット・フィルターのアクセス制御規則は、次の機能を実行します。

- 1 つのアクセス制御規則は、IPSec トンネルに渡すパケットの発信元および宛先アドレスの範囲を定義します。
- もう 1 つのアクセス制御規則は、パケット・フィルターを通して IPSec トラフィックをパスすることを可能にします。

パケット・フィルター *out-router-A* の最初のアクセス制御規則を構成します。このアクセス制御規則では、ネットワーク 1000:1:: から、ルーター B に接続されている宛先ネットワーク 3000:1:: までパケットをパスします。

```
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config> add access
Enter type [E]? IS
Internet source [0::0]? 1000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 3000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
Packet-filter 'out-router-A' Config>
```

out-router-A の 2 番目のアクセス制御規則は、IPSec トンネルの 2 つのエンド間で保護パケットをパスいることを可能にします。

```
Packet-filter 'out-router-A' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::A
Prefix Length [64]? 64
Internet destination [0::0]? 2000::B
Prefix Length [64]? 64
Packet-filter 'out-router-A' Config>
```

他のパケット・フィルターと同様に、*out-router-A* に対してワイルドカード・アクセス制御規則を構成して、どのアクセス制御規則にも一致しないトラフィックをパスさせるようにすることも可能です。

ルーター A での IP セキュリティーと IP のリセット

ポリシーの構成が済んだら、Talk 5 **reset ipsec** コマンドを使用して、新しい IPSec 構成で SRAM を再ロードします。**reset ipsec** コマンドは、IP 構成には影響しません。そこで、Talk 5 **reset ipv6** コマンドを使用して、ルーター内で IPv6 を動的にリセットしてください。代わりに、各コンポーネントをリセットするために、ルーターをリスタートすることもできます。IPSec および IPv6 をリセットするか、あるいはルーターを再始動して、フィルター規則が再ロードされていることを確認する必要があります。そうしないと、構成がインターフェース上で正しくサポートされない可能性があります。詳しくは、*プロトコルの構成と監視 解説書 第 2 巻* の 419ページの『第22章 IP セキュリティーの構成と監視』および **reset ipv6** コマンドの個所を参照してください。

411ページの図38 に示されているとおり、IPSec トンネル 2 のエンドポイントは、ルーター B のインターフェース 1 上にあります。次のステップに従って、ルーター B を手動で構成します。

1. IPSec トンネルを作成する。
2. IPSec トンネルのエンドポイントであるルーター・インターフェース上に、1 つのアウトバウンド・フィルターを作成する。
3. パケット・フィルターのアクセス制御規則を作成する。
4. IPSec をリセットする。
5. IPv6 をリセットする。

ルーター B の IP セキュリティー・トンネルの作成

ルーター B 内に、ルーター A に構成したのと同じ IPSec トンネル (IPsec トンネル 2) を構成する必要があります。ルーター B 内のこのトンネルのローカル IP アドレスは 2000::B で、リモート IP アドレスは 2000::A です。その他すべての IPSec トンネル・パラメーターは、ルーター A について指定されたものと一致していなければなりません。

ルーター B のパケット・フィルターの構成

ルーター A で行ったのと同様に、インターフェース 1 に、アウトバウンド・パケット・フィルター (*out-router-B*) を構成します。このインターフェースは、IPSec トンネル 1 のエンドポイントである ルーター B 内のインターフェースです。

ルーター B のパケット・フィルター・アクセス制御規則の構成

out-router-B に対するアクセス制御規則を、IPSec トンネル 2 を通じて処理して送信するためにネットワーク 3000:1:: から IPSec までアウトバウンド・パケットをパスさせるよう構成します。このアクセス制御規則はタイプ I および S です。

```
Packet-filter name [ ]? out-router-B
Packet-filter 'out-router-B' Config> add access
Enter type [E]? IS
Internet source [0::0]? 3000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 1000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
Packet-filter 'out-router-B' Config>
```

ここで、*out-router-B* に対して包括的アクセス制御規則を作成して、IPSec によって処理されたパケットを IPSec トンネル 2 を通してパスするようにします。

```
Packet-filter 'out-router-B' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::B
Prefix Length [64]? 64
Internet destination [0::0]? 2000::A
Prefix Length [64]? 64
Packet-filter 'out-router-B' Config>
```

out-router-B に対して、2 つのアクセス制御規則のどれにも一致しないパケット (たとえば、IPSec トンネル 2 あてでないトラフィック) を廃棄せずにパスさせたい場合は、包括的ワイルドカード・アクセス制御規則を作成します。

ルーター B での IP セキュリティーと IPv6 のリセット

IPSec 機能が働き、フィルターが活動化される前に、IPSec と IPv6 をリセットする必要があります。IPSec と IPv6 をリセットするには、Talk 5 **reset IPSec** コマンドを使用します。IPSec のリセットについては、439ページの『ルーター A での IP セキュリティーと IP のリセット』を参照してください。 IPSec をリセットした後で、Talk 5 **reset IPv6** コマンドを使用して IPv6 をリセットします。代わりに、各コンポーネントをリセットするために、ルーターをリスタートすることもできます。

例 : ESP を使用した IP セキュリティー・トンネルの構成

この例には、IPSec トンネルの構成だけを示しています (パケット・フィルターの構成は示しません)。

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? (Yes or [No]):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? (Yes or [No]):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No][No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

例 : ESP および ESP-NULL を使用した IP セキュリティー・トンネルの構成

認証が必要であることに注意してください。

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
```

```
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

手動 IP セキュリティー (IPv4) の監視

ここでは、IPv4 を使用した手動 IPSec の監視方法について説明します。インターネット・キー交換環境へのアクセス方法と使用可能なコマンドについて説明しています。

インターネット・キー交換環境へのアクセス

ここでは、IPv4 でのインターネット・キー・プロトコル (IKE) の使用方法について説明します。

IP セキュリティー IKE 監視環境にアクセスするには、**+** プロンプトで次の一連のコマンドを入力します。

```
+ feature ipsec
IPSP>ike
IKE>
```

インターネット・キー交換監視コマンド

ここでは、IKE 監視コマンドについて説明します。

表 50. IKE 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Delete	特定のトンネルの ISAKMP フェーズ 1 SA か、またはすべてのフェーズ 1 SA を動的に削除します。
List	特定のトンネルの フェーズ 1 SA か、またはすべてのフェーズ 1 SA に関する情報を表示します。
Stats	トンネルの統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Delete

IKE **delete** コマンドは、1 つのトンネルのフェーズ 1 SA またはすべてのフェーズ 1 SA を動的に削除するのに使用します。

構文:

delete tunnel
all

tunnel 特定のトンネルについてフェーズ 1 SA を削除することを指定します。

all すべてのフェーズ 1 SA を削除することを指定します。

例 : トンネルの削除

```
PKI config>delete tunnel
Peer address [10.0.0.3]?
```

List

IKE **list** コマンドは、特定のトンネルのフェーズ 1 SA またはすべての SA に関する情報を表示するのに使用します。

構文:

list tunnel
all

tunnel 特定のトンネルの SA について情報を表示することを指定します。

all すべての SA について情報を表示することを指定します。

例 : すべての SA についての情報のリスト

```
IKE>list all

Phase 1 ISAKMP Tunnels for IPv4:
------------------------------------------------------------
 Peer Address    I/R  Mode  Auto    State         Auth
---------------  ---  ----  ----  ----------  ------------
       10.0.0.3   R   Aggr   N    QM_IDLE       pre-shared


IKE>list tunnel 10.0.0.3

                    Peer IKE address: 10.0.0.3
                   Local IKE address: 10.0.0.1
                                Role: Responder
                            Exchange: Aggr
                           Autostart: No
                        Oakley State: QM_IDLE
               Authentication Method: Pre-shared Key
                Encryption algorithm: des3
                       Hash function: md5
                Diffie-Hellman group: 1
                   Refresh threshold: 85
                     Lifetime (secs): 15000
```

Stats

IKE **stats** コマンドは、トンネル統計を表示するのに使用します。

構文:

stats tunnel

tunnel トンネルの SA に関する統計情報を表示します。

有効値: 任意の構成されたトンネル名またはトンネル ID

例 : トンネルの SA 統計の表示

```
IKE>stats

Peer address [10.0.0.3]?

    Peer IP address......:        10.0.0.3
    Active time (secs)...:             187

                                       In              Out
                                       ---             ---
    Octets..............:             1229            1248
    Packets.............:               14              16
    Drop pkts...........:                0               1
    Notifys.............:                6               0
    Deletes.............:                0               0
```

```
Phase 2 Proposals....:              16              18
Invalid Proposals....:               0
Rejected Proposals...:               0               0
```

公開キー・インフラストラクチャー環境へのアクセス (IPv4)

ここでは、IPv4 での公開キー・インフラストラクチャー (PKI) の使用方法について説明します。

IP セキュリティー PKI 監視環境にアクセスするには、**+** プロンプトで次の一連のコマンドを入力します。

```
+ feature ipsec
IPSP>pki
PKI>
```

公開キー・インフラストラクチャー監視コマンド

ここでは、公開キー・インフラストラクチャー (PKI) 監視コマンドについて説明します。

表 51. PKI 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Cert-load	ルーターの SRAM に証明書をロードします。
Cert-req	認証要求を CA に実行依頼します。
Cert-save	考えられる将来の使用に備えて、証明書をキャッシュに保管します。
List certificate	証明書に関する情報を表示します。
List configured-servers	構成済みのサーバーに関する情報を表示します。
Load certificate	証明書が入っているレコードを SRAM から 実行時キャッシュにロードします。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Cert-load

PKI **cert-load** コマンドは、証明書とプライベート・キーが入っているレコードを SRAM から 実行時証明書キャッシュにロードします。

構文:

cert-load

例 : SRAM からキャッシュへの証明書レコードのロード

```
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
Name []? test
mystr=1.1.1.1
Box certificate and private key saved into cache successfully
```

Cert-req

PKI **cert-req** コマンドは、CA に証明書を要求するのに使用します。

構文:

cert-req

例 : CA への証明書の要求

```
Enter the following part for the subject name
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? ibm
   Organization Unit Name(Max 32 characters) []? nhd
   Common Name(Max 32 characters) []?
Key modulus size (512|768|1024)
 [512]?
Certificate subject-alt-name type:
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 1.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? test
Bad address, try again
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Certificate request TFTP to remote host successfully.
```

Cert-save

PKI **cert-save** コマンドは、証明書およびプライベート・キーが入っているレコードを SRAM に保管するのに使用します。

構文:

cert-save

例 : SRAM への証明書レコードの保管

```
Enter type of certificate to be stored into SRAM:
     1)Root certificate;
     2)Box  certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? test
Load as default router certificate at initialization? [No]:
Private key TEST written into SRAM
Both Certificate and private key saved into SRAM successfully
```

List Certificate

PKI **list certificate** コマンドは、X.509 ディジタル証明書に関する情報を表示するのに使用します。

構文:

list certificate

例 : 証明書情報のリスト

```
Router   certificate
      Serial Number:   914034877
      Subject  Name:   /c=US/o=ibm/ou=nhd/cn=testip
      Issuer   Name:   /c=US/o=ibm/ou=nhd
   Subject alt Name:   1.1.1.1
         Key Usuage:   Sign & Encipherment
           Validity:   1999/1/19 23:24:27 -- 2002/1/19 23:54:27
```

List Configured-servers

PKI **list configured-servers** コマンドは、構成済みサーバーに関する情報を表示するのに使用します。

構文:

list configured-servers

例 : 構成済みサーバーに関する情報のリスト

```
1)  Name: SERVER1
    Type: LDAP
    IP addr: 0.0.0.0
        LDAP search timeout (secs): 0
        LDAP retry interval (mins): 0
        LDAP server port number: 0
        LDAP version: 0
        LDAP version: 0
        Anonymous bind ?: y


2)  Name: TEST
    Type: TFTP
    IP addr: 9.9.9.9


3)  Name: TFTP
    Type: TFTP
    IP addr: 2.2.2.2
```

Load Certificate

PKI **load certificate** コマンドは、証明書を SRAM から実行時キャッシュにロードするのに使用します。

構文:

load certificate

例 : キャッシュへの保証書のロード

```
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]?
Server info name []? test
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /tmp/test.cert

Attempting to load certificate file. Please wait ...
Router Certificate  loaded into run-time cache
```

IP セキュリティー監視環境へのアクセス (IPv4)

IPv4 IP セキュリティー監視環境にアクセスするには、OPCON プロンプト (*) で **t 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで、次の一連のコマンドを入力します。

```
+ feature ipsec
IPSP>ipv4
IPV4-IPsec>
```

IP セキュリティー監視コマンド (IPv4)

ここでは、IP セキュリティー監視コマンドについて説明します。

表 52. IP セキュリティー監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Change tunnel	保護トンネル構成パラメーター値を動的に変更します。
Delete tunnel	保護トンネルを動的に削除します。
Disable	安全な方法でのすべての IP セキュリティー処理 (パケット・フィルターに一致するパケットをドロップする) を動的に使用不可にする、無保護な方法でのすべての IP セキュリティー処理 (パケット・フィルターに一致するパケットをパスさせる) を動的に使用不可にする、または特定の保護トンネルを動的に使用不可にします。
Enable	すべての IP セキュリティー処理を動的に使用可能にする、または保護トンネルを動的に使用可能にします。
Itp	IP Security tunnel ping。IPSec トンネルの他端のパーティーを接続するかどうかを決めます。
List	IP セキュリティーに関するグローバル情報を、通信中の定義済みトンネルに関して表示します。
Reset	IP セキュリティーをリセットするか、または保護トンネルをリセットします。このコマンドは、Talk 6 で作成された構成を再ロードします。リセットすると、Talk 5を使用して構成されたパラメーター値は、Talk 6 を使用して構成されたパラメーター値でオーバーライドされます。
Set	パス MTU (PMTU) 経時タイマーを動的に設定します。
Stats	すべてのトンネルまたは活動トンネルの統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Change Tunnel

保護トンネルを動的に変更します。

構文:

change tunnel ...

パラメーターの説明は、425ページの『手動 IP セキュリティー構成コマンド』 の **add tunnel** コマンドの項を参照してください。

Delete Tunnel

delete は、1 つの保護トンネルまたはすべての保護トンネルを動的に削除するのに使用します。

構文:

delete tunnel

tunnel-id
tunnel-name

all

tunnel-id

削除する IPSec トンネルの識別子を指定します。

有効値: 1 ～ 65535

デフォルト値: 1

tunnel-name
削除する IPSec トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all このインターフェース上のすべての IPSec トンネルを削除することを指定します。

Disable

disable コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを動的に使用不可にするのに使用します。

構文:

disable ipsec drop
ipsec pass
tunnel ...

ipsec drop
ルーター上の IP セキュリティーを安全な方法で使用不可にします。すべての IPSec トンネルが使用不可にされますが、パケット・フィルター規則の保護トンネル情報を使用して、IPSec トンネル・パケット・フィルターに一致するパケットを識別します。一致するパケットはドロップされます。

ipsec pass
ルーター上の IP セキュリティーを無保護な方法で使用不可にします。すべての IPSec トンネルが使用不可にされます。IPSec トンネル・パケット・フィルターに一致するパケットは、通常のトラフィックとして転送されます。

tunnel *tunnel-id* **all**
指定されたトンネルまたはすべてのトンネル上の IP セキュリティーを使用不可にします。

tunnel-id
使用不可にする保護トンネルの識別子を指定します。

有効値: 1 ～ 65535

デフォルト値: 1

all すべてのトンネル

Enable

enable コマンドは、すべてのインターフェースまたは 1 つのトンネルの IP セキュリティー・プロトコルを動的に使用可能にするのに使用します。ルーター上の IPSec をグローバルに使用可能にしないと、個別に使用可能にされた IPSec トンネルは活動状態になりません。

注: IPSec を使用不可に設定してルーターをリスタートした場合は、IPSec を動的に使用可能にすることはできません。

構文:

enable ipsec
tunnel ...

ipsec ルーター全体の IP セキュリティーを使用可能にします。

tunnel *tunnel-id* **| all**

tunnel-id
使用可能にする保護トンネルの識別子を指定します。

有効値: 1 ～ 65535

デフォルト値: 1

all すべてのトンネル

Itp

itp コマンド (IPSec tunnel ping) は、IPSec トンネルを経由して特別の IP パケットを作成して送信するのに使用します。これは、トンネルの他端のルーターがパケットを戻すことによって応答できることを検証します。パケットは、**Enter** を押してコマンドを終了するまで、レート引き数によって指定された頻度で繰り返し送信されます。 **Enter** を押すと、itp は、送信したすべてのパケットの状況を印刷します。

注: itp コマンドは、トンネル・モードで稼働しているトンネルにだけ機能します。また、他のルーターには IP 転送機能があって使用可能になっている必要があります。

構文:

itp tunnel-id
size
rate

tunnel-id
必須です。特定のトンネルに割り当てられた 2 バイトの整数値

size 任意指定。ping パケットのデータ・ペイロードのサイズ。この値は、itp が作成した最小サイズより大きく、トンネルの MTU 値より小さくする必要があります。

rate 任意指定。ping データ・パケットを転送する頻度 (秒単位)

デフォルト値: 1

List

list コマンドは、現行の IP セキュリティー構成を表示するのに使用します。グローバル・トンネル (global tunnels) には、ルーター上のすべてのトンネル (活動および定義済みの両方) が含まれます。すべてのトンネル (all tunnels) には、このインターフェースに構成されたすべてのトンネル (活動および定義済みの両方) が含まれます。活動トンネル (active tunnels) は、現在活動状態のトンネルです。定義済みトンネル (defined tunnels) は、定義されているが活動状態ではないトンネルです。

構文:

list ... all

global
tunnel

active *tunnel-id tunnel-name* all
defined *tunnel-id tunnel-name* all

例: すべての定義済みトンネルのリスト

```
IPV4-IPsec>LIST TUNNEL DEFINED
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

Defined Tunnels for IPv4:
------------------------------------------------------------------------------
   ID     Type    Local IP Addr   Remote IP Addr   Mode    State
 ------  ------  --------------  --------------  -----  --------
      3  ISAKMP       211.0.1.17        211.0.5.2  TUNN   Enabled
      4  ISAKMP       211.0.1.17        211.0.5.3  TUNN   Enabled
      5  ISAKMP       211.0.1.17        211.0.5.4  TUNN   Enabled


Defined Manual Tunnels for IPv6:
------------------------------------------------------------------------------
IPV4-IPsec>
```

例: 1 つの定義済みトンネルのリスト

```
IPV4-IPsec>LIST TUNNEL DEFINED
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? 1

Tunnel    Type     Mode   Policy    Life    Replay     State
  ID                                                              Prev
------    ------  -----   ------   -----   -------     ---------     -----------
     1    ISAKMP   TUNN      ESP       0        No     Enabled


Tunnel Name: ---------------

Local (Outbound) Information:
      IP Address: 211.0.1.17
  Authentication:  SPI: ----------          Algorithm: --------
      Encryption:  SPI: 2305164930    Encryption Algorithm: DES-CBC
                                                Extra Pad:   0
                                ESP Authentication Algorithm: HMAC-MD5

Remote (Inbound) Information:
      IP Address: 211.0.5.3
  Authentication:  SPI: ----------          Algorithm: --------
      Encryption:  SPI: 2661613010    Encryption Algorithm: DES-CBC
                                             Verify Pad?:  No
                                ESP Authentication Algorithm: HMAC-MD5
IPV4-IPsec>
```

例: すべての活動トンネルのリスト

```
IPV4-IPsec>LIST TUNNEL ACTIVE
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]?

Tunnel Cache for IPv4:
------------------------------------------------------------------------------
 ID     Local IP Addr   Remote IP Addr   Mode   Policy  Tunnel Expiration
----   -------------   --------------   ----   --------    ------------------
  1       211.0.1.17      211.0.5.214   TUNN        ESP                  none
  2       211.0.1.17      211.0.5.215   TUNN        ESP                  none
  3       211.0.1.17       211.0.5.41   TUNN        ESP                  none
```

```
Tunnel Cache for IPv6:
------------------------------------------------------------------------------
IPV4-IPsec>
```

例: 1 つの活動トンネルのリスト

```
IPV4-IPsec>LIST TUNNEL ACTIVE 1
                                Tunnel ID: 1
                            Tunnel Name: ---------------
                                    Type: ISAKMP
                                    Mode: TUNN
                                  Policy: ESP
                            Replay Prevention: No
                              Tunnel LifeTime: 0 secs
                            Tunnel Expiration: None
                                    PMTU: n/a
                                Tunnel State: Enabled
                              DF bit handling: COPY
                                   SA State: Working
                                SA LifeTime: 360 secs
                                SA LifeSize: 50000 KBytes
                               SA Threshold: 85 percent
Local (Outbound) Information:
        IP Address: 211.0.1.17
    Authentication:  SPI: ----------              Algorithm: --------
        Encryption:  SPI: 2861614221   Encryption Algorithm: DES-CBC
                                                  Extra Pad:   0
                               ESP Authentication Algorithm: HMAC-MD5

Remote (Inbound) Information:
        IP Address: 211.0.5.41
    Authentication:  SPI: ----------              Algorithm: --------
        Encryption:  SPI: 2266666369   Encryption Algorithm: DES-CBC
                                                 Verify Pad?:  No
                               ESP Authentication Algorithm: HMAC-MD5
   IPV4-IPsec>
```

2 これは IPv6 アドレスです。IP バージョンが IPv4 の場合、DF ビットの扱い方 (COPY、SET、または CLEAR) を定義するメッセージが表示されます。

Reset

reset コマンドは、ルーター上または 1 つのトンネル上の IP セキュリティーを動的にリセットするのに使用します。IPSec またはトンネルをリセットした後で、必ず **reset IP** コマンドを使用して、IP 構成をリセットしてください。これは、パケット・フィルターやそのアクセス制御規則などのアクセス制御情報を再ロードするために必要です。IP をリセットしないと、パケット・フィルターおよびアクセス制御規則が、新規の IPSec 構成をサポートしない可能性があります。

reset コマンドを使用する代わりに、ルーターをリブートすることもできます。ただし、ルーターをリブートするとネットワークがしばらく切断されますが、**reset** コマンドは IP 機能だけを中断します。

構文:

reset ipsec
tunnel *tunnel-id tunnel-name* all

ipsec 2216 上の IP セキュリティーをリセットします。IP セキュリティーは一時的に使用不可になった後、リスタートします。IP セキュリティーが使用不可の間、通常は IPSec トンネルによって処理されるパケットは、リセット

が完了するまで廃棄されます。IP セキュリティーをリセットしても、2216 上の他の機能には影響を与えません。このコマンドは、Talk 6 を使用して作成された IP セキュリティー構成をアクティブにします。Talk 6 IP セキュリティー構成は Talk 5 構成を上書きします。

tunnel 指定されたトンネルの IP セキュリティーをリセットします。リセット時にトンネルが使用不可にされている場合、トンネル構成は SRAM 構成から再作成されますが、リセット後もトンネルは使用不可のままです。

tunnel-id
リセットする保護トンネルの識別子を指定します。

有効値: 1 〜 65535

デフォルト値: 1

tunnel-name
リセットする保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

デフォルト値: なし

all すべてのトンネル

Set

パス MTU (PMTU) 経時タイマーを動的に設定します。

構文:

set path

パス (path)
このパラメーターは、2216 がトンネル MTU を最大値に戻す前に経過する時間 (分)を定義します。

デフォルト値: 10 (0 は使用不可 (disabled) を意味します)

Stats

stats コマンドは、特定のトンネルまたはすべてのトンネルに関する統計を表示するのに使用します。たとえば、**stats** コマンドは、送受信されたパケットを表示します。

構文:

stats *tunnel-id*
tunnel-name
all

tunnel-id
保護トンネルの識別子を指定します。

有効値: 1 〜 65535

デフォルト値: 1

tunnel-name
構成された保護トンネルの名前を指定します。

有効値: 任意の構成されたトンネル名

IP セキュリティー監視コマンド (Talk 5)

デフォルト値: なし

all 2216 上に構成されたすべてのトンネルの統計を表示します。

例:

```
IPV6-IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all

                          Global IPSec Statistics
Received:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           0            0             0             0            0            0

Sent:
  total pkts   AH packets   ESP packets   total bytes    AH bytes     ESP bytes
  ----------   ----------   -----------   -----------   ----------   ----------
           0            0             0             0            0            0

Receive Packet Errors:
  total errs    AH errors   AH bad seq   ESP errors   ESP bad seq
  ----------   ----------   ----------   ----------   -----------
           0            0            0            0             0

Send Packet Errors:
  total errs    AH errors   ESP errors
  ----------   ----------   ----------
           0            0            0
```

手動 IP セキュリティーの監視 (IPv6)

ここでは、IPv6 を使用した手動 IPSec の監視方法について説明します。IP セキュリティー環境へのアクセス方法と使用可能なコマンドについて説明しています。

IP セキュリティー監視環境へのアクセス

IP セキュリティー監視環境にアクセスするには、OPCON prompt (*) プロンプトで **t 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで、次の一連のコマンドを入力します。

```
+ feature ipsec
IPSP>ipv6
IPV6-IPsec>
```

IP セキュリティー監視コマンド (IPv6)

IPv6 の IP セキュリティー監視コマンドは、特別に指示のない限り、IPv4 に使用されるものと同じです。コマンドの説明については、446ページの『IP セキュリティー監視コマンド (IPv4)』を参照してください。コマンドは、IPV6-IPsec> プロンプトで入力します。

IP セキュリティー動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

IP セキュリティー (IPSec) は、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、IPSec には適用できません。IPSec は、特定のインターフェースから独立しています。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、IPSec には適用できません。 IPSec は、特定のインターフェースから独立しています。

GWCON (Talk 5) 構成要素リセット・コマンド

IPSec は、次の IPSec 固有 GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature IPSec, Ipv4, Reset IPSec コマンド

説明: IPSec は再初期設定されます。

ネットワークへの影響:

IPSec をリセットすると、すべてのトンネルはなくなります。手動トンネルが SRAM から再構築されます。ネゴシエーションされたトンネルは消えてしまいます。これによって、これらのトンネルを使用するトラフィックは瞬間的に停止します。

制限事項:

なし。

次の表では、**GWCON, feature IPSec, ipv4, reset IPSec** コマンドが起動されると活動化される IP セキュリティー・フィーチャーの構成変更を要約します。

GWCON, feature ipsec, ipv4, reset ipsec コマンドによって変更が活動化されるコマンド
CONFIG, feature ipsec, ipv4, enable tunnel
CONFIG, feature ipsec, ipv4, disable tunnel
CONFIG, feature ipsec, ipv4, disable ipsec
CONFIG, feature ipsec, ipv4, add tunnel
CONFIG, feature ipsec, ipv4, delete tunnel
CONFIG, feature ipsec, ipv4, change tunnel

GWCON, Feature IPSec, Ipv4, Reset Tunnel コマンド

説明: トンネルまたはすべてのトンネルは再初期設定されます。

ネットワークへの影響:

トンネルまたはすべてのトンネルはリセットできます。手動トンネルが SRAM から再構築されます。ネゴシエーションされたトンネルは消えてしまいます。これによって、これらのトンネルを使用するトラフィックは瞬間的に停止します。

制限事項:

なし。

次の表では、**GWCON, feature IPSec, ipv4, reset tunnel** コマンドが起動されると活動化される IP セキュリティー・フィーチャーの構成変更を要約します。

GWCON, feature ipsec, ipv4, reset tunnel コマンドによって変更が活動化されるコマンド
CONFIG, feature ipsec, ipv4, add tunnel
CONFIG, feature ipsec, ipv4, delete tunnel
CONFIG, feature ipsec, ipv4, change tunnel
CONFIG, feature ipsec, ipv4, disable tunnel

GWCON (Talk 5) 一時変更コマンド

IPSec は、装置の操作状態を一時変更する、次の GWCON コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行すると、行われません。

コマンド
GWCON, feature ipsec, ipv4, change tunnel **注:** トンネルのパラメーターはメモリー内で変更できます。
GWCON, feature ipsec, ipv4, disable tunnel **注:** トンネルまたはすべてのトンネルは使用不可にできます。これらのトンネルのトラフィックは停止します。
GWCON, feature ipsec, ipv4, disable IPSec pass **注:** IPSec は使用不可になり、トラフィックはセキュリティーなしで転送されます。
GWCON, feature ipsec, ipv4, disable IPSec stop **注:** IPSec は使用不可になり、トラフィックは廃棄されます。
GWCON, feature ipsec, ipv4, delete tunnel **注:** 1 つまたはすべてのトンネルを削除します。これらのトンネルのトラフィックはドロップします。
GWCON, feature ipsec, ipv4, enable tunnel **注:** 1 つまたはすべてのトンネルを使用可能にします。これらのトンネルのトラフィックは許可されます。
GWCON, feature ipsec, ipv4, enable IPSec **注:** IPSec を使用可能にします。IPSec はトラフィックを処理できます。
GWCON, feature ipsec, ipv4, set path-MTU-age-timer **注:** パス MTU エージング・タイマーを変更します。

非動的再構成可能コマンド

次の表には、動的に変更できない IP セキュリティー・フィーチャーの構成コマンドを記載します。これらのコマンドを活動化するには、装置を再ロードしたり、リスタートする必要があります。

コマンド
CONFIG, enable ipsec **注:** 装置を初期設定したあとで、IPSec を最初に使用可能にしたときに、装置は再ロードまたはリスタートする必要があります。

第23章 ディファレンシェーテッド・サービス・フィーチャーの使用

この章では、ルーターが該当する IP データ・パケットに優先サービスを提供できるようにディファレンシェーテッド (差別化された) サービス (DiffServ) フィーチャーを使用する方法について説明します。IP ヘッダー内の情報に基づいて、ルーターは、パケットを (ポリシー・フィーチャーで作成された) ポリシー・データベース内の事前定義済み構成と突き合わせることによってパケットを分類します。詳しくは、325ページの『第19章 ポリシー・フィーチャーの使用』を参照してください。結果として、一部のパケットが優先サービスを受け取ることがあります。この章には、次の内容が記載されています。

ディファレンシェーテッド・サービスの概説

IP ネットワーク内に導入されているほとんどの転送装置は、現在、標準的な best-effort サービスを先入れ先処理ベースでデータ・パケットに引き渡します。この送達方式は、ほとんどのトラフィックには適していますが、特定のパケットのより高速かつ早い転送を必要とする新しいアプリケーションが出現してきています。

ディファレンシェーテッド・サービス (DiffServ) フィーチャーは、ルーターが伝送できるように IP パケットを処理する際に各種レベルのサービスをそれらのパケットに提供します。DiffServ は、システム・リソース (バッファー) およびリンク・リソース (帯域幅) を一部のパケットのために予約することによって優先サービスをそれらに提供します。DiffServ 分類機能は、IP ヘッダー内の各種フィールドを検査することにより、IP パケットに与えられるサービスのタイプを決定します。たとえば、IP 発信元および宛先アドレスとポート番号の範囲、プロトコル・タイプ、着信 DS (TOS) バイトなどです。これをスケーラブルが容易な方法で行うために、個々のフローはストリームで終結されます。ストリームは、DiffServ がバッファーや帯域幅へのアクセスを管理するときのエンティティーです。図39 は、DiffServ がストリームのパケットを処理する方法を示しています。

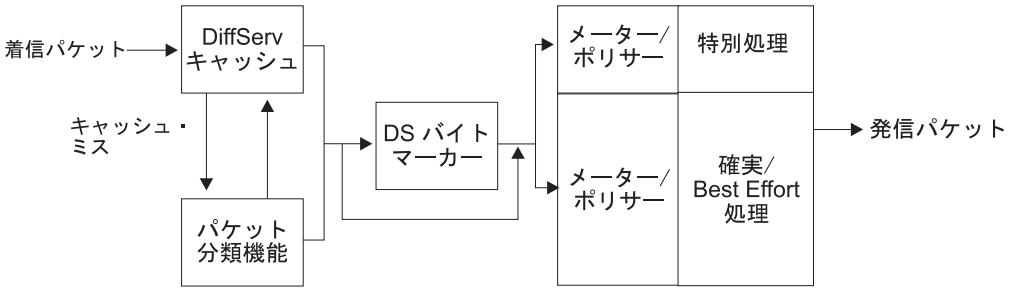


図 39. DiffServ データ・パケット・パス

従来の best-effort サービスのほかに、DiffServ は、次のタイプのサービスを提供します。

優先転送 (EF)

優先転送サービスは特別サービスの DiffServ 設定を表すもので、次の記述では、両方の用語が混用されています。このサービスにより、特定の伝送速度と、確実転送または ベストエフォート・ サービスのどちらかよりも小さい遅延が保証されます。余分なトラフィックが発生すると、DiffServ はその余分なトラフィックをドロップします。特別待ち行列は、EF サービスを提供するもので、457ページの図40 では EF 待ち行列として示されています。

確実転送 (AF)

確実転送サービスは確実サービスの DiffServ 設定を表すもので、次の記述では、両方の用語 (確実転送サービスおよび確実サービス) が混用されています。AF サービスは、特定の伝送速度は保証されますが、遅延保証はありません。使用されていないリソースがあると、DiffServ は、さらに高速で余分なトラフィックを送信できます。

AF トラフィックは、オプションとして測定され、ポリシー内の構成を使用して規制されます。サポートされているポリシングのタイプは、単一レートと 2 レートの 3 色マーカー (TCM) です。 TCM によって、着信トラフィックの特性に基づいてパケットを分類したり、マークを付け直すことができます。提供されている 3 つの分類は、緑、黄、および赤です。ポリシーでは、色分類のしきい値の指定ができます。AF/BE 待ち行列は AF サービスを提供するもので、457ページの図40 に示されています。

ベストエフォート (BE)

これは、標準的な ベストエフォート・ サービスで、サービス保証や遅延保証は提供しません。ユーザーは、EF および AF サービスについて予約リソース間でバランスを取り、ベストエフォート・ トラフィックが適度のサービスを受けられるように十分なリソースを空けておく必要があります。
AF/BE 待ち行列は BE サービスを提供するもので、457ページの図40 に示されています。

ローカル・ルーターは、制御パケットを作成して送信するため、ユーザーは、それらが十分なサービスを受けられるように十分なリソースを空けておく必要もあります。

エッジ・ルーターでの DiffServ の測定、マーク付け、およびポリシングによって、DiffServ 使用可能ネットワークのコア・ルーターは、DS (TOS) コード・ポイントに基づいてパケットを分類したり、基準に適合しないトラフィックをドロップしたりサービス・レベルを下げることによって輻輳を制御できます。たとえば、コア・ルーターはすべての赤色のパケットを廃棄し、best effort として黄色のパケットを転送し、そしてドロップされる可能性が少ない緑色のパケットを転送します。このことは、スループットの向上を達成し、DiffServ 使用可能ネットワークでの優先トラフィックの遅延を短くするのに役立ちます。

DiffServ は、現在、PPP 、マルチリンク PPP、およびフレーム・リレーの各リンクに設定されており、RSVP サブシステムで使用することができます。 455ページの図39 は、ストリームのパケットが処理される方法を示しています。ルーターがフローの最初のパケット (特別サービス用に指定されているものと想定しています) を受信したときに、DiffServ キャッシュ内にそのサービス・カテゴリーを指示するものはないため、パケットは低速パスで処理されます。DiffServ は、パケット処理基準 (ポリシー) を入手するためにポリシー・データの検索を起動します。ポリシー定義

アクションは、DiffServ キャッシュに保管されています。ルーターは、このフローの後続のパケットを受信すると、そのフローの DiffServ キャッシュ内にエントリーがすでに存在していることを検出し、そのポリシー定義アクションが適用され、パケットは高速パスを取ります。したがって、このフローからの後続のパケットは、特別サービスを受け取ります。

図40 は、ポリサー、バッファー管理、待ち行列、およびスケジューラーといった、異なる品質のサービス・レベルを提供する一部のコンポーネント間の関係を示しています。

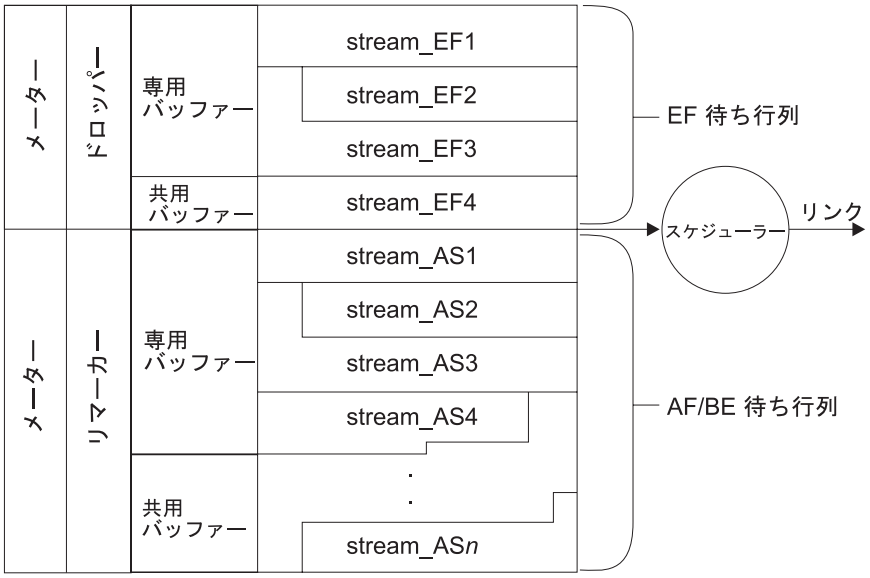


図 40. ポリサー、バッファー、待ち行列、およびスケジューラーの関係

優先転送 (EF) サービスと確実転送 (AF) サービスの特性は異なりますが、それらの特性はルーター内の 3 つの機能、すなわち、(1) メーターおよびポリサー、(2) バッファーおよび待ち行列管理、および (3) スケジューラーによってサポートされます。これらの機能により、従来の BE ルーター装置で使用可能であったものより高度なトラフィック制御が提供されます。

ポリシー・フィーチャーを使用して適切なポリシーを構成すると、DiffServ を設定する最初ステップとして、DiffServ **enable ds** コマンドを使用して、DiffServ フィーチャーを使用可能にして、**set interface** コマンドを使用して egress インターフェースを使用可能にします。

ネットワーク・リソースが能力以上に割り当てられていたり、オーバーブッキングされるような DiffServ オプション、すなわち、実際に利用しきれないほどの帯域幅やバッファー処理が行われている場合と同様にトラフィック調整制御が構成されるようにオプションを構成することがあり得ます。DiffServ では、オーバーブッキングをサポートしていません。

DiffServ ストリームがアイドル状態になる (しばらくの間、ストリームでパケットが送信されていない) と、システムは、他のストリームがリソースを使用できるようにリソースを再利用します。ストリームが再起動すると、リソースはそのストリ

ームに戻されます。リソースがオーバーブッキングのために利用できなくなると、DiffServ は、定期的にリソースの再割り当てを試みます。

DiffServ コード・ポイントについて

DiffServ には、RFC791 に定義されている、IPv4 TOS オクテットの置換ヘッダーがあります。このヘッダーには Diffserv (DS) フィールドと呼ばれる 1 バイトが入っています (図41に示します)。The six high order bits of the DS フィールドの上位の 6 ビットは、DiffServ コード・ポイント (DSCP) として使用して per-hop-behavior (PHB) を判別します。残りの 2 ビットは、将来使用するために予約済みです。次の例は、DS フィールドの形式を示します。

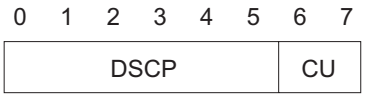


図 41. IPv4 TOS オクテット・ヘッダーの DiffServ コード・ポイント形式

ここで、　　DSCP = ディファレンシェーテッド・サービス・コード・ポイント
　　CU = 現在使用されていない

お勧めする、EF PHB のコード・ポイントは 101110xx です。

図42 は、shows the format of the DS field for the AF PHB:

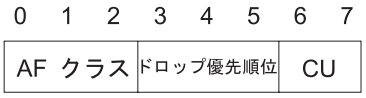


図 42. AF PHB ヘッダーの DiffServ コード・ポイントの形式

ここで、　　AF クラス・タイプの 3 ビット
　　001 - AF11 クラス
　　010 - AF21 クラス
　　011 - AF31 クラス
　　100 - AF41 クラス
　　ドロップ優先順位の 3 ビット
　　010 - 低ドロップ優先順位、TCM の緑色を意味します
　　100 - 中位ドロップ優先順位、TCM の黄色を意味します
　　110 - 高ドロップ優先順位、TCM の赤色を意味します
　　CU = 現在使用されていない

次のリストは、AF クラスとドロップ優先順位値に関してお勧めする AF コード・ポイント値を示します。

クラス 1	クラス 2	クラス 3	クラス 4
AF11 = 001010xx	AF21 = 010010xx	AF31 = 011010xx	AF41 = 100010xx
AF12 = 001100xx	AF22 = 010100xx	AF32 = 011100xx	AF42 = 100100xx
AF13 = 001110xx	AF23 = 010110xx	AF33 = 011110xx	AF43 = 100110xx

メーターとポリサーについて

測定とポリシングが、ポリシーに指定されているように、EF および AF トラフィックについて提供されています。EF アルゴリズムは、トラフィックを測定して、指定したしきい値を超えるトラフィックをドロップします。AF アルゴリズムは、トラフィックを測定して、パケットのマークを付け直すこともありますが、ドロップはしません。

優先転送 (EF)

EF トラフィックには、デフォルトとしてトークン・バケット・ベースのポリサーがありますが、これはポリシー帯域幅パラメーターの設定中に指定した速度を超過した場合にパケットをドロップします。Token Rate (TR) および Token Bucket Size (TBS) パラメーターを指定してポリサーのデフォルト操作を変更することもできます。メーターは、パケットを送信するのに十分な数のトークンがバケットに入っているかどうかを判別します。トークンが使用可能である場合には、パケットが送信されます。トークンが使用できない場合には、ポリサーはパケットをドロップします。バケットは、Token Rate パラメーターに指定した速度でトークンを減らします。このトークン速度は、秒当たりのバイト数単位で測定されます。これには、IP ヘッダーが含まれますが、リンク固有ヘッダーは含まれません。トークン速度は、IP ヘッダー圧縮およびレイヤー 2 のデータ暗号化と圧縮の前に測定されます。Token Bucket Size を使用して、ペナルティーなしで、速度制限を超える一時的なバーストを処理します。

確実転送 (AF)

AF トラフィックには、次の 3 つのポリシング・オプションがあります。(1) 単一レート 3 色マーカー (srTCM)、(2) 2 レート 3 色マーカー (trTCM)、および (3) なし (ポリシングなし)。これらのポリシング・オプションは、AF1、AF2、AF3 および AF4 の各クラスで使用可能で、ポリシーの設定時に指定されます。

srTCM は、2 つのバケットと 1 つの低減速度を使用したトークン・バケット・アルゴリズムに基づいてトラフィック・ストリームを測定します。そのパケットは、次の 3 つのトラフィック・パラメーターに従って、緑、黄、または赤のいずれかにマーク付けられます。(1) コミット情報速度 (CIR)、(2) コミット・バースト速度 (CBS)、および (3) 超過バースト・サイズ (EBS)。パケットは、CBS を超えない場合には緑色に、CBS を超えるが EBS ではない場合には黄色に、その他の場合には赤色にマーク付けられます。CIR は、秒当たりの IP パケットのバイト数単位で測定されます。これには、IP ヘッダーが含まれますが、リンク固有ヘッダーは含まれません。CIR は、IP ヘッダー圧縮およびレイヤー 2 のデータ暗号化と圧縮の前に測定されます。CBS と EBS はバイト単位で測定します。

メーターは、color-blind または color-aware のいずれかのモードで操作します。color-blind モードでは、着信パケットは、DS コード・ポイントにあるドロップ優先順位の設定値に関係なく、緑色にマークされているものと見なします。CBS は緑色のバケットのサイズを表し、EBS は黄色のバケットのサイズを表します。最初に、緑色のバケットで使用可能のトークンを検査します。十分な緑色のトークンがある場合には、パケットは緑のマークが付けられ、送信されます。十分な緑のトークンがない場合には、黄色のバケットを検査します。十分な黄色のトークンがある場合には、パケットは黄色のマーク付けをされて送信されます。十分な黄色のトークンがない場合には、パケットは赤色のマーク付けをされます。color-aware モードで

は、着信パケットの色を検査して、対応するトークン・バケットを最初に検査します。トークンが使用可能であれば、パケットは、受信次第送信されます。トークンが使用可能でなければ、ドロップ優先順位値は、それに従って、下げられます。Color-aware モードが有用なのは、ingress パケットがすでに分類されていて、前もって色付けがされている場合です。

trTCM も、srTCM には緑色と黄色のバケットについて別個の低減速度がある点を除いては、srTCM と同様の、トークン・バケット・アルゴリズムです。構成パラメーターは、次の 4 つです。(1) コミット情報速度 (CIR)、(2) コミット・バースト・サイズ (CBS)、(3) ピーク情報速度 (PIR)、および (4) ピーク・バースト速度 (PBS)。CBS は緑色のバケットのサイズを表し、PBS は黄色のバケットのサイズを表します。アルゴリズムは、CIR 値が緑色のバケット低減速度を決め、PIR 値が黄色のバケット低減速度を決める点を除いては、srTCM の場合と同じです。trTCM が有用なのは、コミット情報速度とは別個にピーク速度を強制する場合です。PIR を超えるパケットは、赤色 (ドロップの可能性が最も高い) にマーク付けられます。

バッファーおよび待ち行列管理について

トラフィックが EF 用であったり、あるいはポリサーが許可している AF または BE トラフィックである場合は、速度に基づくバッファー*管理* 機能がそれを処理します。この機能は、専用プールまたは DiffServ 使用可能出力インターフェースの共通の共用プールのいずれかからバッファーを割り振ります。EF トラフィックのバッファーが割り当てられるのは、専用プールからだけです。

Talk 6 **set receive-buffers** 構成コマンド (説明と構文については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* を参照) を使用して、1 つのインターフェースで使用できる物理バッファー・スペースの総量を指定します。DiffServ Talk 6 **set interface** コマンドを使用して、特別待ち行列および確実待ち行列の egress バッファー・サイズを設定してください。これは、DiffServ が管理するバッファー・スペースです。

DiffServ は、2 つの別個のプールを管理します。1 つは特別転送 (EF) 待ち行列のためのものであり、もう 1 つは確実転送 (AF) 待ち行列のためのものです。指定したバッファー・スペースがシステム内で使用可能な実際のバッファー・スペースの量に反映されていることを確認してください。

バッファー管理は、そのインターフェースの専用プールからのバッファーがパケットで使用できるかどうかを決めます。パケットで使用可能なバッファーがある場合は、そのパケットが受け入れられ、待ち行列化されます。そうでない場合には、バッファー管理は共用プールからバッファー・スペースを割り振ろうと試み、割り振りが可能であれば、そのパケットは待ち行列化されます。共用バッファー・スペースが使用可能でない場合、バッファー管理はそのパケットをドロップします。

スケジューラーについて

スケジューラー 機能は、定期的に待ち行列を調べ、待ち行列に入っているパケットを待ち行列から外し、それらを転送するためにインターフェース・アダプターに送信します。これは、自己計時機能付きで、公正な待ち行列化を行うスケジューラーであり、重み付きの公正な待ち行列化のバリエーションです。スケジューラーの重みを設定し、スケジューラーが待ち行列を調べる頻度を指定することができます。

ディファレンシェーテッド・サービスの用語

DiffServ を説明するために、次の用語が使用されています。

コミット情報速度 (CIR)
このパラメーターは、ユーザーの AF トラフィック・ストリームが送信超過と見なされることになる前に操作できる最大速度を指定します。CIR は、秒当たりの IP パケットのバイト数単位で測定されます。これには、IP ヘッダーが含まれますが、リンク固有ヘッダーは含まれません。これは、AF ストリーム用の単一レートおよび 2 レート両方の TCM 機能によって使用されます。

コミット・バースト・サイズ (CBS)
このパラメーターは、CIR を超える速度でバーストで送信できる最大のバイト数を指定 (IP パケットのバイト数で) します。 CBS は、単一レートの TCM および 2 レートの TCM の両方の機能でコミット・トークン・バケットのサイズを制限します。

DiffServ キャッシュ
このキャッシュには、ルーターのサービスを受けている最新のアクティブ IP フローのトラフィックおよびサービス・プロファイルが含まれます。

超過バースト・サイズ (EBS)
このパラメーターは、CIR を超える速度で、CBS を超過したバーストで送信できる最大のバイト数を指定 (IP パケットのバイト数で) します。このパラメーターは、単一レートの TCM 機能によって使用され、超過トークン・バケットのサイズを制限します。

フロー 同一の発信元アドレスとポート、IP プロトコル、および宛先アドレスとポートをもつ一連のパケット。

トークン速度
このパラメーターは、ユーザーの EF トラフィック・ストリームが送信超過と見なされることになる前に操作できる最大速度を指定します。CIR は、秒当たりの IP パケットのバイト数単位で測定されます。これには、IP ヘッダーが含まれますが、リンク固有ヘッダーは含まれません。

トークン・バケット・サイズ
このパラメーターは、CIR を超える速度で、バーストで送信できる EF トラフィック・ストリームの IP パケットの最大のバイト数を測定します。

ピーク・バケット・サイズ (PBS)
このパラメーターは、2 レート TCM 機能だけによって使用されます。このパラメーターは、PIR を超える速度でバーストで送信できる最大のバイト数を指定 (IP パケットのバイト数で) します。このパラメーターは、ピーク・トークン・バケットの最大サイズを制限します。

ピーク情報速度 (PIR)
このパラメーターは、2 レート TCM 機能だけによって使用されます。これは、最も高い値に設定されたドロップ優先順位を超えた、AF ストリーム・パケットを送信できるピーク速度 (IP ヘッダーを含み、リンク固有ヘッダーは含まれない、秒当たりの IP パケットのバイト数で) を表します。

ストリーム
フローの集合。

バーチャル・インターフェース (VIF)
フレーム・リレー回線の場合、各 DLCI 接続は、バーチャル・インターフェースであると見なされます。

ディファレンシェーテッド・サービスの構成

次の手順により、選択されたパケットに優先サービスを提供するよう DiffServ を構成する方法について高度な説明がなされます。まず、DiffServ フィーチャーにアクセスします。

1. * プロンプトで、**talk 6** と入力する。
2. Config> プロンプトで、**feature ds** と入力する。こう入力すると、DS config> プロンプトが表示され、構成ダイアログがオープンされます。

```
* talk 6
Config>feature ds
DS config>
```

3. 次のように入力して、ルーター上で DiffServ フィーチャーを使用可能にする。

```
DS config> enable ds
DiffServ enabled
```

4. 次のように入力して、インターフェース・パラメーターを使用可能にする。

```
DS config>set interface
Enter Diffserv Interface number [0]? 2
Set Premium Queue Bandwidth (%) (1 - 99) [20]?
    Assured Queue Bandwidth (%) = 80
Configure Advanced setting (y/n)? [No]: no
Accept input (y/n)? [Yes]:
```

注: Configure Advanced setting のプロンプトに対して no を指定した場合は、Premium Queue および Assured/BE queue のデフォルト値が使用されます。

```
Configure Advanced setting (y/n)? [No]: yes
Set Premium Queue Weight (%) (20 - 99) [90]?
    Assured Queue Weight (%) = 10
EGRESS BufSize for Premium Queue (in bytes) (550 - 27500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?
EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?
```

この例では、回線帯域幅の 20 パーセントおよびスケジューラーの重みの 90 パーセントが EF 待ち行列に与えられています。EF 待ち行列の egress バッファー・サイズは 5500 バイト (平均 550 バイトのパケットをもつ 10 パケットです) で、その 95 パーセントは QOS ストリームに割り当てることが可能です。AF/BE 待ち行列の egress バッファー・サイズは、27 500 バイト (平均 550 バイトのパケット・サイズをもつ 50 パケットです) で、その 80 パーセントは QOS ストリームに割り当てることが可能です。

5. ルーターで DiffServ を使用可能化し、インターフェース・パラメーターの設定が済んだら、**Ctrl-P** を押して * プロンプトに戻る。

DiffServ を使用可能化し、インターフェース・パラメーターを設定した後で、装置をリスタートまたは再ロードして DiffServ を起動する必要があります。DiffServ コマンドの指定について詳しくは、463ページの『第24章 ディファレンシェーテッド・サービス・フィーチャーの構成と監視』を参照してください。

第24章 ディファレンシェーテッド・サービス・フィーチャーの構成と監視

この章では、選択されたデータ・パケットに優先サービスを提供するようルーターおよびインターフェースを構成するためにディファレンシェーテッド・サービス (DiffServ) フィーチャーによって提供されるコマンドについて説明します。この章には、次の内容が記載されています。

- 『ディファレンシェーテッド・サービス構成プロンプトへのアクセス』
- 『ディファレンシェーテッド・サービス構成コマンド』
- 468ページの『ディファレンシェーテッド・サービス監視環境へのアクセス』
- 468ページの『ディファレンシェーテッド・サービス監視コマンド』
- 475ページの『ディファレンシェーテッド・サービス動的再構成サポート』

ディファレンシェーテッド・サービス構成プロンプトへのアクセス

DiffServ 構成コマンドを入力するには、次のように行います。

1. OPCON (*) プロンプトで **talk 6** と入力する。
2. `Config>` プロンプトで **feature ds** と入力する。

`DS Config>` プロンプトが表示されます。これで、DiffServ 構成コマンドを入力できます。

ディファレンシェーテッド・サービス構成コマンド

これらのコマンドを使用すると、選択されたデータ・パケットに優先サービスを指定する DiffServ オプションを構成することができます。表53 は DiffServ 構成コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて詳しく説明します。コマンドは `DS Config>` プロンプトで入力します。コマンドとオプションを 1 行に入力することもできますが、コマンドだけを入力して、プロンプトに応答することもできます。有効なコマンド・オプションを見るためには、オプションの代わりに疑問符を付けてコマンドを入力してください。

表 53. DiffServ 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Delete	DiffServ 構成レコードをルーターの SRAM から削除します。
Disable	ルーター内または特定の egress インターフェース上で DiffServ を使用不可にします。
Enable	ルーター内または特定の egress インターフェース上で DiffServ を使用可能にします。
List	ルーターの DiffServ システムおよびインターフェース関連の設定に関する情報を表示します。
Set	ルーターの DiffServ 関連の設定を指定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Delete

delete コマンドは、DiffServ システム構成レコードまたはインターフェース・レコードをルーターの SRAM から削除するのに使用します。

構文 : delete ds
interface

ds ルーターの DiffServ システム構成レコードを削除します。

例 :

```
DS Config>  delete ds
Diffserv system config record deleted
```

interface 削除するインターフェース番号を入力するようプロンプト指示します。

例 :

```
DS Config> delete interface
Enter Diffserv Interface number to delete [0]?  3
Diffserv interface config record deleted
```

Disable

disable コマンドは、ルーター内または特定の egress インターフェース上で DiffServ 機能を使用不可にするのに使用します。

構文 : disable ds
interface

ds ルーターの DiffServ 機能を使用不可にします。

例 :

```
DS Config> disable ds
DiffServe feature disabled
```

interface 使用不可にするインターフェースの番号を入力するようプロンプト指示します。

例 :

```
DS Config> disable interface
Enter Interface number [0]? 2
DiffServe interface disabled
```

Enable

enable コマンドは、ルーター内または特定の egress インターフェース上で DiffServ 機能を使用可能にするのに使用します。

構文 : enable ds
interface

ds ルーターの DiffServ 機能を使用可能にします。

例 :

```
DS Config> enable ds
DiffServe feature enabled
```

interface 使用可能にするインターフェースの番号を入力するようプロンプト指示します。

例 :

```
DS Config> enable interface
Enter Interface number [0]? 2
DiffServe interface enabled
```

注: DiffServ は、PPP リンクおよびフレーム・リレー・リンク上でだけ使用可能にすることができます。

List

list コマンドは、ルーターの DiffServ システムおよびインターフェース関連の設定に関する情報を表示するのに使用します。

構文 : list　all / ds / interface

all ルーターの DiffServ およびインターフェース構成に関する情報を表示します。

ds ルーターの DiffServ 構成を表示します。

例 :

```
DS Config> list ds

System Parameters:

        DiffServ:               ENABLED
        Packet_size:            550
        Min BE_Alloc (%):       10
        Min CTL Alloc (%):      5
        Number_of_Q:            2
```

interface ルーター内のインターフェース、それぞれの DiffServ 使用可能 / 使用不可状況、および各インターフェースおよび待ち行列のパラメーターを表示します。

例 :

```
DS Config> list interface
-------------------------------------------------------------------------------
                          ---------- Premium -------   --------- Assured --------
Net If     Status  NumQ Bwdth  Wght  OutBuf  MaxQos Bwdth  Wght  OutBuf  MaxQos
Num                 (%)   (%) (bytes)     (%)   (%)   (%) (bytes)     (%)
-------------------------------------------------------------------------------
2   PPP   Enabled     2    20    90    5500      95    80    10   27500      80
3   PPP   Enabled     2    20    90    5500      95    80    10   55000      80
```

Set

set コマンドは、ルーターの DiffServ システムおよびインターフェース関連パラメーターを設定するのに使用します。

構文: set　be-alloc-min / ctl-alloc-min / interface / pkt-size

be-alloc-min best-effort サービスに割り振るための合計出力バッファーの最小パーセンテージを指定します。

デフォルト値 : 10

例 :

```
DS Config>  set be-alloc-min
Enter Minimum percent output BW allocated to BE service (10 - 50) [10]?
```

ctl-alloc-min ネットワーク制御サービスに割り振るための合計出力バッファーの最小パーセンテージを指定します。

デフォルト値 : 5

例 :

```
DS Config>  set ctl-alloc-min
Enter Minimum percent output BW allocated to CTL service (5 - 20) [5]?
```

interface DiffServ について使用可能にするインターフェースを指定し、インターフェース固有のパラメーターを入力するようプロンプト指示します。

Queue bandwidth
特別待ち行列に使用する出力リンクのパーセンテージを指定します。残りのパーセンテージは、確実待ち行列値のために使用されます。

デフォルト値 : 20

Queue weight
スケジューラーが特別待ち行列を監視する時間のパーセンテージを指定します。残りのパーセンテージは、確実待ち行列値のために使用されます。待ち行列の重みのデフォルトは 90 パーセントで、この場合、スケジューラーは EF トラフィックに対して即時に反応します。

デフォルト値 : 90

Egress buffer size
特別待ち行列および確実待ち行列上で待ち行列化できるデータの量 (バイト単位) を指定します。

特別待ち行列の場合、このパラメーターは、特別待ち行列上で待ち行列化できるデータの量 (バイト単位) を制御します。このパラメーターに指定する値が大きすぎると、特別トラフィックの待ち行列化遅延が大きくなる可能性があります。たとえば、これを 25 K バイトに設定し、出力リンク速度が 1.5 Mbps (T1 速度) である場合、133 msec (25 000 バイト * 8 ビット/バイト)/1 500 000 bps、つまり 0.133 秒 (133 ミリ秒) の潜在的待ち行列化遅延が起こります。このパラメーターの値が小さすぎると、小さなバーストをバッファーに入れることができなくなることがあります。たとえば、これを 2 Kb に設定すると、1500 バイト・パケットの 2 パケット・バーストに十分なバッファリングが行われないことを意味します。

上記 2 つの極端な値の妥協案として、デフォルト値が 5500 バイトに設定されています。これは、550 というデフォルトのパケット・サイズの 10 倍です。

デフォルト値 : 5500 (特別待ち行列)

確実待ち行列の場合、このパラメーターは、確実待ち行列上で待ち行列化できるデータの量 (バイト単位) を制御します。このパラメーター値に関する考慮事項は、特別待ち行列の場合と同じです。ただし、確実待ち行列内のトラフィックには、さほど厳密な遅延要件はありません。むしろ、確実待ち行列トラフィックは、TCP フローで構成されることが多く、このフローは本質的にバースト性が高いものです。このため、いくつかのフローからのバーストに適応するために、十分なバッファー・スペースを定義する必要があります。

デフォルト・サイズの 27 500 バイトは、デフォルトのパケット・サイズ 550 の 50 倍です。

デフォルト値 : 27500 (確実待ち行列)

Egress QoS allocation

すべての DiffServ ストリームが予約できる egress バッファー・サイズ値の量をパーセントとして指定します。残りのパーセンテージは、共用プールの最小サイズのために使用されます。

デフォルト値 : 95 (特別待ち行列)

デフォルト値 : 80 (確実待ち行列)

注:

1. マルチリンク PPP の場合、バンドル・バーチャル・インターフェースで DiffServ を使用可能にします。バンドル・インターフェースの個々のリンクで DiffServ を使用可能にすることはできません。
2. フレーム・リレー・サブインターフェースの場合、ベースのフレーム・リレー・ネットで DiffServ を使用可能にします。サブインターフェースで DiffServ 使用可能にすることはできません。

例 :

```
DS Config> set interface
Enter Diffserv Interface number [0]? 2

DiffServ Interface enabled

Set Premium Queue Bandwidth (%) (1 - 99) [20]?
    Assured Queue Bandwidth (%) = 80

Configure Advanced setting (y/n)? [No]: y

Set Premium Queue Weight (%) (20 - 99) [90]?
    Assured Queue Weight (%) = 10

EGRESS BufSize for Premium Queue (in bytes) (550 - 27500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?

EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?

        DiffServ Interface: ENABLED
PREMIUM Queue Bandwidth (%) =                          20
PREMIUM Queue Weight (%) =                             80
```

```
PREMIUM Queue EGRESS BufSize in bytes =             5500
PREMIUM Queue Max EGRESS QoS allocation (%) =         95
ASSURED/BE Queue Bandwidth (%) =                      80
ASSURED/BE Queue Weight (%) =                         20
ASSURED/BE Queue EGRESS BufSize in bytes =         27500
ASSURED/BE Queue Max EGRESS QoS allocation (%) =      80
Accept input (y/n)? [Yes]:
```

pkt-size

トラフィック・フローの平均パケット・サイズ (バイト単位) を指定します。これを指定すると、DiffServ は、ingress インターフェースおよび egress インターフェース上で使用可能なバッファーを判別することができます。これを変更した場合は、ルーターをリスタートし、DiffServ **set interface** コマンドを検討し、必要であれば変更しなければなりません。

デフォルト値 : 550

例 :

```
DS Config>  set pkt-size
Average packet size (64 - 64000) [550]?
```

ディファレンシェーテッド・サービス監視環境へのアクセス

DiffServ フィーチャーのコンソール部分により、ユーザーは DiffServ 関連の設定を表示したり、管理することができます。DiffServ 監視環境にアクセスするには、次のように OPCON プロンプト (*) で **talk 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで次のコマンドを入力します。

```
+ feature ds
DS Console>
```

ディファレンシェーテッド・サービス監視コマンド

これらのコマンドを使用すると、DiffServ 関連の設定を表示することができます。表54 は DiffServ 監視コマンドの要約を示し、ここでの残りの部分でそれらについて説明しています。コマンドは DS Console> プロンプトで入力します。コマンドとオプションを 1 行に入力することもできますが、コマンドだけを入力して、プロンプトに応答することもできます。有効なコマンド・オプションを見るためには、オプションの代わりに疑問符を付けてコマンドを入力してください。

表 54. DiffServ 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Clear	特定の ingress および egress インターフェースの対間のストリームの統計をクリアします。
DScache	ルーターの DiffServ キャッシュ内の情報をクリアしたり、表示したりします。
List	ルーターの DiffServ システムおよびインターフェース関連の設定に関する情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Clear

clear コマンドは、特定の ingress および egress インターフェースの対間のストリームの統計をクリアするのに使用します。

構文 : clear stream-stats

例 :

```
DS Console>  clear stream-stats
Incoming Network number : 0
Outgoing Network number : 2
Net 0->2 stream stats cleared at sysclock 85327 Second.
```

DScache

dscache コマンドは、ルーターの DiffServ キャッシュ内の情報をクリアまたは表示するのに使用します。

構文 : dscache actions
clear
nexthop
order
stats

actions 指定された IP 発信元から指定された IP 宛先へ送信されたパケットについて取られるアクションと、DiffServ ストリーム ID (存在する場合) を表示します。

例 :

```
DS Console> dscache actions
Source Address to list []?
Destination Address to list []?
Source          Destination     Pro ProtocolInf Net TosIn/Out Action StrmID
10.1.100.1      9.1.140.1         1 T:x08 C:x00   0 x00->x15  PASS   85
9.1.140.1       10.1.100.1        1 T:x00 C:x00   1 x00->x15  PASS   null
```

clear DiffServ キャッシュ全体のクリアを指定します。

nexthop ネクスト・ホップ IP アドレスを表示します。

例 :

```
DS Console> dscache nexthop
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source          Destination     Pro ProtocolInf Net  Tos  NextHop
5.0.13.248      5.0.11.249       17  1031> 1031   0  x00  5.0.61.7      (PPP/1)
5.0.13.248      5.0.11.249       17  1032> 1032   0  x00  5.0.61.7      (PPP/1)
5.0.13.248      5.0.11.249       17  1033> 1033   0  x00  5.0.67.1      (PPP/1)
```

order パケットが到着した順序を表示します。

例 :

```
DS Console> dscache order
Order Source          Destination     Pro ProtocolInf Net  Tos
   1  5.0.16.246      5.0.13.248        1 T:x03 C:x03   2  x00
   2  5.0.13.248      5.0.16.246       17  4000> 5678   0  x00
   3  5.0.16.246      5.0.13.244        1 T:x03 C:x03   1  x00
   4  5.0.13.248      5.0.15.243       17   123>  123   0  x00
```

stats 指定された IP 発信元から指定された IP 宛先へ送信されたパケットの統計を表示します。

例 :

```
DS Console> dscache stats
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source          Destination     Pro ProtocolInf Net  Tos    RxPkts    RxBytes
5.0.13.248      5.0.11.249       17  1031> 1031   0  x00       432     444096
5.0.13.248      5.0.11.249       17  1032> 1032   0  x00       432     444096
5.0.13.248      5.0.11.249       17  1033> 1033   0  x00       437     459516
```

List

list コマンドは、ルーターの DiffServ システムおよびインターフェース関連の設定に関する情報を表示するのに使用します。

構文 : list　　interface

queue

stream

vifs

interface　ルーター内のインターフェース、それぞれの DiffServ 使用可能 / 使用不可状況、およびそれぞれの ingress バッファー割り振り、およびその他の情報を表示します。

Net　インターフェース番号を表示します。

Status
DiffServ 状況を表示します。

KB/s　リンク速度を、秒当たり kb で表示します。

VirtTime
スケジューラーが使用するバーチャル時刻を表示します (非 DiffServ リンクの場合は n/a を示し、進行中のパケットがない場合は 0 を示します)。

InMax　確実転送用に構成された最大バッファー・サイズを表示します。

InCurr　入力ストリームに現在使用されているバッファー・スペースの量を表示します。バッファーには、進行中のパケットが含まれています。

InShar
この egress インターフェースに使用可能な共用バッファー・スペースの量を表示します。

InMaxA
集合内のすべての QoS ストリームに割り振ることのできるバッファー・スペースの最大量を表示します。

InCurA
入力ストリームが使用できるように割り振られたバッファー・スペースの量を表示します。

NumI　入力ストリームの数を表示します。

NumO　出力ストリームの数を表示します。

例 :

```
DS Console> list interface
DiffServ interfaces:
Net Status   KB/s  VirtTime InMax  InCurr InShar InMaxA InCurA NumI NumO
--- -------- ----- -------- ------ ------ ------ ------ ------ ---- ----
  0 Disabled  1250      n/a  55000    550  49775  44000   5225   22  n/a
  1 Disabled  1250      n/a  27500      0  27500  22000      0   20  n/a
  2 Enabled    256        0  27500      0  27500  22000      0   20    3
  3 Enabled    256        0  55000      0  55000  44000      0   20    3
  4 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  5 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  6 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  7 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
  8 Disabled  2000      n/a  27500      0  27500  22000      0   20  n/a
  9 Disabled     0      n/a 550000      0 550000 550000      0   20  n/a
```

queue DiffServ egress 待ち行列に割り当てられた重みと、egress インターフェースのバッファー割り当て状況を表示します。

Queued packets
現在待ち行列化されているパケットの数を表示します (0 は現在待ち行列化されているパケットがないことを示します)。

Svc Tag
この待ち行列がサービスを受け取る次のバーチャル時刻を表示します。

Weight
この待ち行列の構成済みスケジューラーの重みを表示します。

out_max_alloc
DiffServ ストリームに割り振ることのできるバッファー・スペースの最大量を表示します。

out_curr_alloc
割り振り済みのバッファー・スペースの現在量を表示します。

out_max_buff
この待ち行列のバッファー・スペースの最大量を表示します。

out_curr_buff
パケットに使用されている、現在割り振り済みのバッファー・スペースの量を表示します。

out_share_buff
現在共用プール内にあるバッファー・スペースの量を表示します。

例 :

```
DS Console> list queue
OUT Network number : 1

Premium Queue:
        Queued packets: 0
        Svc Tag:        4294967295
        Weight: 90
        out_max_alloc:  5225 (Bytes)
        out_curr_alloc: 0 (Bytes)
        out_max_buff:   5500 (Bytes)
        out_curr_buff:  0 (Bytes)
        out_share_buff: 5500 (Bytes)
```

```
Assured Queue:
        Queued packets: 0
        Svc Tag:        4294967295
        Weight: 10
        out_max_alloc:  22000 (Bytes)
        out_curr_alloc: 4125 (Bytes)
        out_max_buff:   27500 (Bytes)
        out_curr_buff:  0 (Bytes)
        out_share_buff: 23375 (Bytes)
```

stream meter-mark

AF ストリームについての測定とマーク付けの情報を表示します。

Id ストリーム識別番号

t ストリーム・タイプ

- **D** DiffServ ストリーム
- **B** Best-effort ストリーム
- **C** ネットワーク制御ストリーム
- **R** RSVP ストリーム

I/o q 出力インターフェース待ち行列タイプ

- **q1** 特別待ち行列
- **q2** 確実 /BE 待ち行列

pkt snt
このストリームによって送信された合計パケット数

buf drp
使用可能なバッファー・スペースがないためにこのストリームからドロップされたパケットの数

snt g 送信された緑色にマーク付けされたパケット数

snt y 送信された黄色にマーク付けされたパケット数

snt r 送信された赤色にマーク付けされたパケット数

g->y color-aware モードで、黄色マークで送信された緑色マークのパケット数

g->r color-aware モードで、赤色マークで送信された緑色マークのパケット数

y->r color-aware モードで、赤色マークで送信された黄色マークのパケット数

例 :

```
DS Console> list stream meter-mark 0 1
At interface 0, 4 in-streams; clock=25493 sec.
Streams from net 0 to net 1:
 Id   t I/o q  pkt snt  buf drp   mrk g    mrk y   mrk r   g->y    g->r    y->r
 ---- - -----  -------  -------  -------  ------  ------  ------  ------  ------
(af1)
 101  D   in     3615        0        0       0       0       0       0       0
         o-q2    3615        0     1223    1222    1770       0       0       0
```

stream packet-stats

ストリーム内のパケットの情報を表示します。

Id ストリーム識別番号

t ストリーム・タイプ

- **D** DiffServ ストリーム
- **B** Best-effort ストリーム
- **C** ネットワーク制御ストリーム
- **R** RSVP ストリーム

I/o q 出力インターフェース待ち行列タイプ

- **q1** 特別待ち行列
- **q2** 確実 /BE 待ち行列

allo/cur(K)
このストリームによって割り振られ、現在使用されている合計バッファー・スペース (K バイト単位)

tot pkt
このストリームによって伝送するために受信された合計パケット数

tot Kby
このストリームによって伝送するために受信された合計 K バイト数

pkt snt
このストリームによって送信された合計パケット数

Kby snt
このストリームによって送信された合計 K バイト数

ovr snt
共用バッファーを使用して送信されたパケットの数

buf drp
使用可能なバッファー・スペースがないためにこのストリームからドロップされたパケットの数

pol drop
特別待ち行列上の、ポリサーによってドロップされたパケットの数

例 :

```
DS Console> list stream packet-stats 0 1
At interface 0, 4 in-streams; clock=25496 sec.
Streams from net 0 to net 1:
 Id   t I/o q  allo/cur(K)  tot pkt  tot Kby  pkt snt  Kby snt  ovr snt  buf drp pol drp
 ---- - -----  -----------  -------  -------  -------  -------  -------  ------- -------
(af1)
 101  D    in   6.3/   0.0     3615     3730     3615     3730        0        0
          o-q2   6.3/   0.0                       3615     3730        0        0       0

(ef)
 100  D    in   5.2/   0.0     2393     2469     2393     2469        0        0
          o-q1   5.2/   0.0                       2393     2469        0        0     132

(-)
 40   B    in   0.0/   0.0        0        0        0        0        0        0       0
          o-q2   2.8/   0.0                          0        0        0        0       0

(-)   C    in   0.0/   0.0        0        0        0        0        0        0
          o-q2   1.4/   0.0                          0        0        0        0       0
```

stream police-para

EF と AF のストリーム用の構成済みポリシング・パラメーターの情報を表示します。

Id ストリーム識別番号

t ストリーム・タイプ

- **D** DiffServ ストリーム
- **B** ベストエフォート・ストリーム
- **C** ネットワーク制御ストリーム
- **R** RSVP ストリーム

I/o q 出力インターフェース待ち行列タイプ

- **q1** 特別待ち行列
- **q2** 確実 /BE 待ち行列

TR/CIR in B/s
秒当たりのバイト数で表される構成済みトークン速度またはコミット情報速度。

TBS/CBS in bytes
バイト数で表される構成済みトークン・バケット・サイズまたはコミット・バースト・サイズ

PIR in B/s
秒当たりのバイト数で表される構成済みピーク情報速度

EBS/PBS in bytes
バイト数で表される構成済み超過バケット・サイズまたはピーク・バースト・サイズ

pol typ
ポリシング・アクションのタイプ

- **None** ポリシングなし
- **SRCB** 単一レート、color blind TCM
- **SRCA** 単一レート、color-aware TCM
- **TRCB** 2 レート、color blind TCM
- **TRCA** 2 レート、color-aware TCM
- **EF-DRP**
  デフォルトのドロップ・アクションをもつ EF ポリサー

例 :

```
DS Console> list stream police-para 0 1
At interface 0, 16 in-streams; clock=18429 sec.
Streams from net 0 to net 1:
 Id   t I/o q     TR/CIR    TBS/CBS    PIR      EBS/PBS  pol typ
                  in B/s   in bytes   in B/s   in bytes
 ---- - -----  ---------  ---------  -------  ---------  -------
(af1)
 101  D   in
         o-q2      25000       4000        0       4000  SRCB
```

```
(ef)
 100  D   in
        o-q1      48706       5225                        EF-DRP
```

vifs フレーム・リレー・バーチャル・インターフェースに関する情報を表示します。

例 :

```
DS Console> list vifs 1

DiffServ virtual interface for dlci:  17
     Status: Inactive - no packets queued for transmission
     CIR: 64000 (bits/sec)
     Virtual Time: 0
     Service Tag:  0

DiffServ virtual interface for dlci:  16
     Status: Inactive - no packets queued for transmission
     CIR: 64000 (bits/sec)
     Virtual Time: 0
     Service Tag:  0
```

ディファレンシェーテッド・サービス動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

ディファレンシェーテッド・サービス (または DiffServ または DS) は、CONFIG (Talk 6) **delete interface** コマンドをサポートしますが、次の考慮が必要です。

これは、対応する DiffServ インターフェース SRAM レコードを削除します。この変更を活動化するためには装置をリブートする必要があります。

GWCON (Talk 5) Activate Interface

DiffServ は、GWCON (Talk 5) **activate interface** コマンドをサポートしますが、次の考慮が必要です。

DS は、DS 構成インターフェースが活動化された場合には、通常のネットアップ/ネットダウン・シーケンスに続きます。

GWCON (Talk 5) Reset Interface

DiffServ は、GWCON (Talk 5) **reset interface** コマンドをサポートしますが、次の考慮が必要です。

- DiffServ をこのインターフェースで使用可能にした場合、次のことが発生します。**reset interface** が、このインターフェースとの間での、作成されたすべてのストリームを消去します。diffserv キャッシュも消去されます。BRS を使用可能にすると、BRS はこのインターフェースで DiffServ より優先します。DiffServ インターフェース SRAM レコードに add/del/change があった場合には、変更を活動化するためには装置をリブートする必要があります。

非動的再構成可能コマンド

次の表には、動的に変更できない DiffServ の構成コマンドを記載します。これらのコマンドを活動化するには、装置を再ロードしたり、リスタートする必要があります。

DiffServ 監視コマンド (Talk 5)

コマンド
CONFIG, feature DS, enable/disable/del ds
CONFIG, feature DS, enable/disable/del/set interface
CONFIG, feature DS, set be-alloc-min
CONFIG, feature DS, set ctl-alloc-min
CONFIG, feature DS, set pkt-size

第25章 ランダム早期検出フィーチャーの使用

この章では、構成済みのドロップの確率に基づいて、ネットワーク装置が、輻輳が発生した場合にドロップするランダム着信パケットにマークを付けて、オーバーフローを回避できるように、ランダム早期検出 (RED) フィーチャーの使用方法を説明します。これは、転送のウィンドウ・サイズを小さくして、競合の徴候に反応する、TCP などの規則正しく動作するトラフィックに有効です。RED は、PPP、マルチリンク PPP、およびフレーム・リレー・リンクをサポートします。本省は、次のセクションから構成されます。

- 『ランダム早期検出の使用』

ランダム早期検出の使用

RED によって、輻輳が発生してもオーバーフローを回避できます。RED は、平均の待ち行列の長さを計算し、それが指定した制限値内であれば、構成可能なドロップの確率に基づいて、着信パケットにドロップのマークを付けます。現在の待ち行列サイズの代わりに、平均の待ち行列の長さを使用して、突発的なトラフィック待ち行列がドロップ・レートに影響を与えることをできなくします。

RED パラメーターについて次の値が指定されているものとします。

```
1 Weight factor: 4
2 Exponential Maximum Packet Drop Probability: 9
3 Minimum Threshold Value: 70
4 Maximum threshold Value: 100
5 Initial Average Queue Size: 60
```

1 この値は、現在の待ち行列が平均の待ち行列の長さの計算に与える影響の大きさを決定します。

このパラメーターの最小値 (1) は、重みが小さいことを示し、消極的な設定となります。この値を用いると、特定の時点での平均の待ち行列の長さは、直前の平均の待ち行列の長さにより近い値に留まり、このため大きい待ち行列の長さをもつ突発的なトラフィックは新しい待ち行列の長さの計算にあまり影響を与えません。

このパラメーターの最大値 (8) は、より大きい重みを示し、積極的な設定となります。この値を用いると、平均の待ち行列の長さは、現在の平均の待ち行列の長さと同じになり、このため大きい待ち行列の長さをもつ突発的なトラフィックは新しい待ち行列の長さの計算に大きい影響を与えます。

2 この値は、ピークの平均待ち行列の長さでパケットをドロップする確率です。

平均の待ち行列の長さが最大のしきい値に常に等しい場合には、2^9 (512) パケットごとに 1 つにドロップのマークが付けられます。ドロップの確率は、平均の待ち行列の長さが最小のしきい値から最大のしきい値に大きくなるにつれて定率で大きくなります。

3 この値は、パケットのドロップの確率を計算するための最小の待ち行列要件を示し、それに従ってパケットにマークを付けます。

これは、最大の装置の待ち行列値のパーセント (これはレイヤー 2 プロトコルで決定され、構成可能ではない値) として表されます。たとえば、40 パーセントを指定し、最大の装置の待ち行列値が 16 である場合には、最小のしきい値は、6 (0.4*16) に設定されます。

4 この値は、パケットのドロップの確率を計算するための最大の待ち行列要件を示し、それに従ってパケットにマークを付けます。

これは、最大の装置の待ち行列値のパーセント (これはレイヤー 2 プロトコルで決定され、構成可能ではない値) として表されます。たとえば、100 パーセントを指定し、最大の装置の待ち行列値が 16 である場合には、最大のしきい値は、16 (1.0*16) に設定されます。

5 この値は、パケットのドロップの確率の計算に使用される最初の設定値を示します。

これは、最大の装置の待ち行列値のパーセント (これはレイヤー 2 プロトコルで決定され、構成可能ではない値) として表されます。これは、トラフィック自身が平均の待ち行列値を設定する前に突発的なトラフィックが平均待ち行列の長さの計算での重みを大きくできないようにします。(装置を初期設定したとき、待ち行列の長さはゼロで、前の平均待ち行列の長さを示すものは存在しません。) 前の例に示したように、相対的に低い値を指定する必要があります。

RED を使用可能にし、インターフェース・パラメーターを設定したあとで、REDを活動化するために装置をリスタートまたは再ロードする必要があります。RED コマンドの指定の詳細については、479ページの『第26章 ランダム早期検出フィーチャーの構成と監視』を参照してください。

第26章 ランダム早期検出フィーチャーの構成と監視

この章では、輻輳状態にある間にパケットをランダムにドロップするようにインターフェースを構成するためのランダム早期検出 (RED) フィーチャーが提供するコマンドを説明します。この章には、次の内容が記載されています。

- 『ランダム早期検出構成プロンプトへのアクセス』
- 『ランダム早期検出構成コマンド』
- 481ページの『ランダム早期検出監視環境へのアクセス』
- 482ページの『ランダム早期検出監視コマンド』

ランダム早期検出構成プロンプトへのアクセス

RED 構成コマンドを入力するには、次のようにします。

1. OPCON (*) プロンプトで **talk 6** と入力する。
2. Config> プロンプトで **feature red** と入力する。

RED Config> プロンプトが表示されます。これで、RED 構成コマンドを入力できます。

ランダム早期検出構成コマンド

これらのコマンドを使用すると、RED オプションを構成できます。これらのオプションによって、輻輳トラフィックの間中のパケットのドロップ方法が決められます。これによって、オーバーフローやグローバル再同期が回避されます。表55 は RED 構成コマンドの要約を示し、ここでの残りの部分でこれらのコマンドについて詳しく説明します。コマンドは、RED Config> プロンプトで入力します。コマンドとオプションを 1 行に入力することもできますが、コマンドだけを入力して、プロンプトに応答することもできます。有効なコマンド・オプションを見るためには、オプションの代わりに疑問符を付けてコマンドを入力してください。

表 55. ランダム早期検出構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Delete	RED 構成レコードまたはインターフェース・レコードをネットワーク装置の SRAM から削除します。
Disable	ネットワーク装置内のまたは特定の egress インターフェースの RED を使用不可にします。
Enable	ネットワーク装置内のまたは特定の egress インターフェースの RED を使用可能にします。
List	ネットワーク装置の RED 状況およびインターフェース関連の設定に関する情報を表示します。
Set	ネットワーク装置の特定インターフェースの RED 設定値を指定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Delete

delete コマンドは、インターフェースの RED 構成レコードをネットワーク装置の SRAM から削除します。

構文 : delete interface

interface 削除するインターフェース番号を入力するようプロンプト指示します。

例 :

```
RED Config> delete interface
Enter RED Interface number to delete [0]? 3
RED interface config record deleted
```

Disable

disable コマンドは、ネットワーク装置のまたは特定の egress インターフェースのいずれかで RED を使用不可にするのに使用します。

構文 : disable red
interface

red ネットワーク装置の RED を使用不可にします。

例 :

```
RED Config> disable red
RED disabled
```

interface 特定の egress インターフェースの RED を使用不可にします。

例 :

```
RED Config> disable interface
Enter RED Interface number [0]? 2
RED interface disabled
```

Enable

enable コマンドは、ネットワーク装置のまたは特定の egress インターフェースのいずれかで RED を使用可能にするのに使用します。

構文 : enable red
interface

red ネットワーク装置の RED を使用可能にします。

例 :

```
RED Config> enable red
RED enabled
```

interface 特定の egress インターフェースの RED を使用可能にします。

例 :

```
RED Config> enable interface
Enter RED Interface number [0]? 2
RED interface enabled
```

注: RED は、PPP、マルチリンク PPP、およびフレーム・リレー・リンクでのみ使用可能にできます。

List

list コマンドは、ネットワーク装置の RED 状況およびインターフェース関連の設定に関する情報を表示するのに使用します。

構文 : list all

all ネットワーク装置の RED 状況を表示します。

例 :

```
RED Config>list all

        RED Status: Enabled

-----------------------------------------------------
Status  Net If   qW   maxP   minT   maxT    initAvgQ
                              ------ %ofdevQ --------
-----------------------------------------------------
Enable  6   PPP  4    1/512  70     100     60


Abbreviation:

qW = Queue Weight
minT = Minimum Threshold, maxT = Maximum Threshold
maxP = Maximum Drop Probability: 1 drop in 512 pkts
%ofdevQ = A percentage of the Maximum Device Queue
```

Set

set コマンドは、ネットワーク装置の特定インターフェースの RED 設定値を指定するのに使用します。

構文: set interface

interface *number*

RED オプションを設定するインターフェースの番号を指定します。

デフォルト値: なし

例 :

```
RED config>set interface
Enter RED Interface number [0]? [6]
RED Interface enabled
Exponential Maximum Packet Drop Probability (9 for 1/2e9) (5 - 10) [9]?
Advanced Setting (y/n)? [Yes]: yes

Maximum Device Queue = 5
Weight Factor (1 - 8) [4]?
Minimum Threshold value (% of the max device queue) (0 - 100) [70]?
Maximum Threshold value (% of the max device queue) (0 - 100) [100]?
Initial Average Queue Size (% of the max device queue) (0 - 100) [60]?
Accept input (y/n)? [Yes]: yes
```

ランダム早期検出監視環境へのアクセス

ランダム早期検出フィーチャーのコンソール部分により、ユーザーは RED 関連の設定を表示したり、管理することができます。RED 監視環境にアクセスするには、次のように OPCON プロンプト (*) で **talk 5** と入力します。

```
* t 5
```

次に、**+** プロンプトで次のコマンドを入力します。

```
+ feature red
RED Console>
```

ランダム早期検出監視コマンド

これらのコマンドを使用すると、RED 関連の設定を表示することができます。 表 56 は RED 監視コマンドの要約を示し、ここでの残りの部分でそれらについて説明しています。コマンドは、RED Console> プロンプトで入力します。コマンドとオプションを 1 行に入力することもできますが、コマンドだけを入力して、プロンプトに応答することもできます。有効なコマンド・オプションを見るためには、オプションの代わりに疑問符を付けてコマンドを入力してください。

表 56. RED 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Clear	インターフェースの RED パラメーター設定値をリセットします。
List	RED 使用可能ネットワーク装置のインターフェース設定値を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Clear

clear コマンドは、インターフェースの RED パラメーター設定値をリセットするのに使用します。**list** コマンドの説明にある例は、**clear** コマンドの結果を示します。

構文 : clear *interface-number*

List

list コマンドは、RED 使用可能ネットワーク装置のインターフェース設定値に関する情報を表示するのに使用します。

構文 : list *interface-number*

interface-number

ネットワーク装置の指定したインターフェースの RED 設定値をリストします。

例 :

```
RED Console>list 6
-------------------------------------------------------------------------------
Status  If   maxQ   avgQ   minT   maxT  qW   maxP  pktCnt    pdpDepth  passCnt  drpCnt
                           (dvQ)  (dvQ)       (pkt)  til drp     count     pkt      pkt
-------------------------------------------------------------------------------
Enable   6       5      3      3      5  4  1/512    1:3787        285     4283       1


Abbreviations:

maxQ = Maximum Queue Length, avgQ = Average Queue Size
minT = Minimum Threshold, maxT = Maximum Threshold
dvQ = Device Queue, qW = Queue Weight
```

```
maxP = Maximum Drop Probability: 1 drop in 512 pkts
pktCnt til drp = Packet Count before a drop occurs
pdpDepth = Probability Drop Depth: 1 drop in 2048 depth count

RED Console>clear 6

RED Console>list 6
-------------------------------------------------------------------------------------------
Status  If   maxQ   avgQ   minT   maxT  qW   maxP  pktCnt    pdpDepth  passCnt  drpCnt
                           (dvQ)  (dvQ)       (pkt)  til drp     count     pkt      pkt
-------------------------------------------------------------------------------------------
Enable   6      5      3      3      5   4  1/512   1:3530   0         0        0


Abbreviations:

maxQ = Maximum Queue Length, avgQ = Average Queue Size
minT = Minimum Threshold, maxT = Maximum Threshold
dvQ = Device Queue, qW = Queue Weight
maxP = Maximum Drop Probability: 1 drop in 512 pkts
pdkCnt til drp = Packet Count before a drop occurs
pdpDepth = Probability drop Depth: 1 drop in 2048 depth count
```

第27章 レイヤー 2 トンネル伝送 (L2TP、PPTP、L2F) の使用

この章では、レイヤー 2 トンネル伝送を説明します。この章は、以下のセクションから構成されます。

レイヤー 2 トンネル伝送 (L2T) は、L2TP、L2F、および PPTP トンネル伝送プロトコルで構成されます。

レイヤー 2 トンネル伝送プロトコル (L2TP) は、UDP/IP のようなパケット・ネットワークを通して PPP をトンネル伝送するための IETF 標準トラック・プロトコルです。L2TP は接続型です。

レイヤー 2 転送 (L2F) およびポイントツーポイント・トンネル伝送プロトコル (PPTP) は、IP ネットワークを通じて PPP をトンネル伝送するための IETF 通知プロトコルです。

L2TP の概説

L2TP は、多数の個別の自立走行式プロトコル・ドメインが、モデム、アクセス・サーバー、および ISDN ルーターを含む共通のアクセス・インフラストラクチャーを共用することを可能にします。L2TP は、PPP リンク・レイヤー (たとえば、HDLC および非同期 HDLC) のトンネル伝送を許します。このようなトンネルを使用すると、接続するダイヤルアップ・サーバーの場所とネットワークへのアクセスを提供する場所とを分離することが可能になります。

従来のインターネット上のダイヤルアップ・ネットワーク・サービスは、登録された IP アドレスに対してだけ提供されています。L2TP は、インターネット上の複数プロトコルおよび未登録 IP アドレスを許容する新しいクラスのバーチャル・ダイヤルアップ・アプリケーションを定義しています。このクラスのネットワーク・アプリケーションは、既存のインターネット・インフラストラクチャーを利用して PPP 経由で私設アドレス IP、IPX、および AppleTalk ダイヤルアップをサポートするのに便利です。

このようなマルチプロトコル・バーチャル・ダイヤルアップ・アプリケーションに対するサポートは、アクセスおよびコア・インフラストラクチャーへの巨額の投資を分担することができ、エンド・ユーザーはローカル・コールを使用してサービスにアクセスできるなど、エンド・ユーザー、企業、およびインターネット・サービス提供者のどちらにとっても有益です。

L2TP では、既存のインターネット・インフラストラクチャーの IP 以外のプロトコル・アプリケーションへの現行投資も活用できることが保証されます。

図43 は、ISDN を使用する L2TP ネットワークの例を示します。このネットワークでは、L2TP ネットワーク・アクセス・コンセントレーター (LAC) と L2TP ネットワーク・サーバー (LNS) の間に、任意の媒体タイプを使用することができます。この例では、必須トンネル伝送モデルを使用します。また、この章で任意トンネル伝送モデル構成についても説明します。

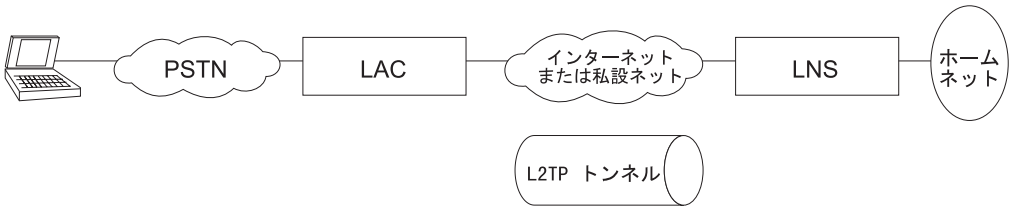


図 43. L2TP ネットワークの例

L2TP の用語

L2TP を説明するために、次の用語が使用されています。

属性値ペア (AVP)
メッセージ・タイプおよび本文をコード化する統一方式。この方式は、L2TP のインターオペラビリティーを可能にすると同時に、拡張性を最大化します。

L2TP アクセス集線装置 (LAC)
PPP 運用と L2TP プロトコルの両方を扱える、1 つまたは複数の公衆電話網 (PSTN) または ISDN 回線に接続された装置。LAC は、L2TP を運用する媒体を設定しています。L2TP は、トラフィックを 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) にパスします。L2TP は PPP ネットワークによって運ばれたプロトコルをトンネル伝送することができます。

L2TP ネットワーク・サーバー (LNS)
LNS は、PPP エンド・ステーションとして使用できる任意のプラットフォーム上で稼働します。LNS は、L2TP プロトコルのサーバー側を扱います。L2TP は単一媒体にだけ依存して L2TP トンネル伝送を行うので、LNS は 1 つの LAN または WAN インターフェースしか持つことができませんが、LAC がサポートする任意の PPP インターフェースから到着したコールを終了させることができます。

ネットワーク・アクセス・サーバー (NAS)
ユーザーに一時的に、要求時にネットワーク・アクセスを提供する装置。このアクセスは、PSTN または ISDN 回線を使用するポイントツーポイントです。

セッション (コール)
L2TP は、ダイヤル・ユーザーと LNS 間でエンドツーエンド PPP 接続が試みられると、セッションを作成します。セッションのデータグラムは、LAC と LNS 間のトンネルを介して伝送されます。LNS 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します。

トンネル
トンネルは LNS と LAC の対によって定義されます。トンネルは、LAC と LNS 間で PPP データグラムを伝送します。1 つのトンネルが多数のセ

ッションを多重化することができます。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確立、解放、および保守を制御します。

サポートされるフィーチャー

L2TP は UDP/IP を介して稼働し、次の機能をサポートします。

- 単一ユーザー・ダイヤルイン・クライアントのトンネル伝送
- 小規模ルーター (たとえば、認証ユーザーのプロファイルに基づいて単一静的ルートを確立するルーター) のトンネル伝送
- コールは、LAC から LNS へ (インバウンド)、LNS から LAC へ (アウトバウンド)、またはどちらかのピアによって (両方) 開始することができます。アウトバウンド・コールは、*固定* (常に起動) または要求に応じた L2 トンネル伝送セッションから開始できます。
- 1 つのトンネルでの複数のコール
- PAP、CHAP、および MS-CHAP のプロキシー認証
- プロキシー LCP
- プロキシー LCP が LAC で使用されない場合の LCP のリスタート
- トンネル・エンドポイント認証
- プロキシー PAP パスワードを転送するための隠し AVP
- ローカル rhelm (つまり、user@rhelm) ルックアップ・テーブルを使用したトンネル伝送
- AAA サブシステム内の PPP ユーザー名ルックアップを使用したトンネル伝送
- SNMP を使用した L2TP トンネルの管理。*プロトコルの構成と監視 解説書 第 1 巻* の『SNMP 管理』の項を参照してください。

注: Rhelm トンネル伝送では、*name@rhelm* 形式のユーザー名が必要です。この方式のトンネル伝送では、ソフトウェアは 2 つのテーブルを使用して、ダイヤルイン・ユーザーのトンネル伝送の宛先を解決する必要があります。このトンネル伝送方式の利点は、ユーザーは rhelm を定義するだけで済み、その rhelm に一致するすべてのユーザー名が同じ宛先にトンネル伝送されます。

ユーザー・ベースのトンネル伝送の場合は、1 つのテーブルで解決されます。この方式では、各ユーザーを個別に固有の宛先にトンネル伝送することができます。

- LNS 用の BRS (PPP エンドポイントとして)
- **delete interface** コマンドを使用して L2TP 装置を削除する機能
- 動的に L2TP 装置を再構成する機能
- 順序制御、待ち行列化、再送、およびフロー制御チャネルの設定。L2TP は、データ・チャネルでの順序制御も実行します。
- ユーザーが UDP ポートに基づいて IP セキュリティー・フィルターを作成できるように L2TP UDP ポートを設定する機能
- L2TP ルーター・クライアント。L2TP ルーター・クライアントは、『クライアント開始』 (自発的トンネル伝送とも呼ばれます) モデルです。この機能は、サービス提供者のトポロジーとは無関係に、保護されたトンネル伝送によるマルチプロ

トコル・バーチャル・プライベート・ネットワーク (VPN) サービスを提供します。この機能に より、クライアントと LAC を 1 つの物理ハードウェアに結集することができます。

- インバウンド・コールをリモート・ホスト名に照合して、該当するインターフェースに接続。リモート・ホスト名が、ホスト名照合用に構成されたインターフェースのどれにも一致しない場合、そのコールはリモート・ホスト名照合を使用しないインバウンド・インターフェース上で終了します。

  注: 同じ LAC と LNS の対に対して複数のネット・マッピングを構成した場合、各マッピングにつき 1 つだけトンネルが存在することを確認してください。

- リモート・ホスト名照合を使用しないインバウンド・ネットの自動 IP、IPX、およびブリッジング構成。リモート・ホスト名照合を使用するアウトバウンド・ネットおよびインバウンド・ネットは、手動で構成する必要があります。

その他のサポートされているレイヤー 2 トンネル伝送プロトコルには、次のものがあります。

- L2F。NAS 機能とゲートウェイ機能の両方がサポートされます。
- PPTP。ルーター・クライアント、PAC (PPTP アクセス集線装置)、および PNS (PPTP ネットワーク・サーバー) がサポートされます。

L2F は、L2TP をサポートしないネットワーク装置に接続する場合に相互運用可能なレイヤー 2 トンネル伝送を提供します。

PPTP は、L2TP をサポートしないネットワーク装置に接続する場合に相互運用可能なレイヤー 2 トンネル伝送を提供します。特に PPTP は、Microsoft Windows 95 (DUN 1.2 およびそれ以降)、Windows 98、および Windows NT から IBM ルーターへの VPN サービスに使用できます。

注: レイヤー 2 トンネル伝送フィーチャーでは、L2F と PPTP の両方が構成されます。

タイミングに関する考慮事項

ルーティング・ネットワークを介した PPP パケットのトンネル伝送は、その性質上、タイミングに関するいくつかの問題を考慮する必要があります。L2TP では、LAC と LNS の間の接続には、トンネル伝送のピアがタイムアウトになるほどの遅延はないものと想定しています。ピア間の待ち時間が PPP 状態遷移タイムアウト (通常は 3 秒) に達したり、それを超える状態が繰り返される場合は、接続性が妨げられる可能性があります。LAC と LNS 間の待ち時間がこのように悪い場合、接続全般が悪い状況になり、PPP 状態遷移を人為的に活動状態に維持しても、適正が接続が得られなくなります。接続の両側に PPP タイムアウトを延長する機能が備わっている場合は、これを使用すると、接続が非常に悪い状況でも接続できることがあります。

待ち時間の他に、LAC/LNS のペアと LAC/クライアントのペアの間の帯域幅の不一致も問題の原因になることがあります。たとえば、LAC と LNS の実際の帯域幅が PPP クライアントの帯域幅を大きく下回っている場合、LAC は LNS にパケットを送信するのに長時間かかる可能性があります。一方、LNS と LNS ホーム・ネット

ワーク上のホストとの間の接続が、ダイヤルイン・クライアントに比べて極端に速い場合、LNS は LAC にデータを送信するのに過剰な負担がかかる可能性があります。

LCP に関する考慮事項

プロキシー LCP を使用している場合、LAC が LCP とネゴシエーションし、PPP は LNS で処理を継続します。LAC は LCP オプションを LNS に転送するので、LNS はネゴシエーションの結果を知ることができます。LNS は、クライアントと LAC 間でネゴシエーションされるパラメーターに対して柔軟であることが必要です。LNS に受け入れられないパラメーターがあった場合、L2TP はトンネルを介してクライアントに *LCP 構成要求* を送って LCP と再ネゴシエーションします。

LNS が柔軟性を保つという要件は、MRU については特に重要です。IBM LNS では、構成された MRU は、プロキシー LCP に許容される最大値です。LAC からのプロキシー LCP メッセージの値が、LNS に構成された MRU 値より大きい場合、L2TP は LCP と再ネゴシエーションして、LAC からの他の LCP オプションは変更せずに、MRU を構成された MRU 値に等しくしようと試みます。

レイヤー 2 トンネル伝送の構成

L2T を構成するには、次のようにします。

1. **feature** コマンドを使用して、レイヤー 2 トンネル伝送フィーチャーにアクセスする。

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. 必要に応じて、L2TP、L2F、および PPTP を使用可能にする。

```
Layer-2-Tunneling config> enable L2TP

Layer-2-Tunneling config> enable L2F

Layer-2-Tunneling config>  enable pptp
```

3. 必要な L2T ネットワークを追加する。LAC、L2F NAS、または PPTP PAC に限定される場合は、L2T ネットワークを追加する必要はありません。同時トンネル伝送 PPP 接続ごとに L2T ネットを 1 つ定義してください。

```
Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 10
Add unnumbered IP addresses for each L2 net? [Yes]: yes
Adding device as interface 31
Defaulting Data-link protocol to PPP
Adding device as interface 32
Defaulting Data-link protocol to PPP
Adding device as interface 33
Defaulting Data-link protocol to PPP
Adding device as interface 34
Defaulting Data-link protocol to PPP
Adding device as interface 35
Defaulting Data-link protocol to PPP
Adding device as interface 36
Defaulting Data-link protocol to PPP
Adding device as interface 37
Defaulting Data-link protocol to PPP
Adding device as interface 38
Defaulting Data-link protocol to PPP
Adding device as interface 39
Defaulting Data-link protocol to PPP
Adding device as interface 40
Defaulting Data-link protocol to PPP
```

   a. L2TP、L2F、または PPTP トンネルを構成する。

AAA ローカル・リストを使用して L2TP トンネルを構成するには、次のように指定します。

```
Config>add tunnel-profile
Enter name:  []? lns.org
Tunneling Protocol? (PPTP, L2F, L2TP): L2TP
Enter local hostname: []? lac.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

      PPP user name: lns.org
      Tunnel Server: 11.0.0.1
      Hostname: lac.org

 User 'lns.org' has been added
 Config>
```

上の例を使用して、LAC 上のトンネル認証、および『user@lns.org』形式の『rhelm』トンネル伝送を構成することができます。

トンネル認証を特定の RADIUS サーバーで実行するように設定することも可能です。*フィーチャーの使用と構成* の 『認証、許可、および会計 (AAA) セキュリティーの使用』を参照してください。

LNS を構成しようとしており、LAC と LNS の両方でトンネル認証が使用不可になっている場合は、トンネル・プロファイルを構成する必要はありません。

AAA ローカル・リストまたは RADIUS を使用して、LAC 上の PPP ユーザー名に基づいてトンネル伝送する場合は、次のように指定します。

```
Config>add ppp-user
Enter name:  []? peter
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No):[Yes]
Will 'peter' be tunneled? (Yes, No): [No] Y
Tunneling Protocol (PPTP, L2F, L2TP): [L2TP] L2TP
Enter local hostname: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

     PPP user name: peter
     Tunnel Server: 11.0.0.1
     Hostname: lac.org

Is information correct? (Yes, No, Quit): [Yes]

User 'peter' has been added
Config>
```

b. インバウンド・トンネルのリモート・ホスト名照合を構成します (必要な場合)。

クライアント・ダイヤルイン・シナリオの場合は、このステップは、通常、必要ありません。このオプションは、接続が特定のネットを使用する必要がある場合に使用してください。

前の構成はネット 10 に対するものと想定します。

```
Config> net 10
     L2TP 10> set remote-hostname
     Remote Tunnel Hostname: [] ibm.com
```

注: リモート・ホスト名照合をオフにするには、次のコマンドを使用します。

```
Config> net 10
     L2TP 10> set any-remote-hostname
```

4. L2TP 発信コールを構成する。次の例は、IP アドレス 1.1.1.1 を持つ LAC および IP アドレス 1.1.1.2 を持つ LNS を示しています。LNS は、LAC から 5552160 へのダイヤル・オンデマンド ISDN コールを発信するように構成されています。

LNS 構成:

```
Config> add tunnel-profile
     Enter name:  []? lac.org
     Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? lns.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

            Tunnel name: lac.org
               TunnType: L2TP
               Endpoint: 1.1.1.1
               Hostname: lns.org

     User 'lac.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction outbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lac.org
     L2TP 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN)? [ISDN]
        Outbound calling address: 5552160
        Outbound calling subaddress:
     L2TP 10>
     L2TP 10> encapsulator
     PPP 10> set name vickie  a
     L2TP 10>
     L2TP 10> exit
     Config> add ppp-user larry  b
```

注:

a. LNS 装置が認証される場合は、認証名を設定します。この例には示されていない追加のプロンプトが出されます。詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の “ポイントツーポイント・プロトコル・インターフェースの使用” の章の 『PPP 認証の構成』の項を参照してください。

b. LNS で認証されるユーザーを追加します。この例には示されていない追加のプロンプトが出されます。コマンド構文およびオプションについては、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*の “CONFIG プロセス (CONFIG - Talk 6) およびコマンド” の章の Add の項を参照してください。

LAC 構成:

```
Config> add tunnel-profile
     Enter name:  []? lns.org
     Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? lac.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

            Tunnel name: lns.org
```

```
                TunnType: L2TP
                Endpoint: 1.1.1.1
                Hostname: lac.org

     User 'lns.org' has been added
     Config>
     Config> add dev dial-in a
```

注: 物理的にコールするのに使用されます。

5. L2T ルーター・クライアントを構成する。次の例は、L2TP ルーター・クライアント機能を使用した L2TPボックス・ボックス接続を示しています。この接続は単方向に設定され、要求に応じて設定されます。

クライアント構成 :

```
Config> add tunnel-profile
     Enter name:  []? lns.org
     Tunnel Protocol? (PPTP, L2T, L2TP): [L2TP]
     Enter local hostname: []? client.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

            Tunnel name: lns.org
               TunnType: L2TP
               Endpoint: 1.1.1.1
               Hostname: client.org

     User 'lns.org' has been added
     Config>
     Config> add dev layer-2-tunneling
     Config> net 10
     L2TP 10> set connection-direction outbound
     L2TP 10> set idle 30
     L2TP 10> set remote-hostname lns.org
     L2TP 10> encapsulator
     PPP 10> set name donald  a
     PPP 10> exit
     L2TP 10> exit
     Config>
```

注: クライアント装置が認証される場合は認証名を設定します。この例には示されていない追加のプロンプトが出されます。詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の『PPP 認証の構成』を参照してください。

.

LNS 構成:

```
Config> add tunnel-profile
     Enter name:  []? client.org
     Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
     Enter local hostname: []? lns.org
     set shared secret? (Yes, No): [No] Y
     Shared secret for tunnel authentication:
     Enter again to verify:
     Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

            Tunnel name: client.org
               TunnType: L2TP
               Endpoint: 1.1.1.2
               Hostname: lns.org
```

```
User 'client.org' has been added
Config>
Config> add dev layer-2-tunneling
Config> net 10
L2TP 10> set connection-direction inbound
L2TP 10> set remote-hostname client.org
Config>
Config> add ppp-user donald b
Config>
```

注: b-- LNS で認証されるユーザーを追加します。この例には示されていない追加のプロンプトが出されます。詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の 『**add** 構成コマンド』の項を参照してください。

6. **set** コマンドおよび **enable** コマンドを使用して各種のフィーチャー L2T パラメーターを構成する (必要な場合)。

```
Layer-2-Tunneling Config> set ?
Layer-2-Tunneling Config>enable ?
```

7. encapsulator コマンドを使用して、インバウンドおよび *any* インバウンド・トンネル・ホスト名に設定されているすべての L2 ネットの PPP パラメーターを構成する (必要な場合)。

```
Layer-2-Tunneling Config> encapsulator
PPP-L2TP Config>
```

PPP の構成が完了したら、**exit** を押して、L2T 構成環境に戻ります。

第28章 レイヤー 2 トンネル伝送プロトコルの構成と監視

この章では、レイヤー 2 トンネル伝送 (L2T) 構成および作動可能コマンドについて説明します。 L2T には、レイヤー 2 トンネル伝送プロトコル (L2TP)、レイヤー 2 転送プロトコル (L2F)、およびポイントツーポイント・トンネル伝送プロトコル (PPTP) があります。この章には、次の内容が記載されています。

L2T インターフェース構成プロンプトへのアクセス

L2T インターフェース構成プロンプトにアクセスするには、次のように行います。

1. OPCON (*) プロンプトで **talk 6** と入力する。
2. `Config>` プロンプトで **add dev layer-2-tunneling** と入力する (あるいは **add l2-nets** コマンドを使用する。498ページの『Add』 を参照)。
3. `Config>` プロンプトで **n** *interface#* と入力する。

```
Config> add device layer-2-tunneling
Enter the number of Layer-2-Tunneling interfaces [1]
Adding device as interface 8
Defaulting Data-link protocol to PPP
Config> n 8
Session configuration
L2T config:   8>
```

L2 トンネル伝送インターフェース構成コマンド

表57 は、L2T インターフェース構成コマンドを要約しています。これらのコマンドは、`L2T Config n>` プロンプトで入力します (この場合、*n* はネット番号です)。

表 57. L2 トンネル伝送インターフェース構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Disable	発信コールを使用不可にします。
Enable	発信コールを使用可能にします。
Encapsulator	L2T インターフェースの PPP パラメーターを構成できるようにします。 **注:** encapsulator オプションは、インターフェースでリモート・ホスト名が構成されている場合にだけ使用できます。
List	L2T インターフェースに関する情報を表示します。
Set	各種の L2T インターフェース・パラメーターを設定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。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Disable

disable コマンドは、L2TP アクセス集線装置 (LAC) からのアウトバウンド・コールを使用不可にするのに使用します。

構文:

disable outbound-calls-from-lac

outbound-calls-from-lac

LNS が L2TP トンネルを通じて LAC からダイヤル信号を開始できないようにします。

Enable

enable コマンドは、L2TP アクセス集線装置 (LAC) からのアウトバウンド・コールを使用可能にするのに使用します。このコマンドは、L2TP でだけ使用してください。

構文:

enable outbound-calls-from-lac

outbound-calls-from-lac

LNS が L2TP トンネルを通じて LAC からダイヤル信号を開始できるようにします。

例:

```
L2T 10> enable outbound-call-from-lac
        Outbound Call Type (ISDN)? [ISDN]
        Outbound calling address: 1234
        Outbound calling subaddress:
L2T 10>
```

Encapsulator

encapsulator コマンドは、L2T インターフェースの PPP パラメーターを構成するのに使用します。

構文:

encapsulator

このコマンドは、リモート・ホスト名が構成されている場合にだけ使用できます。ppp-L2tp config>プロンプトで使用できるコマンドのリストについては、501ページの『Encapsulator』を参照してください。

List

list コマンドは、各種の L2T インターフェース構成パラメーターの状態を表示するのに使用します。

構文:

list

```
Layer-2-Tunneling Config>list
CONNECTION TYPE
---------- -----
  Connection Direction            INBOUND
  Remote Tunnel Hostname           *ANY*
```

Set

set コマンドは、L2T インターフェース稼働パラメーターを構成するのに使用します。

構文:

set
- any-remote-hostname
- connection-direction
- idle
- remote-hostname

any-remote-hostname

このネット上のアウトバウンド・リモート・ホスト名を消去し、インバウンド・リモート・ホスト名照合を使用不可にします。

connection-direction [inbound] or [outbound] or [both]

接続を開始できるのは、このネット上のピア (インバウンド)、ローカル装置 (アウトバウンド)、あるいはピアまたはローカル装置のどちらか (両方) を指定します。「両方」を指定した場合は、アイドル時間をゼロに指定することはできません。

デフォルト値 : インバウンド

idle-time *seconds*

L2 トンネル伝送がこのネット上のトンネル・セッションを切断する前に非活動状態になっている秒数を指定します。値ゼロは、そのトンネルは固定であり、切断してはならないことを示します。

有効範囲 : 0 〜 1024

デフォルト値 : 0

remote-hostname *hostname*

ピアのトンネル・ホスト名を指定します。

アウトバウンド・トンネルの場合、ホスト名は AAA サブシステム内に構成されたトンネル・プロファイルを指定します。これは、ピアが自らを識別するのに使用するトンネル・ホスト名でなければなりません。

インバウンド・トンネルの場合、このホスト名で自らを識別するトンネルのピアだけがこのインターフェースに接続できます。

有効値 : 1 〜 64 桁の ASCII 文字から成る任意の名前

デフォルト値 : *Name*

L2 トンネル伝送フィーチャー構成プロンプトへのアクセス

L2 トンネル伝送フィーチャー構成プロンプトにアクセスするには、次のように行います。

1. OPCON (*) プロンプトで **talk 6** と入力する。
2. `Config>` プロンプトで **feature layer-2-tunneling** と入力する。

L2 トンネル伝送インターフェース構成コマンド

表58 は、L2 トンネル伝送フィーチャー構成コマンドの要約を示し、ここでの残りの部分で、これらのコマンドについて説明します。これらのコマンドは、`Layer-2-Tunneling Config>` プロンプトで入力します。

表 58. L2 トンネル伝送フィーチャー構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add	L2 トンネル伝送ネットおよびピアを追加します。
Disable	L2 トンネル伝送機能を使用不可にします。
Enable	L2 トンネル伝送機能を使用可能にします。
Encapsulator	リモート・ホスト名 (ANY) で構成されていないすべての L2 トンネル伝送ネットの PPP パラメーターを構成できるようにします。
List	L2 トンネル伝送構成に関する情報を表示します。
Set	バッファー、コール受信ウィンドウ、およびその他の L2 トンネル伝送パラメーターを設定できるようにします。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Add

add コマンドは、L2 ネットを追加するのに使用します。このルーターで終端する各並行 PPP セッションごとに 1 つの L2 ネットが必要です。トンネル伝送 PPP セッションの終端は、トンネルの LNS エンドポイントです。

構文:

add L2-nets

L2-nets

注: このコマンドは、すべて小文字で入力できます。分かりやすくするために、最初の文字は大文字で示してあります。

L2 ネットを L2 トンネル伝送構成に追加します。このルーターで転送される各並行 PPP セッションごとに 1 つの L2 ネットが必要です。このルーターを LAC としてだけ使用する場合は、バーチャル L2 ネットは必要ありません。このコマンドを入力すると、追加するネットの数および各 L2 ネットの無番号 IP アドレスを追加するかどうかを尋ねるプロンプトが出ます。

追加するネットの数は、今回自動的に追加されるネットの数を指しています。これらのネットは、既存の L2 ネットに追加されます。

各 L2 ネットの無番号 IP アドレスを追加すると、各 L2 ネットの IP ルーティング・テーブルに無番号 IP エントリーが自動的に追加されます。無番号 IP アドレスは、推奨されている運用方式です。L2 ネットで番号アドレスを使用する必要がある場合は、IP プロトコル構成環境で変更することができます (*プロトコルの構成と監視 解説書 第 1 巻* の 『IP の構成』の章を参照してください)。

Disable

disable コマンドは、L2 トンネル伝送機能を使用不可にするのに使用します。

構文:

disable	fixed-ip-source-address
	fixed-udp-source-port
	force-chap-challenge
	hiding-for-pap-attributes
	L2f
	L2tp
	pptp
	proxy-auth
	proxy-lcp
	sequencing
	tunnel-auth

fixed-ip-source-address
指定した発信元アドレスをルーターが使用不可にします。

fixed-udp-source-port
固定 UDP ポートの使用をクリアします。このパラメーターを使用不可にした場合、ユーザーは LAC と LNS の間に IP アドレスによる IP セキュリティー・フィルターを構成することを強制されます。

force-chap-challenge
クライアントの LNS CHAP 再チャレンジを使用不可にします。PPP クライアントによる CHAP 再チャレンジが困難な場合、CHAP 再チャレンジを使用不可にすることが必要になります。

hiding-for-pap-attributes
LAC と LNS の間のプロキシー PAP 情報の暗号化を使用不可にします。

L2f このルーター上の L2F プロトコルを使用不可にします。

L2tp このルーター上の L2TP プロトコルを使用不可にします。

pptp このルーター上の PPTP プロトコルを使用不可にします。

proxy-auth
LAC からLNS へ PPP プロキシー認証を送信するのを使用不可にします。

proxy-lcp
LAC からLNS へ LCP 情報を送信するのを使用不可にします。

sequencing
データ・チャネルでの順序制御を使用不可にします。

tunnel-auth
このルーターに共有の機密に基づくピアの認証を使用不可にします。

Enable

enable コマンドは、L2 トンネル伝送機能を使用可能にするのに使用します。

構文:

enable
- fixed-ip-source-address
- fixed-udp-source-port
- force-chap-challenge
- hiding-for-pap-attributes
- L2f
- L2tp
- pptp
- proxy-auth
- proxy-lcp
- sequencing
- tunnel-auth

fixed-ip-source-address
インバウンド宛先アドレスと同じ発信元アドレスを用いてルーターが応答します。

fixed-udp-source-port
このパラメーターを使用可能にすると、L2 に対して UDP ポートに基づく IP セキュリティー・フィルターを構成することが可能になり、L2 トラフィックの暗号化または認証を容易に行うことができます。L2TP について 1701 で UDP ポートを設定します。

force-chap-challenge
LNS がプロキシー CHAP を受信する場合も、クライアントの LNS CHAP 再チャレンジを使用可能にします。クライアントがこのような再チャレンジを問題なく扱えることが分かっている場合には、セキュリティーの観点から、これを使用可能にすることが望まれます。

hiding-for-pap-attributes
LAC と LNS の間のプロキシー PAP 情報の暗号化を使用可能にします。

L2f このルーター上の L2F を使用可能にします。

L2tp このルーター上の L2TP を使用可能にします。

pptp このルーター上の PPTP を使用可能にします。

proxy-auth
LAC からLNS へ PPP プロキシー認証を送信するのを使用可能にします。

proxy-lcp
LAC からLNS へ LCP 情報を送信するのを使用可能にします。

sequencing
データ・チャネルでの順序制御を使用可能にします。

tunnel-auth
このルーターに共有の機密に基づくピアの認証を使用可能にします。

Encapsulator

encapsulator コマンドは、インバウンドおよび *any* リモート・ホスト名として構成されたすべてのレイヤー 2 トンネル伝送インターフェースの PPP パラメーターを構成するために ppp-L2tp config> プロンプトにアクセスするのに使用します。

構文:

encapsulator

List

list コマンドは、各種の L2 トンネル伝送構成パラメーターの状態を表示するのに使用します。

構文:

list

```
Layer-2-Tunneling Config>list
GENERAL ADMINISTRATION
------- --------------
  L2TP                                = Enabled
  L2F                                 = Disabled
  PPTP                                = Disabled
  Maximum number of tunnels           = 20
  Maximum number of calls (total)     = 50
  Buffers Requested                   = 300

CONTROL CHANNEL SETTINGS
------- ------- --------
  Tunnel Auth                         = Enabled
  Tunnel Rcv Window                   = 4
  Retransmit Retries                  = 6
  Local Hostname                      = Host6

DATA CHANNEL SETTINGS
---- ------- --------
  Force CHAP Challenge (extra security)= Disabled
  Hiding for PAP Attributes           = Disabled
  Hardware Error Polling Period (Sec)  = 120
  Sequencing                          = Enabled

MISCELLANEOUS
-------------
  SEND PROXY-LCP FROM LAC             = Enabled
  SEND PROXY-AUTH FROM LAC            = Enabled
  Fixed UDP Source Port (1701)        = Enabled
  Fixed Source IP Address             = Enabled
```

Set

set コマンドは、L2 トンネル伝送稼働パラメーターを構成するのに使用します。

構文:

set buffers

error-check-direction

host-lookup-password

local-hostname

max-calls

max-tunnels

transmit-retries

tunnel-rcv-window

buffers

要求された内部 L2 トンネル伝送バッファーの数を指定します。要求を満たすのに十分なメモリーがない場合、リブートするとバッファーの一部分が利用可能になります。L2T が活動状態のときにメモリーの量を確認するには、**memory** コマンドを使用します (506ページの『Memory』を参照)。

有効範囲: 1 〜 4000

デフォルト値: 900

error-check-period [seconds]

LAC のハードウェア・エラー・ポーリング期間を指定します。各ポーリング期間ごとに、WAN エラー通知メッセージが LAC から LNS に送信されます。期間の範囲は、60 〜 65 000 秒です。

デフォルト値 : 120 秒。

host-lookup-password

RADIUS トンネル許可に共有の機密を指定します。これは、サーバー上で設定された機密と一致するものでなければなりません。

デフォルト値 : なし。

local-hostname

トンネル・セットアップ・メッセージに入れて送信されるローカル・ルーターを識別するホスト名ストリングを指定します。

デフォルト値 : IBM

max-calls

LAC または LNS として同時に活動状態にできる、すべてのトンネルを通るコールの最大数を指定します。

有効範囲: 1 〜 2500

デフォルト値: 300

max-tunnels

LAC または LNS として同時に活動状態にできるトンネルの最大数を指定します。

有効範囲: 1 〜 2500

デフォルト値: 300

transmit-retries

セッションまたはトンネルが非活動状態として宣言されて遮断される前に、制御チャネル上で L2TP パケットが再送される回数を指定します。

有効範囲 : 2 ～ 100

デフォルト値 : 6

tunnel-rcv-window

高信頼制御接続トランスポートの L2TP 受信ウィンドウ・サイズを指定します。このトランスポートでは、トンネルまたはセッションの設定、切断、および保守のために必要なメッセージを送受信します。

有効範囲 : 1 ～ 100

デフォルト値 : 4

L2 トンネル伝送監視プロンプトへのアクセス

L2 トンネル伝送監視プロンプトにアクセスするには、次のように行います。

1. OPCON (*) プロンプトで **talk 5** と入力する。
2. GWCON (+) プロンプトで **feature layer-2-tunneling** コマンドを入力する。

L2 トンネル伝送監視コマンド

ここでは、L2 トンネル伝送監視コマンドの要約を示し、個々のコマンドについて説明します。コマンドは `Layer-2-Tunneling Console>` プロンプトで入力します。

表59 は、L2 トンネル伝送監視コマンドの要約を示しています。

表 59. L2 トンネル伝送監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Call	コール設定中の各コールに関する統計と情報を表示します。
Kill	トンネルを即時に終了します。
Memory	現在の L2 トンネル伝送バッファー割り振りと使用状況を表示します。
Start	別のピアとのトンネル伝送を開始します。
Stop	トンネルを停止し、各ピアが必要な管理を実行できるようにします。
Tunnel	既存の各トンネルに関する統計と情報を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Call

call コマンドは、コールの統計と情報を表示するのに使用します。

構文:

call

- errors
- physical-errors
- queue
- state
- statistics

errors このコールで発生した一般的な伝送エラーを表示します。

例:

```
Layer-2-Tunneling Console> call errors
CallID │ Serial # │ ACK-timeout │ Dropped pkts
 56744 │        1 │           0 │            0
```

CallID このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

ACK-timeout
ピアからタイムアウト通知を受信した回数

Dropped pkts
このコールで紛失を宣言されたパケットの数。これは、受信するはずであったが、ピアによって紛失として通知されたパケットです。

physical-errors
コールで発生したデータ・エラーを表示します。

例:

```
Layer-2-Tunneling Console>  call physical-errors
CallID │ Serial# │ CRC    │framing│   HW    │ buffer│timeout│ align-│ time since
       │         │ Errors │ Errors│overrun│overrun│ Errors│ ment  │ updated
 56744 │       1 │      0 │      0 │      0 │      0 │      0 │     0 │
```

CallID このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

CRC Errors
CRC が一致しなかったパケットの数

framing errors
フレーム・エラーを含むパケットの数

HW overrun
ハードウェア・オーバーランが発生した回数

buffer overrun
バッファー・オーバーランが発生した回数

timeout errors
インターフェースがタイムアウトになった回数

alignment
配列エラーが発生した回数

time since updated
前回のエラーのポーリングからの経過時間

queue 各コールの待ち行列に関する情報を表示します。

例:

```
Layer-2-Tunneling Console>  call queue
CallID │ Serial # │Tx Win│Rx Win│    Ns    │    Nr    │Rx Q│Tx Q│priority│ out Q
 56744 │        1 │    4 │    4 │      100 │      200 │  0 │  0 │      0 │     0
```

CallID このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

Tx Win
ピアのデータの最大受信ウィンドウ

Rx Win
ローカル最大送信ウィンドウ

Ns このコールで送信される次のパケット・シーケンス番号

Nr このコールで受信が期待されている次のパケット・シーケンス番号

Rx Q 受信待ち行列の現在のパケット数

Tx Q 送信待ち行列の現在のパケット数

priority
L2TP による送信を待っている優先順位 PPP パケットの数

out Q L2TP による送信を待っている通常の PPP パケットの数

state 各コールの現在の状態を表示します。

例:

```
Layer-2-Tunneling Console>  call state
CallID │ Serial # │ Net #  │    State     │ Time Since Chg │ PeerID │ TunnelID
 56744 │       1  │    2   │ Established  │   00:00:00     │  345   │ 45678
```

CallID このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

Net # このコールに対応する装置番号。LNS のコールの場合、これは L2 ネットです。LAC のコールの場合、これは最初のコールを受信した PPP 装置です。

State 現在のコールの状態。有効なコールの状態は、次のとおりです。

Established
トンネル・ネットワーク・トラフィックの伝送準備完了。

Idle コールはアイドル状態です。

Wait Cs Answer
通信リンクがオープンするのを待っています。

Wait Reply
ピアからの応答を待っています。

Wait Tunnel
トンネルの確立を待っています。

Time since chg
前回の状態変更からの経過時間

PeerID
ピアのコール ID

TunnelID
このコールに対応するローカル・トンネル

statistics
各コールのデータ伝送に関する統計を表示します。

例:

```
Layer-2-Tunneling Console> call statistics
CallID │ Serial # │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │ ATO
 56744 │        1 │      34 │     1056 │      45 │     1567 │   10  │ 34
```

CallID このコールに対応するローカル識別子

Serial #
このコールをログに記録するのに使用された番号

Tx Pkts
このコールの送信されたパケット数

Tx Bytes
このコールの送信されたバイト数

Rx Pkts
このコールの受信されたパケット数

Rx Bytes
このコールの受信されたバイト数

RTT このコールの現行の算定一巡時間

ATO このコールの現行の算定適応タイムアウト

Kill

kill は、トンネルを即時に終了するのに使用します。このコマンドは、トンネルのすべてのローカル資源を解放して、強制的に接続を終了させます。トンネルの終了はピアに通知されません。

注: このコマンドを使用するのは、**stop** コマンドではトンネルを終了させることができない場合だけに限ってください。

構文:

kill tunnel *tunnelid*

tunnel *tunnelid*
終了させるトンネルを指定します。

Memory

memory コマンドは、L2TP の現在のメモリーの使用状況を表示するのに使用します。

構文:

memory

例:

```
Layer-2-Tunneling Console>  mem
Number of layer-2-tunneling buffers: Requested = 2000, Total = 1200, Free = 1000
```

この例では、ユーザーは 2000 のバッファーを構成しましたが、1200 しか割り当てることができませんでした。現在、200 のバッファーが使用中で、1000 が空いています。

Start

start コマンドは、別のピアとのトンネル伝送を開始するのに使用します。

構文:

start　　**tunnel** *hostname*

(hostname を要求してプロンプト指示を出すパラメーターはない)

tunnel*hostname*
L2T がトンネルを確立する相手のホストの名前

Stop

stop コマンドは、トンネル伝送を停止するのに使用します。トンネルを終了する前に、必要な終結処置を完了させます。

構文:

stop　　tunnel *tunnelid*

tunnel *tunnelid*
終了させるトンネルを指定します。

Tunnel

tunnel コマンドは、すべてのトンネルに関する統計と情報を表示するのに使用します。

構文:

tunnel　　call
errors
peer
queue
state
statistics
transport

calls すべてのトンネルと、各トンネル内の各コールの状態を表示します。

errors トンネル上で発生したエラーを表示します。

例:

```
Layer-2-Tunneling Console> tunnel errors
Tunnel ID │ Type │ACK-timeouts
 96785    │ L2TP │    0
 43690    │ PPTP │    2
 96785    │ L2F  │    0
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用されるトンネル伝送プロトコルのタイプ

ACK-timeouts
ピアからタイムアウト通知を受信した回数

peer トンネルとそのトンネルに対応するピアを表示します。

例:

```
Layer-2-Tunneling Console> tunnel peer
Tunnel ID │ Type │ Peer ID │ Peer Hostname
 96785    │ L2TP │   89777 │ peer1
 11264    │ L2F  │   46538 │ peer2
 34653    │ L2F  │   11209 │ peer3
 87511    │ PPTP │   55377 │ peer4
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用されるトンネル伝送プロトコルのタイプ

Peer ID
このトンネルに割り当てられたピアのトンネル識別子

Peer Hostname
ローカル・データベースに表示されるピアのホスト名

queue 各トンネルの待ち行列に関する情報を表示します。

例:

```
Layer-2-Tunneling Console> tunnel queue
Tunnel ID │ Type │ Rx Win │ Tx Win │   Ns   │   Nr   │ Rx Q │ Tx Q
 96785    │ L2TP │      4 │      4 │      5 │      6 │    0 │    0
 76488    │ L2F  │      4 │      4 │      5 │      6 │    0 │    0
 22209    │ PPTP │      4 │      4 │      5 │      6 │    0 │    0
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用されるトンネル伝送プロトコルのタイプ

Rx Win
ローカルの受信ウィンドウを構成するパケットの最大数

Tx Win
ピアの受信ウィンドウを構成するパケットの最大数

Ns 送信する次のパケットのシーケンス番号

Nr 受信する次のパケットのシーケンス番号

Rx Q 現在受信待ち行列にあるパケットの数

Tx Q 現在送信待ち行列にあるパケットの数

state すべてのトンネルの現在の状態を表示します。

例:

```
Layer-2-Tunneling Console> tunnel state
Tunnel ID │ Type │ Peer ID │    State    │ Time Since Chg │ # Calls │ Flags
 17404    │ PPTP │  0      │ Established │   00:00:00     │      1  │  0
 96785    │ L2TP │  0      │ Established │   00:02:05     │      2  │  0
 38237    │ L2F  │  0      │ Established │   00:00:00     │      1  │  0
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用されるトンネル伝送プロトコルのタイプ

Peer ID
このトンネルに割り当てられたピアのトンネル識別子

State 現在のトンネルの状態。有効なトンネル状態は、次のとおりです。

Established
トンネルは確立されました。

Idle トンネルはアイドル状態です。

Wait Ctrl Reply
ホストはピアからの応答を待っています。

Wait Ctrl Conn
ホストはピアからの接続標識を待っています。

Time since chg
前回の状態変更からの経過時間

 # Calls
このトンネル上の活動状態のコールの数

Flags このトンネル上の接続メッセージを制御するのに使用されたフラグ

statistics
トンネルに関連する統計を表示します。

例:

```
Layer-2-Tunneling Console> tunnel statistics
Tunnel ID │ Type │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │ ATO
 96785    │ L2TP │      4  │      78  │      5  │     89   │    10 │ 31
 96366    │ L2F  │   9344  │   34578  │    305  │   4300   │    10 │ 31
 12344    │ PPTP │     24  │     478  │    115  │    2745  │    10 │ 31
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用されるトンネル伝送プロトコルのタイプ

Tx Pkts
送信されたパケット数

Tx Bytes
送信されたバイト数

Rx Pkts
受信されたパケット数

Rx Bytes
受信されたバイト数

RTT トンネル制御接続メッセージの現行の算定一巡時間

ATO トンネル制御接続メッセージの現行の算定適応タイムアウト

transport
トンネルに関する UDP 情報を表示します。

例:

```
Layer-2-Tunneling Console>  tunnel transport
Tunnel ID │ Type │ Peer IP Address │ UDP Src │ UDP Dest
 96785    │ L2TP │  11.0.0.102     │  1056   │   1089
 30000    │ L2F  │  11.0.0.104     │  1058   │   1090
 45772    │ PPTP │  11.4.4.027     │  1345   │   1020
```

Tunnel ID
このコールに対応するローカル識別子

Type 使用されるトンネル伝送プロトコルのタイプ

Peer IP address
このトンネルのピアの IP アドレス

UDP Src
このトンネルの UDP 発信元ポート

UDP Dest
このトンネルの UDP 宛先ポート

L2 トンネル伝送動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

レイヤー 2 トンネル伝送は、CONFIG (Talk 6) **delete interface** コマンドを制限なしでサポートします。

GWCON (Talk 5) Activate Interface

レイヤー 2 トンネル伝送は、GWCON (Talk 5) **activate interface** コマンドをサポートしますが、次の考慮が必要です。

他の PPP インターフェースについて追加の制限事項はありません。

すべてのレイヤー 2 トンネル伝送の構成変更は、以下を除いて自動的に活動化されます。

GWCON (Talk 5) activate interface コマンドによって変更が活動化されないコマンド
CONFIG, net, enable ccp **注:** 圧縮は、これが CCP を使用可能にした最初の PPP ネットである場合に、使用可能になりません。
CONFIG, net, set lcp options (mru option) **注:** MRU 値は、リブート時にルーターに割り振られたバッファー・サイズより大きく設定されません。

GWCON (Talk 5) Reset Interface

レイヤー 2 トンネル伝送は、GWCON (Talk 5) **reset interface** コマンドをサポートしますが、次の考慮が必要です。

他の PPP インターフェースについて追加の制限事項はありません。

すべてのレイヤー 2 トンネル伝送の構成変更は、以下を除いて自動的に活動化されます。

GWCON (Talk 5) reset interface コマンドによって変更が活動化されないコマンド
CONFIG, net, enable ccp **注:** 圧縮は、これが CCP を使用可能にした最初の PPP ネットである場合に、使用可能になりません。

CONFIG, net, set lcp options (mru option) **注:** MRU 値は、リブート時に PPP インターフェースに割り振られたバッファー・サイズより大きく設定されません。

CONFIG (Talk 6) 即時変更コマンド

レイヤー 2 トンネル伝送は、装置の操作状態を即時に変更する、次の CONFIG コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行する場合には、保管されて保存されます。

コマンド
CONFIG, feature layer-2-tunneling, disable fixed-ip-source-address
CONFIG, feature layer-2-tunneling, disable fixed-udp-source-port
CONFIG, feature layer-2-tunneling, disable force-chap-challenge
CONFIG, feature layer-2-tunneling, disable hiding-for-pap-attributes
CONFIG, feature layer-2-tunneling, disable proxy-auth
CONFIG, feature layer-2-tunneling, disable proxy-lcp
CONFIG, feature layer-2-tunneling, disable sequencing
CONFIG, feature layer-2-tunneling, disable tunnel-auth
CONFIG, feature layer-2-tunneling, enable fixed-ip-source-address
CONFIG, feature layer-2-tunneling, enable fixed-udp-source-port
CONFIG, feature layer-2-tunneling, enable force-chap-challenge
CONFIG, feature layer-2-tunneling, enable hiding-for-pap-attributes
CONFIG, feature layer-2-tunneling, enable proxy-auth
CONFIG, feature layer-2-tunneling, enable proxy-lcp
CONFIG, feature layer-2-tunneling, enable sequencing
CONFIG, feature layer-2-tunneling, enable tunnel-auth
CONFIG, feature layer-2-tunneling, set error-check-period
CONFIG, feature layer-2-tunneling, set host-lookup-password
CONFIG, feature layer-2-tunneling, set local-hostname
CONFIG, feature layer-2-tunneling, set transmit-retries
CONFIG, feature layer-2-tunneling, set tunnel-rcv-window
CONFIG, add tunnel-profile

非動的再構成可能コマンド

次の表には、動的に変更できないレイヤー 2 トンネル伝送の構成コマンドを記載します。これらのコマンドを活動化するには、装置を再ロードしたり、リスタートする必要があります。

L2 監視コマンド (Talk 5)

コマンド
CONFIG, feature layer-2-tunneling, enable l2f
CONFIG, feature layer-2-tunneling, enable l2tp
CONFIG, feature layer-2-tunneling, enable pptp
CONFIG, feature layer-2-tunneling, disable l2f
CONFIG, feature layer-2-tunneling, disable l2tp
CONFIG, feature layer-2-tunneling, disable pptp
CONFIG, feature layer-2-tunneling, set buffers
CONFIG, feature layer-2-tunneling, set max-calls
CONFIG, feature layer-2-tunneling, set max-tunnels

第29章 ネットワーク・アドレス変換の使用

ネットワーク・アドレス変換 (NAT) とその拡張機能であるネットワーク・アドレスおよびポート変換 (NAPT) は、組織の利用可能な IP アドレスの数を拡張することができ、公衆ネットワークのユーザーに私設ネットワークの一部のアドレスを知られるのを防止することができます。NAT では、公衆 IP アドレスを使用して私設 IP アドレスを表します。

公衆 IP アドレスとは、IP 公衆ネットワークのホストの有効なアドレスであり、公衆ネットワーク内で固有であることが必要です。公衆ネットワークがインターネットの場合、公衆 IP アドレスは、ネットワーク情報センター (NIC) によって提供される固有の IP アドレスでなければなりません。

私設アドレスはルーターには分かりますが、公衆ネットワークには分かりません。各私設ネットワーク内ではアドレスは固有であることが必要ですが、2 つの異なる私設ネットワークに同じアドレスが重複して存在しても構いません。私設アドレスは、スタブ・ネットワーク内のホストに割り当てられます。スタブ・ネットワークというのは、1 つのルーターだけを通して公衆ネットワークにアクセスできるネットワークのことです。

NAT は、いくつかの方法で、利用可能な IP アドレスを拡張します。

- 公衆アドレスを回転して使用することにより、1 つの公衆アドレスで複数の私設アドレスを表すことができる。
- アドレスの重複が可能である (重複アドレスがそれぞれ異なる私設ネットワークで使用されている場合に限られる)。
- ネットワーク管理者が、資源が限られてきている NIC アドレスの代わりに、任意の IP アドレスを私設ネットワークで使用することができる。

私設アドレスを使用すれば、アドレスを外界から隠すこともできます。NAT のこのフィーチャーは、私設アドレスが知られるのを防止するための一種のファイアウォールとしての役目を果たします。

重要: NAT を定義しているインターネット草案のセクション 5.4 に、“アプリケーション内の IP アドレス (および、NAPT の場合は、TCP/UDP ポート) を持つ (および、使用する) アプリケーションは、NAT を通すと機能しない...” と記述されています。DLSw および XTP は、エンドポイント IP アドレスに基づいて (特に、どの相手がより高いアドレスを持っているかに基づいて) 決定を下すことに注意する必要があります。NAT を通して実行されているアプリケーション (DLSw や XTP など) は、そのアドレスは私設アドレスであると考えているのに対して、他のルーター内の相手のアプリケーションは、そのアプリケーションのアドレスは公衆アドレスであると考えるので、間違った決定がなされる可能性があります。

514ページの図44 に示されている、スタブ・ネットワーク内のワークステーションの例を見てください。この例では、スタブ・ネットワークは IP アドレスが 10.33.96.0、サブネット・マスクが 255.255.255.0 の IP サブネットから構成されています。

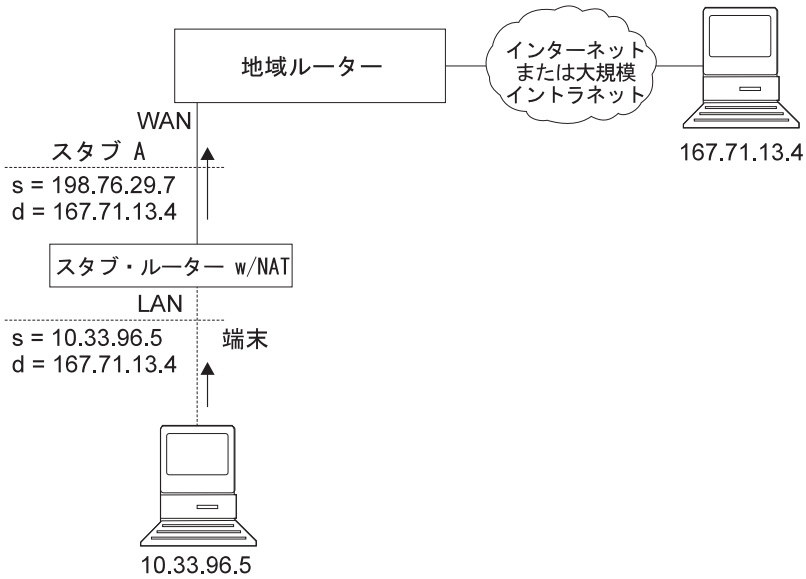


図 44. NAT を実行するネットワーク

NAT を使用するには、ネットワーク管理者は 1 つまたは複数の公衆 IP アドレスを 2216 内の公衆アドレス・プールに割り当て、私設 IP アドレスをスタブ・ネットワーク内の各ワークステーションに割り当てます。公衆 IP アドレスは *reserve pool* に割り当て、私設 IP アドレスは *translate range* に割り当てます。

NAT 機能は、最初に私設ネットワーク内のステーションの私設アドレスを公衆アドレスの 1 つに結合します。結合とは、その私設アドレスをもつパケットはすべて、パケットがアウトバウンドされるときに、その公衆 IP アドレスに変換されることを意味しています。インバウンド・パケットは、宛先として公衆 IP アドレスを持っています。NAT は公衆アドレスを認知し、それを私設 IP アドレスに変換して、パケットを転送します。トラフィックが停止した後、ユーザーが設定できるタイマーがタイムアウトになるまで、結合は維持されます。タイムアウトになった時点で、NAT は結合を終了し、その公衆アドレスを再利用できるようにします。

この例では、パケットは、発信元私設アドレス 10.33.96.5 からインターネット内の宛先アドレス 167.71.13.4 に転送されます。2216 内の NAT は、私設アドレス 10.33.96.5 を公衆アドレス 198.76.29.7 に変換します。この変換によって、私設アドレス 10.33.96.5 は公衆ネットワークから隠されるので、私設アドレス 10.33.96.5 を直接アドレス指定する着信パケットはありません。代わりに、167.71.13.4からの着信パケットは公衆アドレス 198.76.29.7 あてに送られます。NAT ルーターは 198.76.29.7 をアドレス指定したパケットを受信すると、その宛先公衆アドレスを私設アドレス 10.33.96.5 に変換し、パケットを転送します。

ネットワーク・アドレス・ポート変換

NAPT は、TCP および UDP トラフィックにだけ使用できます。NAPT では、複数の私設アドレスが 1 つの公衆アドレスを同時に使用することができます。NAT は、1 つの公衆アドレスを 1 つの私設アドレスにマップするのに対して、NAPT は、NAPT 公衆アドレス**および** 公衆ポート番号を、私設アドレスおよび私設ポート番号にマップします。各公衆アドレス・プールにつき 1 つの NAPT アドレスしか構成できません。

NAPT の構成は、NAPT トラフィックに使用する公衆アドレスを 1 つまたは動的アドレス・インターフェース (これは、公衆アドレスを取り出すのに PPP/IPCP を使用します) を 1 つ指定するだけで済みます。NAPT の利点は、公衆 IP アドレス・プールからの 1 つのアドレスが、複数の私設 IP アドレスを同時にサポートできることです。

静的アドレス・マッピング

ときには、公衆ネットワークから直接アクセスできるステーションまたはサーバーを私設ネットワーク内に構成したい場合があります。その場合は、ステーションの私設アドレスを特定の公衆アドレスに静的にマッピングする必要があります。私設アドレスから発信されるすべてのメッセージは、宛先の公衆アドレスに変換され、公衆アドレスあてのインバウンド・メッセージはすべて、対応する私設アドレスに自動的に転送されます。静的アドレス・マッピングには、NAT と NAPT の 2 種類があります。

NAT 静的アドレス・マッピング

NAT マッピングでは、すべての IP プロトコルがホストにアクセスできます。次に示すのは、NAT マッピングの構成例です。

私設アドレス	10.1.1.2
私設ポート	0
公衆 NAT アドレス	9.67.1.1
公衆ポート	0

NAPT 静的アドレス・マッピング

TCP または UDP アプリケーションを指定する場合、事前割り当てされた私設ポートを組み込んだ NAPT マッピングを指定するオプションがあります。NAPT 静的アドレス・マッピングでは、NAPT 公衆アドレスを構成する必要があります。たとえば、私設アドレス 10.1.1.1 の Telnet ホストが NAPT 公衆アドレス 9.67.1.2 を使用するように構成する場合、静的マッピングは次のように構成します。

私設アドレス	10.1.1.1
私設ポート	23
公衆 NAPT アドレス	9.67.1.2
公衆ポート	23

私設ポートと公衆ポートは、Telnet 用に事前割り当てされたポートであるポート 23 にマップされます。この管理者は、同じ私設アドレス 10.1.1.1 に FTP サーバー

(事前割り当てアドレス 21) も持っており、これを NAPT 公衆アドレス 9.67.1.2 にマップする場合、このマッピングは次のようになります。

私設アドレス	10.1.1.1
私設ポート	21
公衆 NAPT アドレス	9.67.1.2
公衆ポート	21

アドレス 10.1.1.1 のサーバーは、両方のアプリケーションに同じ NAPT 公衆アドレス (9.67.1.2) を使用していますが、NAPT は異なるポート番号 (23 と 21) を使用することによって、この 2 つを区別することができます。しかし NAPT は、2 つのサーバーが同じ NAPT 公衆アドレスを使用し、同じアプリケーションおよびポート番号を持っている場合は、それらを区別することはできません。たとえば、NAPT 公衆アドレスと事前割り当てポート番号が、10.1.1.3 ポート 21 と 10.1.1.1 ポート 21 で同じである場合、NAPT は着信 FTP トラフィックをサーバー 10.1.1.3 と 10.1.1.1 のどちらに送るのか判断できません。同じ NAPT アドレスとアプリケーションを使用するサーバーを 2 つ以上構成する場合は、サーバーの事前割り当てポート以外のポートを使用する必要があります (たとえば、FTP デーモンをポート 200 で開始するなど)。

NAT 用のパケット・フィルターおよびアクセス制御規則の設定

管理者は、NAT または NAPT によって変換される私設アドレスの範囲を識別するのに加えて、2216 内の IP 用のパケット・フィルターとアクセス制御規則も設定する必要があります。NAT 構成では、公衆ネットワークに接続されているインターフェースに、1 つのインバウンド・パケット・フィルターと 1 つのアウトバウンド・パケット・フィルターを構成することが必要です。インバウンド・パケット・フィルターに対して 1 つまたは複数のアクセス制御規則を構成し、アウトバウンド・パケット・フィルターに対しても 1 つまたは複数のアクセス制御規則を構成することも必要です。着信フィルター・アクセス制御規則は、該当する定義済み公衆アドレスをもつインバウンド・パケットを NAT にパスします。アウトバウンド・フィルター・アクセス制御規則は、該当する定義済み私設アドレスをもつアウトバウンド・パケットを NAT にパスします。

NAT に適用されるアクセス制御規則は、アクセス制御規則タイプ ***I*** (包括的) および ***N*** (NAT) を持っています。 IP アクセス制御の構成については、*プロトコルの構成と監視 解説書 第 1 巻* を参照してください。

注: NAT は、IPsec トンネルと合わせて構成することもできます。この構成の例は、438ページの『ルーター A のパケット・フィルター・アクセス制御規則の構成』 にあります。

例: IP フィルターとアクセス制御規則をもつ NAT の構成

この例は、517ページの図45 に示したネットワーク内のスタブ・ルーターの NAT を構成する方法を示しています。コマンドの説明は、521ページの『第30章 ネットワーク・アドレス変換の構成と監視』を参照してください。

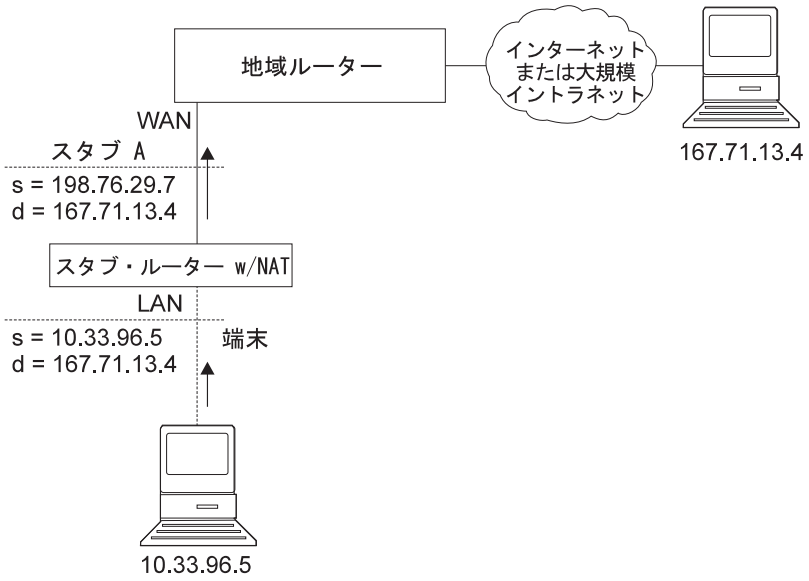


図 45. NAT を実行するネットワーク

次の手順で行います。

1. NAT および NAPT によって使用される公衆アドレスのプールを設定します。これには **reserve** コマンドを使用します。

   ```
   NAT config> reserve No 198.76.29.7 255.255.255.0 6 pool1 198.76.29.7
   NAT config> reserve No 198.76.29.15 255.255.255.0 3 pool1 0.0.0.0
   ```

   この例では、*pool1* と呼ばれるプールが設定されました。プール内の NAPT アドレスは 198.76.29.7 です。アドレス 198.76.29.13 および 198.76.29.14 は利用不能なので、プールはそれら除外するように設定されています。入力するパラメーターは *public-address*、*mask*、*number-in-group*、*name*、および *napt-address* です。NAPT アドレスの値 0.0.0.0 は、このグループ内のアドレスはどれも NAPT アドレスではないことを意味しています。プールに NAPT を構成しない場合は、すべてのグループに NAPT アドレス 0.0.0.0 を使用します。

2. **translate** コマンドを使用して、pool1 内の公衆アドレスに変換される私設アドレスの範囲を設定します。入力するパラメーターは、*private-address*、*mask*、および *name* です。

   ```
   NAT config> translate 10.33.96.0 255.255.255.0 pool1
   ```

3. 公衆アドレスの 1 つに固定的にマップする、私設ネットワーク内部のステーションの静的マッピングを設定します。次のコマンドは、公衆ネットワークから任意のタイプのトラフィックを受信するマシン (10.33.96.5) を識別します。2 番目のマシン (10.33.96.4) は、Telnet サーバーと HTTP サーバーの両方の役目を果たします。パラメーターは、
   private-address、*private-port-number*、*public-address*、および *public-port-number* です。pool1 の NAPT アドレスは、2 つのポート番号を持つように構成されているホストの公衆アドレスとして使用されていることに注意してください。

   ```
   NAT config> map 10.33.96.5 0 198.76.29.8 0
   NAT config> map 10.33.96.4 23 198.76.29.7 23
   NAT config> map 10.33.96.4 80 198.76.29.7 80
   ```

4. NAT を使用可能にします。

   ```
   NAT config> enable NAT
   ```

5. 2 つの IP パケット・フィルターを作成して、IP がパケットを NAT にパスするようにします。これらは、インターフェース 0 (公衆ネットワークに接続されているインターフェース) のインバウンド・パケット・フィルターとアウトバウンド・パケット・フィルターです。

```
IP Config>  add packet-filter outbound out-0 0
IP Config> add packet-filter inbound in-0 0
```

6. **update** コマンドを使用して、packet-filter '*filter-name*' Config> プロンプトを表示します。NAT 用のアクセス制御規則をインバウンド・フィルターに追加します。公衆インターフェース (ネット 0)を介して受信した NAT の予約済み公衆アドレス・プールあてのパケットを、NAT にパスする必要があります。NAT は公衆アドレス (および、パケットが NAPT アドレスあての場合は、公衆ポート) を正しい私設アドレス (および、パケットが NAPT アドレスあての場合は、私設ポート) で置き換えます。インターネット発信元の 0.0.0.0 のアドレスとマスクは、公衆ネットワークからのすべての発信元アドレスを NAT にパスすることを示しています。

```
IP Config> update packet-filter
Packet-filter name [ ]? in-0
Packet-filter 'in-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]?
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 198.76.29.0
Destination mask [255.255.255.255]?255.255.255.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

   アクセス制御規則の範囲は、pool1 に定義されたアドレスの範囲より大きくなっています。 NAT にパスされたパケットのアドレスが、アクセス制御規則に定義された範囲内であるが、公衆アドレス・プール内のアドレスの 1 つではない場合、NAT はそのパケットを変更せずに IP に戻します。

7. ルーターが、アクセス制御規則に一致しないパケットをドロップせずにパスするようにしたい場合は、ワイルドカード・アクセス制御規則を作成することができます。次の例は、このようなアクセス制御規則を示しています。

```
Packet-filter 'in-0' Config> add access
Enter type [E]? I
Internet source [0.0.0.0]? 0.0.0.0
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 0.0.0.0
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'in-0' Config>
```

8. NAT 用のアクセス制御規則を発信フィルターに追加します。ネット 0 インターフェースから転送された、私設ネットワーク上の発信元アドレスを持っているパケットを識別し、IP がそれらを NAT にパスされるようにします。NAT は私設アドレスを pool1 内の公衆アドレスの 1 つで置き換えます。

```
Packet-filter 'out-0' Config> add access
Enter type [E]? IN
Internet source [0.0.0.0]? 10.33.96.0
Source mask [255.255.255.255]? 255.255.255.0
Internet destination [0.0.0.0]?
Destination mask [255.255.255.255]?0.0.0.0
Enter starting protocol number ([0] for all protocols) [0]?
Enable logging? (Yes or [No]):
Packet-filter 'out-0' Config>
```

アクセス制御規則に一致しないパケットを転送する計画の場合は、フィルター *in-0* の場合と同様に、このパケット・フィルターを使用して、ワイルドカード包括的アクセス制御規則を最後のアクセス制御規則として追加することができます。

9. IP Config> プロンプトから **list packet-filter** *filter-name* コマンドを使用して、各パケット・フィルターのアクセス制御規則の正確性とシーケンスを検査できます。
10. IP 用のアクセス制御を使用可能にします。

```
IP Config> set access-control on
```

11. talk 5 を使用して、IP および NAT をリセットします。ここまでは、ルーター構成の変更を作成してきましたが、これらの変更はルーターには影響を与えていません。IP および NAT の reset コマンドにより、ルーターは新規構成を読み取り、構成に定義された規則を使用して稼働するようになります。

```
NAT> reset NAT
IP> reset IP
```

第30章 ネットワーク・アドレス変換の構成と監視

この章では、ネットワーク・アドレス変換 (NAT) 構成コマンドと監視コマンドについて説明し、次の内容が記載されています。

- 『ネットワーク・アドレス変換の構成環境へのアクセス』
- 『ネットワーク・アドレス変換の構成コマンド』
- 528ページの『ネットワーク・アドレス変換監視環境へのアクセス』
- 528ページの『ネットワーク・アドレス変換監視コマンド』
- 530ページの『NAT 動的再構成サポート』

ネットワーク・アドレス変換の構成環境へのアクセス

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

```
Config> feature nat
Network Address Protocol user configuration
NAT config>
```

ネットワーク・アドレス変換の構成コマンド

ここでは、ネットワーク・アドレス変換 (NAT) 構成コマンドについて説明します。NAT を構成するには、これらのコマンドを NAT config> プロンプトで入力します。

表 60. NAT 構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Change	公衆 IP アドレス予約プール、私設アドレス変換範囲、および静的マッピングを変更します。
Delete	公衆 IP アドレス予約プール、私設アドレス変換範囲、および静的マッピングを削除します。
Disable	NAT を使用不可にします。
Enable	NAT を使用可能にします。
List	NAT 構成に関する情報を表示します。
Map	ステーションまたはサーバーの静的 NAT または NAPT 結合を作成します。
Reserve	公衆 IP アドレス・プールを作成し、そのプールにアドレスを追加します。
Reset	ルーターが NAT 構成を読み込み、構成された NAT 規則に従って稼働するようにします。
Set	タイムアウトを設定します。
Translate	NAT 公衆アドレス・プールによって変換される私設 IP アドレスを識別します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Change

change コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、および静的マッピングを変更するのに使用します。

構文:

change reserve
translate
mappings

reserve *pools*
公衆 IP アドレス予約プールの特性 (IP アドレスおよびマスクなど) を変更することができるプロンプトを表示します。

有効値: 構成されたプールを識別するインデックス番号。この番号は **list reserve pools** コマンドを入力すると表示されます。

デフォルト値: なし

translate *ranges*
私設 IP アドレス変換範囲の特性 (IP アドレスおよびマスクなど) を変更することができるプロンプトを表示します。

有効値: 構成された変換範囲を識別するインデックス番号。この番号は **list translate** コマンドを入力すると表示されます。

デフォルト値: なし

mappings
静的アドレス・マッピングの特性 (IP アドレスおよびポートなど) を変更することができるプロンプトを表示します。

有効値: 構成されたマッピングを識別するインデックス番号。この番号は **list mappings** コマンドを入力すると表示されます。

デフォルト値: なし

Delete

delete コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、およびマッピングを削除するのに使用します。

構文:

delete reserve
translate
mappings

reserve *pools*
公衆 IP アドレス予約プールを削除することができるプロンプトを表示します。

有効値: 構成されたプールを識別するインデックス番号。この番号は **list reserve pools** コマンドを入力すると表示されます。

デフォルト値: なし

translate *ranges*

私設 IP アドレス変換範囲を削除することができるプロンプトを表示します。

有効値: 構成された変換範囲を識別するインデックス番号。この番号は **list translate** コマンドを入力すると表示されます。

デフォルト値: なし

mappings

静的アドレス・マッピングを削除することができるプロンプトを表示します。

有効値: 構成されたマッピングを識別するインデックス番号。この番号は **list mappings** コマンドを入力すると表示されます。

デフォルト値: なし

Disable

disable コマンドは、NAT を使用不可にするのに使用します。変換を必要とするパケットを廃棄させて NAT を使用不可にすることも、変換を必要とするパケットを通過させて NAT を使用不可にすることもできます。

構文:

disable nat

drop

pass

drop 変換を必要とするパケットを廃棄させて NAT を使用不可にします。

pass 変換を必要とするパケットを通過させて NAT を使用不可にします。

Enable

enable コマンドは、NAT を使用可能にするのに使用できます。NAT を使用可能にすると、実行の準備が整いますが、**reset**コマンドを使用するか、ルーターをリスタートするまでは実行されません。

構文:

enable nat

List

list コマンドは、公衆 IP アドレス予約プール、私設 IP アドレス変換範囲、マッピング、グローバル設定値、またはすべての NAT 情報を表示するのに使用します。

構文:

list

reserve

addresses

pools

translate

mappings

global

all

次の例では、時間は、時、分、および秒で表示されます。エントリー経過時間は、そのエントリーが最後に使用されてから経過した時間です。結合は、これらの 2 つのアドレス間をトラフィックが流れることを意味しています。タイムアウトは、結合を除去する前の、最後の通信後に経過する時間を決めます。タイムアウトについて詳しくは、**set** コマンドの項を参照してください。

例:

```
NAT config>list all
NAT Globals:
NAT is ENABLED
Tcp Timeout....:   24:00:00
Non-Tcp Timeout:    0:01:00
NAT Reserved Address Pool(s):
Index First Address    Mask            Count NAPT Address     Pool Name
1     9.8.7.1          255.255.255.0   3     0.0.0.0         pool1
2     9.8.7.6          255.255.255.0   12    9.8.7.9         pool1
NAT Translate Range(s):
Index IP Address       IP Mask         Associated Pool Name
1     7.1.1.0          255.255.255.0   pool1
2     10.0.0.0         255.0.0.0       pool1
NAT Static Mapping(s):
Index Private Address:Port    Public Address.:Port
1     10.1.2.3        0       9.8.7.1        0
2     7.1.1.1         21      9.8.7.9        21
```

Map

map コマンドは、私設ネットワーク内のホストまたはサーバーを公衆アドレスに静的に結合するのに使用します。このコマンドは、私設ネットワークのサーバーを設定するのに使用することができ、NAT の始動時のアソシエーションを確立します (これは、決して変更されることはありません)。

公衆および私設ポート番号 0 をもつ静的マッピングは NAT マッピングです。ポート番号に他の値をもつ静的マッピングは NAPT マッピングです。

構文:

map *private-address private-port-number public-address public-port-number*

private-address

ワークステーションの私設アドレス。

有効値: 有効な IP フォーマットのインターネット・ホスト・アドレス。これは、公衆ネットワークから永続的にアクセスする必要があるスタブ・ネットワーク内のステーション (サーバーなど) に割り当てられたアドレスでなければなりません。

デフォルト値: なし

private-port-number

私設アドレスをもつ装置で実行されているアプリケーションの TCP/UDP ポート番号。 **0** を入力すると NAT 結合が作成され、それ以外の値を入力すると NAPT 結合が作成されます。NAPT の一般的なポート値は、Telnet は 23、FTP は 21、HTTP は 80 です。

有効値: 0 ～ 65535

デフォルト値: 0

public-address

この私設アドレスがマップされる公衆 IP アドレス。これは、NAPT マッピングの場合は NAPT アドレス、NAT マッピングの場合は NAT アドレスでなければなりません。

有効値: 公衆ネットワークに固有の有効な IP アドレス。公衆ネットワークは、ネットワークの設計に応じて、インターネットまたはイントラネットが可能です。

デフォルト値: なし

public-port-number

公衆アドレスで変換されるパケットのポート番号。値 0 は、すべてのポートを表します。一般的な値は、Telnet は 23、FTP は 21、HTTP は 80 です。

有効値: 0 ～ 65535

デフォルト値: 0

この例では、私設 IP アドレス 10.11.12.200 をもつサーバーは、インターネットからのすべてのトラフィックを受け入れます。私設アドレス 10.11.12.199 をもつサーバーは、Telnet サーバーおよび FTP サーバーです。

例:

```
map 10.11.12.200 0 9.8.7.2 0
map 10.11.12.199 23 9.8.7.9 23
map 10.11.12.199 21 9.8.7.9 21
```

Reserve

reserve コマンドは、一定範囲の IP アドレスを作成し、公衆アドレス・プールに追加するのに使用します。このコマンドを使用して、動的 IP インターフェースを公衆アドレス・プールに付加することもできます。

構文:

reserve *dynamic [interface][public-address][mask][number-in-group] name [napt-address]*

注: 大括弧で囲まれている値は、ここでは任意により表示されています。

- Dynamic - このエントリーが公衆アドレスのグループまたは動的アドレス・インターフェース (IPCP を使用する PPP 接続からその IP アドレスを取り出します) のためのものであるかどうかを指定します。有効値は、*yes* または *no*です。デフォルト値は *no* です。Dynamic=*yes* の場合は、インターフェースと名前を指定するだけで済みます。 Dynamic=*no* の場合には、インターフェースは指定しませんが、その他の値はすべて指定する必要があります。

- Interface - 動的アドレス・インターフェースを IP 内に構成されているとおりに指定します。有効なインターフェース番号であればどれでも指定できます。デフォルトはゼロです。

public-address
プール内のこの範囲またはグループを構成する一連のアドレスの最初の公衆 IP アドレス。たとえば、プール内のこのグループに 9.8.7.6 〜 9.8.7.17 の一連の 12 個のアドレスが含まれている場合、この値は 9.8.7.6 になります。

注: 別の範囲のアドレスを公衆アドレス・プールに追加するには、各グループごとに別々に **reserve** コマンドを使用し、同じプール名を使用して各グループを対応付けます。たとえば、9.8.7.6 〜 9.8.7.17 のアドレスを pool1 内の 1 つのグループとして構成し、アドレス 9.8.7.1 〜 9.8.7.3 を同じプール内の別のグループとして構成するといったことが可能です。この場合、アドレス 9.8.7.4 と 9.8.7.5 は構成されず、そのプールでは使用されません。

有効値: 公衆ネットワークに固有の有効な IP アドレス

デフォルト値: なし

mask IP アドレスからビットを選択するマスク。このマスクは、IP アドレスと同様に、32 ビットの長さです。マスク内の 1 は、アドレスのネットワークまたはサブネット部分を選択します。0 はホスト部分を選択します。たとえば、アドレスが 9.8.7.6 でマスクが 255.255.0.0 の場合は、最初の 2 バイトが 9.8 であるすべてのアドレス範囲 (つまり、9.8.0.0 〜 9.8.255.255) が含まれます。

有効値: 任意の有効な IP マスク

デフォルト値: なし

number-in-group
グループ内に *public-address* から始まる順次アドレスがいくつ含まれるかを指定しますアドレス 9.8.7.6 〜 9.8.7.17 の場合、この値は 12 です。

有効値: 1 〜 IP マスクによって定義できる値

デフォルト値: なし

name 公衆アドレス予約プールの名前。この文字列は、対応する **translate** コマンドのプール名と一致していることが必要です。

有効値: 最大 16 字の印刷可能文字を使用した任意の名前。先頭と末尾のブランクは無視されます。

デフォルト値: なし

napt-address
ネットワーク・アドレス・ポート変換 (NAPT) によって使用される公衆アドレス・プールからの 1 つの IP アドレス。このアドレスは、TCP および UDP トラフィックで、プロトコル・ポート番号に従って複数の私設アドレスを 1 つの NAPT アドレスにマップするのに使用されます。NAPT の使用はオプションです。これを使用する場合、1 つの公衆アドレス・プールには 1 つの NAPT アドレスしか入れることができません。プールまたはグル

ープに NAPT アドレスが存在しない場合は、値 **0.0.0.0** を入力します。NAPT アドレスは 1 回だけプールに入力すれば済みます。

有効値: 公衆 IP アドレスの 1 つ。必ずしも公衆アドレス・プールに定義された値の範囲に含まれている必要はありませんが、同じサブネット内に存在することが必要です。

デフォルト値: 0.0.0.0 (NAPT がないことを意味します)

例:

```
reserve no 9.8.7.1 255.255.255.0 3  pool1 0.0.0.0
reserve no 9.8.7.6 255.255.255.0 12 pool1 9.8.7.9
reserve yes 2 dynamic_ip_pool
```

Reset

reset コマンドは、NAT をリセットするのに使用します。このコマンドは、すべての結合を削除し、NAT が使用しているすべてのメモリーを解放し、現行の Talk 6 構成に基づいて NAT をリスタートします。NAT をリセットしても、2216 の他のコンポーネントを中断させることはありません。

構文:

reset nat

NAT が無効な構成を検出すると、それを知らせるメッセージを出します。NAT ELS メッセージを検討して、NAT 初期設定に失敗した理由を調べてください。

Set

set コマンドは、TCP および非 TCP タイムアウトを設定するのに使用します。

構文:

set **tcp**

nontcp

tcp *timeout*

2 つの結合されたワークステーション間で最後のメッセージを渡した後、NAT が TCP 結合を保持する時間。結合とは、私設アドレスと公衆 IP アドレスの 1 つとの間の関係を保持することです。

有効値: 0 ～ 65535 分 (0 分 ～約 45 日間)

デフォルト値: 1440 分 (24 時間)

nontcp *timeout*

2 つの結合されたワークステーション間で最後のメッセージを渡した後、NAT が非 TCP 結合を保持する時間。結合とは、私設アドレスと公衆 IP アドレスの 1 つとの間の関係を保持することです。

有効値: 0 ～ 65535 分 (0 分 ～約 45 日間)

デフォルト値: 1 分

Translate

translate コマンドは、NAT が変換するアドレスのリストにサブネットを追加するのに使用します。各サブネットは、1 つの変換範囲です。NAT が知っている必要がある各変換範囲ごとに、このコマンドを 1 回入力する必要があります。任意の個数の変換範囲が、1 つの公衆アドレス予約プールを使用できます。

構文:

translate *private-address mask name*

private-address
変換する必要がある IP ホストまたはサブネットのアドレス。

有効値: 有効な小数点付き 10 進数の IP フォーマットのアドレス。サブネット・マスクと AND すると、このアドレスはスタブ・サブネット内のすべてのアドレスを識別します。スタブ・サブネットとは、そのルーターを介してのみ公衆ネットワークにアクセスするネットワークのことです。

デフォルト値: なし

mask **有効値**: 変換するスタブ・ネットワークに対応したネットワーク・マスクまたはサブネット・マスク

デフォルト値: 私設アドレスのクラス・マスク

name この範囲の私設アドレスのために NAT が使用する必要がある公衆アドレス・プールの名前

有効値: 最大 16 字の印刷可能文字を使用した任意の名前。これは **reserve** コマンドによって作成された公衆アドレス・プール名と一致していることが必要です。

デフォルト値: なし

ネットワーク・アドレス変換監視環境へのアクセス

NAT 監視環境にアクセスするには、次のように入力します。

```
* t 5
```

次に、**+** プロンプトで次のコマンドを入力します。

```
+ feature NAT
NAT>
```

NAT> プロンプトが表示されます。

ネットワーク・アドレス変換監視コマンド

ここでは、IP セキュリティー監視コマンドについて説明します。次のコマンドは NAT> プロンプトで入力します。

表 61. NAT 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。

表 61. NAT 監視コマンド (続き)

コマンド	機能
List	NAT に関する情報を表示します。
Reset	ルーターが NAT 構成を読み込み、構成された NAT アクセス規則に従って稼働するようにします。**reset NAT** コマンドを入力するまでは、NAT はルーターの稼働に影響を与えません。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

List

list コマンドは、NAT 構成に関する情報を表示するのに使用します。

構文:

list all
binding
fragment
global
reserve
pools
addresses
statistics
translate

次の例では、時間は、時、分、および秒で表示されます。エントリー経過時間は、そのエントリーが最後に使用されてから経過した時間です。結合は、これらの 2 つのアドレス間にセッションが確立されることを意味しています。タイムアウトは、結合を除去する前の、最後の通信後に経過する時間を決めます。タイムアウトについて詳しくは、Talk 6 の **set** コマンドの項を参照してください。

例:

```
NAT>list all
NAT Globals:
Current State    Tcp Timeout    Non-Tcp Timeout    Memory Usage (in bytes)
ENABLED            24:00:00           0:01:00           408

NAT Statistics:
Requests :     Passes      Drops      Holds
       0 :          0          0          0

NAT Address Binding(s):
Private Address//Port  Public Address//Port  Bind Type  Entry Age
        7.1.1.1    21         9.1.1.1    21  STATIC       0:00:13
       10.1.2.3     0         9.1.1.2     0  STATIC       0:00:13

NAT TCP Session Information:
Private Address//Port  Public Address//Port  Tcp State  Data Delta  Entry Age
        7.1.1.1    21         9.1.1.1    21  ESTAB'ED      0        0:00:56

NAT Translate Range(s):
Base Ip Address        Range Mask      Associated Reserve Pool
       7.1.1.0         255.255.255.0   carol
      10.0.0.0         255.0.0.0       carol

NAT Reserve Pool(s):
Reserve Pool     Pool Size    NAPT Address   1st Available Address
carol               21           9.1.1.1          9.1.1.12
```

```
------------------------------------------------------------
Number of Reserve Pools using NAPT.....:     1
Number of configured Reserved Addresses:    21

NAT Fragment Information:
Number of Entries    Number of Saved Fragments
          0                          0
```

Reset

reset コマンドは、NAT をリセットするのに使用します。このコマンドは、すべての結合を削除し、NAT が使用しているすべてのメモリーを解放し、現行の Talk 6 構成に基づいて NAT をリスタートします。NAT をリセットしても、2216 の他のコンポーネントを中断させることはありません。

構文:

reset nat

NAT 動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

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

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、NAT には適用されません。NAT には、インターフェースに関連する SRAM レコードがありません。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、NAT には適用できません。NAT には、インターフェースに関連する SRAM レコードがありません。

GWCON (Talk 5) 構成要素リセット・コマンド

NAT は、次の NAT 固有 GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature NAT, Reset NAT コマンド

説明: **Reset** は、すべての NAT タイマーを停止し、NAT 状態を使用不可に設定し、NAT が使用したすべてのメモリーを解放します。すべての変換マッピング、パケット・フラグメント、および TCP セッションの情報が消去されます。NAT の初期設定ルーチンは、NAT の状態を構成レコードから読み込みます。NAT を使用可能にすると、公的アドレスのプール、私用アドレスの範囲、マッピング・テーブル、フラグメント再組み立てテーブル、タイムアウト、およびタイマーは、すべて構成レコードから初期設定されます。この時点で、NAT は、IP パケット・フィルターから NAT に与えられるパケットに再び使用できるようになります。

ネットワークへの影響:

NAT が前に使用可能になっていた場合、すべての TCP セッションは期限

切れになり、アプリケーションに通知されます。UDP およびデータグラムのマッピングが消失して、これらのデータ・ストリーム上のパケットはドロップされます。NAT を再初期設定すると、UDP および他のデータグラム・パケット・ストリームの場合と同様に、TCP セッションを再確立できます。

制限事項:

IP パケット・フィルターは、IP がパケットを NAT に渡すことができるように正しく構成する必要があります。

すべての NAT コマンドは、**GWCON, feature nat, reset nat** コマンドによってサポートされます。

CONFIG (Talk 6) 即時変更コマンド

NAT は、装置の操作状態を即時に変更する、次の CONFIG コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行する場合には、保管されて保存されます。

コマンド
CONFIG, feature nat, reset nat

第31章 LAN へのダイヤルイン・アクセス (DIAL) サーバーの使用

DIAL サーバーを使用すると、リモート・ユーザーが LAN にダイヤルインし、LAN アダプターによってローカル接続されている場合と同じ方法で LAN の資源にアクセスすることが可能になります。

IBM DIAL ダイヤルイン・クライアントは、リモート・ワークステーション上で稼働し、ダイヤルイン機能を提供します。図46 は、ダイ ヤルイン機能をサポートする DIAL サーバーとして使用される装置の例を示しています。

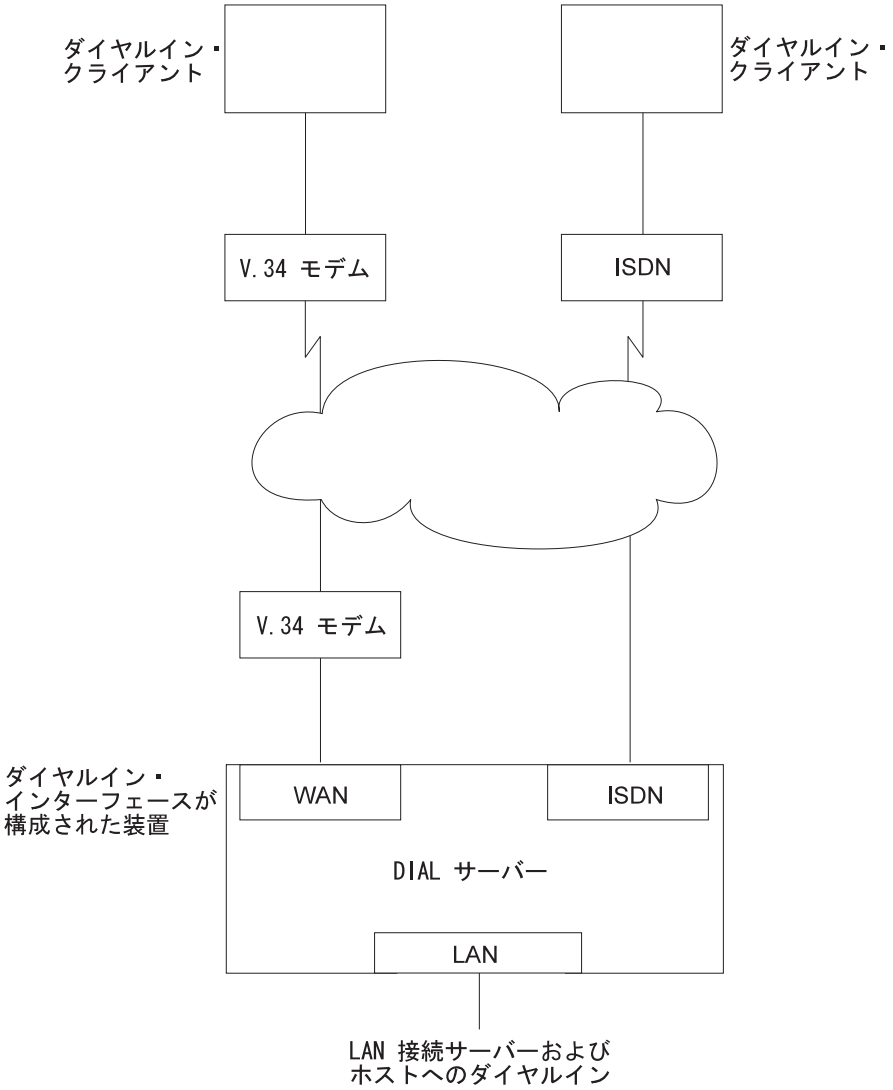


図 46. ダイヤルインをサポートする DIAL サーバーの例

注: 2216は、ダイヤルアウト・インターフェースをサポートしません。

ダイヤルイン・アクセスを使用する前に

ダイヤルイン・アクセスを使用する前に、次の要件を満たしていることが必要です。

- ワークステーションで、IBM DIAL ダイヤルイン・クライアントまたは別の PPP ダイヤルイン・クライアント (以降では、***ダイヤルイン・クライアント*** または ***PPP ダイヤルイン・クライアント*** と呼びます) が稼働している。
- クライアント・マシンのプロトコル構成が完了している。
- ISDN PRI 回線が、単一ユーザー・ダイヤルインに使用する 2216 に接続されている。
- LAN に DIAL サーバーが完全に構成されている。

ダイヤルイン・アクセスの構成

ここでは、DIAL サーバー上の ダイヤルイン機能両方を 構成する方法について説明します。ダイヤルイン・アクセスを使用するためのクライアントの構成方法は、ワークステーションが使用するクライアントに付属の資料に記載されています。

ダイヤルイン・インターフェースの構成

2216 上のダイヤルイン・インターフェースは、ダイヤル回線の特殊なタイプです。通常のダイヤル回線の設定値のほとんどは、単一ユーザー・ダイヤルイン・アプリケーションには該当しないので、***ダイヤルイン*** という名前の新しい装置タイプを追加して、このダイヤル回線用の適切なデフォルト値を設定することができます。ダイヤルイン装置を追加すると、IBM DIAL ダイヤルイン・クライアントを含めた大多数の PPP ダイヤルイン・クライアントに適用できる PPP カプセル化機能構成のデフォルト値も設定されます。これらのデフォルト値については、『ダイヤルイン・インターフェースのダイヤル回線パラメーターのデフォルト値』、および 535 ページの『ダイヤルイン回線のダイヤル回線 PPP カプセル化機能パラメーター』で説明します。

注: DIAL 機能は、ダイヤルイン回線でしか使用可能にできません。基本ネットが ISDN である場合、ダイヤルイン回線でしかサポートされません。

ダイヤルイン・インターフェースのダイヤル回線パラメーターのデフォルト値

注:

1. ここで説明するパラメーターは、オーバーライドしてはなりません。オーバーライドすると、ダイヤルイン機能が正しく動作しなくなります。
2. 一部のパラメーターは、表示されなかったり、構成できない場合があります。パラメーターについての詳しい説明は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の 『ダイヤル回線の構成および監視』の章を参照してください。

ダイヤルイン・インターフェースを追加すると、次のデフォルト値が設定されます。

- ***Idle time*** は 0 に設定されます。標準回線は、アイドル・タイマーが意味をもたない回線として定義されていることに注意してください。これは、自動的にダイ

ヤルアウトする固定回線ではありません。この回線がダイヤルアウトするのは、PPP コールバックがネゴシエーションされた場合、あるいはこの回線でマルチリンク PPP が使用可能にされている場合だけです。*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の 『Shiva パスワード認証プロトコル (SPAP)』および 『マルチリンク PPP プロトコルの使用』の項を参照してください。

- ***Inbound calls*** は許可されます。PPP ダイヤルイン・クライアントは Nways ダイヤル回線によって実現された LID 交換を使用しないので、任意のインバウンドを設定することができます。
- ***Outbound calls*** は許可されます。
- 『default_address』 に対してデフォルトの宛先アドレスが設定されます。このアドレスは、 ISDN アドレスのリストに追加されます。これらのコールはインバウンドであり、アウトバウンド・コールはコールバックまたはマルチリンク PPP 交換の結果だけになるので、宛先アドレスは無意味になります。ただし、このアドレスは、回線パラメーター用として必要です。このアドレスは削除してはなりません。削除すると、回線が使用不可になります。

ダイヤルイン回線のダイヤル回線 PPP カプセル化機能パラメーター

注: パラメーターについての詳しい説明は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の 『ポイント・ポイント・プロトコル・インターフェースの使用』の章を参照してください。

ダイヤルイン・インターフェースを追加すると、次のデフォルト値が設定されます。

- SPAP、CHAP、および PAP に対する認証は使用可能です。
- PPP MRU は 1522 に設定されます。この MRU サイズは、Windows 3.1、OS/2、および DOS バージョンの IBM DIAL ダイヤルイン・クライアント用に必要です。これらのクライアントを使用していないことが明らかでない限り、この設定値を変更しないでください。
- PPP カプセル化機能上の DIAL を自動的に使用可能にします。これにより、NetBIOS 制御プロトコル、NetBIOS フレーム制御プロトコル、残り時間、SPAP 認証、コールバック、LCP 識別、およびクライアントへの IP 静的ルートの自動追加と削除など、LAN へのダイヤルイン・アクセス のユーザーにとって重要な機能がオンになります。DIAL 機能について詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の『ポイント・ポイント・プロトコル・インターフェースの使用』の章を参照してください。

ダイヤルイン・インターフェースの追加

ダイヤルイン・インターフェースを追加するには、次のようにします。

1. 2216 上に利用可能な ISDN 基本ネットを構成する。構成についての詳しい説明は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の 『ISDN インターフェースの使用』の章を参照してください。
2. **talk 6** コマンドを入力して、`Config >` プロンプトにアクセスする。
3. `Config >` プロンプトで **add device dial-in** と入力して、ダイヤルイン・インターフェースを追加する。ダイヤルイン回線をいくつ追加するかを尋ねられます。このコマンドは、新しいネットワークを作成し、それぞれのネットワーク番

号を報告し、基本ネットの番号の入力を求め、マルチリンク PPP の場合は、使用可能にするように指示するプロンプトを出します。

例: 現行の最大ネットが 1 で、基本 1 ネットに 2 つのダイヤルイン・ネットを追加したいと想定します。

図47 は、ダイヤルイン・インターフェースの定義例です。

図 47. ダイヤルイン・インターフェースの追加

```
*talk 6
Config>add device dial-in
Enter the number of PPP Dial-in Circuit interfaces [1]? 2
Adding devices as interfaces 2-3
Defaulting data-link protocol to PPP

Base net for this circuit [0]? 1
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.

Base net for this circuit [0]? 1
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.

Use "set data-link" command to change the data-link  protocol
Use "net " command to configure dial circuit parameters.
Config>li dev
Ifc 0     Ethernet                        Slot: 1    Port 1
Ifc 1     8-port ISDN Primary T1/J1       Slot: 4    Port 1
Ifc 2     PPP Dial-in Circuit
Ifc 3     PPP Dial-in Circuit
```

ヌル・モデムの使用法

ヌル・モデムを使用する際には、D25NM-3 全機能ハンドシェークを使用してください。

ピン・マッピング :

1 〜 1　　1 〜1

2 〜 3　　3 〜 2

4 〜 5　　5 〜 4

6 〜 8、20　　8、20 〜 6

7 〜 7　　7 〜 7

グローバル DIAL パラメーターの構成の前に

ここでは、グローバル DIAL サーバー パラメーターについて説明します。

サーバー提供の IP アドレス

ルーターを構成して、ダイヤルイン・クライアントが接続期間中に使用する IP アドレスを提供できるようにすることが可能です。ルーターがクライアントに割り当てるアドレスは、4 通りの方法で取り出すことができます。その方法を次のように優先順に示します。

1. ユーザー ID

   IP アドレスを、各クライアントの PPP ユーザー・プロファイルに保管することができます。クライアントが接続して IP アドレスを要求したときに、ルーター

はそのユーザーの PPP ユーザー・プロファイルに構成されているアドレスを取り出します。この方法では、ユーザーは毎回同じ IP アドレスを入手することができますが、各ユーザーごとに固有の IP アドレスが必要です。

PPP ユーザー・プロファイルに IP アドレスを構成するには、Config> **add ppp-user** コマンドを使用します。

2. インターフェース

   IP アドレスを、ダイヤルイン・インターフェース構成に保管することができます。クライアントが接続して IP アドレスを要求したときに、ルーターは接続に使用されたインターフェースからアドレスを取り出します。この方法は、各ダイヤルイン・インターフェースごとに固有の IP アドレスが必要です。

   インターフェース IP アドレスを設定するには、次のようにします。

   - Config> **list devices** コマンドを使用して、ハードウェア・インターフェースに割り当てられているインターフェース番号を表示する。
   - Config> **net 'x'** コマンド ('x' は、構成されたインターフェース番号) を使用して、インターフェースのコマンド・プロンプトにアクセスする。
   - PPP Config> **set ipcp** コマンドを使用して、インターフェース IP アドレスを設定する。

3. プール

   IP アドレスの集合を、IP アドレス・プールに保管することができます。クライアントが接続してアドレスを要求したときに、ルーターはプールからアドレスを取り出します。クライアントが切断すると、アドレスはプールに戻されます。この方法は、ダイヤルイン・クライアントの IP アドレスを構成するための単一の場所を提供するので、アドレス・サーバーは必要ありません。

   IP アドレスのプールを追加するには、DIAL config> **add ip-pool** コマンドを使用します。

4. DHCP プロキシー

   IP アドレスを DHCP サーバーからリースすることができます。クライアントが接続してアドレスを要求したときに、ルーターはクライアントの代わりに DHCP サーバーからアドレスを要求します。この方法は、DHCP サーバーが LAN 上に存在するか、あるいはルーターに構成されていることが必要です。1 つの DHCP サーバーが、複数のルーター上のクライアントのアドレスを提供することができます。詳しくは、538ページの『動的ホスト構成プロトコル (DHCP)』を参照してください。

   DHCP サーバーを追加するには、DIAL config> **add dhcp-server** コマンドを使用します。

IP アドレス割り当て方式

接続期間中にダイヤルイン・クライアントが使用する IP アドレスは、5 つの異なるソースから入手できます。ソースを優先順に示すと、次のようになります。

1. クライアント提供
2. ユーザー ID 割り当て
3. インターフェース割り当て
4. アドレス・プール
5. DHCP サーバー

ダイヤルイン・クライアントが接続すると、ルーターはアドレスが見つかるまで、またはすべてのソースが尽きるまで、これらのソースを順次に検索します。IP アドレスが見つからなかった場合、IPCP ネゴシエーションは失敗します。これらの方式は、任意の組み合わせで使用できます。

デフォルト構成は、次のとおりです。

```
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
```

注: デフォルトでは、PPP ユーザー・プロファイル、インターフェース、または IP アドレス・プールには、アドレスは構成されていません。

動的ホスト構成プロトコル (DHCP)

動的ホスト構成プロトコル (DHCP) は、ネットワーク上のホストに構成パラメーターを提供するために開発されたものです。DHCP は、他の構成パラメーターと一緒に、ネットワーク・アドレスをホストに割り当てる機構を備えています。

プロキシー DHCP フィーチャーは、ダイヤルイン PPP ユーザーに代わって、クライアントとしての役目を果たします。これによって、装置はダイヤルイン・セッションの期間、またはリース期間が満了するまでの間、IP アドレスのリースを受けることができます。DHCP サーバーから割り当てられる IP アドレスは、PPP IPCP を通してダイヤルイン・クライアントに通知されます (IPCP についての説明は、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の『IP 制御プロトコル』の項を参照してください)。ダイヤルイン・クライアント・ソフトウェアは、IP アドレスを割り当てるために DHCP が使用されたことは知らないので、DHCP を活動化する必要はまったくありません。

プロキシー DHCP を使用するためには、少なくとも 1 つの DHCP サーバーが構成されており、ルーターからアクセス可能であることが必要です。

プロキシー DHCP では、ダイヤルイン・ユーザーに割り当てられるアドレスは、直接接続された LAN の同じサブネット内に存在することが必要です。標準的な構成では、プロキシー ARP サブネット・ルーティングを使用可能にし、ルーターがダイヤルイン・クライアントに代わってローカル・ネットワーク上のホストへの ARP 要求に応答できるようにする必要があります。

基本 DHCP の設定

最も基本的な構成では、ルーターと同じネットワーク上に 1 つの DHCP サーバーが存在し、リースされるダイヤルイン・アドレスがこの LAN と同じサブネット内にあることが必要です。

クライアントはダイヤルインするときに、DHCP サーバーから IP アドレスをリースし、クライアントとの IPCP ネゴシエーションに使用します。

1. 2216 と DHCP を同じ LAN に接続する。
2. DHCP サーバーを構成して、開始する (IP アドレスをリースするためのサーバーの設定方法については、DHCP サーバーの資料を参照してください。リースす

る IP アドレスは、直接接続された LAN のサブネット内に存在しなければならず、プロキシー ARP が 2216 上で使用可能にされていなければならないことを覚えておいてください。)

3. プロキシー DHCP の標準的な設定では、Client-Specified、Userid、Interface、および Pool の IP アドレス・ネゴシエーション・オプションを使用不可にします。

```
DIAL Config>list ip
DIAL client IP address specification:
Client : disabled
UserID : disabled
Interface : disabled
DHCP Proxy : enabled
```

4. DHCP サーバーを追加する (`DIAL Config>` **add dhcp 10.0.0.111**)。
5. ダイヤルイン・クライアント・ソフトウェアを *Server assigned* に設定する。

   注:

   a. *Server assigned* 構成は、ダイヤルイン・クライアントの実現によって異なります。

   b. クライアント・ソフトウェアは、そのアドレスを DHCP から入手するように構成してはなりません。クライアントのアドレスは、初期構成要求時に、アドレス 0.0.0.0 を IPCP に送信して入手することが必要です。
6. この設定では、DHCP GATEWAY ADDRESS はデフォルトの 0.0.0.0 にします。

DHCP サーバーへの複数のホップ

構成済みの DHCP サーバーは、接続されたルーターから到達可能な IP アドレスに存在しなければなりません。常にリモート・アクセス・ボックスからサーバーに PING できることが必要です。

DHCP サーバーが複数ホップと離れた場所にある場合、サーバーは応答の送信先のアドレスを知っている必要があり、どのプールから IP アドレスを割り当てるかを示すことも必要です。DHCP サーバーを利用して多数のサブネットにアドレスを提供できるようにする上で、IP を割り当てるプールは重要であり、どのアドレス・プールから選択するかについて何らかの指示をする必要があります。そのために、DHCP ゲートウェイ・アドレス (*giaddr*) が使用されます (この用語は RFC 2131 の定義に準拠しています)。*giaddr* は、2216 にローカルのアドレス (たとえば、トークンリングまたはイーサネット LAN ポートなど) でなければなりません。*giaddr* は DHCP サーバーが応答に使用するアドレスなので、DHCP サーバー自体からこのアドレスに PING できることも確認する必要があります。

複数 DHCP サーバー・ネットワーク

冗長度のために、複数の DHCP サーバーを構成することも可能です。複数のサーバーを構成した場合、プロキシー DHCP クライアントはすべてのサーバーにアドレスを尋ね、最初に受信した応答を受け入れます。DHCP サーバーのどれかが 2 ホップ以上離れていたり、プール内のアドレスに対応していないサブネットに接続されている場合には、*giaddr* を構成する必要があります。『DHCP サーバーへの複数のホップ』を参照してください。

複数の DHCP サーバーがアドレスを提供する可能性があるので、各サーバーに構成するアドレス・プールはオーバーラップしないようにすることが重要です。DHCP

サーバーが応答および検索を行う *giaddr* は 1 つしかないので、各アドレス・プールはお互いに同じサブネット内に存在することが必要です。

動的ドメイン名サーバー (DDNS)

ドメイン名サーバー (DNS) は、IP アドレスをホスト名にマップするもので、通常は静的な性質を持っています。動的 DNS フィーチャーというのは、DDNS DHCP サーバーおよび DNS サーバーと一緒に使用した場合、DHCP が IP アドレスとホスト名のマッピングを用いて DNS サーバーを動的に更新することができるフィーチャーをいいます。このフィーチャーは、プロキシー DHCP と一緒にしか使用できません。

2216 上の DNS を使用可能にし、ユーザー・プロファイルにホスト名を構成すると (*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の『PPP 認証プロトコル』の項を参照)、このホスト名がオプション 81 (DDNS) として DHCP サーバーにパスされます。DDNS に対して DHCP サーバーが正しく構成されている場合、DHCP サーバーは、ルーターにリースされた IP アドレスと、ルーターが送信したホスト名を使用して、DDNS サーバーを更新します。これにより、他のユーザーはホスト名を使用してダイヤルイン・クライアントにアクセスすることが可能になり、クライアントは動的に選択された IP アドレスを知っている必要はありません。

第32章 DIAL の構成

この章では、DIAL 構成コマンドおよび作動可能コマンドについて説明します。この章には、次の内容が記載されています。

- 『DIAL グローバル構成環境へのアクセス』
- 『DIAL グローバル構成コマンド』
- 549ページの『DIAL グローバル監視環境へのアクセス』
- 549ページの『DIAL グローバル監視コマンド』
- 552ページの『DIAL サーバー動的再構成サポート』

DIAL グローバル構成環境へのアクセス

グローバル構成プロセスにアクセスするには、次の手順を使用します。

1. OPCON プロンプトで、**talk 6** と入力する。 (このコマンドについて詳しくは、Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引きの *OPCON プロセスおよびコマンド* の章を参照してください。) たとえば、次のように入力します。

   ```
   * talk 6
   Config>
   ```

   talk 6 コマンドを入力すると、CONFIG プロンプト (Config>) が端末に表示されます。初めて構成に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. CONFIG プロンプトで **feature dials** コマンドを入力して DIAL Config> プロンプトを表示し、DIAL グローバル・パラメーター構成環境にアクセスします。

DIAL グローバル構成コマンド

表 62. DIAL グローバル構成コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add	DHCP (動的ホスト構成プロトコル) サーバーを DHCP サーバーのリストに追加するか、または IP アドレス・プールを追加します。
Delete	DHCP サーバーをリストから削除するか、またはアドレス・ブロックを IP アドレス・プールから除去します。
Disable	IP アドレス割り当て方式、 マルチシャシー MP、SPAP バナー、および動的 DNS を使用不可にします。
Enable	各種の IP アドレス割り当て方式、 マルチシャシー MP、SPAP バナー、および動的 DNS を使用可能にします。
List	グローバル DIAL パラメーターとその値を表示します。
Set	許容時間、dhcp ゲートウェイ・アドレス、NetBIOS ネーム・サーバー・アドレス、ローカル割り当て MAC アドレス、バーチャル・コネクション (VC)、および動的ネーム・サーバー・ 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。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Add

add コマンドは、新しいプロキシー DHCP サーバーをサーバーのリストに追加するか、または IP アドレス・プールを追加するのに使用します。

プロキシー DHCP サーバー・リストには DHCP サーバーの IP アドレスが入っており、この IP アドレスがダイヤルイン・クライアントにリースされます。冗長度のために、複数のサーバーを追加することも可能です。サーバーの最大数は 20 です。

IP アドレス・プール・フィーチャーは、ルーターがローカル定義されたアドレス・プールからダイヤルイン・クライアントへの IP アドレスを取り出すことができる方法を提供します。クライアントは、ルーターへの接続期間中、このアドレスを使用することができます。プールは、1 つまたは複数のブロックの IP アドレスから構成されます。ブロックの最大数は 20 です。各ブロックは、基本 IP アドレスとブロック内のアドレスの個数によって定義されます。各ブロック内のアドレスは、基本アドレスから始まって、昇順に連続しています。

構文:

add dhcp-server *ipaddress*

ip-pool *baseaddress #addresses*

dhcp-server *ipaddress*
指定の IP アドレスをもつ dhcp サーバーを追加します。

例:

```
DIAL Config>  add dhcp-server
DIAL Proxy DHCP server address [0.0.0.0]? 10.0.0.1
```

ip-pool *baseaddress #addresses*
アドレス・ブロックを IP プールに追加します。

例:

```
DIAL Config> add ip-pool
Base address []? 192.1.100.18
Number of addresses [1]? 57
DIAL config>add ip-pool
Base address []? 192.2.200.1
Number of addresses [1]? 250
DIAL config>list ip-pools
     Configured IP address pools:
          Base Address      Last Address        Number
          ------------      ------------        ------
          192.1.100.18      192.1.100.74            57
           192.2.200.1     192.2.200.250           250
```

Delete

delete コマンドは、サーバーのリストから既存のプロキシー DHCP サーバーを削除するか、または IP アドレス・プールからアドレス・ブロックを削除するのに使用します。

構文:

delete dhcp-server *ip address*

ip-pool *baseaddress #addresses*

dhcp-server *ipaddress*
指定の IP アドレスをもつ dhcp サーバーを削除します。

例:

```
DIAL Config>  delete dhcp-server
Enter the address to be deleted [0.0.0.0]? 10.0.0.1
```

ip-pool *baseaddress #addresses*
IP プールからアドレス・ブロックを削除します。

例:

```
DIAL Config> delete ip-pool
Base IP address of the block to be removed []? 192.2.200.1
```

Disable

disable コマンドは、IP アドレス割り当て方式、 SPAP バナー、および動的 DNS を使用不可にするのに使用します。

構文:

disable dynamic-dns
ip-address-assignment *type*
spap-banner

dynamic-dns
ユーザーのホスト名の DHCP オプション 81 を送信するのを使用不可にします。詳しくは、540ページの『動的ドメイン名サーバー (DDNS)』を参照してください。

IP-address-assignment *type*
各種の IPCP アドレス割り当て方式を使用不可にします。以下のいずれも指定できます。

- Client - クライアント指定 IP アドレス割り当てを防止します。
- Userid - 認証ユーザー・プロファイルを使用して IP アドレスを調べるのを防止します。
- Interface - ルーターがインターフェースの IPCP 設定値を使用するのを防止します。
- Pool - ルーターが IP アドレス・プールを使用してクライアントにアドレスを割り当てるのを防止します。
- DHCP-proxy - ルーターが DHCP サーバーからアドレスをリースするのを防止します。

割り当て方式について詳しくは、536ページの『サーバー提供の IP アドレス』を参照してください。

spap-banner
SPAP バナーを SPAP によって認証されたリモート・ユーザーに送信するのを使用不可にします。

注: \n を入力すると、バナーの改行文字がクライアントに表示されます。

Enable

enable コマンドは、IP アドレス割り当て方式、 SPAP バナー、および動的 DNS を使用可能にするのに使用します。

構文:

enable dynamic-dns

ip-address-assignment . . .

spap-banner

dynamic-dns

ユーザーのホスト名の DHCP オプション 81 を送信するのを使用可能にします。詳しくは、540ページの『動的ドメイン名サーバー (DDNS)』を参照してください。

IP-address-assignment ***type***

各種の IPCP アドレス割り当て方式を使用可能にします。ルーターは使用可能にされている各方式をリスト順に試行します。以下のいずれも指定できます。

- client - クライアントは、使用するアドレスを指定することができます。
- Userid - ルーターは認証された PPP ユーザー・プロファイルで IP アドレスを調べます。アドレスが非ゼロの場合、そのアドレスがクライアントに提供されます。
- Interface - ルーターはインターフェースに構成された IP アドレスを調べます。アドレスが非ゼロの場合、そのアドレスがクライアントに提供されます。
- Pool - ルーターは IP アドレス・プールからアドレスを要求します。アドレスが利用可能の場合、それがクライアントに提供されます。
- DHCP-proxy - ルーターは DHCP からアドレスのリースを試みます。成功した場合、そのアドレスがクライアントに提供されます。

割り当て方式について詳しくは、536ページの『サーバー提供の IP アドレス』を参照してください。

spap-banner

SPAP バナーを SPAP によって認証されたリモート・ユーザーに送信するのを使用可能にします。SPAP バナーのテキストを入力するのには、546ページの『Set』に説明されている **set spap-banner** コマンドを使用します。詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の 『Shiva パスワード認証プロトコル (SPAP)』を参照してください。

List

list コマンドは、現行の構成を表示するのに使用します。ポイント・ポイント・コンソールから、各ネットワークの DHCP 状態およびリース時間を監視することができます。例については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* の **listipcp** コマンドの項を参照してください。

構文:

list all

dhcp-servers

dynamic-dns

ip-address-assignment

ip-pools

name-servers

spap-banner

time-allowed

vc-parameters

例:

```
DIAL config> li all
DIAL client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled


Configured IP address pools:
     Base Address      Last Address        Number
     ------------      ------------        ------
       11.0.0.100        11.0.0.129            30
       11.0.0.210        11.0.0.229            20

Configured DHCP servers:           11.0.0.2         11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10

Dynamic DNS: Enabled

Primary Domain Name Server     (DNS): 11.0.0.2
Secondary Domain Name Server   (DNS): None
Primary NetBIOS Name Server   (NBNS): 11.0.0.2
Secondary NetBIOS Name Server (NBNS): None

Time allowed for connections: Unlimited

SPAP banner  :Enabled
Welcome to the network...


Number of Mac Addresses defined = 0
Base MAC Address: 000000000000

VC: Maximum Virtual Connections = 50
VC: Maximum suspend time (hours) (0 is unlimited) = 12
VC: Idle timeout period (seconds) = 30

Multi-chassis MP: Endpoint discriminator (0 means use box s/n) = 0

DIAL config>
```

この例は、次のことを示しています。

DIAL client IP address specification
: IP アドレス割り当て方式とそれが使用可能かどうかを表示します。ここの表示は、**list ip-address-assignment** コマンドへの応答として受け取ります。

IP address pools
: 構成された IP アドレス・プールを表示します。ここの表示は、**list ip-pool** コマンドへの応答として受け取ります。

Configured DHCP servers
: 現在 DHCP サーバーとして構成されている IP アドレスのリストを表示し

ます。ここには、DHCP ゲートウェイとして使用されているインターフェースも表示されます。ここの表示は、**list dhcp-servers** コマンドへの応答として受け取ります。

Dynamic Name Servers
動的 DNS が使用可能かどうかを表示します。ここの表示は、**list dynamic-dns** コマンドへの応答として受け取ります。

primary domain server (dns)
この行とその下の数行は、構成されている 1 次および 2 次ネーム・サーバーを表示します。ここの表示は、**list name-servers** コマンドへの応答として受け取ります。

time allowed
このユーザーの最大時間 (分) を表示します。ここの表示は、**list time-allowed** コマンドへの応答として受け取ります。

spap banner
spap バナーの内容を表示します。ここの表示は、**list spap-banner** コマンドへの応答として受け取ります。

vc connections
構成されたバーチャル・コネクションに関する情報を表示します。

multi-chassis mp
構成されたエンドポイント識別子を表示します。

Set

set コマンドは、許容時間、DHCP ゲートウェイ・アドレス、NetBIOS ネーム・サーバー・アドレス、動的ネーム・サーバー・アドレス を設定するのに使用します。

構文:

set dhcp-gateway-address
dns . . .
laa
multi-chassis-mp
nbns . . .
spap-banner . . .
time-allowed
vc-parameters

dhcp-gateway-address ***interface# ipaddress***
DHCP ゲートウェイに対応する IP アドレスを設定します。DHCP はアドレスを次の目的で使用します。

1. DHCP の応答先のアドレス
2. DHCP が割り当てる IP アドレスが入っているアドレス・プールの指示

DHCP サーバーが LAN インターフェースに直接接続されていない場合、このアドレスは、DHCP サーバーへの IP 接続を持つ LAN インターフェースのうちの 1 つのアドレスとして構成する必要があります。詳しくは、538

ページの『動的ホスト構成プロトコル (DHCP)』、および RFC 1541 の『giaddr』の定義を参照してください。

dns ***type ipaddress***

1 次および 2 次ドメイン名サーバー (DNS) を構成します。 ***Type*** は、次のどちらかです。

primary

使用するダイヤルイン・クライアントの 1 次 DNS サーバーの IP アドレスを設定します。一部のダイヤルアウト・クライアントでは (特に、Windows® 95)、この値は IPCP 時にネゴシエーションされます。

secondary

使用するダイヤルイン・クライアントの 2 次 DNS サーバーの IP アドレスを設定します。一部のダイヤルアウト・クライアントでは (特に、Windows 95)、この値は IPCP 時にネゴシエーションされます。

laa *#MAC_addresses MAC_address_base*

ローカル管理アドレス (LAA) テーブルの MAC アドレスおよび基本アドレスの数を設定します。LAA アドレスを使用するのは、レイヤー 2 トンネル・ネットワークだけです。

#MAC_addresses

MAC_Address_Base から始まる LAA テーブルに追加する MAC アドレスの数を指定します。

有効値 : 0 ～ 256

デフォルト値 : 0

MAC_address_base

LAA テーブルの基本 MAC アドレスを指定します。

有効値 : 任意の有効な MAC アドレス

デフォルト値 : 000000000000

例:

```
DIAL config>set laa
    Number of Mac Addresses:  [0]? 20
    Locally Administered Mac Address Base (hex) [000000000000]? 002210aaaaaa
    DIAL Config>
```

multi-chassis-mp

使用するエンドポイント識別子を設定します。同じバンドルに結合するすべてのリンクは、同じエンドポイント識別子を持っていなければなりません。

例:

```
DIAL Config> set multi-chassis-mp
   Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
```

nbns ***type ipaddress***

1 次および 2 次 NetBIOS ネーム・サーバーを構成します。***Type*** は、次のどちらかです。

primary

1 次 NetBIOS ネーム・サーバーの IP アドレスを設定します。

secondary

2 次 NetBIOS ネーム・サーバーの IP アドレスを設定します。

spap-banner

SPAP 認証を正常に完了したすべてのクライアントに送信するメッセージを構成することができます。

例:

```
DIAL config>set spap-banner
SPAP banner  :Disabled

Enter Banner: Welcome to the network...
```

time-allowed

PPP ダイヤルイン・ユーザーに許容される時間を設定します。このパラメーターは、ユーザーが接続を維持できる最大時間 (分) を定義します。デフォルト値は 0 で、これはユーザーが無限に接続していられることを意味します。

vc-parameters

このパラメーターは、デフォルトのグローバル・バーチャル・コネクション属性を設定するのに使用します。システムは、接続の最大数、最中断時間、および非活動タイムアウト値の入力を求めるプロンプトを出します。

例:

```
Config> feature DIAL
DIAL Config> set vc-parameters
Maximum Virtual Connections [50]? 40
Maximum suspended time (hours) (0 is unlimited) [10]? 18
Inactivity Timeout (seconds) [30]? 60
DIAL Config>
```

Maximum Virtual Connections

活動状態または中断状態にできるバーチャル・コネクションの最大数。MP で VC を使用する場合、この値は物理接続の数より 1 だけ大きい値に構成してください。

有効値: 0 ～ 255

デフォルト値 : 50

Maximum suspended time

システムが接続を終了する前に、バーチャル・コネクションを中断状態における最大時間。このパラメーターを 0 に指定すると、バーチャル・コネクションは無限に中断状態でいられます。

有効値 : 0 ～ 48

デフォルト値 : 12

Inactivity Timeout

中断する前に、バーチャル・コネクションを非活動状態における秒数

有効値 : 10 ～ 1024

デフォルト値 : 30

DIAL グローバル監視環境へのアクセス

DIAL 監視コマンドにアクセスするには、次の手順を使用します。

1. OPCON プロンプトで **talk 5** と入力する。 (このコマンドについて詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*の “OPCON プロセスおよびコマンド” の章を参照してください。) たとえば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、端末に GWCON プロンプト (+) が表示されます。初めて構成に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. + プロンプトで **feature dials** コマンドを入力して DIALS Console> プロンプトを表示して、グローバル監視環境にアクセスします。

   例:

   ```
   + feature dials
   DIALS Console>
   ```

DIAL グローバル監視コマンド

表 63. DIAL グローバル監視コマンド

コマンド	機能
Clear	特定の中断されたバーチャル・コネクションをクリアします。
List	各種のバーチャル・コネクションの状態、またはすべてのバーチャル・コネクションを表示します。
Reset	DIALS パラメーターを動的に活動化します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Clear

clear コマンドは、特定の中断されたバーチャル・コネクションをクリアするのに使用します。

構文:

clear vc *connection_id*

vc *connection_id*
終了する中断バーチャル・コネクションを指定します。*connection_id* を入手するには、**list all-vc** または **list suspended-vcs** コマンドを入力します。

List

list コマンドは、すべてのバーチャル・コネクション、活動状態のバーチャル・コネクション、中断されたバーチャル・コネクション、または vc-parameters の値を表示するのに使用します。

構文:

list all

active-vcs

all-vcs

dhcp-servers

ip-address-assignment

ip-pool

suspended-vcs

active-vcs

すべての活動状態のバーチャル・コネクションの属性を表示します。属性の説明については、**all-vcs** パラメーターの項を参照してください。

all-vcs

すべての活動状態および中断状態のバーチャル・コネクションの属性を表示します。この表示は、**list active-vcs** コマンドと **list suspended-vcs** コマンドの表示を組み合わせたものです。

例:

```
+ feature dials
DIALS console> list all
 DIAL client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled


Current IP address pools:
     Base Address      Last Address         Total          Free
     ------------      ------------         -----          ----
*      11.0.0.100        11.0.0.129           30            30
       11.0.0.210        11.0.0.229           20            19

Current DHCP servers:           11.0.0.2         11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10


Active VCs:
Conn ID    Interface Idle-Timeout Connected Username
========== ========= ============ HHH:MM:SS ================
1656494850         8           30   0:26:15 don
7293521502         9           30   1:41:57 jane


Suspended VCs:
           Hrs.Max
Conn ID    Suspend Suspended Username
========== =======  HH:MM:SS =====================
9256166098      12   0: 4:13 joe
```

活動および中断 VC の属性は、次のとおりです。

Conn ID

バーチャル・コネクションの接続 ID。システムは、接続を確立するときに ID を割り当てます。

Username

AAA、RADIUS、またはバーチャル・コネクションを確立するローカル・リスト・ユーザー。

活動 VC の場合は次のとおりです。

Interface
バーチャル・コネクションを管理しているネットワーク・インターフェース。

注: VC が中断したこのインターフェースを使用している他のユーザーが問題を起こすのを避けるために、インターフェース割り当てを使用しているダイヤルアップ・クライアントには、IP アドレスを割り当てないでください。

Idle Timeout
システムが VC を中断する前に非活動状態になっている時間数 (分)。これは **set** コマンドの非活動タイマーの値に一致しています。

Connected HHH:MM:SS
VC がインターフェースに接続されていた時間数 (時間、分、秒)
中断 VC の場合は、次のとおりです。

Hrs. Max Suspended
システムが接続を終了する前に VC が中断状態でいられる最大時間。これは **set** コマンドの最大中断時間の値に一致します。

Suspended HH:MM:SS
VC が中断されていた合計時間数 (時間、分、秒)

dhcp-servers
DHCP サーバーとその IP アドレスについて構成された情報を表示します。

ip-address-assignment
IP アドレスをクライアントに割り当てるのに使用できる方式を表示します。

ip-pool
現在のプールの使用状況を表示します。

例:

```
DIAL Console> list ip-pool
Current IP address pools:
     Base Address      Last Address         Total          Free
     ------------      ------------         -----          ----
*    192.1.100.18      192.1.100.74           57            57
      192.2.200.1     192.2.200.250          250           250

Note: The * indicates from which block the next address will be retrieved.
```

suspended-vcs
すべての中断状態のバーチャル・コネクションの属性を表示します。属性の説明については、**all-vcs** パラメーターの項を参照してください。

vc-parameters
set vc-parameters コマンドを使用して設定された vc-parameters の値を表示します。

Reset

reset コマンドは、`talk 6` で DIAL インターフェースに加えられた構成変更を動的に活動化するのに使用します。

構文:

reset all

dhcp-parameters

ip-address-assignment

ip-pool

vc-parameters

all DHCP、IP アドレス割り当て、および IP プールの構成変更を動的に活動化します。

dhcp-parameters
DHCP 構成を動的に活動化します。

ip-address-assignment
IP アドレス割り当て方式の構成を動的に活動化します。

ip-pool
IP アドレス・プールの構成を動的に活動化します。

vc-parameters
VC 構成変更を動的に更新します。

DIAL サーバー動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

Dial-In Access to LANs (DIAL) サーバーは、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

Dial-In Access to LAN (DIAL) サーバーは、GWCON (Talk 5) **activate interface** コマンドを制限なしでサポートします。

次の表では、GWCON (Talk 5) **activate interface** コマンドが起動されると活動化される Dial-In Access to LAN (DIAL) サーバーの構成変更を要約します。

GWCON (Talk 5) activate interface コマンドによって変更が活動化されるコマンド
CONFIG, feature dials, disable spap-banner
CONFIG, feature dials, enable spap-banner
CONFIG, feature dials, set dial-out inactivity-timer
CONFIG, feature dials, set spap-banner

GWCON (Talk 5) Reset Interface

DIAL サーバーは、GWCON (Talk 5) **reset interface** コマンドを制限なしでサポートします。

次の表では、GWCON (Talk 5) **reset interface** コマンドが起動されると活動化される DIAL サーバーの構成変更を要約します。

GWCON (Talk 5) reset interface コマンドによって変更が活動化されるコマンド
CONFIG, feature dials, disable spap-banner
CONFIG, feature dials, enable spap-banner
CONFIG, feature dials, set dial-out inactivity-timer
CONFIG, feature dials, set spap-banner

GWCON (Talk 5) 構成要素リセット・コマンド

DIAL サーバーは、次の DIAL サーバー固有 GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature Dials, Reset DHCP-パラメーター・コマンド

説明: このコマンドは、プロキシー DHCP 機能に関連付けられた DIAL パラメーターをリセットします。

ネットワークへの影響:
なし。

制限事項:
なし。

次の表では、**GWCON, feature dials, reset dhcp-parameters** コマンドが起動されると活動化される DIAL サーバーの構成変更を要約します。

GWCON, feature dials, reset dhcp-parameters コマンドによって変更が活動化されるコマンド
CONFIG, feature dials, add dhcp-server
CONFIG, feature dials, delete dhcp-server
CONFIG, feature dials, set dhcp-gateway-address

GWCON, Feature Dials, Reset IP-Address-Assignment コマンド

説明: このコマンドを使用して、IP アドレス割り振り方法への変更を活動化します。これは、現在割り振られているアドレスを変更しませんが、それ以降の接続で IP アドレスを割り振る方法を指定します。動的 DNS 構成変更もこのコマンドを使用して活動化されます。

ネットワークへの影響:
なし。

制限事項:
なし。

次の表では、**GWCON, feature dials, reset ip-address-assignment** コマンドが起動されると活動化される DIAL サーバーの構成変更を要約します。

GWCON, feature dials, reset ip-address-assignment コマンドによって変更が活動化されるコマンド
CONFIG, feature dials, enable dynamic-dns

CONFIG, feature dials, enable ip-address-assignment
CONFIG, feature dials, disable dynamic-dns
CONFIG, feature dials, disable ip-address-assignment

GWCON, Feature Dials, Reset IP-Pools コマンド

説明: このコマンドは、IP アドレス・プール定義 (追加または除去されたアドレス) をネットワーク接続を中断せずに、リセットします。新しい IP アドレス・プール定義に、プールに前にあって現在使用されているアドレスが含まれている場合には、これらのアドレスはリセットのあとも続けて使用されます。インターフェースがこれらのアドレスを解放されても、これらは IP アドレス・プールに戻されず、再び割り振られません。

ネットワークへの影響:
なし。

制限事項:
なし。

次の表では、**GWCON, feature dials, reset ip-pools** コマンドが起動されると活動化される DIAL サーバーの構成変更を要約します。

GWCON, feature dials, reset ip-pools コマンドによって変更が活動化されるコマンド
CONFIG, feature dials, add ip-pool
CONFIG, feature dials, delete ip-pool

GWCON, Feature Dials, Reset VC-Parameters コマンド

説明: このコマンドは、バーチャル・コネクション・パラメーターおよびテーブル・サイズをリセットします。

ネットワークへの影響:
テーブル・サイズを減らした場合、一部のバーチャル回線を終了できます。

制限事項:
なし。

次の表では、**GWCON, feature dials, reset vc-parameters** コマンドが起動されると活動化される DIAL サーバーの構成変更を要約します。

GWCON, feature dials, reset vc-parameters コマンドによって変更が活動化されるコマンド
CONFIG, feature dials, set vc-parameters

GWCON, Feature Dials, Reset All コマンド

説明: このコマンドは、DIAL reset コマンドを使用してリセットできるすべてのパラメーターをリセットします。

ネットワークへの影響:
個々の reset コマンドを参照してください。

制限事項:
なし。

次の表では、**GWCON, feature dials, reset all** コマンドが起動されると活動化される DIAL サーバーの構成変更を要約します。

GWCON, feature dials, reset all コマンドによって変更が活動化されるコマンド
CONFIG, feature dials, add dhcp-server
CONFIG, feature dials, add ip-pool
CONFIG, feature dials, delete dhcp-server
CONFIG, feature dials, delete ip-pool
CONFIG, feature dials, enable dynamic-dns
CONFIG, feature dials, enable ip-address-assignment
CONFIG, feature dials, disable dynamic-dns
CONFIG, feature dials, disable ip-address-assignment
CONFIG, feature dials, set dhcp-gateway-address
CONFIG, feature dials, set ip-pools
CONFIG, feature dials, set vc-parameters

CONFIG (Talk 6) 即時変更コマンド

DIAL サーバーは、装置の操作状態を即時に変更する、次の CONFIG コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行する場合には、保管されて保存されます。

コマンド
CONFIG, feature dials, set dns
CONFIG, feature dials, set nbns
CONFIG, feature dials, set time-allowed

非動的再構成可能コマンド

次の表には、動的に変更できない DIAL サーバーの構成コマンドを記載します。これらのコマンドを活動化するには、装置を再ロードしたり、リスタートする必要があります。

コマンド
CONFIG, feature dials, set dial-out servername
CONFIG, feature dials, set laa
CONFIG, feature dials, set multi-chassis-mp
CONFIG, feature dials, disable dial-out dials
CONFIG, feature dials, disable dial-out Telnet
CONFIG, feature dials, enable dial-out dials
CONFIG, feature dials, enable dial-out Telnet

第33章 DHCP サーバーの使用

この章では、DHCP サーバーの使用法について説明します。この章には、次の内容が記載されています。

DHCP について

動的ホスト構成プロトコル (DHCP) は、ブートストラップ・プロトコル (BOOTP) に基づくクライアント / サーバー・プロトコルです。DHCP サーバーは、中央で制御される再使用可能な IP アドレスおよびその他の TCP/IP 構成情報を DHCP クライアントのために提供します。その機能性により、ネットワーク管理者に課せられた構成情報を新規および既存のユーザーに分配するという作業が軽減されます。このフィーチャーは、RFC 2131 に適合していますが、その資料に記載されているほかにも数多くのフィーチャーをサポートしています。RFC 951 に定義されているとおりの BOOTP クライアントのためのサポートもあります。

DHCP を使用すると、サポートするクライアントは、ブロードキャスト DISCOVER メッセージを送信することにより、それぞれのネットワーク内で DHCP サーバーを検出することができ、結果として、ネットワークを通じて動的にそれぞれの構成データが提示されます。DHCP は、割り当て済みの BOOTP UDP ポート (サーバーの場合は 68、クライアントの場合は 67) を使用して要求と応答を通信します。DHCP クライアントおよびサーバーは、既存の BOOTP リレー・エージェントを使用して、それぞれのサービス範囲を拡張することができます。DHCP は、変化するネットワークをサポートする能力を含め、静的に構成されたネットワークに対して多くの利点を提供します。クライアントには、それぞれの IP アドレスがリースされるだけであるため、そのアドレスが不要になったり、別のサブネットに移動するときには、アドレスを解放 (RELEASED) して、他のクライアントが使用できるようにすることができます。

DHCP の運用

DHCP により、クライアントは、IP アドレスを含め、IP ネットワーク構成情報を中央の DHCP サーバーから入手できます。DHCP サーバーは、クライアントに提供するアドレスを永続的に割り振るのか、それとも一定の期間だけリースするのかを制御します。クライアントはリースされたアドレスを受信するときに、サーバーがそのアドレスの妥当性を再度検査し、リースを更新するよう定期的に要求する必要があります。

アドレス割り当て、リース、およびリースの更新のプロセスはすべて、DHCP クライアントおよびサーバー・プログラムで扱われるため、エンド・ユーザーからは見

えません。クライアントは、RFC 設計メッセージを使用して、DHCP サーバーにより提供されたオプションを受け入れて使用します。たとえば、次のように行います。

1. クライアントは、その存在を告知し、IP アドレス (DHCPDISCOVER メッセージ) を要求するメッセージ (そのクライアント ID が含まれているもの) のほか、サブネット・マスク、ドメイン名サーバー、ドメイン名、静的ルートといった必要なオプションをブロードキャストします。
2. 任意により、ネットワーク上のルーターが DHCP および BOOTP メッセージを (BOOTP リレーを使用して) 転送するよう構成されている場合は、ブロードキャスト・メッセージは、接続されているネットワーク上の DHCP サーバーに転送されます。
3. クライアントの DHCPDISCOVER メッセージを受信した各 DHCP サーバーは、DHCPOFFER メッセージを、IP アドレスを提示するクライアントに送信します。DHCP サーバーは、提示を行う前にネットワーク上に重複している IP アドレスがないか検査します。サーバーは、静的アドレスまたは動的アドレスをこのクライアントに割り当てるべきかどうかを知るために、構成ファイルを検査します。動的アドレスの場合、サーバーは、アドレス・プールから最も使用頻度の低いアドレスを選びます。アドレス・プールとは、クライアントにリースされる IP アドレスの範囲です。静的アドレスの場合には、サーバーは、DHCP サーバー構成からの Client (クライアント) ステートメントを使用して、オプションをクライアントに割り当てます。提示を行う際に、DHCP は提示されたアドレスを予約します。
4. クライアントは、提示メッセージ (複数の場合もあります) を受け取り、使用したいサーバーを選択します。DHCP クライアントは、提示を受け取ったときに、その提示に含まれている要求されたオプションの数を書き留めます。DHCP クライアントは、最初の提示を受け取った後の 4 秒間 DHCP サーバーから提示を受け取り続け、各提示に含まれている要求されたオプションの数を書き留めます。その時間が経過すると、DHCP クライアントは、すべての提示を比較し、その基準に適合するものを選択します。
5. クライアントは、メッセージをブロードキャストして、選択したサーバーを示し、そのサーバーによって提示された IP アドレスの使用を要求します (DHCPREQUEST メッセージ)。
6. サーバーは、クライアントがそのサーバーの提示を受け入れたことを示す DHCPREQUEST メッセージを受信した場合、そのアドレスにリースのマークを付けます。サーバーは、クライアントが別のサーバーからの提示を受け入れたことを示す DHCPREQUEST メッセージを受信した場合は、そのアドレスを利用可能なプールに戻します。指定時間内にメッセージを受信しなかった場合、サーバーは、そのアドレスを利用可能なプールに戻します。選択されたサーバーは、追加の構成情報が入っている確認応答をクライアントに対して送信します (DHCPACKメッセージ)。
7. クライアントは、構成情報が有効であるかどうかを判別します。DHCPACK メッセージを受信すると、DHCP クライアントはアドレス解決プロトコル (ARP) 要求を与えられた IP アドレスに送信して、それがすでに使用中であるかどうかを調べます。ARP 要求に対する応答を受信した場合、クライアントは、その提示を断り (DHCPDECLINE メッセージ)、プロセスを再度開始します。応答を受信しなかった場合、クライアントは、その構成情報を受け入れます。

8. クライアントは、有効なリースを受け入れると、DHCP サーバーとのバインド状態に入り、IP アドレスおよびオプションを使用するようになります。DHCP クライアントが動的アドレス・クライアントであると、そのホスト名から IP アドレスへのマッピングについて動的ドメイン名サーバーに通知します。

オプションを要求する DHCP クライアントに対し、DHCP サーバーは、通常、サブネット・マスク、ドメイン名サーバー、ドメイン名、静的ルート、クラス識別 (特定のベンダーを示します)、およびユーザー・クラスを含むオプションを提供します。

ただし、DHCP クライアントは、その独自の固有なオプションのセットを要求することができます。たとえば、Windows NT 3.5.1 DHCP クライアントは、オプションを要求する必要があります。 IBM が提供するクライアント要求 DHCP オプションのデフォルトのセットには、サブネット・マスク、ドメイン・ネーム・サーバー、ドメイン名、および静的ルートが組み込まれています。オプションについては、566ページの『DHCP オプション』を参照してください。

リースの更新

DHCP クライアントは、リースの残り時間を追跡します。リースの有効期限が切れる前の指定の時刻 (通常、リース時間の半分が経過したとき) に、クライアントは、その現在の IP アドレスおよび構成情報が入った更新要求をリースしているサーバーに送信します。サーバーが応答してリースを申し出ると、DHCP クライアントのリースは更新されます。

DHCP サーバーが明示的にその要求を拒否した場合、DHCP クライアントは、リース時間が満了するまでその IP アドレスを引き続き使用し、リース時間が満了した時点で、アドレス要求のブロードキャスティングを含む、アドレス要求プロセスを開始することができます。サーバーに連絡できない場合、クライ アントは、リースが満了するまで、割り当てられたアドレスを引き続き使用することができます。

クライアントの移動

DHCP の利点の 1 つは、新しいサブネットで必要な IP 構成情報を前もって知らなくても 1 つのサブネットから別のサブネットへ移動する自由をクライアント・ホストに与えている点です。ホストの移動先であるサブネットが DHCP サーバーにアクセスできるかぎり、DHCP クライアントは、それらのサブネットに正しくアクセスするよう、クライアント自身を自動的に構成します。

DHCP クライアントが新しいサブネットにアクセスするよう構成し直すためには、クライアント・ホストをリブートする必要があります。新しいサブネット上でホストがリスタートすると、DHCP クライアントは、最初にそのアドレスを割り振った DHCP サーバーとの古いリースを更新しようと試みます。そのアドレスは新しいサブネット上で有効でないため、サーバーは、その要求の更新を拒否します。DHCP サーバーからサーバーの応答や指示がないため、クライアントは、新しい IP アドレスを入手してネットワークにアクセスするために、IP アドレス要求プロセスを開始します。

サーバー・オプションの変更

DHCP を使用すると、サーバーで変更を行い、サーバーを再度初期設定して、その変更をすべての該当するクライアントに配布することができます。DHCP クライアントは、リースの期間に対して DHCP サーバーによって割り当てられた DHCP オプション値を保存します。クライアントがすでに起動して実行している間にサーバーで構成変更を設定した場合、それらの変更は、クライアントがそのリースの更新を試みるまで、あるいはクライアントがリスタートされるまで、DHCP クライアントによって処理されることはありません。

注: サーバーにハード・ディスク・カードまたはフラッシュ記憶カードが入っていないそしてサーバーが (t 5 **reset dhcp** コマンドを使用して) 再初期設定された場合、ルーターによって表示されるリース時間情報は、DHCP クライアントがそれぞれのリースを更新するまでなくなります。

DHCP サーバーの数

必要なサーバーの数は、備えているサブネットの数、サポートしようと計画している DHCP クライアントの数、BOOTP リレーをしようするかどうか、および選択したリース時間により、大きく異なります。DHCP プロトコルは、現在サーバー間通信を定義していないことに注意してください。そのため、サーバーは情報を共用することができず、一方の DHCP サーバーは、他方のサーバーに障害が発生した場合に『ホット・バックアップ』として実行することができません。DHCP クライアントはブロードキャスト・メッセージを送信します。設計上では、ブロードキャスト・メッセージはサブネットをまたがって転送できません。クライアントのメッセージをそのサブネットの外側へ転送できるようにするには、BOOTP リレー・エージェントを使用して DHCP 要求を転送するよう、追加のルーターを構成する必要があります。そうでなければ、各サブネット上に DHCP サーバーを構成する必要があります。

単一の DHCP サーバー

単一の DHCP サーバーを使用して 1 つのサブネット上でホストにサービスするよう選択する場合は、その単一のサーバーに障害が発生した場合の影響を考慮してください。一般的に、サーバーの障害が影響するのは、ネットワークに結合しようとしている DHCP クライアントだけです。通常、すでにネットワーク上にある DHCP クライアントは、それぞれのリースが満了するまで、影響を受けずに操作を続行します。ただし、リース時間の短いクライアントは、サーバーがリスタートできるようになる前にネットワークにアクセスできなくなる場合があります。サブネット用の DHCPサーバーが 1 台しかない場合にサーバーのダウン時間の影響を最小限に抑えるには、障害の発生した DHCP サーバーをリスタートまたはそのサーバーに応答する時間を取ることができるだけの十分に長いリース時間を選択してください。

複数の DHCP サーバー

単一ポイントでの障害を避けるために、同じサブネットにサービスする複数の DHCP サーバーを構成することができます。1 台のサーバーに障害が発生しても、その他のサーバーは、サブネットにサービスし続けることができます。それぞれの DHCP サーバーは、サブネットへの直接接続か、BOOTP リレー・エージェントを使用することによってアクセスできる状態でなければなりません。

2 台の DHCP サーバーが同じアドレスにサービスすることはできないため、1 つのサブネットについて定義されるアドレス・プールは、DHCP サーバー間で固有のものでなければなりません。したがって、複数の DHCP サーバーを使用して特定のサブネットにサービスする場合は、そのサブネットのアドレスの完全リストをサーバー間で分割する必要があります。たとえば、一方のサーバーを、そのサブネットの使用可能なアドレスの 70% で作動できるアドレス・プールで構成し、もう一方のサーバーを、使用可能なアドレスの残りの 30% で作動できるアドレス・プールで構成することができます。

複数の DHCP サーバーを使用すると、DHCP 関連ネットワーク・アクセス障害が発生する確立は低くなりますが、それを防止する保証にはなりません。特定のサブネットの DHCP サーバーで障害が発生すると、他方の DHCP サーバーは新しいクライアントからのすべての要求に対応できない場合があります。そのため、たとえば、サーバーの使用可能なアドレスの限られたプールが使い尽くされることがあります。

ただし、最初にそのアドレスのプールを使い尽くす DHCP サーバーを偏らせることができます。DHCP クライアントは、より多くのオプションを提示する DHCP サーバーを選択する傾向があります。使用可能なアドレスの 70% をもつ DHCP サーバーにサービスを偏らせるには、そのサブネットの使用可能なアドレスの 30% を保持するサーバーから提示する DHCP オプションを少なくします。

BOOTP サーバー

ネットワーク内にすでに BOOTP クライアントおよびサーバーが備わっている場合、BOOTP サーバーを DHCP サーバーと交換することを考慮しなければならないことがあります。DHCP サーバーは、任意により、BOOTP クライアントに、現在の BOOTP サーバーと同じ IP 構成情報をサービスすることができます。BOOTP サーバーを DHCP サーバーと交換できない場合は、次の予防措置を取ることをお勧めします。

- DHCP サーバー内で BOOTP サポートをオフにする。
- BOOTP サーバーと DHCP サーバーが同じアドレスを割り当てないようにする。
- BOOTP ブロードキャストを該当する BOOTP サーバーと DHCP サーバーの両方に転送するようルーター内の BOOTP リレー・サポートを構成する。

DHCP サーバーは、永続 IP アドレスを BOOTP クライアントに割り振ります。BOOTP 割り当てアドレスが使用できないような方法でサブネットの番号が付け直された場合、BOOTP クライアントはリスタートして、新しい IP アドレスを入手する必要があります。

特別な DHCP クライアント

たとえば、次のような個々のまたは特別な管理要件をもつ DHCP クライアントまたはネットワーク・サーバーが備わっている場合があります。

- 永続リース :

  永続リース時間を指定することにより、指定のホストに永続リースを割り当てることができます。また、DHCP サーバーは、BOOTP クライアントのサポートが使用可能であるかぎり、明示的に永続リースを要求する BOOTP クライアントに

は永続リースを割り振ります。DHCP サーバーは、明示的に永続リースを要求する DHCP ホストに対しても永続リースを割り振ります。

- 特定の IP アドレス :

  特定のサブネット上の特定の DHCP または BOOTP クライアント・ホストのために特定のアドレスおよび構成パラメーターを予約することができます。
- 特定の構成パラメーター :

  そのサブネットに関係なく、特定の構成情報をクライアントに割り振ることができます。
- 手動で定義されたワークステーション :

  IP ネットワーク・アクセスを構成するために DHCP または BOOTP を使用しない既存のホストについては、DHCP サブネットからアドレスを明示的に除外しなければなりません。DHCP サーバーおよびクライアントは、IP アドレスを割り振ったり、使用する前に、それが使用中であるかどうかを知るために自動的に検査しますが、ネットワークから切り離されている、または一時的に切り離された手動で定義されたホストのアドレスを検知することはできません。その場合、IP アドレスが明示的に除外されていないかぎり、手動で定義されたホストがネットワークに再度アクセスしたときに重複アドレス問題が発生することがあります。

リース時間

デフォルトのリース時間は 24 時間です。DHCP リース時間はネットワークの操作およびパフォーマンスに影響する可能性があることに注意してください。

- リース時間が短い場合は、DHCP リース更新要求のためにネットワーク・トラフィックの量が増えます。たとえば、リース時間を 5 分に設定すると、各クライアントは、2.5 分ごとに更新要求を送信します。
- リース時間が長過ぎると、IP アドレスを再利用する機能が制限される可能性があります。リース時間が非常に長いと、クライアントがリースをリスタートまたは更新したときに発生する構成変更が遅れます。

選択するリース時間は、必要に応じて大きく異なります。たとえば、次のようなものです。

- 使用可能なアドレスの数に比較した、サポートするホストの数。アドレスよりもホストの方が多い場合は、1 時間ないし 2 時間という短いリース時間を選択しなければなりません。こうすると、使用されないアドレスは、可能なかぎり迅速にプールに戻されます。
- ネットワーク変更を行うのに使用できる時間。ホストは、リスタートされたとき、またはリースを更新したときに構成情報への変更を受け取ります。タイムリーかつ十分なウィンドウがこれらの変更を行えるようにしてください。たとえば、通常、夜間に変更を行う場合は、リース時間を 12 時間に割り当てます。
- 使用可能な DHCP サーバーの数。大きなネットワーク用に DHCP サーバーが 2、3 台しかない場合には、もっと長いリース時間を選択して、サーバーのダウン時間の影響を最小限に抑える必要があります。

ホストのリース要件の組み合わせをサポートする必要がある複合ネットワークについては、DHCP クラスを定義することができます。

概念と用語

DHCP サーバー機能を説明するのに、以下の概念が使用されています。

有効範囲

用語「有効範囲」は、DHCP サーバー構成を説明する場合に、特定のパラメーター値が関係するものを識別するのに使用されます。564ページの図48 は、次の有効範囲を示しています。

- グローバル・オプション 1
- グローバル・オプション 3
- グローバル・クラス ClassA

  ClassA は、オプション 1 を再定義していますが、グローバル有効範囲からオプション 3 の値を継承します。
- グローバル・クライアント ClientA

  ClientA は、オプション 3 を再定義していますが、グローバル有効範囲からオプション 1 の値を継承します。
- サブネット SubA
  - オプション 1 を再定義します。
  - グローバル有効範囲からオプション 3 の値を継承します。
  - SubA の有効範囲内で ClassB を定義します。

    オプション 1 の値を再定義しますが、SubA (これも、偶然グローバル有効範囲から継承されます) からオプションの値を継承します。
  - SubA の有効範囲内で ClientB を定義します。

    ClientB は、オプション 3 を再定義していますが、SubA からオプション 1 の値を継承します。
- ベンダー・オプション vendorA

  ベンダー・オプションは例外です。ベンダー・オプションは独立しており、ベンダー・オプション有効範囲の外側では継承されません。

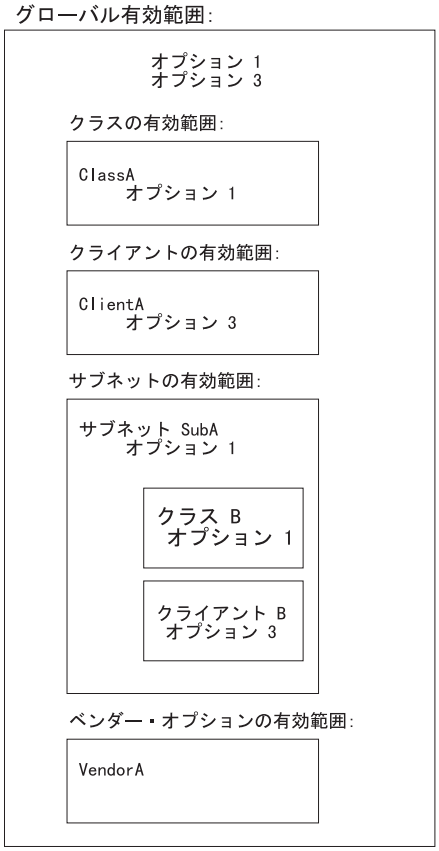


図 48. 有効範囲の概念

サブネット

サブネットは、DHCP サーバーによって管理されるアドレス・プールのためのパラメーターを定義します。アドレス・プールとは、クライアントにリースされる IP アドレスの範囲です。指定できるパラメーターには、アドレス・プールを使用するクライアントのためのリース時間およびその他のオプションが含まれます。リース時間およびその他のオプションは、グローバル有効範囲から継承できます。

サブネット・グループ

サブネット・グループは、同じインターフェース上で 1 つにまとめられる複数のサブネットを識別する方法です。与えられたグループ内のすべてのサブネットに、同じサブネット・グループ名と固有の優先順位が与えられます。優先順位は、そのグループが関連付けられているアドレス・ポリシーに従ってアドレスが割り当てられる順序を決定するために使用されます。1 つのサブネットは、次の 2 つのアドレス・ポリシーのどちらかに属します。

- Inorder

  このポリシーは、デフォルトです。inorder ポリシーは、優先順位の最も低いサブネットから始まり、優先順位の最も高いサブネットで終わるアドレスを管理します。

- Balance

  balance ポリシーは、ラウンドロビン順の定義済みサブネットのグループからのアドレスを管理します。最初に管理されるアドレスは、優先順位の

最も低いサブネットからのものです。その次に管理されるアドレスは、次に優先順位の低いサブネットからのもの、という具合です。優先順位の最も高いサブネットからのアドレスの管理が済むと、ポリシーは優先順位の最も低いサブネットに戻ります。グループ内のすべてのサブネットからすべてのアドレスの管理が済むまでこれが続きます。

クラス クラスは、DHCP サーバーが管理するクライアントのユーザー定義グループのパラメーターを定義します。クラスは、グローバル有効範囲またはサブネット有効範囲の下に定義できます。クラスがサブネット有効範囲内で定義されると、DHCP サーバーは、指定のサブネットに入っており、しかもそのクラスを要求したクラス内のクライアントだけにサービスします。ある範囲のアドレスを指定できるのは、サブネット有効範囲内で定義されたクラスだけです。範囲は、サブネット範囲のサブセットでも、あるいはサブネット範囲と同じでもかまいません。範囲を使い果たしたクラスに IP アドレスを要求したクライアントには、使用可能であれば、サブネット範囲からの IP アドレスが提示されます。このクライアントには、使い尽くされたクラスと関連付けられたオプションが提示されます。

クライアント

クライアントは、次のことを行うのに使用できます。

- 特定のエンド・ステーションの静的 IP アドレスおよび DHCP オプションを定義する。
- 特定のエンド・ステーションをサービスの対象から除外する。
- 1 つの IP アドレスを使用可能な IP アドレスの範囲から除外する。

各クライアントは、指定のハードウェア・タイプ、クライアント ID、および IP アドレスをもっています。ハードウェア・タイプは、RFC 1340 に定義されているものです。それらを次に示します。 0 以外のすべてのハードウェア・タイプの場合、クライアント ID は、エンド・ステーションのハードウェア・アドレス (または MAC アドレス) です。ハードウェア・タイプ 0 の場合、クライアント ID は文字ストリングです。通常、これはドメイン名になります。

クライアントを定義する際に、IP アドレス、*any*、または *none* のどちらかを入力するようプロンプト指示されます。IP アドレスを定義した場合、その IP アドレスは、そのクライアント用に予約されます。*any* を選択した場合は、そのクライアントにはそのサブネット内の任意の使用可能な IP アドレスが与えられます。同じサブネット内にいくつかのサブネット・レコードが定義され、それぞれが固有の範囲をもっている場合、*any* で構成されたクライアントがサブネット内の最初の使用可能なアドレスを入手しますが、これは必ずしも、クライアントが定義されている特定のサブネット・レコードの範囲からのものではありません。 *none* を選択した場合には、そのエンド・ステーションには IP アドレスは与えられません。ある IP アドレスを管理の対象から外すためには、クライアント・レコードを 0 というハードウェア・タイプとクライアント ID を使って定義してください。

RFC1340 によって定義されているハードウェア・タイプで、IBM 2216 に関係するものは、次のとおりです。

```
Hardware Type                              Value
-------------                              -----
Reserved                                   0
Ethernet                                   1
IEEE 802 Networks (including Token Ring)   6
```

完全リストについては、RFC 1340 を参照してください。

DHCP サーバー・パラメーターおよびリース・パラメーター

次の DHCP サーバー・パラメーターは、グローバル・レベルで定義できます。

- bootstrapserver
- canonical
- lease expire interval
- lease time default
- ping time
- support unlisted clients
- support bootp
- used ip address expire interval

これらのパラメーターの説明については、609ページの『Set』を参照してください。

DHCP オプション

DHCP を使用して、クライアントに対する追加構成情報を提供するオプションを指定できます。オプションは、RFC 2132 およびその他の各種 RFC で定義されています。

オプションの形式

すべてのオプションは、構成データが次の形式のどれか 1 つであると想定しています。

形式	定義
IP address	小数点表記法による単一の IP アドレス。
IP addresses	ブランクで区切られた、小数点表記法による 1 つまたは複数の IP アドレス。
IP address pair	ブランクで区切られた、小数点表記法による 2 つの IP アドレス。
IP address pairs	1 つまたは複数の IP アドレスのペアで、各対は、1 つのブランクで互いに区切られています。
Boolean	0 または 1 (真または偽)。
Byte	-128 ～ 127 (両端の数値を含む) の間の 10 進数。
Unsigned byte	0 ～ 255 (両端の数値を含む) の間の 10 進数。unsigned byte に負の値を指定することはできません。
List of unsigned bytes	ブランクで区切られた、0 ～ 255 (両端の数値を含

	む) の間の 1 つまたは複数の 10 進数。 unsigned byte に負の数値を指定することはできません。
Short	-32768 ～ 32767 (両端の数値を含む) の間の 10 進数。
Unsigned short	0 ～ 65535 (両端の数値を含む) の間の 10 進数。 unsigned short に負の数値を指定することはできません。
List of unsigned shorts	ブランクで区切られた、0 ～ 65535 (両端の数値を含む) の間の 1 つまたは複数の 10 進数。 unsigned short に負の数値を指定することはできません。
Long	-2147483648 ～ 2147483647 (両端の数値を含む) の間の 10 進値。
Unsigned long	0 ～ 4294967295 (両端の数値を含む) の間の 10 進数。unsigned long に負の数値を指定することはできません。
String	文字のストリング。
N/A	クライアントがこの情報を生成するため、指定が不要であることを示します。

各 DHCP オプションは、数字コードで識別されます。

0 ～ 127 の設計済みオプションとオプション 255 は、RFC による定義のために予約されています。 DHCP サーバー、DHCP クライアント、あるいはサーバーとクライアントの両方が、このセットのオプションを使用します。設計済みオプションのなかには、管理者が変更できるものがあります。クライアントおよびサーバーが排他的に使用するためのオプションもあります。

注: 既知の形式をもつ設計済みオプションには、16 進値は使用できません。

次のオプションは、管理者が DHCP サーバーで構成することができないか、あるいは構成してはならないものです。

52 オプション・オーバーロード

53 DHCP メッセージ・タイプ

54 サーバー識別子

55 パラメーター要求リスト

56 メッセージ

57 最大 DHCP メッセージ・サイズ

60 クラス識別子

オプション 128 ～ 254 までは、ユーザー定義オプションを表します。これらのオプションは、サイト固有の構成パラメーターを設定するために情報を DHCP クライアントに渡すよう管理者が定義できます。

さらに、IBM では、IBM 固有オプション、たとえば、オプション 192: TXT RR を用意しています。

ユーザー定義オプションの形式は、次のとおりです。

構文:

option *code value*

ここで、それぞれ次のことを意味します。

code 1 ～ 254 の任意のオプション・コード。ただし、すでに RFC で定義されているコードは除きます。

value 常に文字列でなければなりません。サーバーでは、ASCII ストリングでも 16 進数ストリングでもかまいません。ただし、クライアントでは、処理プログラムに渡されるときに常に 16進数ストリングであるようにみえます。

サーバーは、指定された値をクライアントにパスします。ただし、その値を処理するためにプログラム・ファイルまたはコマンド・ファイルを作成する必要があります。

クライアントに提供される基本オプション

クライアントには、次の基本オプションが提供されます。構成形式については、566 ページの『オプションの形式』を参照してください。

1 **Subnet Mask**。このオプションは、DHCP サーバーでだけ指定します。クライアントのサブネット・マスクは、32 ビットの小数点表記法で指定します。必須ではありませんが、ほとんどの構成で、DHCP サーバーは、オプション 1、subnet mask を DHCP クライアントに送信することになります。クライアントが DHCP サーバーからサブネット・マスクを受信せず、そのサブネットに適していないサブネット・マスクであると想定している場合、クライアントの動作は予想できませんこれが指定されない場合、クライアントは、次に示すデフォルトのサブネット・マスクを使用します。

- クラス A ネットワーク 255.0.0.0
- クラス B ネットワーク 255.255.0.0
- クラス C ネットワーク 255.255.255.0

オプション形式 : IP addresses

2 **Time Offset**。このオプションは、DHCP サーバーでだけ指定します。協定世界時 (UTC) からのクライアントのサブネットのオフセット (秒単位)。このオフセットは、符号付きの 32 ビット整数です。

オプション形式 : Long

3 **Router**。このオプションは、DHCP サーバーでだけ指定します。クライアントのサブネット上の、ルーターの IP アドレス (優先順)。

オプション形式 : IP addresses

4 **Time Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる時間サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

5 **Name Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる IEN 116 ネーム・サーバーの IP アドレス (優先順)。

注: これは、Domain Name Server オプションではありません。ドメイン名サーバーを指定するには、オプション 6 を使用してください。

オプション形式 : IP addresses

6 **Domain Name Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるドメイン・ネーム・システム・サーバーの IP アドレス (優先順)。

オプション形式: IP addresses または un-numbered IP interfaceaddress (たとえば、0.0.0.2)

注: PPP インターフェースの IP 構成で Dynamic-Address (動的アドレス) が使用可能になっている場合は、インターネット・サービス提供者 (ISP) からの IPCP を使用して Primary (1 次) および Secondary (2 次) DNS アドレスを取り出すことができます。これらの DNS アドレスを DHCP クライアントにパスするためには、Dynamic-Address インターフェースに対応する無番号 IP インターフェース・アドレス (たとえば、0.0.0.n) をもつオプション 6 を構成する必要があります。クライアントが要求を送信すると、DHCP サーバーはこれを ISP から取り出した値に変換します。IP 構成でシンプル・インターネット・アクセスを使用可能にすると、無番号 IP インターフェースを用いてオプション 6 を自動的に構成します。PPP インターフェースの活動化の前にこのサーバーから構成情報を要求しているクライアントがあれば、PPP 接続と IPCP が完了する時間として短縮リース時間 (3 分) が与えられます。DNS アドレスが判明したあとで、構成済みのリース回数が与えられます。

7 **Log Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる MIT-LCS UDP ログ・サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

8 **Cookie Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる Cookie または「quote-of-the-day」サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

9 **LPR Server**。このオプションは、DHCP クライアントと DHCP サーバーの両方で指定できます。ただし、DHCP クライアントでだけ指定した場合、構成は不完全なものになります。クライアントが使用できるライン・プリンター・サーバーの IP アドレス (優先順)。オプション 9 が指定された場合、クライアントは LPR_SERVER 環境変数を指定する必要がなくなります。

オプション形式 : IP addresses

10 **Impress Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる Imagen Impress サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

11 **Resource Location Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる Resource Location (RLP) サーバーの IP アドレス (優先順)。RLP サーバーは、ドメイン名サーバーなど、指定されたサービスを提供するリソースをクライアントが探し出せるようにします。

オプション形式 : IP addresses

12 **Host Name**。このオプションは、DHCP クライアントと DHCP サーバーの両方で指定できます。DHCP クライアントがホスト名を提供しない場合、DHCP サーバーはクライアントのオプション 12 Host Name (これには、ローカル・ドメイン名を組み込むことができます) を無視します。Host Name オプションの最小の長さは 1 オクテットで、最大長は 32 文字です。文字セットの制約事項については、RFC 1035 を参照してください。

オプション形式 : String

13 **Boot File Size**。このオプションは、DHCP サーバーでだけ指定します。クライアントのデフォルト・ブート構成ファイルの長さ (512 オクテットのブロック単位)。

オプション形式 : Unsigned short

14 **Merit Dump File**。このオプションは、DHCP サーバーでだけ指定します。クライアントが破損した場合にクライアントのコア・イメージが保管されるメリット・ダンプ・ファイルのパス名。パスは、ネットワーク・バーチャル端末装置 (NVT) ASCII 文字セットからの文字で構成される文字ストリングとして形式化されます。最小の長さは 1 オクテットです。

オプション形式 : String

15 **Domain Name**。このオプションは、DHCP クライアントと DHCPサーバーの両方で指定します。DHCP サーバーでオプション 15 に値が指定されない場合、クライアントは、オプション 12 Host Name およびオプション 15 Domain Name に値を提供する必要があります。このステートメントは、グローバル有効範囲内か、サブネット、クラス、またはクライアント有効範囲と一緒に表示されます。

オプション形式 : String

16 **Swap Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントのスワップ・サーバーの IP アドレス。

オプション形式 : IP address

17 **Root Path**。このオプションは、DHCP サーバーでだけ指定します。クライアントのルート・ディスクが入っているパス。パスは、NVT ASCII 文字セットからの文字で構成される文字ストリングとして形式化されます。最小の長さは 1 オクテットです。

オプション形式 : String

18 **Extension Path**。このオプションは、DHCP サーバーでだけ指定します。Extension Path オプションは、単純ファイル転送プロトコル (TFTP) を使用して取り出せるファイルを識別するのに使用できるストリングを指定します。最小の長さは 1 オクテットです。

オプション形式 : String

ホスト別 IP レイヤー ・パラメーター・オプション

19 **IP Forwarding**。このオプションは、DHCP サーバーでだけ指定します。クライアントによる、その IPレイヤー・パケットの転送を使用可能にする (1) か、使用不可にします (0)。

オプション形式 : Boolean

20 **Non-Local Source Routing**。このオプションは、DHCP サーバーでだけ指定します。クライアントによる、非ローカル発信元ルートを付けた、その IPレイヤー・データグラムの転送を使用可能にする (1) か、使用不可にします (0)。

オプション形式 : Boolean

21 **Policy Filter**。このオプションは、DHCP サーバーでだけ指定します。非ローカル発信元ルート付きでデータグラムをフィルター処理するのに使用される IP アドレス・ネット・マスクの対。フィルターの対の 1 つに一致しないネクスト・ホップ・アドレスをもつデータグラムは、クライアントによって廃棄されます。Policy Filter オプションの最小の長さは 8 オクテットです。

オプション形式 : IP address pairs

22 **Maximum Datagram Reassembly Size**。このオプションは、DHCP サーバーでだけ指定します。クライアントが再組み立てする最大サイズのデータグラム。最小値は 576 です。

オプション形式 : Unsigned short

23 **Default IP Time-to-Live**。このオプションは、DHCP サーバーでだけ指定します。クライアントが発信データグラム上で使用するデフォルトの活動時間 (TTL)。 TTL は、1 ～ 255 の値をもつオクテットです。

オプション形式 : Unsigned byte

24 **Path MTU Aging Timeout**。このオプションは、DHCP サーバーでだけ指定します。RFC 1191 に記載されているメカニズムによって検出される Path Maximum Transmission Unit (MTU) 値の経年処理を行うのに使用される秒単位のタイムアウト。

オプション形式 : Unsigned long

25 **Path MTU Plateau Table**。このオプションは、DHCP サーバーでだけ指定します。RFC 1191 に定義されているとおりの Path MTU ディスカバリーで送信請求するための MTU サイズのテーブル。最小の MTU 値は 68 です。Path MTU Plateau Table オプションの最小の長さは 2 オクテットです。この長さは、2 の倍数でなければなりません。

オプション形式 : Unsigned short

インターフェース別 IP レイヤー・パラメーター・オプション

26 **Interface MTU**。このオプションは、DHCP サーバーでだけ指定します。このインターフェース上で送信請求する最大伝送単位 (MTU)。最小の MTU 値は 68 です。

オプション形式 : Unsigned short

27 **All Subnets are Loca**l。このオプションは、DHCP サーバーでだけ指定します。すべてのサブネットが同じ最大伝送単位 (MTU) を使用するものとクライアントが想定する場合は (1)、想定しない場合は (0)。値 0 は、一部のサブネットはもっと小さい MTU をもっているとクライアントが想定していることを意味します。

オプション形式 : Boolean

28 **Broadcast Address**。このオプションは、DHCP サーバーでだけ指定します。クライアントのサブネット上で使用されるブロードキャスト・アドレス。

オプション形式 : IP address

29 **Perform Mask Discovery**。このオプションは、DHCP サーバーでだけ指定します。クライアントが、インターネット制御メッセージ・プロトコル (ICMP) を使用してサブネット・マスク・ディスカバリーを実行する場合は (1)、実行しない場合は (0)。

オプション形式 : Boolean

30 **Mask Supplier**。このオプションは、DHCP サーバーでだけ指定します。クライアントが、インターネット制御メッセージ・プロトコル (ICMP) を使用してサブネット・マスク要求に応答する場合は (1)、応答しない場合は (0)。

オプション形式 : Boolean

31 **Perform Router Discovery**。このオプションは、DHCP サーバーでだけ指定します。クライアントが、RFC 1256 に定義されているとおり、ルーター・ディスカバリーを使用してルーターを送信請求する場合は (1)、送信請求しない場合は (0)。

オプション形式 : Boolean

32 **Router Solicitation Address**。このオプションは、DHCP サーバーでだけ指定します。クライアントがルーターに送信請求要求を送信する宛先のアドレス。

オプション形式 : IP address

33 **Static Route**。このオプションは、DHCP サーバーでだけ指定します。クライアントがそのルーティング・キャッシュにインストールする静的ルート (優先順の宛先アドレスとルーターのペア)。最初のアドレスは宛先アドレスで、2 番目のアドレスは宛先のルーターです。デフォルトのルート宛先として 0.0.0.0 を指定してはなりません。

オプション形式 : IP address pairs

インターフェース別リンク・レイヤー・パラメーター・オプション

34 **Trailer Encapsulation**。このオプションは、DHCP サーバーでだけ指定します。クライアントが、アドレス解決プロトコル (ARP) を使用するときにトレーラーの使用をネゴシエーションする場合は (1)、ネゴシエーションしない場合は (0)。詳しくは、RFC 893 を参照してください。

オプション形式 : Boolean

35 **ARP Cache Timeout**。このオプションは、DHCP サーバーでだけ指定します。アドレス解決プロトコル (ARP) キャッシュ・エントリーの秒単位のタイムアウト。

オプション形式 : Unsigned long

36 **Ethernet Encapsulation**。このオプションは、DHCP サーバーでだけ指定します。イーサネット・インターフェースの場合、クライアントは、RFC 1042 に記載されている IEEE 802.3 (1) イーサネット・カプセル化または RFC 894 に記載されているイーサネット V2 (0) カプセル化を使用します。

オプション形式 : Boolean

TCP パラメーター・オプション

37 **TCP Default TTL**。このオプションは、DHCP サーバーでだけ指定します。クライアントが TCP セグメントを送信するのに使用するデフォルトの活動回数 (TTL)。

オプション形式 : Unsigned byte

38 **TCP Keep-alive Interval**。このオプションは、DHCP サーバーでだけ指定します。クライアントが、TCP 接続でキープアライブ・メッセージを送信する前に待機する秒単位の間隔。値 0 は、アプリケーションによって要求されないかぎり、クライアントがキープアライブ・メッセージを送信しないことを指示します。

オプション形式 : Unsigned long

39 **TCP Keep-alive Garbage**。このオプションは、DHCP サーバーでだけ指定します。以前の設定と互換性をもたせるために 1 オクテットの不要情報が含まれている TCP キープアライブ・メッセージをクライアントが送信する場合は (1)、送信しない場合は (0)。

オプション形式 : Boolean

アプリケーションおよびサービス・パラメーター・オプション

40 **Network Information Service Domain**。このオプションは、DHCP サーバーでだけ指定します。クライアントのネットワーク情報サービス (NIS) ドメイン。このドメインは、NVT ASCII 文字セットからの文字で構成される文字ストリングとして形式化されます。最小の長さは 1 オクテットです。

オプション形式 : String

41 **Network Information Service Domain**。このオプションは、DHCP サー

バーでだけ指定します。クライアントが使用できるネットワーク情報サービス (NIS) サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

42 **Network Time Protocol Servers**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるネットワーク時間プロトコル (NTP) サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

43 **Vendor-Specific Information**。オプション 43 は、DHCP サーバーでだけ指定します。サーバーはこのオプションを、オプション 60 Class Identifier を送信したクライアントに戻します。この通知オプションは、クライアントとサーバーがベンダー固有の情報を交換するのに使用するもので、ベンダー・オプション定義に指定します。オプション 43 を使用してベンダー情報をカプセル化する際の考慮事項は、次のとおりです。

- 異なるベンダーからのクライアントとサーバー間でのインターオペラビリティーを許可するために、各ベンダーは、RFC 2132 からの標準形式を使用して、そのオプション 43 の内容を明確に文書化する必要がある。
- 各ベンダーは、別のベンダーからの DHCP サーバーが容易に設定できる形式でオプション 43 内にカプセル化できる特定のオプションを指定する必要がある。たとえば、ベンダーは、次のことを行う必要があります。
  - それらのオプションを、DHCP オプションについてすでに定義されているデータ・タイプか、あるいはその他の明確なデータ・タイプで表す。
  - 他のベンダーによって提供されるサーバーと交換できるように構成ファイル内で容易にコード化できるオプションを選ぶ。
  - すべてのサーバーによって容易にサポートできる状態でいる。

クライアントが送信したベンダー固有の情報を解釈できないサーバーは、それを無視する必要があります。必要なベンダー固有の情報を受信しなかったクライアントは、それを使用せずに操作するよう試みる必要があります。このオプションに関する追加情報については、RFC 2131 および RFC 2132 を参照してください。

注: 上記の考慮事項があるため、IBM は、IBM 固有のオプションにオプション 192 と 200 を使用しています。

オプション形式 : String

44 **NetBIOS over TCP/IP Name Server**。このオプションは、DHCPサーバーでだけ指定します。クライアントが使用できる NetBIOS ネーム・サーバー (NBNS) の IP アドレス (優先順)。

オプション形式 : IP addresses

45 **NetBIOS over TCP/IP Datagram Distribution Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる NetBIOS データグラム配布 (NBDD) ネーム・サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

46 **NetBIOS over TCP/IP Node Type**。このオプションは、DHCP サーバーでだけ指定します。RFC 1001 および RFC 1002 に記載されているとおりの NetBIOS over TCP/IP Configurable clients に使用されるノード・タイプ。クライアント・タイプを指定する値には、次のものがあります。

- 0x1 B-node
- 0x2 P-node
- 0x4 M-note
- 0x8 H-node

オプション形式 : Unsigned byte

47 **NetBIOS over TCP/IP Scope**。このオプションは、DHCP サーバーでだけ指定します。RFC 1001/1002 に指定されているとおりのクライアントのための TCP/IP を介した NetBIOS 範囲パラメーター。最小の長さは 1 オクテットです。

オプション形式 : Unsigned byte

48 **X Window System Font Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる X Window System フォント・サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

49 **Window System Display Manager**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる X Window System Display Manager を実行するシステムの IP アドレス (優先順)。

オプション形式 : IP addresses

DHCP 拡張機能オプション

50 **Requested IP Address**。このオプションは、DHCP クライアントでだけ指定します。DHCP サーバーは、特定の IP アドレスを求める DHCP クライアント要求を拒否することができます。クライアントが、特定の IP アドレスを要求 (DHCPDISCOVER) できるようにします。

オプション形式 : N/A

51 **IP Address Lease Time**。このオプションは、DHCP クライアントと DHCP サーバーの両方で指定できます。DHCP クライアントは、オプション 51 を使用して、DHCP サーバーが提示する defaultLeaseInterval 値を上書きできます。クライアントが、IP アドレスについてリース時間を要求 (DHCPDISCOVER または DHCPREQUEST) できるようにします。応答 (DHCPOFFER) で、DHCP サーバーは、このオプションを使用して、リース時間を提示します。このオプションは、グローバル、サブネット、クラス、またはクライアント有効範囲内に指定できます。無限 (永続) を示すには、X'ffffffff' を使用します。

オプション形式 : Unsigned long

58 **Renewal (T1) Time Value**。このオプションは、DHCP サーバーでだけ指定します。サーバーがアドレスを割り当てる時刻と、クライアントが更新状態に変わる時刻との間の秒単位の間隔。

オプション形式 : Unsigned long

59 **Rebinding (T2) Time Value**。このオプションは、DHCP サーバーでだけ指定します。サーバーがアドレスを割り当てる時刻と、クライアントが再バインド状態に入る時刻との間の秒単位の間隔。

オプション形式 : Unsigned long

60 **Class-Identifier**。このオプションは、DHCP サーバーでだけ指定します。この情報は、クライアントによって生成されるため、指定する必要はありません。クライアントがサーバーに提供するクライアントのタイプと構成。たとえば、識別子は、クライアントのベンダー固有のハードウェア構成をコード化します。この情報は、*n* オクテットのストリングで、解釈はサーバーが行います。たとえば、16 進数 : X'01' X'02' X'03' などです。クライアントが送信したクラス固有情報を解釈する装備のないサーバーは、この情報を無視する必要があります。最小の長さは 1 オクテットです。

オプション形式 : N/A

61 **Client Identifier**。このオプションは、DHCP クライアントと DHCP サーバーの両方で指定できます。DHCP クライアントは、オプション 61 を使用して、固有なクライアント識別子を指定することができます。DHCP サーバーは、オプション 61 を使用して、アドレス・バインドのデータベースに索引を付けることができます。この値は、管理ドメイン内のすべてのクライアントについて固有であるものと想定されています。

オプション形式 : String

62 **NetWare/IP Domain Name**。このオプションは、DHCP サーバーでだけ指定します。Netware/IP ドメイン名。最小の長さは 1 オクテットで、最大長は 255 です。

オプション形式 : String

63 **NetWare/IP**。このオプションは、DHCP サーバーでだけ指定します。NetWare/IP ドメイン名以外のすべての NetWare/IP 関連情報を伝達するのに使用される汎用オプション・コード。このオプション・コードを使用して、多数の NetWare/IP サブオプションが伝達されます。最小の長さは 1 で、最大長は 255 です。

オプション形式 : String

64 **NIS domain Name**。このオプションは、DHCP サーバーでだけ指定します。ネットワーク情報サービス (NIS) ドメイン名。このドメインは、NVT ASCII 文字セットからの文字で構成される文字ストリングとして形式化されます。最小の長さは 1 です。

オプション形式 : String

65 **NIS Servers**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるネットワーク情報サービス (NIS) V3 サーバーの IP アドレス (優先順) 。

オプション形式 : IP addresses

66 **Server Name**。このオプションは、DHCP サーバーでだけ指定します。DHCP ヘッダー内の『sname』フィールドが DHCP オプションに使用されている場合に使用される単純ファイル転送プロトコル (TFTP) サーバー名。

オプション形式 : String

67 **Boot File Name**。このオプションは、DHCP サーバーでだけ指定します。DHCP ヘッダー内のファイル・フィールドが DHCP オプションに使用されている場合のブート・ファイルの名前。最小の長さは 1 です。

注: このオプションは、ブート・ファイル名を DHCP クライアントにパスするのに使用します。ブート・ファイル名は、完全修飾パス名が入っており、長さが 128 文字未満でなければなりません。たとえば、オプション 67 c:\path\boot_file_name となります。このファイルには、BOOTP 応答内の 64 オクテットのベンダー拡張機能フィールドと同様に解釈できる情報が入っています。ただし、ファイルの長さは、BOOTP ヘッダーにより 128 文字に制限されています。

オプション形式 : String

68 **Home Address**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるモバイル IP ホーム・エージェントの IP アドレス (優先順)。このオプションを指定すると、モバイル・ホストは、モバイル・ホーム・アドレスを引き出し、ホーム・ネットワークのサブネット・マスクを判別することができます。通常の長さは、単一のホーム・エージェントのホーム・アドレスを含めて 4 オクテットですが、長さはゼロでもかまいません。ゼロの長さは、使用可能なホーム・エージェントがないことを示します。

オプション形式 : IP addresses

69 **SMTP Servers**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるシンプル・メール転送プロトコル (SMTP) サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

70 **POP3 Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるポスト・オフィス・プロトコル (POP) サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

71 **NNTP Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるネットワーク・ニュース転送プロトコル (NNTP) サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

72 **WWW Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるワールド・ワイド・ウェブ (WWW) サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

73 **Finger Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる Finger サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

74 **IRC Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できるインターネット・リレー・チャット (IRC) サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

75 **StreetTalk Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる StreetTalk サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

76 **STDA Server**。このオプションは、DHCP サーバーでだけ指定します。クライアントが使用できる StreetTalk Directory Assistance (STDA) サーバーの IP アドレス (優先順)。

オプション形式 : IP addresses

77 **User Class**。このオプションは、DHCP サーバーでだけ指定します。DHCP クライアントは、オプション 77 を使用して、ホストがメンバーになっているクラスを DHCP サーバーに示します。DHCP サーバーにあるクラスについて定義されたパラメーターを受信するには、オプション 77 の値としてユーザー・クラスを \DHCPCD.CFG ファイルに手動で入力する必要があります。ファイル DHCPCD.CFG は、ディレクトリー ONDEMAND\SERVER\ETC に入っています。

オプション形式 : String

78 **Directory Agent**。このオプションは、DHCP サーバーでだけ指定します。動的ホスト構成プロトコルは、TCP/IP ネットワーク上のホストに構成パラメーターをパスするためのフレームワークを提供します。サービス・ロケーション・プロトコルを使用するエンティティーは、メッセージを処理するためにディレクトリー・エージェントのアドレスを見付け出す必要があります。他の特定のインスタンスにおいては、サービス・ロケーション・プロトコルを使用して交換されるサービス属性および URL と一緒に使用する正しい有効範囲および命名機関を検出しなければならない場合もあります。ディレクトリー・エージェントは特定の有効範囲をもっており、特定の命名機関によって定義された方式について承知している場合があります。

オプション形式 : IP address

79 **Service Scope**。このオプションは、DHCP サーバーでだけ指定します。この拡張機能は、サービス・ロケーション・プロトコルによって指定されたとおりに Service Request (サービス要求) メッセージに応答する際にサービス・エージェントが使用すべき有効範囲を指示します。

オプション形式 : String

80 **Naming Authority**。このオプションは、DHCP サーバーでだけ指定します。この拡張機能は、命名機関を指示します。命名機関は、サービス・ロケーション・プロトコルでエンティティーが使用できるように URL で使用される方式の構文を指定します。

オプション形式 : String

IBM 固有のオプション

IBM では、ユーザー定義範囲 (128 ～ 254) 内にオプションを定義することにより、IBM 固有オプションのセットを提供します。これらのオプションは、IBM 用にベンダー・オプション (オプション 43) の定義の代わりに使用されます。これらのオプションは再定義しないでください。

192 **TXT RR**。このオプションが DHCP サーバーで指定された場合、DHCP クライアント・ユーザーは、システム管理者情報フィールドを記入する必要があります。注 : このオプションは、TCP/IP バージョン 4.1 (OS/2 クライアント用) でだけサポートされています。このオプションは、システム管理者が指定できる必須のテキスト・ラベルまたは入力フィールドを最大 4 つまで提供します。それらは、たとえば、ユーザーの名前、ユーザーの電話番号のほか、DDNS クライアント構成プログラムがユーザーに入力するようプロンプト指示するものです。これらのフィールドを指定すると、システム管理者は、ホスト名またはその他のデータを構成した実際の担当者を識別することができます。システム管理者がこれらのフィールドを指定しないかぎり、DDNS 構成プログラムは表示しません。この情報は、DNS ではテキスト・レコードに保管されます。フィールド・ラベルとデータの対は、1 つの TXT リソース・レコード内に収まるものでなければなりません。使用可能なスペースは、対の間で等分に分割されます。値は、動的アクセス・クライアント上のファイル DDNSCLI.CFG でも更新されます。

オプション形式 : String

ベンダー・オプション

DHCP プロトコルは、RFC 設計オプション 43 および 60 を使用してベンダー固有情報を DHCP クライアントに与える方法を提供します。

60 **オプション 60** は、DHCP クライアントで構成されるもので、そのクライアントを特定のベンダーからのクライアントとして識別するために、DHCP サーバーに送信されます。

43 **オプション 43** は、DHCP サーバーで構成されるもので、クライアントのオプション 60 要求への応答としてクライアントに戻されるベンダー固有情報を定義します。共通コード DHCP サーバーの場合、オプション 43 は、add vendor-option コマンドを使用して構成します。ベンダー・オプションは、グローバル有効範囲内でだけ定義します。ベンダー・オプションは、ベンダーの名前とオプション・データで構成されます。オプション・データの形式は、次の 2 つです。

Hex data

これは、add vendor-option コマンドが出された場合にベンダー名と一緒に入力します。16 進データは、バイト間にブランクが入った16進ストリングとして入力する必要があります。たとえば、『01 AA 55』のようにします。

Options

add option コマンドにより、ベンダー・オプション有効範囲に任意の DHCPオプションを追加できます。

注: Hex data と options をベンダー定義に同時に指定することはできません。定義できるのは、どちらか一方だけであり、両方を定義することはできません。

DHCP のための IP の構成

IP は、DHCP サーバーが、追加されたサブネット上のクライアントのために IP アドレスおよび構成情報を正常に割り当てられるように、適切に構成する必要があります。この構成は、DHCP サーバーが、サポートするよう構成されたサブネットに直接に接続されている場合に行います。

DHCP 要求メッセージをこの DHCP サーバーに転送するために BOOTP リレー・エージェントが使用されている場合、そのサーバーに直接に接続されていないサブネットをサポートする IP 構成はなくてもかまいません。

IP アドレスの追加

DHCP 構成サブネット内にある IP アドレスは、接続するインターフェースに追加する必要があります。

例:

- DHCP が次のようにサブネットを追加している場合 :

```
DHCP Server config> list subnet all
subnet      subnet           subnet           starting         ending
name        address          mask             IP Addr          IP Addr
-------------------------------------------------------------------------
net-one     192.168.8.0      255.255.255.0    192.168.8.2      192.168.8.50
```

- IP が次のものを必要とする場合 :

```
IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list add
IP addresses for each interface:
intf     0   192.168.8.1      255.255.255.0    Local wire broadcast, fill 1
intf     1                                     IP disabled on this interface
intf     2   0.0.0.2          255.255.255.255  Local wire broadcast, fill 1
intf     3                                     IP disabled on this interface
```

IP シンプル・インターネット・アクセスの使用

シンプル IP アドレスが IP で使用可能になっており、しかも DHCP が以前に構成されていない場合、DHCP サーバー内に次の構成が自動的に生成されます。シンプル・インターネット・アクセスは、NAT フィーチャーやその他の IP フィルターも自動的に構成して、制御にアクセスします。DHCP がすでに構成されている場合には、DHCP 構成には変更や追加は行われません。詳細および制約事項については、*プロトコルの構成と監視 解説書 第 1 巻* の『IP の使用』の章の シンプル・インターネット・アクセスの使用の項を参照してください。

- IP は、次のように構成されています。

```
IP config>enable simple-internet-access
Interface to Service Provider [0]? 3
SIMPLE-INTERNET-ACCESS enabled on interface 3
```

```
IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list add
IP addresses for each interface:
intf     0   192.168.8.1      255.255.255.0    Local wire broadcast, fill 1
intf     1                                     IP disabled on this interface
intf     2                                     IP disabled on this interface
intf     3   0.0.0.3          255.255.255.255  Local wire broadcast, fill 1
                                               SIMPLE-INTERNET-ACCESS Enabled
```

- DHCP サーバーでは、次の構成が生成されます。

```
DHCP Server config> list global
.
.
DHCP Server enabled: Yes
.
.
DHCP Server config> list subnet all
subnet      subnet           subnet           starting         ending
name        address          mask             IP Addr          IP Addr
-------------------------------------------------------------------------
simple-net  192.168.8.0      255.255.255.0    192.168.8.2      192.168.8.50

DHCP Server config> list option subnet
Enter the subnet name []? simple-net
option option
code       data
-----------------------------------------------------------------
 1      255.255.255.0
 3       192.168.8.1
 6       0.0.0.3
```

DHCP サーバー構成の例

ASCII テキスト・ファイル

ここでは、ASCII テキスト形式の一般的な DHCP サーバー構成を提供します。この例は、ユーザーになじみの形式で構成を示すための、提示目的専用のものです。IBM 2216 は、ASCII 構成をサポートしていません。

ブロックで囲まれた数字 (**1**) を使用して、この ASCII 例に記載されている機能を、582ページの『OPCON (Talk 6) 構成』に示されている同等の `talk 6` 構成に関連付けることができます。

```
1  Configuration of Server parameters

leaseTimeDefault          120                  # 120 minutes
leaseExpireInterval       20 seconds
supportBOOTP              yes
supportUnlistedClients  yes


2  Global options.  Passed to every client unless overridden at a lower scope.

option 15       "raleigh.ibm.com"         # domain name
option 6         9.67.1.5                         # dns server

class manager
{
```

```
  option 48   6.5.4.3
  option 9    9.37.35.146
  option 210  "manager_authority"   # site specific option given to all managers
}

 3  Vendor-options


vendor  XI-clients hex"01 02 03"

vendor XA-clients
{
   option 23 100   # IP TTL
}

 4  A typical subnet

subnet  9.2.23.0  255.255.255.0        9.2.23.120-9.2.23.126
{
        option 28       9.2.23.127         # broadcast address
        option 9   5.6.7.8
        option 51  200

 5  class manager defined at the subnet scope.  Option 9 here will override
the option 9 specified in the global manager class.
                class manager

        {
                option 9   9.2.23.98
        }


 6  Programmers have their own subnet range

        class developers  9.2.23.125-9.2.23.126
        {
                option 51       -1               # infinite lease.
                option 9        9.37.35.1        # printer used by the developers
        }
}

 7  Example of a client that will accept any address but will have
its own set of options.

client 6        0x10005aa4b9ab  ANY
{
        option 51 999
        option 1 255.255.255.0
}

 8  Exclude an address from service.

client 0       0              9.2.23.121
```

OPCON (Talk 6) 構成

次に、talk 6 を使用した同じ構成の例を示します。

```
 1  Configuration of Server parameters

Config>f dhcp-server
DHCP server user configuration
DHCP Server config> enable dhcp
DHCP Server config>

DHCP Server config> set lease-time-default hours 2
```

```
DHCP Server config>set lease-expire-interval seconds 20
DHCP Server config>set support-bootp yes
DHCP Server config>set support-unlisted-clients global yes

DHCP Server config>li glob
DHCP server Global Parameters
============================

DHCP server enabled: Yes

Balance:  No subnet groups defined

Inorder:  No subnet groups defined

Canonical: No

Lease Expire Interval:  20 second(s)
Lease Time Default:     2 hour(s)


Support BOOTP Clients: Yes
Bootstrap Server: Not configured

Support Unlisted Clients: Yes

Ping Time: 1 second(s)
Used IP Address Expire Interval: 15 minute(s)
```

2 Global options. Passed to every client unless overridden at a lower scope.

```
DHCP Server config>add option global 15 raleigh.ibm.com
DHCP Server config>add option global 6 9.67.1.5

DHCP Server config>li option global
option option
code       data
-----------------------------------------------------------------
15      raleigh.ibm.com
6       9.67.1.5

DHCP Server config> add class global
Enter the class name []? manager
Class record with name manager has been added

DHCP Server config> add option class-global
Enter the class name []? manager
Enter the option code [1]? 48
Enter the option data []? 6.5.4.3

DHCP Server config>add option class-global 9 9.37.35.146
DHCP Server config>add option class-global manager 210 manager_authority

DHCP Server config>li class global manager
class
name
-----------------------------------------------------------------
 manager

 Number of Options: 3
 option option
 code       data
 -----------------------------------------------------------------
 48       6.5.4.3
 9        9.37.35.146
 210     manager_authority
```

3 Vendor-options

```
DHCP Server config>add vendor-option XI-client
Enter the vendor hex data []? 01 02 03
Vendor-option record with name XI-client has been added

DHCP Server config> add vendor-option XA-client
Enter the vendor hex data []?
Vendor-option record with name XA-client has been added
DHCP Server config> add option vendor-option XA-client 23 100

DHCP Server config>li vendor-option all
vendor          hex
name        data
-----------------------------------------------------------
XI-client   01 02 03
XA-client
DHCP Server config>li vendor-option det XA-client
vendor          hex
name        data
-----------------------------------------------------------
XA-client

 Number of Options: 1
 option option
 code       data
 ------------------------------------------------------------
 23      100
```

4 A typical subnet

```
DHCP Server config> add subnet
Enter the subnet name []? sub1
Enter the IP subnet []? 9.2.23.0
Enter the IP subnet mask [255.255.255.0]?
Enter start of IP address range [9.2.23.1]? 9.2.23.120
Enter end of IP address range [9.2.23.150]? 9.2.23.126
Enter the subnet group name []?
Subnet record with name sub1 has been added
DHCP Server config>
DHCP Server config> add option subnet
Enter the subnet name []? sub1
Enter the option code []? 28
Enter the option data []? 9.2.23.127
DHCP Server config> add option subnet 9 5.6.7.8
DHCP Server config>add option subnet sub1 51 200

DHCP Server config>add class subnet
Enter the subnet name []? sub1
Enter the class name []? manager
Enter start of IP address range []?
Class record with name manager has been added

DHCP Server config>add option class-subnet sub1 manager
Enter the option code [1]? 9
Enter the option data []? 9.2.23.98
```

6 Programmers have their own subnet range

```
DHCP Server config>add class subnet
Enter the subnet name []? sub1
Enter the class name []? developers
Enter start of IP address range []? 9.2.23.125
Enter end of IP address range []? 9.2.23.126
Class record with name developers has been added
```

```
DHCP Server config>add option class-subnet sub1 developers 51 -1
DHCP Server config>add option class-subnet sub1 developers 9 9.37.35.1

DHCP Server config>li subnet detailed sub1
subnet      subnet           subnet           starting         ending
name        address          mask             IP Addr          IP Addr
-------------------------------------------------------------------------
sub1        9.2.23.0         255.255.255.0    9.2.23.120       9.2.23.126


 Number of Classes: 2
 class
 name
 ---------------------------------------------------------------
 manager

     Number of Options: 1
     option option
     code       data
  ---------------------------------------------------------------
  9       9.2.23.98
 developers
  starting IP address: 9.2.23.125
  ending   IP address: 9.2.23.126

  Number of Options: 2
  option option
  code       data
  ---------------------------------------------------------------
  51      -1
  9       9.37.35.1

 Number of Options: 3
 option option
 code       data
 ---------------------------------------------------------------
 28      9.2.23.127
 9       5.6.7.8
 51      200
```

7 Example of a client that will accept any address but will have its own set of options.

```
DHCP Server config> add client global
Enter the client name []? any-addr
Enter the client's hardware type (0 - 21) [1]? 6
Enter the client ID (MAC address or string) []? 10005aa4b9ab
Enter the client's IP address (IP address, any, none) []?  any

DHCP Server config>add option client-global any-addr 51 999
DHCP Server config>add option client-global any-addr 1 255.255.255.0
```

8 Exclude an address from service.

```
Enter the client name []? excl-addr
Enter the client's hardware type (0 - 21) [1]? 0
Enter the client ID (MAC address or string) []? 0
Enter the client's IP address (IP address, any, none) []? 9.2.23.121

 DHCP Server config>li cli all
client   client   client         attached    IP
name     type     identifier     to subnet   address
-------------------------------------------------------------------------------
any-addr    6      10005aa4b9ab                   Any
excl-addr   0      0                                        9.2.23.121
```

```
DHCP Server config>li client global any-addr
client     client     client            IP
name       type       identifier        address
------------------------------------------------------------------------
any-addr    6      10005aa4b9ab                   Any

 Number of Options: 2
 option option
 code       data
 ------------------------------------------------------------------
 51      999
 1       255.255.255.0
```

第34章 DHCP サーバーの構成と監視

この章では、DHCP サーバー構成およびオペレーショナル・コマンドの使用法について説明します。この章には、次の内容が記載されています。

- 『DHCP サーバー構成環境へのアクセス』
- 『DHCP サーバー構成コマンド』
- 617ページの『DHCP サーバー監視環境へのアクセス』
- 618ページの『DHCP サーバー監視コマンド』
- 621ページの『DHCP 動的再構成サポート』

DHCP サーバー構成環境へのアクセス

DHCP サーバー*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** と入力する。たとえば、次のようになります。

   ```
   * talk 6
   Config>
   ```

   talk 6 コマンドを入力すると、Config プロンプト (Config>) が端末に表示されます。初めて構成に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. Config プロンプトで、**feature dhcp-server** コマンドを入力して、DHCP Server config> プロンプトを表示する。

DHCP サーバー構成コマンド

表 64. DHCP サーバー構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add	クラス、クライアント、サブネット、またはベンダー・オプションを追加します。
Change	クラス、クライアント、サブネット、またはベンダー・オプションを変更します。
Default	一定のグローバル変数をそれぞれのデフォルト値に戻します。
Delete	クラス、クライアント、サブネット、またはベンダー・オプションを削除します。
Disable	DHCP サーバーをグローバルに使用不可にします。
Enable	DHCP サーバーをグローバルに使用可能にします。
List	クラス、クライアント、グローバル、サブネット、またはベンダー・オプションの定義を表示します。
Set	指定された有効範囲のグローバル・パラメーターまたはオプションについて定義を設定します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Add

add コマンドは、クラス、サブネット、またはベンダー・オプションを追加するのに使用します。

構文:

add class
client
option
subnet
vendor-option

class *scope [subnet_name] class_name [range_start] [range_end]*

Defines a class.

scope クラスが追加される有効範囲を指定します。

有効値 : global または subnet

デフォルト値 : なし

subnet_name

これは、**scope** が *subnet* の場合にだけ有効です。クラスが追加されるサブネットの名前を指示します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

class-name

クラスの名前を指示します。

有効値 : 長さが最大 40 文字の ASCII ストリング

デフォルト値 : なし

range-start

これは、**scope** が *subnet* の場合にだけ有効です。クライアントが割り当てられる IP アドレス・プールの開始 IP アドレスを指定します。

有効値: クラスが追加されるサブネットの範囲内の任意の有効な IP アドレス

デフォルト値 : 指定されたサブネットに属するサブネット範囲の最初の IP アドレス。

range-end

これは、**scope** が *subnet* の場合にだけ有効です。クライアントが割り当てられる IP アドレス・プールの終了 IP アドレスを指定します。

有効値: クラスが追加されるサブネットの範囲内の任意の有効な IP アドレスこの値は、 **range-start** に指定された値よりも大きいものでなければなりません。

デフォルト値 : 指定されたサブネットに属するサブネット範囲の開始 IP アドレスに 5 プラスしたもの。結果として生じる IP アドレスがサブネット範囲内にない場合は、デフォルトとしてサブネット範囲の終了 IP アドレスがとられます。

例:

```
DHCP Server config> add class global
Enter class name? ClassA

DHCP Server config>add class subnet
Enter the subnet name[]? subA
Enter class name[]? ClaA
Enter start of IP address range[10.1.1.1]?
Enter end of IP address range[10.1.1.6]?
```

client *scope [subnet_name] client_name id-type id-value address*

クライアントを定義します。

scope クライアントが追加される有効範囲を指定します。

有効値 : global または subnet

デフォルト値 : なし

subnet-name

scope が *subnet* の場合にだけ有効です。クライアントが追加されるサブネットの名前を指定します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

client-name

クライアントの名前を指示します。

有効値 : 任意の 10 文字の ASCII ストリング

デフォルト値 : なし

id-type

クライアントのハードウェア・タイプを指示します。RFC 1340 に定義されているハードウェア・タイプで、IBM 2216 に適用できるものを、有効値として次に示します。

有効値 :

0 指定なし。クライアントの記号名を指示します。

1 イーサネット

6 IEEE 802 ネットワーク (802.5 トークンリングを含む)

デフォルト値 : 1

id-value

クライアント識別子を指定します。**id-type** が *0* の場合、**id-value** は 64 文字のストリングです。そうでない場合は、**id-value** は MAC アドレスです。

注: id-type が *0* で、**id-value** が *0* の場合は、指定された IP アドレスをサーバーが配布するよう指示されます。

有効値 : 0 または任意の有効な MAC アドレス (12 桁の 16 進数字)

デフォルト値 : なし

address

クライアントに与えられる IP アドレス、またはクライアントがサービスされないことや、クライアントに IP アドレス・プールの任意のアドレスを与えることができることを示す文字ストリングのどちらかを指定します。

有効値 :

Any valid IP address
小数点付き 10 進数形式で指定します。クライアントがサブネット有効範囲内で定義されている場合、IP アドレスはそのサブネット範囲内のものでなければなりません。

none 一致するクライアントはサービスされないことを指示します。

any サブネット・プール内の任意の IP アドレスをクライアントに与えることができることを指示します。

デフォルト値 : なし

注: id-type が *0* で、**id-value** が *0* の場合は、指定された IP アドレスをサーバーが配布するよう指示されます。

例:

```
DHCP Server config> add client global
     Enter the client name []? ClientA
     Enter the client's hardware type (0 - 21) [1]? 0
     Enter the client ID (MAC address or string) []? ClientA
     Enter the client's IP address (IP address, any, none) []? 9.1.1.1
     Client record with name ClientA has been added

DHCP Server config> add client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the client's hardware type (0 - 21) [1]? 1
     Enter the client ID (MAC address or string) []? 400000000010
     Enter the client's IP address (IP address, any, none) []? 10.1.1.10
     Client record with name CliA has been added
```

option *scope [subnet-name] [class-name] [client-name] [vendor-name] code data*

オプションを定義します。オプションは、グローバルに、あるいはサブネット、クラス、クライアント、またはベンダー・オプション有効範囲内に存在することができます。

scope オプションが追加される有効範囲を指定します。

有効値 :

- class-global
- class-subnet
- client-global
- client subnet
- global

- subnet
- vendor-option

デフォルト値 : なし

subnet-name

scope が*subnet*、*class-subnet*、または *client-subnet* の場合にだけ有効です。クライアントが追加されるサブネットの名前を指定します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

class-name

scope が *class-global* または *class-subnet* の場合にだけ有効です。オプションが追加されるクラスの名前を指示します。

有効値 : 既存のクラス名

デフォルト値 : なし

client-name

scope が *client-global* または *client-subnet* の場合にだけ有効です。オプションが追加されるクライアントの名前を指示します。

有効値 : 任意の既存のクライアント名

デフォルト値 : なし

vendor-name

scope が *vendor-option* の場合にだけ有効です。オプションが追加されるベンダーの名前を指示します。

有効値 : 任意の既存のベンダー名

デフォルト値 : なし

code オプション・コードを指定します。DHCP オプションは、RFC 2132 で定義されています。オプションおよびそれぞれの形式については、566ページの『DHCP オプション』を参照してください。

有効値: 1 ～ 255

デフォルト値 : 1

data オプション・データを指定します。オプション・データは、次の 3 とおりの方法で定義できます。

- RFC 2132 に定義された特定の形式の場合は ASCII ストリング。
- 初期設定時は 16 進数変換。データは、*hex: 01 aa 04* として入力してください。
- 文字ストリング。データは、*abcdef* として入力してください。

例:

```
DHCP Server config> add option global
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option subnet
     Enter the subnet name []? subA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option class-global
     Enter the class name []? ClassA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option client
     Enter the client name []? ClientA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the option code [1]? 3
     Enter the option data []? 9.167.100.1
```

例:

```
DHCP Server config> add option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 85
     Enter the option data []? hex:01 AA 04
```

例:

```
DHCP Server config> add option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 86
     Enter the option data []? 9.67.85.4
```

subnet *subnet_name subnet-address subnet-mask range-start range-end [subnet_group_name] [subnet_group_priority] [policy-list]*

サブネットを定義します。

subnet-name

サブネットの名前を指示します。

有効値 : 任意の 10 文字の ASCII ストリング

デフォルト値 : なし

subnet-address

サブネットのアドレスを指示します。アドレスは、小数点付き 10 進数形式で指定します。

有効値 : 任意の有効な IP サブネット・アドレス

デフォルト値 : なし

subnet-mask

サブネット・アドレス・マスクを指定します。サブネット・アドレスは、サブネット・マスク内のものでなければならず、マスクより大きな数のビットを含めることはできません。

有効値 : 小数点付き 10 進数形式の任意の有効な IP マスク

デフォルト値 : サブネット・アドレスに基づいて計算されたもの

range-start

このサーバーがこのサブネットについて管理するアドレスの IP プールの開始 IP アドレスを指定します。*range-start* が指定されない場合は、サブネット内のすべてのアドレスがサーバーによって管理されます。

有効値 : 小数点付き 10 進数形式の、指定されたサブネット内の任意の有効な IP ホスト・アドレス

デフォルト値 : サブネットの最初の IP アドレス

range-end

このサーバーがこのサブネットについて管理するアドレスの IP プールの終了 IP アドレスを指定します。

有効値 : 小数点付き 10 進数形式の、指定されたサブネット内の任意の有効な IP ホスト・アドレス

デフォルト値 : **range-start** に 50 プラスしたもの。結果として生じる IP アドレスがサブネット内にない場合は、デフォルトとしてサブネットの最後の IP アドレスがとられます。

subnet-group-name

このサブネットが属しているサブネット・グループ名を指定します。

有効値 : 長さが最大 64 文字の任意の ASCII ストリング

デフォルト値 : なし

subnet-group-priority

サブネット・グループ内でのこのサブネットの優先順位を指定します。この優先順位は、アドレスが特定のサブネット・グループ内で割り当てられる順序を決定するために使用されます。

有効値: 1 〜 65535

デフォルト値 : 1

policy-list

サブネット・グループが追加されるポリシー・アドレス・リスト (Balance または Inorder のいずれか) を指示します。サブネット・グループが一方のリスト上に存在するのに、もう一方のリストが指定されると、サブネット・グループはその新しいリストに移動されます。

有効値 : Inorder または Balance

デフォルト値 : これが新しいサブネットの場合、デフォルトとして Inorder がとられます。そうでない場合は、サブネット・グループが属している現行ポリシー・リストです。

例:

```
DHCP Server config> add subnet
 Enter the subnet name []? subA
```

```
Enter the IP subnet []? 10.1.1.0
Enter the IP subnet mask [255.255.255.0]?
Enter start of IP address range [10.1.1.1]?
Enter end of IP address range [10.1.1.31]?
Enter the subnet group name []? group1
Enter the subnet group priority (1 - 65535) [1]?
Enter the access policy list (Inorder or Balance) [Inorder]?
Subnet record with name sub1 has been added
Subnet group group1 is being added to the Inorder List
```

vendor-option *vendor_name [hex_value]*

ベンダー・オプションを追加します。ベンダー・オプション・データを提供する方法は、次の 2 とおりです。

- プロンプト指示されたときに 16 進データを入力する方法。
- **add option vendor** コマンドを使用してベンダーに特定のオプションを追加する方法。オプション情報については、590 ページを参照してください。

vendor_name

ベンダーの名前を指示します。

有効値 : 長さが最大 40 文字の ASCII ストリング

デフォルト値 : なし

hex-value

オプションのデータ部分の 16 進値を表す 16 進 ASCII ストリングを指定します。

有効値 : *01 aa 04* という形式の任意の有効な 16 進数ストリング

デフォルト値 : なし

例:

```
DHCP Server config> add vendor-option
     Enter the vendor name []? XA-client
     Enter the vendor hex data [] 01 aa 04?
     Vendor-option record with name XA-client has been added
```

Change

change コマンドは、クラス、クライアント、サブネット、またはベンダー・オプションの構成を変更するのに使用します。

構文:

change class
client
subnet
vendor-option

class *scope [subnet_name] class_name new_class_name [new_range_start] [new_range_end]*

クラスを変更します。

scope 変更されるクラスの有効範囲を指定します。

有効値 : global または subnet

デフォルト値 : なし

subnet-name

scope が *subnet* の場合にだけ有効です。クラスが属しているサブネットの名前を指示します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

class-name

クラスの名前を指示します。

有効値 : 既存のクラスの名前

デフォルト値 : なし

new-class-name

クラスの新しい名前を指示します。

有効値 : 長さが最大 40 文字の ASCII ストリング

デフォルト値 : 既存のクラス名

new-range-start

scope が *subnet* の場合にだけ有効です。クライアントが割り当てられる IP アドレス・プールの新しい開始 IP アドレスを指定します。

有効値 : サブネット範囲内の任意の IP アドレス

デフォルト値 : 既存の範囲の始め

new-range-end

クライアントが割り当てられる IP アドレス・プールの新しい終了 IP アドレスを指定します。

有効値 : **new-range-end** より大きい、サブネット範囲内の任意の有効な IP アドレス

デフォルト値 : 既存の範囲の終わり

例:

```
DHCP Server config> change class global
     Enter the class name []? ClassA
     Enter the new class name [ClassA]?
```

例:

```
DHCP Server config> change class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the new class name [ClaA]?
     Enter start of IP address range [10.1.1.1]?
     Enter end of IP address range [10.1.1.6]?
```

client *scope [subnet_name] client_name new-client_name new-id-type new-id-value new-address*

クライアントを変更します。

scope 変更されるクライアントの有効範囲を指定します。

有効値 : global または subnet

デフォルト値 : なし

subnet-name

scope が *subnet* の場合にだけ有効です。クライアントが属しているサブネットの名前を指示します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

client-name

クライアントの名前を指示します。

有効値 : 既存のクライアント名

デフォルト値 : なし

new-client-name

クライアントの新しい名前を指示します。

有効値 : 長さが最大 10 文字の ASCII ストリング

デフォルト値 : 既存のクライアント名

new-id-type

クライアントの新しいハードウェア・タイプを指示します。

有効値 : 0 ～ 21。589 ページを参照。

デフォルト値 : クライアントの既存のハードウェア・タイプ

new-id-value

新しいクライアント識別子を指定します。

有効値 : 0 または任意の有効な MAC アドレス (12 桁の 16 進数字)

デフォルト値 : 既存のクライアント ID タイプ

注: **id-type** が *0* で、**id-value** が *0* の場合は、指定された IP アドレスをサーバーが配布するよう指示されます。

new-address

クライアントに与えられる新しい IP アドレス、またはクライアントがサービスされないことや、クライアントに IP アドレス・プールの任意のアドレスを与えることができることを示す文字ストリングのどちらかを指定します。

有効値 :

Any valid IP address

none 一致するクライアントはサービスされないことを指示します。

any サブネット・プール内の任意の IP アドレスをクライアントに与えることができることを指示します。

デフォルト値 : なし

注: **id-type** が *0* で、**id-value** が *0* の場合は、指定された IP アドレスをサーバーが配布するよう指示されます。

例:

```
DHCP Server config> change client global
     Enter the client name []? ClientA
     Enter the new client name [ClientA]?
     Enter the new client hardware type (0 - 21) [0]?
     Enter the new client ID  [ClientA]?
     Enter the client's new IP address (IP address, any, none) [9.1.1.1]?
     Client ClientA has been changed
```

例:

```
DHCP Server config> change client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the new client name [ClientA]?
     Enter the new client hardware type (0 - 21) [1]?
     Enter the new client ID  [400000000010]?
     Enter the client's new IP address (IP address, any, none) [10.1.1.10]?
     Client CliA has been changed
```

subnet *subnet_name new_subnet_name new_subnet_address new_subnet_mask new-range_start new-range_end*

サブネットを変更します。

subnet_name

変更される特定のサブネットの名前を指示します。

有効値 : 既存のサブネット名

デフォルト値 : なし

new_subnet_name

指定されたサブネットの新しい名前を指示します。

有効値 : 任意の 10 文字の ASCII ストリング

デフォルト値 : 元のサブネット名

new_subnet_addresss

サブネットの新しいアドレスを指示します。アドレスは、小数点付き 10 進数表記で指定します。

有効値 : 任意の有効な IP サブネット・アドレス

デフォルト値 : 既存のサブネット・アドレス

new_subnet_mask

新しいサブネット・アドレス・マスクを指定します。サブネット・アドレスは、サブネット・マスク内のものでなければならず、マスクより大きな数のビットを含めることはできません。

有効値: 任意の有効な IP マスク

デフォルト値 : 既存のサブネット・マスク

new-range-start

このサーバーがこのサブネットについて管理するアドレスの IP プールの新しい開始 IP アドレスを指定します。*range-start* が指定されない場合は、サブネット内のすべてのアドレスがサーバーによって管理されます。

有効値: サブネット範囲内の任意の有効な IP アドレス

デフォルト値 : 既存のプール開始アドレス

new-range-end

このサーバーがこのサブネットについて管理するアドレスの IP プールの新しい終了 IP アドレスを指定します。

有効値: サブネット範囲内にあり、しかも開始プール・アドレスより大きな任意の有効な IP アドレス

デフォルト値 : 既存のプール終了アドレス

例:

```
DHCP Server config> change subnet
     Enter the subnet name []? subA
     Enter the new subnet name [subA]?
     Enter the new IP subnet[10.1.1.0]?
     Enter the new IP subnet mask[255.255.0.0]?
     Enter new start of IP address range [10.1.1.1]?
     Enter new end of IP address range [10.1.1.31]?
     Enter the new subnet group name [group11]?
     Enter the new subnet group priority [1]?
     Enter the new access policy list (Inorder or Balance) [Inorder]?
```

vendor-option *vendor_name new_vendor_name [new_hex_value]*

ベンダー・オプションを変更します。

vendor_name

ベンダー・オプションの新しい名前を指定します。

有効値 : 既存のベンダー名

デフォルト値 : なし

new_vendor_name

ベンダー・オプションの新しい名前を指定します。

有効値 : 長さが最大 40 文字の ASCII ストリング

デフォルト値 : 既存のベンダー・オプション名

new_hex_value

オプションのデータ部分の 16 進値を表す新しい 16 進 ASCII ストリングを指定します。このベンダー・オプションに特定のオプションが追加されている場合は、16 進数値を追加できません。

有効値: 任意の有効な 16 進数ストリング

デフォルト値 : 既存の 16 進数ストリング

例:

```
DHCP Server config> change vendor-option
     Enter the vendor name []? XA-clients
     Enter the new vendor name [XA-clients]?
     Enter the new vendor data [01 aa 04]?
```

Delete

delete コマンドは、クラス、クライアント、オプション、サブネット、サブネット・グループ、またはベンダー・オプションを削除するのに使用します。

構文:

delete class

client

option

subnet

subnet-group

vendor-option

class *scope [subnet_name] class_name*
クラスと、その有効範囲内で定義されたすべてのオプションを削除します。

scope クラスが削除される有効範囲を指定します。

有効値 : global または subnet

デフォルト値 : なし

subnet-name

scope が *subnet* の場合にだけ有効です。クラスが削除されるサブネットの名前を指定します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

class-name

削除されるクラスの名前を指示します。

有効値 : 既存のクラス名

デフォルト値 : なし

例:

```
DHCP Server config> delete class global
     Enter the class name []? ClassA
```

例:

```
DHCP Server config> delete class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
```

client *scope [subnet_name] client_name*
クライアントと、その有効範囲内で定義されたすべてのオプションを削除します。

scope クライアントが削除される有効範囲を指定します。

有効値 : global または subnet

デフォルト値 : なし

subnet_name

scope が *subnet* の場合にだけ有効です。クライアントが削除されるサブネットの名前を指定します。

有効値 : 既存のサブネット名

デフォルト値 : なし

client_name

削除されるクライアントの名前を指示します。

有効値 : 既存のクライアント名

デフォルト値 : なし

例:

```
DHCP Server config>  delete client global
     Enter the client name []? ClientA
```

例:

```
DHCP Server config> delete client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
```

option *scope [subnet_name] [class_name] [client_name] [vendor_name] code*
指定された有効範囲内のオプションを削除します。

scope オプションが削除される有効範囲を指定します。

有効値 :

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

デフォルト値 : なし

subnet-name

scope が*subnet*、*class-subnet*、または *client-subnet* の場合にだけ有効です。クライアントが削除されるサブネットの名前を指定します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

class-name

scope が *class-global* または *class-subnet* の場合にだけ有効です。オプションが削除されるクラスの名前を指示します。

有効値 : 既存のクラス名

デフォルト値 : なし

client-name

scope が *client-global* または *client-subnet* の場合にだけ有効です。オプションが追加されるクライアントの名前を指示します。

有効値 : 任意の既存のクライアント名

デフォルト値 : なし

vendor-name

scope が *vendor-option* の場合にだけ有効です。オプションが削除されるベンダーの名前を指示します。

有効値 : 任意の既存のベンダー名

デフォルト値 : なし

code オプション・コードを指定します。DHCP オプションは、RFC 2132

で定義されています。オプションおよびそれぞれの形式については、566ページの『DHCP オプション』を参照してください。

有効値: 1 ～ 255

デフォルト値 : 1

例:

```
DHCP Server config>  delete option global
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option subnet
     Enter the subnet name []? subA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option class-global
     Enter the class name []? ClassA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option client
     Enter the client name []? ClientA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA
     Enter the option code [1]? 3
```

例:

```
DHCP Server config> delete option vendor-option
     Enter the vendor name []? XI-clients
     Enter the option code [1]? 85
```

例:

```
DHCP Server config> delete option vendor-option
     Enter the vendor name []? 200
     Enter the option code [1]? 86
```

subnet *subnet_name*

サブネットと、その有効範囲内で定義されたすべてのクラス、クライアント、およびオプションを削除します。

subnet_name

削除されるサブネットの名前を指定します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

例:

```
DHCP Server config> delete subnet
     Enter the subnet name []? subA
```

```
You are about to delete a subnet subA
and all the associated class, client, and option records associated with it
Are you sure you want to continue? [No]:
```

subnet-group *subnet_group_name*

特定のサブネット・グループと、サブネット有効範囲内で定義されたすべてのクラス、クライアント、およびオプションと関連付けられたすべてのサブネットを削除します。

subnet_group_name

サブネット・グループを識別する名前を指定します。

有効値 : 既存のサブネット・グループ名

デフォルト値 : なし

例:

```
DHCP Server config> delete subnet-group
     Enter the subnet group name []? group2
     You are about to delete a all subnets in group group2
     and all the associated class, client, and option records associated with them
     Are you sure you want to continue? [No]:
```

vendor-option *vendor_name*

ベンダー・オプションと、その有効範囲内で定義されたあらゆるオプションを削除します。

vendor_name

ベンダーの名前を指示します。

有効値 : 長さが最大 40 文字の ASCII ストリング

デフォルト値 : なし

例:

```
DHCP Server config> delete vendor-option
     Enter the vendor name []? XA-clients
```

Disable

disable コマンドは、DHCP サーバーをグローバルに使用不可にするのに使用します。

構文:

disable dhcp-server

例:

```
DHCP Server config> disable dhcp-server
```

Enable

enable コマンドは、DHCP サーバーをグローバルに使用可能にするのに使用します。

構文:

enable dhcp-server

例:

```
DHCP Server config> enable dhcp-server
```

List

list コマンドは、クラス、クライアント、グローバル・パラメーター、サブネット、またはベンダー・オプションに関する構成情報のほか、関連付けられたすべてのオプションを表示するのに使用します。

構文:

list class
client
global
option
subnet
vendor-option

class all
global *class-name*
subnet *class-name*

構成されたすべてのクラスの要約または特定のクラスの詳細のどちらかを表示します。

class-name
表示されるクラスの名前を指示します。

有効値 : 既存のクラス名

デフォルト値 : なし

例:

```
DHCP Server config> list class all

     class              attached
     name               to subnet
     ------------------------------------------------------------
     ClassA
     ClaA               subA
```

例:

```
DHCP Server config> list class global
     Enter the class name []? ClassA

     class
     name
     ------------------------------------------------------------
     ClassA
     Bootstrap Server: 100.100.100.100
     Canonical: Yes
     Support Unlisted Clients: Yes
     Number of Options: 1
     option option
```

```
     code       data
     ------------------------------------------------------------
     1          255.255.0.0
```

例:

```
DHCP Server config> list class subnet
     Enter the subnet name []? subA
     Enter the class name []? ClaA

     class
     name
     ------------------------------------------------------------
     ClaA
     starting IP address: 10.1.1.3
     ending IP address: 10.1.1.5
     Bootstrap Server: 100.100.100.100
     Canonical: Yes
     Support Unlisted Clients: DHCP

     Number of Options: 1
     option option
     code       data
     ------------------------------------------------------------
     6        9.67.100.1
```

client all

global *client-name*

subnet *client-name*

構成されたすべてのクライアントの要約または特定のクライアントの詳細のどちらかを表示します。

client-name

表示されるクライアントの名前を指示します。

有効値 : 既存のクライアント名

デフォルト値 : なし

例:

```
DHCP Server config> list client all
     client   client   client         attached    IP
     name     type     identifier     to subnet   address
     ------------------------------------------------------------------------------
     ClientA  0        ClientA                    9.1.1.1

     CliA     1        400000000010    subA       10.1.1.10
```

例:

```
DHCP Server config> list client global
     Enter the client name []? ClientA
```

例:

```
DHCP Server config> list client subnet
     Enter the subnet name []? subA
     Enter the client name []? CliA

     client     client     client           IP
     name       type       identifier       address
     ------------------------------------------------------------------
```

```
CliA       1          400000000010      10.1.1.10
Bootstrap Server: 200.200.200.200
Canonical: Yes

Number of Options: 1
option option
code       data
----------------------------------------------------------------
6        9.67.100.1
```

global

グローバル・パラメーターを表示します。

例:

```
DHCP Server config> list global

    DHCP server Global Parameters
    =============================
    DHCP server enabled: Yes

    Balance: group2

    Inorder: group1

    Canonical: No

    Lease Expire Interval: 1 minute(s)
    Lease Time Default: 1 day(s)

    Support BOOTP Clients: No
    Bootstrap Server: Not configured

    Support Unlisted Clients: Yes
    Ping Time: 1 second(s)
    Used IP Address Expire Interval: 15 minute(s)
```

option *scope [subnet-name] [class-name] [client-name] [vendor-name] code*

scope オプションが表示される有効範囲を指定します。

有効値 :

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

デフォルト値 : なし

subnet-name

scope が *subnet*、*class-subnet*、または *client-subnet* の場合にだけ有効です。表示されているオプションが属しているサブネットの名前を指定します。

有効値 : 任意の既存のサブネット名

デフォルト値 : なし

class-name

scope が *class-global* または *class-subnet* の場合にだけ有効です。表示されているオプションが属しているクラスの名前を指示します。

有効値 : 既存のクラス名

デフォルト値 : なし

client-name

scope が *client-global* または *client-subnet* の場合にだけ有効です。表示されているオプションが属しているクライアントの名前を指示します。

有効値 : 任意の既存のクライアント名

デフォルト値 : なし

vendor-name

scope が *vendor-option* の場合にだけ有効です。表示されているオプションが属しているベンダーの名前を指示します。

有効値 : 任意の既存のベンダー名

デフォルト値 : なし

code オプション・コードを指定します。DHCP オプションは、RFC 2132 で定義されています。オプションおよびそれぞれの形式については、566ページの『DHCP オプション』を参照してください。

有効値: 1 〜 255

デフォルト値 : 1

例:

```
DHCP Server config> list option global

     option option
     code       data
     ------------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option class-global
     Enter the class name []? ClassA
     option option
     code       data
     ------------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option class-subnet
     Enter the subnet name []? subA
     Enter the class name []? claA

     option option
     code       data
     ------------------------------------------------------------------
```

```
     3        9.67.100.1
```

例:

```
DHCP Server config> list option client-global
     Enter the client name []? ClientA
     option option
     code       data
     ------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option client-subnet
     Enter the subnet name []? subA
     Enter the client name []? cliA

     option option
     code       data
     ------------------------------------------------------------
     3        9.67.100.1
```

例:

```
DHCP Server config> list option subnet
     Enter the subnet name []? subA


     option option
     code       data
     ------------------------------------------------------------
     6        9.67.100.1
```

例:

```
DHCP Server config> list option vendor-option
      Enter the vendor name []? XI-clients


     option option
     code       data
     ------------------------------------------------------------
     85        hex:01 aa 04
     86        9.67.85.4
```

subnet

all

detailed *subnet-name*

構成されたすべてのサブネットの要約または特定のサブネットの詳細のどちらかを表示します。

subnet-name

表示されるサブネットの名前を指示します。

有効値 : 既存のサブネット名

デフォルト値 : なし

例:

```
DHCP Server config> list subnet all
```

```
name    address    mask          IP Addr    IP Addr
------------------------------------------------------------------------
subA    10.1.1.0   255.255.0.0   10.1.1.1   10.1.1.31
subB    11.1.1.0   255.255.0.0   11.1.1.1   11.1.1.31
```

例:

```
DHCP Server config> list subnet detailed
     Enter the subnet name []? subA

     subnet    subnet     subnet        starting      ending
     name      address    mask          IP Addr       IP Addr
     ------------------------------------------------------------------------
     subA      10.1.1.0   255.255.0.0   10.1.1.1      10.1.1.31
     Subnet Group: group1/1

     Number of Classes: 1
     class
     name
    ------------------------------------------------------------
     ClaA
     starting IP address: 10.1.1.1
     ending   IP address: 10.1.1.6
     Bootstrap Server:   100.100.100.100
     Canonical: Yes
     Support Unlisted Clients: DHCP

     Number of Options: 1
     option   option
     code     data
     ------------------------------------------------------------
     6        9.67.100.1

     Number of Clients: 1
     client     client     client            IP
     name       type       identifier        address
     ------------------------------------------------------------------------
     CliA       1          400000000010      10.1.1.10
     Bootstrap Server: 200.200.200.200
     Canonical: Yes

     Number of Options: 1
     option option
     code   data
     ------------------------------------------------------------
     6      9.67.100.1

     Number of Options: 1
     option option
     code   data
     ------------------------------------------------------------
     1      255.255.255.0
```

vendor-option all

detailed *vendor-name*

構成されたすべてのベンダーの要約または特定のベンダーの詳細のどちらかを表示します。

vendor-name

表示されるベンダーの名前を指示します。

有効値 : 既存のベンダー名

デフォルト値 : なし

例:

```
DHCP Server config> list vendor-option all

          vendor          hex
          name            data
          ----------------------------------------------------------------
          XA-clients      01 AA 04
          XI-clients

DHCP Server config> list vendor-option detailed
          Enter the vendor name []? XI-clients
          vendor          hex
          name            data
          ----------------------------------------------------------------
          XI-clients

          Number of Options: 2
          option    option
          code      data
          ----------------------------------------------------------------
          85        hex:01 AA 04
          86        9.67.85.4
```

Set

set コマンドは、グローバル・パラメーターの値を指定したり、Balance および Inorder リストにサブネット・グループを追加するのに使用します。

構文:

set

- balance
- bootstrapserver
- canonical
- inorder
- lease-expire-interval
- lease-time-default
- ping-time
- support-bootp
- support-unlisted-clients
- used-ip-address-expire-interval

balance *subnet_group_name*

Balance リストにサブネット・グループを追加または移動します。アドレスは、それぞれの優先順位に応じて、サブネット・グループ内に定義されたグループ (複数の場合もあり) と関連付けられたすべてのサブネットからラウンドロビン方式で割り当てられます。

subnet_group_name

このサブネットが属しているサブネット・グループ名を指定します。

有効値 : 既存のサブネット・グループ名

デフォルト値 : なし

例:

```
DHCP Server config> set balance
     Enter the subnet group name []? group1
```

bootstrapserver *scope [subnet-name] [class-name] [client-name] address*

DHCP サーバーがクライアントのブートストラップ・サーバーを指定するかどうかを指定します。DHCP サーバーにブートストラップ・サーバーを指定させたくない場合は、そのサーバーの IP アドレスを定義してください。このパラメーターは、グローバル、サブネット、クラス、またはクライアント有効範囲内に指定できます。

scope bootstrapserver パラメーターの有効範囲を指定します。

有効値 :

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

デフォルト値 : なし

subnet-name

scope が *subnet*、*class-subnet*、または *client-subnet* の場合にだけ有効です。ブートストラップ・サーバーが属しているサブネットの名前を指示します。

有効値 : 既存のサブネット名

デフォルト値 : なし

class-name

scope が *class-global* または *class-subnet* の場合にだけ有効です。ブートストラップ・サーバーが属しているクラスの名前を指示します。

有効値 : 既存のクラス名

デフォルト値 : なし

client-name

scope が *client-global* または *client-subnet* の場合にだけ有効です。ブートストラップ・サーバーが属しているクライアントの名前を指示します。

有効値 : 既存のクライアント名

デフォルト値 : なし

IP address of the server

ブートストラップ・サーバーの IP アドレスを指定します。

有効値: 小数点付き 10 進数形式の任意の有効な IP アドレス

デフォルト値 : なし

例:

```
DHCP Server config> set bootstrap-server class-global
     Enter the class name []? ClassA
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server class-subnet
     Enter the subnet name []? subA
     Enter the class name []? ClassA
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server client-global
     Enter the client name []? ClientA
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server client-subnet
     Enter the subnet name []? subA
     Enter the client name []? ClientA
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server global
     Enter the IP address of the server []? 100.100.100.100
```

例:

```
DHCP Server config> set bootstrap-server subnet
     Enter the subnet name []? subA
     Enter the IP address of the server []? 100.100.100.100
```

canonical *scope [subnet-name] [class-name] [client-name] value*

DHCP サーバーが MAC アドレスを標準形式に変換するかどうかを指定します。

イーサネット /802.3 クライアントの MAC アドレスは、標準 (バイトは最下位ビットから始まります) 形式で保管されます。トークンリング・クライアントの MAC アドレスは、非標準 (バイトは最上位ビットから始まります) 形式で保管されます。このパラメーターは、DHCP サーバーが一方のメディア・タイプ (トークンリングまたはイーサネット /802.3) 上にあり、クライアントがもう一方のメディア・タイプ上にあり、その 2 つを結ぶ変換ブリッジがある場合に使用します。このパラメーターを *yes* に設定すると、DHCP サーバーにより、クライアントの MAC アドレスは canonical (標準) から non-canonical (非標準) へ、あるいは non-canonical (非標準) から canonical (標準) へ切り替えられます。DHCP サーバーには MAC アドレスの本来の形式が分からないため、このパラメーターを *yes* に設定しても、アドレスが切り替えられるだけです。Canonical は、グローバル、サブネット、クラス、またはクライアント有効範囲内で設定できます。

scope bootstrapserver パラメーターの有効範囲を指定します。

有効値 :

- class-global
- class-subnet
- client-global
- client-subnet
- global

- subnet

デフォルト値 : なし

subnet-name

scope が *subnet*、*class-subnet*、または *client-subnet* の場合にだけ有効です。canonical が指定されるサブネットの名前を指示します。

有効値 : 既存のサブネット名

デフォルト値 : なし

class-name

scope が *class-global* または *class-subnet* の場合にだけ有効です。canonical が指定されるクラスの名前を指示します。

有効値 : 既存のクラス名

デフォルト値 : なし

client-name

scope が *client-global* または *client-subnet* の場合にだけ有効です。canonical が指定されるクライアントの名前を指示します。

有効値 : 既存のクライアント名

デフォルト値 : なし

value MAC アドレスを canonical 形式に変換するかどうかを指定します。

有効値 : yes、no

デフォルト値 : no (**scope** が *global* の場合)。それ以外の場合、デフォルト値は、有効範囲階層によって決定されます。有効範囲の説明については、563ページの『概念と用語』を参照してください。

例:

```
DHCP Server config> set canonical class-global
     Enter the class name []? ClassA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical class-subnet
 Enter the subnet name []? subA
 Enter the class name []? ClassA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical client-global
 Enter the client name []? ClientA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical client-subnet
 Enter the subnet name []? subA
 Enter the client name []? ClientA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical global
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

例:

```
DHCP Server config> set canonical subnet
 Enter the subnet name []? subA
 Would you like MAC addresses to be transformed to canonical format? [No] yes
```

inorder *label-list*

Inorder リストにサブネット・グループを追加または移動します。アドレスは、サブネットに割り当てられた優先順位順にサブネット・グループ内のサブネットから割り当てられます。

subnet_group_name

このサブネットが属しているサブネット・グループを指定します。

有効値 : 既存のサブネット・グループ名

デフォルト値 : なし

例:

```
DHCP Server config> set inorder
     Enter the subnet group name []? g2
```

lease-expire-interval *time length*

満了したリースを判別するためにアドレス・プール内のすべてのアドレスのリース条件を調べる間隔を指定します。リースの満了間隔は、グローバル・レベルでだけ設定できます。

time 時間の測定単位を指定します。

有効値 : seconds、minutes、hours

デフォルト値 : なし

length 間隔の長さを指定します。

有効値 : 15 秒 ～ 12 時間

デフォルト値 :

- 15 (時間単位が seconds (秒) の場合)
- 1 (時間単位が minutes (分) の場合)
- 1 (時間単位が hours (時間) の場合)

例:

```
DHCP Server config> set lease-expire-interval seconds
     How long is the interval in seconds (max:59) [15]? 59
```

例:

```
DHCP Server config> set lease-expire-interval minutes
     How long is the interval in minutes (max:59) [1]? 45
```

例:

```
DHCP Server config> set lease-expire-interval hours
     How long is the interval in hours (max:12) [1]?  2
```

lease-time-default *time length*

DHCP サーバーが発行したリースのデフォルトのリース期間を指定します。infinity (無限大) という間隔は、リースが満了しないことを意味します。リース時間のデフォルトは、グローバル・レベルでだけ設定できます。

time 時間の測定単位を指定します。

有効値 : minutes、hours、days、weeks、months、years、infinity

デフォルト値 : なし

length 間隔の長さを指定します。

有効値 : 3 分 ～ 無限大

デフォルト値 :

- 3 (時間単位が minutes (分) の場合)
- 1 (時間単位が hours (時間) の場合)
- 1 (時間単位が days (日) の場合)
- 1 (時間単位が months (月) の場合)
- 1 (時間単位が years (年) の場合)

例:

```
DHCP Server config> set lease-time-default minutes
     How long is the interval in minutes (max:59) [3]?  2
```

例:

```
DHCP Server config> set lease-time-default hours
     How long is the interval in hours (max:23) [1]? 12
```

例:

```
DHCP Server config> set lease-time-default days
     How long is the interval in days (max:6) [1]?  2
```

例:

```
DHCP Server config> set lease-time-default weeks
     How long is the interval in weeks (max:3) [1]?  1
```

例:

```
DHCP Server config> set lease-time-default months
     How long is the interval in months (max:11) [1]?  3
```

例:

```
DHCP Server config> set lease-time-default years
     How long is the interval in years (max:10) [1]?  3
```

例:

```
DHCP Server config> set lease-time-default infinity
```

ping-time *time length*

IP アドレスを割り当てる前に、DHCP サーバーは、その IP アドレスが使用中でないかテストして確認します。この値は、DHCP サーバーがアドレスを使用可能とマークする前に ping 応答を待つ時間を指定します。値 0 の場合は ping が使用不可にされ、その結果、DHCP サーバーはアドレスを割り当てる前にテストを行いません。

time 時間の測定単位を指定します。

有効値 : seconds

デフォルト値 : なし

length 間隔の長さを指定します。

有効値 : 0 ～ 5 秒

デフォルト値 : 1

例:

```
DHCP Server config> set ping-time seconds
   How long is the interval in seconds (max:5) [1]? 3
```

support-bootp *value*

サーバーが BOOTP クライアントからの要求に応答するかどうかを指定します。DHCP サーバーが以前、BOOTP クライアントをサポートするよう構成されており、BOOTP クライアントをサポートしないように再構成されていない場合は、再構成の前に確立された BOOTP クライアントについてのアドレス・バインドは、BOOTP クライアントが別の要求を送信するまで (リスタートするとき) 保持されます。クライアントが別の要求を送信したときに、サーバーは応答せず、バインドは消去されます。このパラメーターは、グローバル・レベルでだけ設定できます。

有効値 : yes または no

デフォルト値: no

例:

```
DHCP Server config> set support-bootp
     Would you like the server to support BOOTP clients? [No] yes
```

support-unlisted-clients *scope [subnet-name] [class-name] value*

サーバーが、この構成内に特別に表示されているクライアント ID をもっている DHCPクライアント以外のクライアントからの要求に応答するかどうかを指定します。このパラメーターの可能な値は、次のものです。

scope **support-unlisted-clients** パラメーターの有効範囲を指定します。

有効値 :

- class-global
- class-subnet
- global
- subnet

デフォルト値 : なし

subnet-name

scope が *subnet*、*class-subnet*、または *client-subnet* の場合にだけ有効です。このパラメーターが指定されるサブネットの名前を指示します。

有効値 : 既存のサブネット名

デフォルト値 : なし

class-name

scope が *class-global* または *class-subnet* の場合にだけ有効です。このパラメーターが指定されるクラスの名前を指示します。

有効値 : 既存のクラス名

デフォルト値 : なし

value

yes DHCP サーバーは、クライアントのタイプがなんであれ、

また、クライアントが構成済みであろうとなかろうと、あらゆるクライアントに応答する必要があります。

no DHCP サーバーは、構成済みの DHCP クライアントからの要求にだけ応答します。

bootp DHCP サーバーは、表示されていない BOOTP クライアントはサポートしますが、表示されていない DHCP クライアントはサポートしません。

dhcp DHCP サーバーは、表示されていない DHCP クライアントには応答しますが、表示されていない BOOTP クライアントには応答しません。

有効値 : yes、no、bootp、dhcp

デフォルト値 : yes (**scope** が *global* の場合)。それ以外の場合、デフォルト値は、有効範囲階層によって決定されます。有効範囲の説明については、563ページの『概念と用語』を参照してください。

例:

```
DHCP Server config> set support-unlisted-clients class-global yes
     Enter the class name []? ClassA
```

例:

```
DHCP Server config> set support-unlisted-clients class-subnet no
     Enter the subnet name []? subA
     Enter the class name []? ClassA
```

例:

```
DHCP Server config> set support-unlisted-clients global bootp
```

例:

```
DHCP Server config> set support-unlisted-clients subnet dhcp
     Enter the subnet name []? subA
```

used-ip-address-expire-interval *time length*

アドレスを割り当てに使用できるようにする前に使用中の IP アドレスをサーバーが保持する間隔を指定します。サーバーは IP アドレスを割り振る前に、そのアドレスがネットワーク上ですでに使用されていないか確認するために ping します。サーバーは、次に、使用中のアドレスに予約済みのマークを付けます。このパラメーターは、使用中のアドレスを割り当てに使用できるようにする前に予約済みとして保持する期間を指定します。このパラメーターは、グローバル・レベルでだけ設定できます。

time 時間の測定単位を指定します。

有効値 :
seconds、minutes、hours、days、weeks、months、years、infinity

デフォルト値 : なし

length 間隔の長さを指定します。

有効値 : 30 秒 ～ 無限大

デフォルト値 :

- 30 (時間単位が seconds (秒) の場合)

- 15 (時間単位が minutes (分) の場合)
- 1 (時間単位が hours (時間) の場合)
- 1 (時間単位が days (日) の場合)
- 1 (時間単位が months (月) の場合)
- 1 (時間単位が years (年) の場合)

例:

```
DHCP Server config> set used-ip-address-expire-interval seconds
     How long is the interval in seconds (max:59) [30]? 2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval minutes
     How long is the interval in minutes (max:59) [15]? 2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval hours
     How long is the interval in hours (max:23) [1]?  5
```

例:

```
DHCP Server config> set used-ip-address-expire-interval days
     How long is the interval in days (max:6) [1]?  2
```

例:

```
DHCP Server config> set used-ip-address-expire-interval weeks
     How long is the interval in weeks (max:3) [1]?  1
```

例:

```
DHCP Server config> set used-ip-address-expire-interval months
     How long is the interval in months (max:11) [1]?  3
```

例:

```
DHCP Server config> set used-ip-address-expire-interval years
     How long is the interval in years (max:10) [1]?  3
```

例:

```
DHCP Server config> set used-ip-address-expire-interval infinity
```

DHCP サーバー監視環境へのアクセス

DHCP サーバー*監視* 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 5** と入力する。たとえば、次のようになります。

   ```
   * talk 5
   Config>
   ```

   talk 5 コマンドを入力すると、端末に CONFIG プロンプト (+) が表示されます。初めて構成に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. + プロンプトで、**feature dhcp-server** コマンドを入力して、DHCP Server> プロンプトを表示する。

DHCP サーバー監視コマンド

表 65. DHCP サーバー監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Disable	DHCP サーバーを動的に使用不可にします。
Enable	DHCP サーバーを動的に使用可能にします。
List	クラス、クライアント、グローバル、サブネット、およびベンダー・オプションのパラメーターを表示します。
Reset	DHCP サーバー構成を動的にリセットします。
Request	
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Disable

disable コマンドは、DHCP サーバーを動的に使用不可にするのに使用します。

構文:

disable dhcp

Enable

enable コマンドは、DHCP サーバーを動的に使用可能にするのに使用します。

構文:

enable dhcp

List

list コマンドは、クラス、クライアント、グローバル・パラメーター、サブネット、またはベンダー・オプションに関する構成情報のほか、関連付けられたすべてのオプションを表示するのに使用します。**list** コマンドの例については、603ページの『List』を参照してください。

構文:

list class
client
global
option
subnet
vendor-option

Reset

reset コマンドは、DHCP サーバー構成を動的にリセットするのに使用します。

構文:

reset dhcp

例:

```
DHCP Server> reset dhcp
You are about to reset the DHCP Server.
Are you sure you want to continue? [No]: y
DHCP Server has been reset
DHCP Server>
```

Request

request コマンドは、管理情報を表示するのに使用します。

構文:

request clientid

delete

ipquery

poolquery

stats

status

clientid *client_id*

クライアントの情報を表示します。

client_id

クライアントの識別子を指示します。

有効値 : 既存のクライアント ID

デフォルト値 : なし

例:

```
DHCP Server>  request clientid
     Enter the client name []? 0020351FB371

     Client id:             1-0x0020351FB371
     Status: BOUND
     Address last assigned: 192.9.200.10
     Most recent lease time: 16:41:25 December 3, 1998
     Proxy flag: FALSE
     Hostname:              Win-XY-1
     Domain name:           city.net
```

delete *address*

特定のクライアントの IP アドレスについてリースを削除します。

address

削除されるクライアントの IP アドレスを指示します。

有効値: 既存のクライアントの任意の有効な IP アドレス

デフォルト値 : なし

例:

```
DHCP Server>  request delete
Enter the client's IP address []? 194.3.200.10
```

ipquery *address*

IP アドレスの情報を表示します。

例:

```
DHCP Server>req ipquery 192.168.8.3
IP address:       192.168.8.3
Status:           RECLAIMED
Lease time:            86400 seconds
Start time:       Not Leased
Last time leased: 04:16:33  March 9, 1999
DHCP Server>
```

poolquery *address*

IP アドレスのプールの情報を表示します。

address

表示されるプール内の IP アドレスを指示します。

有効値 : 表示されるプール内の任意の有効な IP アドレス

デフォルト値 : なし

例:

```
DHCP Server>  request poolquery

Enter the client's IP address []? 194.3.200.10
     IP address:            194.3.200.10
     Status:                LEASED
     Lease time:            86400 seconds
     Start time:            16:41:25 December 3, 1998
     Last time leased:      16:41:25 December 3, 1998
     Client id:             1-0x0020351FB371
     Hostname:              Win-XY-1
     Domain name:           city.net
     IP address:            194.3.200.11
     Status:                STOCKED
     IP address:            194.3.200.12
     Status:                STOCKED
```

stats サーバーが管理するアドレスのプールに関する統計情報を表示します。統計情報には、処理されたディスカバー・パケット、応答のなかったディスカバー・パケット、行われた提示、許可されたリース、否定応答 (NAK) 、処理された通知 (通知プラス確認応答 (ACK) を含む)、更新、リリース、処理された BOOTP クライアント、更新を試みられた proxyARec、サポートされていないパケットが含まれます。

構文 : request stats

例:

```
DHCP Server> request stats
       Number of DISCOVER requests received:      8
       Number of OFFER responses sent:            4
       Number of ACK responses sent:              3
       Number of NACK responses sent:             0
       Number of RELEASE requests received:       0
       Number of DECLINE packets received:        0
       Number of INFORM requests received:        0
       Number of BOOTP requests received:         0
       Number of requests received via proxy:     0
       Number of UNSUPPORTED requests received:   0
       Total number of request/responses:        15
       Number of lease expirations:               0
```

status アドレス・プールに関する情報を表示します。

例:

```
DHCP Server> request status

     IP address:            194.3.200.10
     Status:                LEASED
     Lease time:            86400 seconds
     Start time:            16:41:25 December 3, 1998
```

```
Last time leased:       16:41:25 December 3, 1998
Client id:              1-0x0020351FB371
Hostname:               Win-XY-1
Domain name:            city.net

IP address:             194.3.200.11
Status:                 STOCKED

IP address:             194.3.200.12
Status:                 STOCKED

IP address:             194.3.200.10
Status:                 STOCKED
```

DHCP 動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

動的ホスト構成プロトコル (DHCP) は、CONFIG (Talk 6) **delete interface** コマンドをサポートしません。

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、動的ホスト構成プロトコル (DHCP) には適用できません。DHCP 構成は、特定のインターフェースに基づいていません。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、動的ホスト構成プロトコル (DHCP) には適用できません。DHCP 構成は、特定のインターフェースに基づいていません。

GWCON (Talk 5) 構成要素リセット・コマンド

動的ホスト構成プロトコル (DHCP) は、次の動的ホスト構成プロトコル (DHCP) 固有 GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature DHCP, Reset DHCP コマンド

説明: DHCP サーバーをリセットし、変更済みの構成で初期設定します。

ネットワークへの影響:

変更済みの構成が同じクライアントをサポートする場合、クライアントには更新時に新しいリースが与えられます。変更済み構成が同じクライアントをサポートしない場合には、そのリースは期限切れになります。

制限事項:

- ハード・ディスクまたはフラッシュ記憶カードのないルーターで、リセットのあと、DHCP クライアントは、それらのリースを用いて稼働し続けますが、DHCP サーバーにはそれらについての情報がなくなります。

- ハード・ディスクまたはフラッシュ記憶カードのないルーターで、DHCP サーバーが前にリースした IP アドレスは、このアドレスを再びリースしようとすると、“GWCON, feature DHCP, request status” コマンドに “USED” とマークが付けられます。

次の表では、**GWCON, feature DHCP, reset dhcp** コマンドが起動されると活動化される動的ホスト構成プロトコル (DHCP) の構成変更を要約します。

GWCON, feature DHCP, reset dhcp コマンドによって変更が活動化されるコマンド
CONFIG, feature DHCP, add class
CONFIG, feature DHCP, add client
CONFIG, feature DHCP, add option
CONFIG, feature DHCP, add subnet
CONFIG, feature DHCP, add vendor-option
CONFIG, feature DHCP, change class
CONFIG, feature DHCP, change client
CONFIG, feature DHCP, change subnet
CONFIG, feature DHCP, change vendor-option
CONFIG, feature DHCP, delete class
CONFIG, feature DHCP, delete client
CONFIG, feature DHCP, delete option
CONFIG, feature DHCP, delete subnet
CONFIG, feature DHCP, delete subnet-group
CONFIG, feature DHCP, delete vendor-option
CONFIG, feature DHCP, disable dhcp-server
CONFIG, feature DHCP, enable dhcp-server
CONFIG, feature DHCP, set balance
CONFIG, feature DHCP, set bootstrapserver
CONFIG, feature DHCP, set canonical
CONFIG, feature DHCP, set inorder
CONFIG, feature DHCP, set lease-expire-interval
CONFIG, feature DHCP, set lease-time-default
CONFIG, feature DHCP, set ping-time
CONFIG, feature DHCP, set support-bootp
CONFIG, feature DHCP, set support-unlisted-clients
CONFIG, feature DHCP, set used-ip-address-expire-interval

GWCON (Talk 5) 一時変更コマンド

動的ホスト構成プロトコル (DHCP) は、装置の操作状態を一時変更する、次の GWCON コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行すると、行われません。

・コマンド

GWCON, feature DHCP, disable dhcp
GWCON, feature DHCP, enable dhcp

非動的再構成可能コマンド

動的ホスト構成プロトコル (DHCP) の構成パラメーターは、動的に変更できます。

第35章 シン・サーバー・フィーチャーの使用

この章では、IBM 2216 のシン・サーバー・フィーチャー (TSF) の使用法について説明します。

ネットワーク・ステーションの概説

ネットワーク・ステーションは、パーソナル・コンピューター (PC) に似ており、キーボード、ディスプレイ、およびマウスを備えています。ネットワーク・ステーションと PC の主な相違点は、ネットワーク・ステーションのファイルは、マシン内部のハード・ディスク上ではなく、ネットワーク・サーバー上に常駐することです。ネットワーク・ステーションはグラフィカル・ユーザー・インターフェース (GUI) を提供し、ユーザーはこれを使用してエミュレーター、リモート X アプリケーション、Web ブラウザー、アプリケーション、およびプリンターなど、さまざまなリソースにアクセスできます。

ネットワーク・ステーションは、トークンリングまたはイーサネット接続を介し、TCP/IP を使用して、サーバーと通信します。ネットワーク・ステーションの電源オン・プロセスは、次のとおりです。

- 不揮発性ランダム・アクセス・メモリーに常駐するブート・モニター・プログラムが開始し、電源オン自己テストが実行されます。
- ネットワーク・ステーションが、IP アドレス、サーバー・アドレス、ブート・ファイルのパスと名前などの情報をネットワーク・ステーションに提供する BootP または DHCP サーバーに接続します。代わりに、ネットワーク・ステーションは、不揮発性ランダム・アクセス・メモリーに保管されている値からこの情報を取り出すこともできます。
- ネットワーク・ステーションが、トリビアル・ファイル転送プロトコル (TFTP)、リモート・ファイル・システム/400 (RFS/400)、またはネットワーク・ファイル・システム (NFS) を使用して、オペレーティング・システム、ハードウェア構成ファイル、およびアプリケーション・プログラムなどの基本コードを、基本コード・サーバーからダウンロードします。
- ネットワーク・ステーションが、ネットワーク・ステーションに接続されているプリンターの構成やネットワーク・ステーションのキーボード言語などの端末ベース構成情報を、端末構成サーバーからダウンロードします。
- ネットワーク・ステーションがログオン画面を表示します。ここで、ユーザー ID とパスワードを入力することができます。
- 認証サーバーがユーザー ID とパスワードの妥当性検査を行い、パーソナル・ユーザー・ファイルへのアクセスを許可します。
- ユーザーの個別設定環境の変更がダウンロードされます。
- ネットワーク・ステーションが個別設定デスクトップを表示します。

ネットワーク・ステーションについて詳しくは、*IBM Network Station Manager Installation and Use* を参照してください

シン・サーバー・フィーチャーの概説

1 台の物理装置が BootP/DHCP サーバー、ブート・サーバー、端末構成サーバー、および認証サーバーとして機能することも、それぞれのサーバーを別々の装置にすることもできます。たとえば、ネットワーク・ステーションを AS/400® に接続し、AS/400 が BootP サーバー、基本コード・サーバー、端末構成サーバー、および認証サーバーの役割を果たすことができます。代わりに、各サーバーを別々の物理装置にすることもできます。たとえば、Windows® NT サーバーが DHCP サーバーとして働き、AS/400 が基本コード・サーバー、別の AS/400 が端末構成サーバー、さらに別の AS/400 が認証サーバーとして働くネットワークにネットワーク・ステーションを接続するといったことが可能です。

シン・サーバー・フィーチャーを使用すると、2216 を基本コード・サーバーにすることができます。TSF の使用が望ましい理由を示す 1 つの例を、627ページの図49 と 627ページの図50 に示します。 627ページの図49 では、ネットワーク・ステーションに必要なファイルはすべて単一のサーバーからダウンロードされます。ネットワーク・ステーションの電源オン時には、ダウンロードは数メガバイトに達します。これは、特に多数のネットワーク・ステーションが同時に電源を入れた場合、ネットワーク・インフラストラクチャーだけではなく、基本コード / 端末構成サーバーまたは認証サーバーとして働く装置にとっても、非常に大きな負担がかかる可能性があります。627ページの図50 は、リモート側で シン・サーバーが使用されているネットワークを示しています。ネットワーク・ステーションのブート・コードに関連するファイルの多くは、シン・サーバーによってキャッシュされます。ネットワーク・ステーションの電源をオンにしたとき、ほとんどのブート・コードは シン・サーバーからロードされ、ネットワーク・インフラストラクチャーを通してトランスポートする必要があるデータはわずかな量だけになります。このように 1 つのサーバーの処理が減ることにより、ネットワーク・トラフィックが減少し、ネットワーク・ステーションの電源オンを完了させるのに必要な時間を短縮することができます。

シン・サーバーによってキャッシュされるファイルは、マスター・ファイル・サーバーに常駐するファイルのコピーなので、マスター・ファイル・サーバー上のバージョンが変更された場合、シン・サーバーはそのファイルのバージョンを更新する必要があります。次の時点で、シン・サーバーは、すべてのキャッシュ・ファイルがマスター・ファイル・サーバーのバージョンと同一であることを確認します。

1. IBM 2216 の電源オン時
2. IBM 2216 の再ロードまたはリスタート時
3. TSF のリスタート時
4. TSF 構成で指定された時間間隔に達したとき
5. SNMP MIB アクション・パラメーターによって起動されたとき
6. TSF `talk 5` **refresh** コマンドが出されたとき
7. ファイルにアクセスするたびに (TFTP を除く)。TSF は、アクセスした各ファイルが、マスター・ファイル・サーバー上のバージョンに一致していることを確認します。相違が検出された場合、ファイルは更新されます。その後で TSF は、残りのファイルもマスター・ファイル・サーバーに一致していることを確認します。

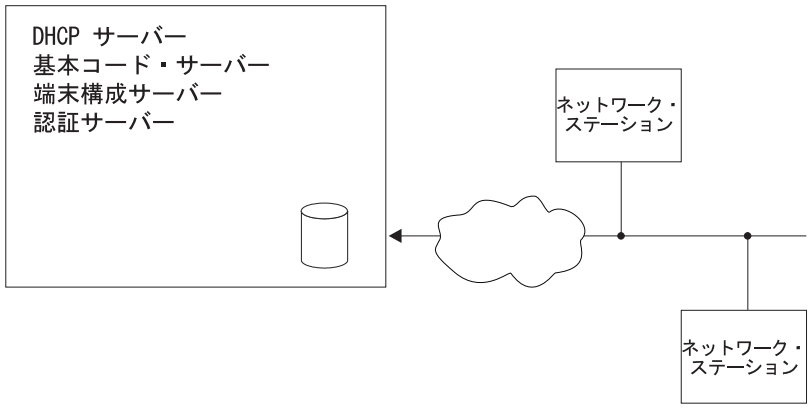


図 49. シン・サーバーのないリモート・ネットワーク・ステーション

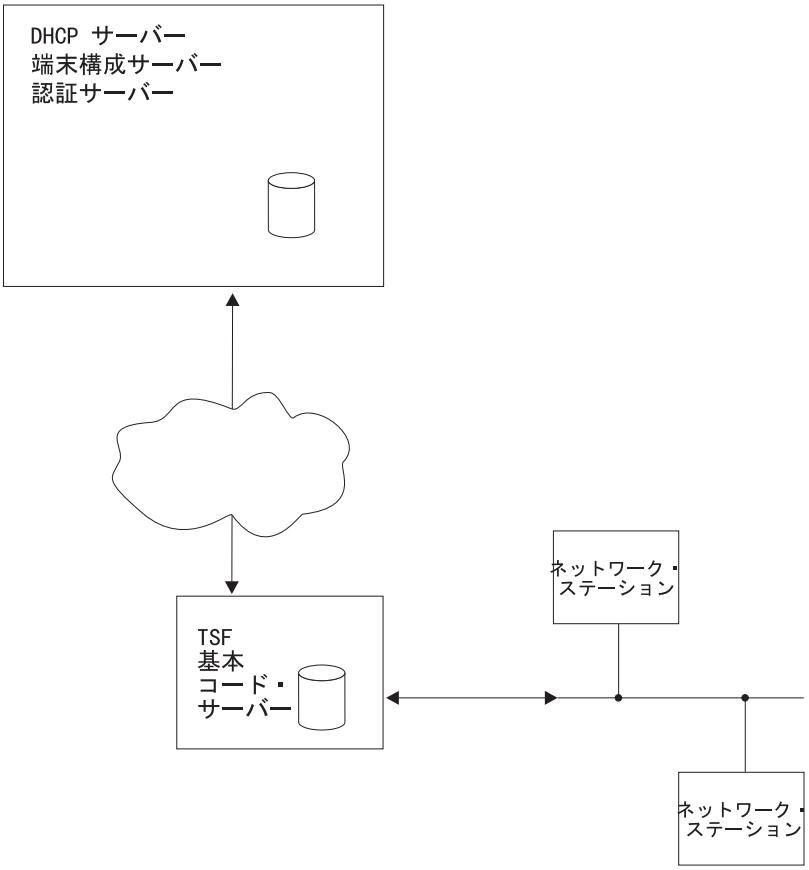


図 50. シン・サーバーのあるリモート・ネットワーク・ステーション

BootP/DHCP サポート

BootP/DHCP サーバー・サポートには、次の 2 つのオプションがあります。

- IBM 2216 DHCP サーバー・サポートを使用する。 557ページの『第33章 DHCP サーバーの使用』を参照してください。

- BootP/DHCP 要求の中継エージェントとして働くよう IBM 2216 を構成する。詳細については、*プロトコルの構成と監視 解説書 第 1 巻* の章を参照してください。

複数サーバー環境については、*IBM Network Station Manager Installation and Use* を参照してください。

ネットワーク・ステーションとの通信に使用するプロトコル

ネットワーク・ステーションとそのサーバー間の通信に使用するプロトコルは、BootP/DHCP の構成またはネットワーク・ステーション NVRAM の構成のどちらかで決めます。どちらの場合も、ネットワーク・ステーションが使用するプロトコルは、TSF の構成と互換性がなければなりません。

TSF がマスター・ファイル・サーバーとの通信にリモート・ファイル・システム (RFS) を使用するように構成されている場合、TSF はネットワーク・ステーションからの RFS および TFTP 要求に応答しますが、ネットワーク・ステーションからのネットワーク・ファイル・システム (NFS) 要求には応答しません。

NFS ネットワーク・ファイル・システムは、リモート・ディスクへの透過的なアクセスを可能にする分散ファイル・システムです。

RFS リモート・ファイル・システム (AS/400-特有) は、基本的に、システム間でファイルを転送するために使用します。

同様に、TSF がマスター・ファイル・サーバーとの通信に NFS を使用するように構成されている場合、TSF はネットワーク・ステーションからの NFS および TFTP 要求に応答しますが、ネットワーク・ステーションからの RFS 要求には応答しません。

RFS の使用

TSF は、RFS を使用して AS/400 への接続を確立します。ネットワーク・ステーションがファイルのオープンを要求すると、TSF は認証のためにその要求を AS/400 に転送します。ネットワーク・ステーションが認証されなかった場合、TSF は要求されたファイルをネットワーク・ステーションに送りません。ネットワーク・ステーションが認証され、AS/400 上の要求されたファイルのバージョンが IBM 2216 TSF に保管されているバージョンと異なっている場合、ネットワーク・ステーションの要求は AS/400 に渡されます。AS/400 上のファイルが、TSF がキャッシュしたファイルと同じバージョンの場合には、TSF はそのファイルをネットワーク・ステーションに提供します。

TSF が disconnected モード用に構成されている場合、TSF はネットワーク・ステーションのすべてのトラフィックをローカルに処理しますが、キャッシュされている場合にはファイルにサービスし、またはキャッシュされていない場合には File Not Found (ファイルが見つからない) というメッセージを戻します。このように、ネットワーク・ステーションが要求しているすべてのファイルをキャッシュに入れることが絶対必要となります。TSF は、マスター・ファイル・サーバーに接続して更新を行いますが、ファイルのオープンまたはファイルごとの認証はマスター・ファイル・サーバーに中継されません。

TSF から AS/400 への接続が利用不能か、または TSF が disconnected モードになっている場合は、TSF は現在キャッシュされているファイルをネットワーク・ステーションに提供します。

TFTP の使用

ネットワーク・ステーションと TSF の間の通信に TFTP が使用されている場合、ファイルが利用可能であれば、TSF はネットワーク・ステーションからのファイルの要求に応じます。TSF とマスター・ファイル・サーバーの間のバージョンの確認は行われません。ファイルが TSF キャッシュ内にない場合には、ネットワーク・ステーションからの要求はマスター・ファイル・サーバーに転送されます。

TSF が disconnected モード用に構成されている場合、TSF はすべてのネットワーク・ステーションをローカルで処理します。ファイルが TSF キャッシュで使用可能ではない場合、TSF は、要求をマスター・ファイル・サーバーに中継する代わりに、File Not Found (ファイルが見つからない) というメッセージを戻します。

NFS の使用

ネットワーク・ステーションと TSF の間の通信に NFS が使用されている場合、ネットワーク・ステーションからファイルの要求があると、TSF はそのファイルがキャッシュ内にある場合は、ファイルのサービスを開始します。同時に、そのファイルがマスター・ファイル・サーバー内のものと同じバージョンであるかどうかを確認します。同じでない場合、TSF はファイルのサービスを打ち切り、ただちにマスター・ファイル・サーバーから新しいバージョンをダウンロードし始めます。

TSF が disconnected モード用に構成されている場合には、TSF は、要求があるたびにそれぞれのファイルを確認しません。

TSF がそのファイルをキャッシュしていない場合、TSF は File Not Found (ファイルが見つからない) というメッセージを戻します。要求されたファイルが、サブディレクトリー*組み込み* として構成されているディレクトリー内に常駐している場合、またはそのような構成のディレクトリー下のサブディレクトリー内に常駐している場合、ファイルがマスター・ファイル・サーバー内に存在すれば、TSF はファイルのキャッシュを開始します。

ファイル・キャッシュの更新

ネットワーク装置上のファイル・キャッシュに使用するプロトコルは、TSF の構成によって決まります。**add master-file-server** コマンドを使用して、マスター・サーバーを指定します。

TSF は、ファイル・サーバーと 2 次ファイル・サーバーの 2 つのマスター・ファイル・サーバーの構成用です。2 次ファイル・サーバーは、バックアップ・ファイル・サーバーです。

RFS と NFS の両方のマスター・ファイル・サーバーについて、ファイル・サーバーと 2 次ファイル・サーバーのアドレスを要求してプロンプト指示が出されます。ファイル・サーバーのアドレスは必須であり、2 次ファイル・サーバーのアドレスは任意指定です。ファイル・サーバーは、この TSF の 1 次マスター・ファイル・サーバーにする必要があります。複数のサーバーが NSM を稼働していて、ファイ

ル・サーバーとして指定したサーバーが使用可能でないときに TSF が使用することになるバックアップまたは代替ファイル・サーバーを指定する必要がある場合には、2 次ファイル・サーバーを指定できます。2 次マスター・ファイル・サーバーが存在しない場合、2 次ファイル・サーバーのアドレスを 0.0.0.0 に設定します。両方のマスター・ファイル・サーバーが NSM の同じバージョンを実行することをお勧めします。RFS を使用する場合、両方の事前ロード・リストを同じにすることをお勧めします。そのようにしなければ、ネットワーク・ステーションの動作が、TSF は 2 次マスター・ファイル・サーバーに切り替えると、変わる場合があります。

ファイル・サーバーと 2 次ファイル・サーバーとを切り替えるまたはそのいずれかを選択することは、Talk 6 **set selection** コマンドによって制御されます。選択を 1 次、2 次、または自動に設定することもできます。選択を 1 次に設定すると、2 次ファイル・サーバーは無視されます。1 次だけが接続されます。構成済みの回数だけ再試行しても 1 次サーバーに接続しない場合には、TSF は、次の更新までこのサーバーへの接続への試行を停止します。選択を 2 次に設定すると、1 次ファイル・サーバー・アドレスは無視されます。2 次だけが接続されます。構成済みの回数だけ再試行しても 2 次サーバーに接続しない場合には、TSF は、次の更新までこのサーバーへの接続への試行を停止します。選択を自動に設定すると、TSF は 1 次ファイル・サーバーに接続しようとします。構成済みの回数だけ再試行しても接続しない場合には、TSF は、2 次ファイル・サーバーに自動的に接続しようとします。

rfs を指定すると、事前ロード・リスト・ファイル名の入力を求めるプロンプトが出ます。事前ロード・リストとは、TSF がキャッシュする必要があるファイルの完全修飾ファイル名を指定する ASCII ファイルです。

nfs を指定すると、キャッシュするディレクトリー名の入力を求めるプロンプトが出ます (いくつかのデフォルト値が提供される場合もあります)。ディレクトリーを指定すると、サブディレクトリーを組み込むかどうかを指定するプロンプトが出ます。*no* (サブディレクトリーを組み込まない) を指定すると、TSF は指定されたディレクトリー内のすべてのファイルを TSF キャッシュに事前ロードします。 *yes* (サブディレクトリーを組み込む) を指定すると、TSF はそのディレクトリーからはどのファイルも事前ロードせず、ネットワーク・ステーションがファイルを要求した時点で、そのディレクトリーとサブディレクトリーから動的にファイルを取り出します。

更新処理が進行中のファイルは、処理中はネットワーク・ステーションに送られません。

シン・サーバー環境の構成

TSF を導入する場合、TSF 自体の他にいくつかの構成を考慮することが必要になります。ここでは、BootP/DHCP サーバー、マスター・ファイル・サーバー、IBM 2216 BootP リレー、IBM 2216 内部 IP アドレス、および IBM 2216 TSF 構成に加える必要がある変更について説明します。Network Station Manager (NSM) リリース 2.5 を実行している AS/400 に接続されたシン・サーバーの例を 633ページの『サンプル構成』に示します。

シン・サーバー環境の構成プロセスについては、次で説明しています。

構成に関する推奨事項

TSF を最大限に活用するのに役立つ、構成に関する推奨事項を次に示します。

- ハード・ディスクを使用する。

  TSF は必ずしもハード・ディスクを必要としませんが、構成されている TSF メモリー・キャッシュが小さ過ぎる場合 (または、2216 内の他の機能のために十分な大きさに構成できない場合)、これを使用すると効率を高めることができます。ハード・ディスクを使用すると、TSF や 2216 をリスタートまたは再ロードした場合にも、効率が改善されます。

- ネットワーク・ステーションの最大数

  TSF は、一度に最大 200 の RFS ネットワーク・ステーションを接続することができます。 80 台以上のネットワーク・ステーションの電源を同時にオンにすると、ネットワーク・ステーションのタイムアウト値を超える遅延が発生します。回復には、ネットワーク・ステーションの電源をもう一度オンにする必要があります。

- マスター・ファイル・サーバーは、Network Station Manager (NSM) を稼働するサーバーにする。1 次および 2 次の両方のマスター・ファイル・サーバーは、NSM の同じバージョンを使用するようにする必要があります。

  TSF では、マスター・ファイル・サーバー IP アドレスは任意の値にすることができますが、これは NSM を稼働する装置のアドレスに設定することをお勧めします。これにより、ファイル構造がネットワーク・ステーションと互換性を持ち (つまり、TSF とも互換性を持ち)、TSF が要求するファイルを提供できるようになります。

- すべてのキャッシュ・ファイルをメモリーに保管できる十分な量のメモリーを定義する。

  ハード・ディスクを使用しない場合は、これは必須の要件です。ハード・ディスクを使用する場合でも、メモリーへのアクセスはハード・ディスクへのアクセスよりはるかに高速です。必要なメモリーの量は、ユーザーの環境によって異なります。`Talk 5` **list config** コマンドを使用して、ユーザーの特定状況下でのファイル・セットの大きさを調べてください。*Hard File storage being used for Thin Server* (シン・サーバー用に使用されているハード・ディスク記憶域) に表示される値は、ファイル・セットのサイズを KB 単位で示しています。ただし、異なるタイプのネットワーク・ステーションまたはアプリケーションをユーザー環境に追加または削除した場合、この値は変更される可能性があります。

- NFS を使用している場合、TSF は必要なファイルを動的に確認する。

この確認プロセスでは、TSF がすべての必要なファイルを識別するために、ネットワーク・ステーション電源オン・シーケンスを数回実行することが必要になる場合があります。

- TSF が disconnected モード用に構成されている場合には、TSF は、すべての必要なファイルをキャッシュに入れることを確認してください。

  TSF が disconnected モード用に構成されている場合には、ネットワーク・ステーションが TSF に要求したすべてのファイルは、シン・サーバーによってキャッシュに入れられる必要があります。RFS を使用する場合、事前ロード・リストにはすべての必要なファイルが入っている必要があります。 NFS を使用する場合、TSF は該当のディレクトリーをキャッシュに入れるように構成する必要があります。(TSF は、必要に応じて、引き続きファイルの識別/ダウンロードを行います。) 事前ロード・リストまたは該当するディレクトリーが正しく構成されない場合には、ネットワーク・ステーションは正しくブートしない場合があります。構成が正しいことを確認する 1 つの方法は、使用可能モードで TSF を実行し、disconnected モードで実行する前に該当する ELS メッセージと TSF カウンターを監視する方法です。

BootP/DHCP サーバーの構成

Network Station Manager Release 3 を稼働している場合、シン・サーバーを使用するためには DHCP が必要です。AS/400 をマスター・ファイル・サーバーとして使用している場合は、Network Station Manager Release 2.5 を使用することも可能で、その場合は DHCP の代わりに BootP を使用できます。

BootP の場合は、1 つのサーバー・アドレスしか指定できません。そのアドレスは **sa** タグを使用して指定します。このタグは、ネットワーク・ステーションの BootP レコード内にすでに存在する場合も、存在しない場合もあります。存在しない場合は、タグを作成し、その値を 2216 の内部 IP アドレスに設定してください。すでに存在する場合は、その値を 2216 の内部 IP アドレスに変更してください。

DHCP では、シン・サーバーを使用する場合に変更が必要になるフィールドは、次のとおりです。

- オプション 66 またはブートストラップ・サーバー - 基本コード・サーバー IP アドレス

  この値は、IBM 2216 内部 IP アドレスに設定する必要があります。

- オプション 211 - 基本コード・サーバーに使用するプロトコル

  シン・サーバーのマスター・ファイル・サーバー・タイプを NFS に構成する場合、これは *nfs* または *tftp* のどちらかでなければなりません。シン・サーバーのマスター・ファイル・サーバー・タイプを RFS に構成する場合、これは *rfs/400* または *tftp* のどちらかでなければなりません。

- オプション 212 - 端末構成サーバー

  このアドレスは、マスター・ファイル・サーバー IP アドレスと同じでなければなりません。

NSs が BootP および DHCP と対話する方法の詳細については、*IBM Network Station Manager Installation and Use*を参照してください。

シン・サーバー環境用のサーバーの構成

RFS の場合、事前ロード・リストを AS/400 にインストールする必要があります。事前ロード・リストは、インターネットの http://www.networking.ibm.com/netprod.html#routers から入手できます。このサイトから LoadList.file をファイル転送し、それを AS/400 上の /QIBM/ProdData/OS400/NetStationRmtController に入れます。NetStationRmtController ディレクトリーを作成することが必要になる場合があります。

NFS の場合は、マスター・サーバーで特別な変更はシン・サーバー用に必要ありません。

BootP リレーの構成

IBM 2216 の BootP リレー・エージェントを使用可能にし、適切な BootP および DHCP サーバーを構成しないと、BootP リレーはこれらのサーバーに転送されません。詳しくは、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き* を参照してください。

内部 IP アドレスの構成

内部 IP アドレスがすでに存在する場合は、特別な変更は必要ありません。現在、内部 IP アドレスが指定されていない場合は、指定する必要があります。詳しくは、*プロトコルの構成と監視 解説書 第 1 巻* を参照してください。

TSF の構成

639ページの『第36章 シン・サーバー機能の構成と監視』に説明されているコマンドを使用して、シン・サーバーを構成します。

最小限として、次のコマンドを入力する必要があります。

1. **load add package thin-server**
2. **set mode enable** または **set mode disconnected**
3. **add master-server**

サンプル構成

次の例は、Network Station Manager R2.5 を稼働する AS/400 に接続する TSF を構成します。

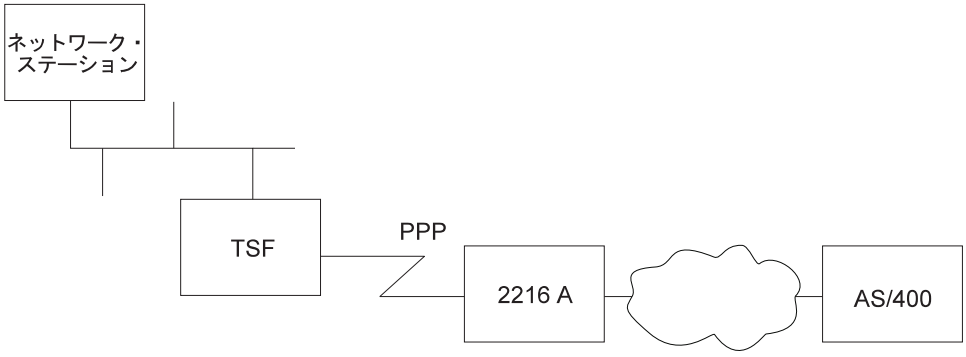


図 51. TSF サンプル構成

次の説明は、上記のネットワークに基づき、次の条件を想定して シン・サーバー機能を構成する場合を示しています。

- AS/400 は BootP サーバーである。
- 2216 A はルーターである (TSF は構成されず、TSF 用の特別な構成もない)。
- ネットワーク IP 接続性は確認済みである。つまり、AS/400 は IBM 2216 (TSF) に PING でき、IBM 2216 は AS/400 に PING できる。
- BootP リレーは現在、IBM 2216 (TSF) で使用可能にされていない。
- IP 内部アドレスは現在、IBM 2216 (TSF) に構成されていない。

AS/400 の構成

BootP (NSM リリース 2.5)

1. NSM を使用して、NS を定義する。
2. BootP テーブルを、ASCII エディターを備えたシステムに ftp (ファイル転送) する。

```
c:\>ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password. Password:
230 QSECOFR logged on.
ftp> ascii
ftp> get qusrsys/qatodbtp.bootptab bootp.tab
ftp> quit
```

3. ASCII エディターを使用してファイルを編集し、2216 (TSF) の内部 IP アドレスが指定された ″sa″ タグを追加する。

```
OLD LINE
--------
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION

MODIFIED LINE
-------------
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION:sa=192.9.250.6
```

ここで、192.9.250.6 は 2216 (TSF) の内部 IP アドレスです。

4. BootP テーブルを ftp (ファイル転送) して AS/400 に戻す。

```
c:\> ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password.
Password:
230 QSECOFR logged on.
ftp> ascii
ftp> put bootp.tab qusrsys/qatodbtp.bootptab
ftp> quit
```

事前ロード・リストの設定

事前ロード・リストは、インターネット
http://www.networking.ibm.com/netprod.html#routers から入手できます。

事前ロード・リストを入手したら、それを AS/400 に ″ftp″ することができます。

1. ローカル・ディレクトリーが ″LoadList.file″ の場所に設定されていることを確認する。
2. AS/400 に ftp する - ″test400″ は、この例の AS/400 の名前です。

```
 ftp test400
 Connected to test400.raleigh.ibm.com.
 Name (test400:root): qsecofr
 Enter password.
 Password:
 QSECOFR logged on.
```

3. ターゲット AS/400 上の正しいディレクトリーに変更する。

```
ftp>  cd /
Current directory changed to /.
ftp> cd qibm/proddata/os400/
Current directory changed to /qibm/proddata/os400.
ftp> dir
PORT subcommand request successful.
 List started.
QTCP            34816 04/30/97 02:50:36 *DIR     REXEC/
QSECOFR         33792 07/24/98 08:04:55 *DIR     NetStationRmtController/
 List completed.
```

4. ディレクトリー ″NetStationRmtController″ が存在しない場合は、それを作成することが必要になります。

```
ftp> MKD
(directory - name) NetStationRmtController
Created directory /qibm/proddata/os400/netstationrmtcontroller
```

5. NetStationRmtController ディレクトリーに変更する。

```
ftp>  cd NetStationRmtController
Current directory changed to /qibm/proddata/os400/Netstationrmtcontroller.
```

6. ファイルを AS/400 に転送する。

```
ftp> ascii
Representation type is ASCII nonprint.
ftp> put LoadList.file
 PORT subcommand request successful.
 Sending file to /qibm/proddata/os400/Netstationrmtcontroller
 File transfer completed successfully.
```

TCP/IP の構成

TCP/IP 構成は、ユーザー特定の環境に依存します。

IBM 2216 (TSF) の構成

BootP リレー

1. BootP リレーがすでに構成されているかどうかを調べる。

```
*
*
t 6
Config>protocol ip
Internet protocol user configuration
IP config>list bootp
BOOTP forwarding: enabled
Max number of BOOTP forwarding hops: 4
Min secs of retry before forwarding: 0
Configured BOOTP servers:      192.9.220.21
IP config>
```

2. すでに使用可能にされていない場合は、それを使用可能にする。

```
IP config> enable bootp
Maximum number of forwarding hops [4]?
Minimum seconds before forwarding [0]?
IP config>
```

3. ネットワーク・ステーション BootP または DHCP サーバーが、構成されたサーバーのリストに含まれていない場合は、それを追加する。

```
IP config>add bootp-server
BOOTP server address [0.0.0.0]? 9.37.121.6
IP config>
```

内部 IP アドレス

1. 内部 IP アドレスがすでに構成されているかどうかを調べる。

```
Config>protocol ip
Internet protocol user configuration
IP config>list addresses
IP addresses for each interface:
    intf     0   9.37.177.97      255.255.248.0    Local wire...
    intf     1   192.9.220.2      255.255.255.0    Local wire...
    intf     2   192.9.250.6      255.255.255.0    Local wire...
    intf     3   192.9.222.2      255.255.255.0    Local wire...
    intf     4                                     IP disabled...
    intf     5                                     IP disabled...
    intf     6   192.9.223.2      255.255.255.0    Local wire...
IP config>
```

2. 内部 IP アドレスを構成する。

```
IP config>set internal-ip-address
Internal IP address [192.9.223.2]? 192.9.250.6
IP config>
```

3. 再度、アドレスを表示する。

```
IP config>list addresses
IP addresses for each interface:
   intf     0   9.37.177.97      255.255.248.0    Local wire
   intf     1   192.9.220.2      255.255.255.0    Local wire
   intf     2   192.9.250.6      255.255.255.0    Local wire
   intf     3   192.9.222.2      255.255.255.0    Local wire
   intf     4                                     IP disabled
```

```
   intf     5                                      IP disabled
   intf     6   192.9.223.2      255.255.255.0    Local wire
Internal IP address: 192.9.250.6
IP config>
```

シン・サーバー・フィーチャー

1. ロード・パッケージ thin-server を追加する。

   ロード・パッケージを追加しておかないと、シン・サーバー・フィーチャーを構成することができません。

   最初に シン・サーバー・パッケージが利用可能であることを確認します。

   ```
   Config>load list available
   Available Packages
   ------------------
   appn package
   tn3270e package
   thin-server package
   Config>
   ```

   利用可能でない場合は、先に進む前に、正しいソフトウェア・バージョンを入手する必要があります。

   利用可能の場合は、パッケージがすでにロードされていないことを確認します。

   ```
   Config>load list configured
   Configured Packages
   -------------------
   thin-server package
   Config>
   ```

   すでにロード / 構成されている場合は (上記のように)、TSF の構成に進むことができます。まだロードされていない場合は、シン・サーバー・パッケージを追加することが必要です。

   ```
   Config> load add package thin-server
   thin-server package configured successfully
   This change requires a reload.
   Config>
   ```

2. 再ロードする。

   シン・サーバー・パッケージを追加しなければならなかった場合は、ここで構成を書き込み、IBM 2216 を再ロードする必要があります。

3. モードを設定する。

   パッケージをロードした場合、初期時には シン・サーバーは使用不可になっています。モードを使用可能に設定しないと、他のシン・サーバー・パラメーターを構成できません。

   ```
   *
   *
   t 6
   Config>feature tsf
   Thin server config>set mode enable

   Thin server feature (TSF) is fully enabled once
   you have entered a Master File Server for either
   RFS or NFS. Please add a master-file-server if
   one is not already configured.
   Thin server config>
   ```

4. master-file-server を追加する。

シン・サーバー・フィーチャーを使用可能にしたら、マスター・ファイル・サーバーを構成する必要があります。この例では、マスター・ファイル・サーバーは AS/400 なので、RFS マスター・ファイル・サーバーを追加します。このネットワークの場合は、デフォルトの TFTP タイムアウトおよび再試行パラメーターが適当です。

```
Thin server config>add master-file-server rfs-as400
File Server IP address [0.0.0.0]? 192.9.221.21
Secondary File Server IP address [0.0.0.0]? 192.9.225.20
Master Server Refresh Retry Limit (1-20) [10]?
TFTP Packet Timeout in seconds (5 - 10) [5]?
TFTP Max Retry Limit (1 - 10) [1]? 7
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192)
                                                                [8192]?
Pre-load File name
   [/QIBM/ProdData/OS400/NetstationRmtController/Loadlist.file]?
Thin server config>
```

トークンリング・インターフェース上の AS/400 の IP アドレスは 9.37.100.68 です。事前ロード・リスト・ファイルを AS/400 にインストールしたときに、その名前を シン・サーバーのデフォルト名に一致するように指定したので、変更する必要はありません。

5. time-to-refresh-pre-load-list を設定する (オプション)。

   リフレッシュを実行する時間のデフォルト値は 1:00 AM です。この時間は、大きなファイルが変更され、シン・サーバーがダウンロードすることが必要になった場合、パフォーマンスへの影響を最小限にするために選択されたものです。

6. interval-pre-load-list を設定する (オプション)。

   キャッシュ・ファイルを検査する間隔のデフォルト値は、master-file-server と同じレベルで、毎日です。このパラメーターの値と time-to-refresh-pre-load-list パラメーターの値によって、ファイルを検査する頻度が決まります。ネットワーク・ステーションのファイルの変更が頻繁に行われない場合、これらの値は、1 週間に 1 回、または 1 か月に 1 回更新するように設定することができます。

7. メモリーを設定する (オプション)。

   ファイル・キャッシュ用のデフォルト・メモリーは 16 MB RAM キャッシュで、これで十分のはずです。複数のネットワーク・ステーションが TSF を使用している場合は、631ページの『構成に関する推奨事項』の推奨値を参照してください。

8. ハード・ディスクを設定する (オプション)。

   ハード・ディスクの使用をお勧めします。ハード・ディスクを使用しない場合は、このパラメーターを *no* に設定します。

9. 選択を設定する (オプション)。

   デフォルト値は、1 次です。2 次マスター・ファイル・サーバーがある場合、自動選択を指定することもできます。詳しくは、629ページの『ファイル・キャッシュの更新』を参照してください。

第36章 シン・サーバー機能の構成と監視

この章では、シン・サーバー機能 (TSF) の構成およびオペレーショナル・コマンドの使用法について説明し、次の内容が記載されています。

- 『TSF 構成環境へのアクセス』
- 『TSF 構成コマンド』
- 651ページの『TSF 監視環境へのアクセス』
- 652ページの『TSF 監視コマンド』
- 657ページの『TSF 動的再構成サポート』

TSF 構成環境へのアクセス

TSF 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** と入力する。 (このコマンドの詳細については、*Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引き*の “OPCON プロセスおよびコマンド” の章を参照してください。) たとえば、次のように入力します。

   ```
   * talk 6
   Config>
   ```

   talk 6 コマンドを入力すると、CONFIG プロンプト (Config>) が端末に表示されます。初めて構成に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。
2. CONFIG プロンプトで **feature tsf** コマンドを入力して Thin server config> プロンプトを表示する。

TSF 構成コマンド

TSF を構成するには、Thin server config> プロンプトでコマンドを入力します。

表 66. TSF 構成コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Add	マスター・ファイル・サーバー--リモート・ファイル・システム (RFS) またはネットワーク・ファイル・システム (NFS) を追加します。
Delete	Deletes マスター・ファイル・サーバー (RFS または NFS) を削除します。
List	シン・サーバー構成を表示します。
Modify	Modifies マスター・ファイル・サーバー (RFS または NFS) を変更します。
Set	シン・サーバー・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。 xxxv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、マスター・ファイル・サーバー構成を追加するのに使用します。

master-file-server タイプとして *nfs* を選択した場合、シン・サーバーは NFS を使用してマスター・ファイル・サーバーと通信してファイルを同期化し、NS は TFTP

または NFS を使用してシン・サーバーと通信することができます。
master-file-server タイプとして *rfs* を選択した場合、シン・サーバーは RFS を使用してマスター・ファイル・サーバーと通信してファイルを同期化し、NS は TFTP または RFS を使用して シン・サーバーと通信することができます。

構文:

add master-file-server nfs-s390
nfs-nt
nfs-aix
nfs-other
rfs-as400

nfs-s390

TSF が S/390® に接続されている場合に使用します。

File Server IP address

マスター・ファイル・サーバーの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Secondary File Server IP address

バックアップ・マスター・ファイル・サーバーの IP アドレスを指定します。詳しくは、629ページの『ファイル・キャッシュの更新』を参照してください。このパラメーターの使用方法については、**set selection** コマンドを参照してください。

注: これは、**set selection** コマンドが 2 次または自動のいずれかを指定した場合、0.0.0.0 に設定できません。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Master Server Refresh Retry Limit

TSF がマスター・ファイル・サーバーを到達不能と宣言するまでに再試行する回数を指定します。

範囲: 1 ～ 20

デフォルト値 : 10

tftp packet timeout

有効値 : 5 ～ 10 秒

デフォルト値: 5

tftp maximum retry limit

有効値 : 1 ～ 10

デフォルト値 : 1

maximum segment size

最大パケット・セグメント・サイズを指定します。

有効値 : 512、1024、2048、4096、8192 (バイト)

デフォルト値 : 8192

additional Include subdirectories
組み込みサブディレクトリーを追加するかどうかを指定します。追加のサブディレクトリーは、TSF がデフォルト・ディレクトリー内に存在しないファイルをキャッシュする必要がある場合に指定できます。

有効値 : yes または no

デフォルト値 : yes

additional Include subdirectory path
追加する組み込みサブディレクトリーのパスを指定します。

有効値 : a ～ z、A ～ Z、0 ～ 9、.、_、--、/

デフォルト値: なし

include all subdirectories under this directory
指定した追加サブディレクトリー・パス内のすべてのネストされたサブディレクトリーを含めるかどうかを指定します。

有効値 :

- No

  TSF は、指定されたディレクトリー内のすべてのファイルを事前ロードします。

- Yes

  TSF は、指定されたディレクトリー内のファイルを事前ロードしません。代わりに、TSF は必要になった時点で、ディレクトリーとそのサブディレクトリーからファイルをロードします。

デフォルト値: no

nfs-nt TSF が Windows NT に接続されている場合に使用します。

File Server IP address
マスター・ファイル・サーバーの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Secondary File Server IP address
バックアップ・マスター・ファイル・サーバーの IP アドレスを指定します。詳しくは、629ページの『ファイル・キャッシュの更新』を参照してください。このパラメーターの使用方法については、**set selection** コマンドを参照してください。

注: これは、**set selection** コマンドが 2 次または自動のいずれかを指定した場合、0.0.0.0 に設定できません。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Master Server Refresh Retry Limit
TSF がマスター・ファイル・サーバーを到達不能と宣言するまでに再試行する回数を指定します。

範囲: 1 ～ 20

デフォルト値 : 10

tftp packet timeout

有効値 : 5 ～ 10 秒

デフォルト値: 5

tftp max retry limit

有効値 : 1 ～ 10

デフォルト値 : 1

maximum segment size
最大パケット・セグメント・サイズを指定します。

有効値 : 512、1024、2048、4096、8192 (バイト)

デフォルト値 : 8192

additional Include subdirectories
組み込みサブディレクトリーを追加するかどうかを指定します。

有効値 : yes または no

デフォルト値 : yes

additional Include subdirectory path
追加する組み込みサブディレクトリーのパスを指定します。

有効値 : a ～ z、A ～ Z、0 ～ 9、.、_、--、/

デフォルト値: なし

include all subdirectories under this directory
指定した追加サブディレクトリー・パス内のすべてのネストされたサブディレクトリーを含めるかどうかを指定します。

有効値 :

- No

  TSF は、指定されたディレクトリー内のすべてのファイルを事前ロードします。

- Yes

  TSF は、指定されたディレクトリー内のファイルを事前ロードしません。代わりに、TSF は必要になった時点で、ディレクトリーとそのサブディレクトリーからファイルをロードします。

デフォルト値: no

nfs-aix
TSF が AIX® に接続されている場合に使用します。

File Server IP address
マスター・ファイル・サーバーの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Secondary File Server IP address
バックアップ・マスター・ファイル・サーバーの IP アドレスを指定します。詳しくは、629ページの『ファイル・キャッシュの更新』を参照してください。このパラメーターの使用方法については、**set selection** コマンドを参照してください。

注: これは、**set selection** コマンドが 2 次または自動のいずれかを指定した場合、0.0.0.0 に設定できません。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Master Server Refresh Retry Limit
TSF がマスター・ファイル・サーバーを到達不能と宣言するまでに再試行する回数を指定します。

範囲: 1 ～ 20

デフォルト値 : 10

tftp packet timeout

有効値 : 5 ～ 10 秒

デフォルト値: 5

tftp maximum retry limit

有効値 : 1 ～ 10

デフォルト値 : 1

maximum segment size
最大パケット・セグメント・サイズを指定します。

有効値 : 512、1024、2048、4096、8192 (バイト)

デフォルト値 : 8192

additional Include subdirectories
組み込みサブディレクトリーを追加するかどうかを指定します。

有効値 : yes または no

デフォルト値 : yes

additional Include subdirectory path
追加する組み込みサブディレクトリーのパスを指定します。

有効値 : a ～ z、A ～ Z、0 ～ 9、.、_、--、/

デフォルト値: なし

include all subdirectories under this directory
指定した追加サブディレクトリー・パス内のすべてのネストされたサブディレクトリーを含めるかどうかを指定します。

有効値 :

- No

  TSF は、指定されたディレクトリー内のすべてのファイルを事前ロードします。

- Yes

  TSF は、指定されたディレクトリー内のファイルを事前ロードしません。代わりに、TSF は必要になった時点で、ディレクトリーとそのサブディレクトリーからファイルをロードします。

デフォルト値: no

nfs-other

手動ですべてのサブディレクトリーを指定したい場合に使用します。

File Server IP address

マスター・ファイル・サーバーの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Secondary File Server IP address

バックアップ・マスター・ファイル・サーバーの IP アドレスを指定します。詳しくは、629ページの『ファイル・キャッシュの更新』を参照してください。このパラメーターの使用方法については、**set selection** コマンドを参照してください。

注: これは、**set selection** コマンドが 2 次または自動のいずれかを指定した場合、0.0.0.0 に設定できません。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Master Server Refresh Retry Limit

TSF がマスター・ファイル・サーバーを到達不能と宣言するまでに再試行する回数を指定します。

範囲: 1 ～ 20

デフォルト値 : 10

tftp packet timeout

有効値 : 5 ～ 10 秒

デフォルト値: 5

tftp maximum retry limit

有効値 : 1 ～ 10

デフォルト値 : 1

maximum segment size

最大パケット・セグメント・サイズを指定します。

有効値 : 512、1024、2048、4096、8192 (バイト)

デフォルト値 : 8192

additional Include subdirectories
組み込みサブディレクトリーを追加するかどうかを指定します。

有効値 : yes または no

デフォルト値 : yes

additional Include subdirectory path
追加する組み込みサブディレクトリーのパスを指定します。

有効値 : a ～ z、A ～ Z、0 ～ 9、.、_、--、/

デフォルト値: なし

include all subdirectories under this directory
指定した追加サブディレクトリー・パス内のすべてのネストされたサブディレクトリーを含めるかどうかを指定します。

有効値 :

- No

  TSF は、指定されたディレクトリー内のすべてのファイルを事前ロードします。

- Yes

  TSF は、指定されたディレクトリー内のファイルを事前ロードしません。代わりに、TSF は必要になった時点で、ディレクトリーとそのサブディレクトリーからファイルをロードします。

デフォルト値: no

rfs-as400
TSF が AS/400 に接続されている場合に使用します。

File Server IP address
マスター・ファイル・サーバーの IP アドレスを指定します。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Secondary File Server IP address
バックアップ・マスター・ファイル・サーバーの IP アドレスを指定します。詳しくは、629ページの『ファイル・キャッシュの更新』を参照してください。このパラメーターの使用方法については、**set selection** コマンドを参照してください。

注: これは、**set selection** コマンドが 2 次または自動のいずれかを指定した場合、0.0.0.0 に設定できません。

有効値: 任意の有効な IP アドレス

デフォルト値: 0.0.0.0

Master Server Refresh Retry Limit
TSF がマスター・ファイル・サーバーを到達不能と宣言するまでに再試行する回数を指定します。

範囲: 1 ～ 20

デフォルト値 : 10

tftp packet timeout

有効値 : 5 ～ 10 秒

デフォルト値: 5

tftp maximum retry limit

有効値 : 1 ～ 10

デフォルト値 : 1

maximum segment size

最大パケット・セグメント・サイズを指定します。

有効値 : 512、1024、2048、4096、8192 (バイト)

デフォルト値 : 8192

pre-load file name

事前ロード・ファイルの名前とパスを指定します。

有効値 : a ～ z、A ～ Z、0 ～ 9、.、_、--、/

デフォルト値:
/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file

例: NFS の場合

```
Thin server config> add master-file-server nfs-nt
 File Server IP address [0.0.0.0]? 10.22.55.94
 Secondary File Server IP address [0.0.0.0]? 10.22.55.96

 Master Server Refresh Retry Limit (1-20) [10]?

 TFTP Packet Timeout in seconds (5 - 10) ][5]?

 TFTP Max Retry Limit (1 - 10) [1]?

 TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]?

Default Include Directories:

    Include Directory List Follows:

    Include
       all
    Subdirs?   Directory Names
    --------   --------------------------------
       N       /netstation/prodbase
       Y       /netstation/prodbase/mods
       Y       /netstation/prodbase/nls
       Y       /netstation/prodbase/fonts
       Y       /netstation/prodbase/java
       Y       /netstation/prodbase/keyboards
       Y       /netstation/prodbase/proms
       Y       /netstation/prodbase/X11
       Y       /netstation/prodbase/configs
       Y       /netstation/prodbase/SysDef
       Y       /netstation/prodbase/zoneinfo

   Do you want additional Include Subdirectories (Y)es (N)o [N]? y

Include Subdirectory [   ]? /netstation/prodbase/another
```

```
Include all subdirectories under this directory (Y)es or (N)o [N]?

Do you want additional Include Subdirectories (Y)es (N)o [N]?
```

例: RFS の場合

```
Thin server config>  add master-file-server rfs
 File Server IP address [0.0.0.0]? 192.9.225.21
 Secondary File Server IP address [0.0.0.0]? 192.9.225.20
 Master Server Refresh Retry Limit (1-20) [10]?
 TFTP Packet Timeout in seconds (5-10) [5]?
 TFTP Max Retry Limit (1-10) [1]?
 TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) ][8192]?

 Pre-Load File name [/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

Delete

delete コマンドは、マスター・ファイル・サーバー構成を削除するのに使用します。

構文:

delete master-file-server nfs
rfs

nfs NFS マスター・ファイル・サーバーが構成されている場合に使用します。

rfs TSF が RFS マスター・ファイル・サーバー用に構成されている場合に使用します。

List

list コマンドは、TSF 構成を表示するのに使用します。

構文:

list all

例: NFS の場合

```
Thin server config>  list all

Thin Server Feature configuration:

     Mode:                          ENABLED
     Master File Server Selection: PRIMARY
     Interval to refresh cache in day(s): 1
     Time of day (military time) to refresh cache: 0100
     Megabytes used for Thin Server RAM cache: 16
     Use Hard File:  YES


Master Thin Server list:
     Server IP Address: 192.9.221.21
     Secondary Server IP Address: 192.9.225.20
     Server Protocol: NFS

     Master Server Refresh Retry Limit value: 10
     TFTP Packet Timeout value: 5
     TFTP Maximum Retry Limit value: 6
     TFTP Maximum Segment Size value: 512

     Initial directories setup for server type: NFS-AIX
```

```
 NFS Include Directory List follows:

    Include
       all
     subdirs?    Directory Names
     --------    ---------------------------------------

        N        /usr/netstation
        Y        /usr/netstation/mods
        Y        /usr/netstation/nls
        Y        /usr/netstation/fonts
        Y        /usr/netstation/java
        Y        /usr/netstation/keyboards
        Y        /usr/netstation/proms
        Y        /usr/netstation/X11
        Y        /usr/netstation/configs
        Y        /usr/netstation/SysDef
        Y        /usr/netstation/zoneinfo
```

例: RFS の場合

```
Thin server config>  list all

Thin Server Feature configuration:

     Mode:                          DISCONNECTED
     Master File Server Selection: PRIMARY
     Interval to refresh cache in day(s): 1
     Time of day (military time) to refresh cache: 0100
     Megabytes used for Thin Server RAM cache: 16
     Use Hard File:  YES


Master Thin Server list:
     Server IP Address: 192.9.221.21
     Secondary Server IP Address: 192.9.225.20
     Server Protocol: RFS

     Master Server Refresh Retry Limit value: 10
     TFTP Packet Timeout value: 5
     TFTP Maximum Retry Limit value: 1
     TFTP Maximum Segment Size value: 8192

 Protocol RFS List:
     Pre-load File:  /QIBM/ProdData/OS400/NetStationRmtcontroller/Loadlist.file
```

Modify

modify コマンドは、マスター・ファイル・サーバー構成を変更するのに使用します。

構文:

modify master-file-server nfs / rfs

nfs NFS マスター・ファイル・サーバーの 1 つが構成された場合に使用します。

rfs TSF が RFS マスター・ファイル・サーバー用に構成されている場合に使用します。

例: NFS の場合

```
Thin server config>  modify master-file-server nfs
File Server IP address [1.1.1.1]?
Secondary File Server IP address [1.1.1.2]?

Master Server Refresh Retry Limit (1-20) [10]?

TFTP Packet timeout in seconds (5 - 10) [5]?

TFTP Max retry limit value (1 - 10) [1]?

TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]?
Include directory /netstation/prodbase, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [N]?
Include directory /netstation/prodbase/mods, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/nls, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/fonts, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/java, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/keyboards, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/proms, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/X11, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/configs, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/SysDef, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?
Include directory /netstation/prodbase/zoneinfo, (Y)es or (N)o [Y]?
        Include all subdirectories under this directory (Y)es or (N)o [Y]?

Do you want additional Include Subdirectories (Y)es (N)o [N]?
Thin server config>
```

例: RFS の場合

```
Thin server config>  modify master-file-server rfs
File Server IP address [192.9.225.21]? 192.9.225.23
Secondary File Server IP address [192.9.225.20]? 192.9.225.22
Master Server Refresh Retry Limit (1-20) [10]?  8
TFTP Packet Timeout in seconds (5-10) [5]? 7
TFTP Max Retry Limit (1-10) [1]? 15
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]? 4096

 Pre-Load File name [/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

Set

set コマンドは、TSF 構成パラメーターを設定するのに使用します。

構文:

set
- mode
- selection
- interval-pre-load-list
- time-to-refresh-pre-load-list
- memory-cache
- hard-file

mode TSF のモードを指定します。

有効値 :

enable
TSF は完全に機能し、キャッシュ・ファイルをネットワーク・ステーションに提供することを指定します。

disable
TSF は活動状態でなく、ネットワーク・ステーションに応答しないことを指定します。ネットワーク・ステーションはサーバーに直接接続するように構成する必要があります。

passthru
passthru モードは、RFS を使用している場合にのみ有効です。Passthru では、ネットワーク・ステーションは TSF に接続できますが、ファイルは常にマスター・ファイル・サーバーから入手されます。

disconnected
TSF は機能し、キャッシュ・ファイルをネットワーク・ステーションに提供することを指定します。しかし、マスター・ファイル・サーバーへのトラフィックは最少になります。詳しくは、628ページの『ネットワーク・ステーションとの通信に使用するプロトコル』を参照してください。

デフォルト値: disable

selection
TSF がファイル・サーバー IP アドレスに接続するかまたは TSF キャッシュの更新のための 2 次ファイル・サーバー IP アドレスに接続するかどうかを指定します。

有効値 :

primary
TSF が、キャッシュを更新しようとしているときにファイル・サーバー IP アドレスの IP アドレスだけを使用することを指定します。2 次ファイル・サーバー IP アドレスは無視されます。

secondary
TSF が、キャッシュを更新しようとしているときに 2 次ファイル・サーバー IP アドレスの IP アドレスだけを使用することを指定します。ファイル・サーバー IP アドレスは無視されます。

automatic
TSF が、ファイル・サーバー IP アドレスに指定された IP アドレスだけに接続を試みることを指定します。構成済みの回数だけ再試行しても接続しない場合には、TSF は、2 次ファイル・サーバー IP アドレスに指定された IP アドレスに接続を試みます。詳しくは、629ページの『ファイル・キャッシュの更新』を参照してください。

デフォルト値: 1 次

interval-pre-load-list
事前ロード・リストをキャッシュで更新する間隔 (日数) を指定します。

有効値 : 00 ～ 365

デフォルト値 : 01

time-to-refresh-pre-load-list

キャッシュ・ファイルを更新する時刻 (24 時形式) を指定します。

有効値 : 0001 ～ 2400

デフォルト値 : 0100

memory-cache

シン・サーバー RAM キャッシュのメモリー量を MB 単位で指定します。ハード・ディスクを使用する場合、TSF のパフォーマンスと IBM 2216 内の他の機能との平衡が取れる値を選択することが必要です。ハード・ディスクを使用しない場合、この値はすべてのキャッシュ・ファイルを保持できる十分な大きさにする必要があります。詳しくは、631ページの『構成に関する推奨事項』を参照してください。

有効値 : 8 ～ 64 MB

デフォルト値 : 16

hard-file

ハード・ディスクを使用するかどうかを指定します。

有効値 : yes または no

デフォルト値 : yes

例:

```
Thin server config>  set mode passthru
This server feature (TSF) is passthru
Thin server config> set interval-pre-load-list
Interval to refresh the Pre-Load list in days (00-365) [01]? 1
Thin server config> set time-to-refresh-pre-load-list
Time of day to refresh cache in military time (0001-2400) [0100] 0800
Thin server config> set memory-cache
Amount of memory in megabytes for Thin Server RAM cache (8-64MB) [8]
Thin server config> set hard-file
Use the Hard File  (Y)ex N(o) [Y]? yes
```

TSF 監視環境へのアクセス

TSF 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 TSF *監視* プロセスにアクセスできます。

1. OPCON プロンプトで **talk 5** と入力する。 (このコマンドについて詳しくは、Nways マルチプロトコル・アクセス・サービス ソフトウェア使用者の手引きの *OPCON プロセスおよびコマンド* の章を参照してください。) たとえば、次のように入力します。

   ```
   * talk 5
   +
   ```

   talk 5 コマンドを入力すると、端末に GWCON プロンプト (+) が表示されます。初めて構成に入ったときにプロンプトが表示されない場合は、再度 **Return** を押してください。

2. + プロンプトで **f tsf** コマンドを入力して Thin-Server> プロンプトを表示する。

   例:

```
+ f tsf
Thin-Server>
```

TSF 監視コマンド

ここでは、TSF 監視コマンドについて説明します。

表 67. TSF 監視コマンドの要約

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Delete	シン・サーバー・フィーチャー・ファイル・キャッシュからファイルを削除します。
Flush	シン・サーバー・フィーチャー・ファイル・キャッシュをフラッシュします。
List	シン・サーバーの設定および値を表示します。
Refresh	キャッシュをリフレッシュします。
Reset	カウンターをリセットします。
Restart	シン・サーバー・プロセスをリスタートします。
Set	シン・サーバー・フィーチャーの設定を変更します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Delete

delete コマンドは、シン・サーバー・フィーチャー・ファイル・キャッシュからファイルを削除するのに使用します。

構文:

delete *filename*

filename

ファイル・キャッシュから除去するファイルの名前を指定します。

有効値 :

デフォルト値: なし

例:

```
Thin-Server> delete
Enter filename to delete from the File Cache: /ibm/prod/ns/5494.dat
Are you sure that you want to delete this file? (Y/ [N]): y
File successfully deleted
```

Flush

flush コマンドは、TSF メモリーおよびハード・ディスクのキャッシュ・スペースをフラッシュするのに使用します。**flush** コマンドは、すべてのキャッシュ・ファイルを消去します。シン・サーバー・キャッシュは、マスター・サーバーからの次回のリフレッシュ時に更新されます。リフレッシュが完了するまで、ネットワーク・ステーションに遅延が生じることがあります。

構文:

flush

例:

```
Thin-Server> flush
The FLUSH command will erase all cached files.
  The Thin Server cache will be updated on the next refresh
  from the Master Server.  Network Stations may experience
  delays until the refresh is completed.
Are you sure you really want to do this? (Y/ [N]:  y
All Thin Server cached files have been flushed
```

List

list コマンドは、TSF パラメーター設定値を表示するのに使用します。

構文:

list cached-files
config
file-access-counters
file-refresh-counters
pre-load-list
tftp-counters
ts-counters

例:

```
Thin-Server> list cached-files

Cached
File Name     File Size  Time Stamp         Flags  Host File Name
------------  ---------  -----------------  -----  -----------------
00000026.DAT      2729   04/08/98 13:35:07   RYY   /QIBM/ProdData/OS400/Netstat
ionRmtController/Loadlist.file
00000002.DAT   2049220   09/16/97 08:55:39   RYU   /QIBM/PRODDATA/NETWORKSTATIO
N/KERNEL
                 10060   03/04/97 16:12:44   RY-   /QIBM/PRODDATA/NETWORKSTATIO
N/FONTS/PCF/MISC/7X14B.PCF
    List is Complete
```

フラグの意味は次のとおりです。

- WhereFrom
  - R = RFS クライアント
  - N = NFS クライアント
  - - = なし
- InTable
  - - = テーブル内に存在しない
  - u (または m) = 更新開始
  - Y = テーブル内に存在
- FileState
  - - = ディスク上に存在しない
  - D = ダーティー
  - A = 更新中止
  - u = 更新開始
  - U = 更新中

– Y = ディスク上に存在し利用可能

最後の 2 つのフラグの一般的な組み合わせは、次のとおりです (分かりやすいように、3 つのフラグすべてを表示)。

- RYY - 正常なファイル
- RuY - 完全リフレッシュが進行中で、このファイルはまだ検証されていません。
- RYU - このファイルは更新中です。

例: RFS の場合

```
Thin-Server> list config
Thin Server Configuration
    Thin Server feature mode is:                        Disconnected
    Thin Server feature state is:                       Active, all files up-to-date
    Interval to refresh Pre-Load List (#days):          1
    Time of day (Military) to refresh Pre-Load List:    01:00:00
    Memory (KB) currently using for RAM cache:          16384
    Maximum memory (KB) configured for RAM cache:       16384
    Currently using Hard File?:                         Yes
    Hard File storage defined for Thin Server:          817664
    Hard File storage being used for Thin Server:       27328
    Number of Files Cached:                             82
    Master Server IP address:                           192.9.225.21
    Secondary Master Server IP address:                 192.9.225.20
    Master Server Retry Limit:                          10
    Master Server Selection:                            primary
    TFTP Packet Timeout Value:                          5
    TFTP Max Retries:                                   1
    TFTP Max Segment Size:                              8192

    Thin Server Sync Protocol:                          RFS
    Name of Pre-Load List file:
        /QIBM/ProdData/OS400/NetstationRmtController/Loadlist.file
Thin Server>
```

例: NFS の場合

```
Thin-Server> list config

Thin Server Configuration
  Thin Server feature is:                           Enabled
  Thin Server Feature state is:                     Active, initializing file structure
  Interval to refresh Pre-Load List (#days):        1
  Time of day (Military) to refresh Pre-Load List: 01:00:00
  Memory (KB) currently using for RAM cache:        25600
  Maximum memory (KB) configured for RAM cache:     25600
  Currently using Hard File?:                       Yes
  Hard File storage defined for Thin Server:        915424
  Hard File storage being used for Thin Server:     27328
  Number of Files Cached:                           82
  Master Server IP address:                         192.9.225.21
  Secondary Master Server IP address:               192.9.225.20
  Master Server Retry Limit:                        10
  Master Server Selection:                          primary
  TFTP Packet Timeout Value:                        5
  TFTP Max Retries:                                 1
  TFTP Max Segment Size:                            8192

  Thin Server Sync Protocol:                        NFS
  Include Directory List Follows:

  Include
    all
  Subdirs?   Directory Names
  --------   ----------------------------------
```

```
     N       /usr/netstation
     Y       /usr/netstation/mods
     Y       /usr/netstation/nls
     Y       /usr/netstation/fonts
     Y       /usr/netstation/java
     Y       /usr/netstation/keyboards
     Y       /usr/netstation/proms
     Y       /usr/netstation/X11
     Y       /usr/netstation/configs
     Y       /usr/netstation/SysDef
     Y       /usr/netstation/zoneinfo
Thin Server>
```

例:

```
Thin-Server> list file-access-counters

Disk Statistics/Counters:
    Number of files currently open:                20
    Number of Total File Opens:                    23
    Number of Open Fails when File is Locked:       1
    Number of Read misses - Version Mismatch:       4
    Number of Read misses - File Not Present:       3
    Number of Write misses - Hard File Full:        4
```

例:

```
Thin-Server> list file-refresh-counters

File Refresh Statistics/Counters
    Last Successful refresh Master Server IP address:  192.9.225.20
    Current refresh Master Server IP address:          192.9.225.21
    Number of Files Updated during last refresh:       0
    Number of Update Failures during last refresh:     0
    Number of Refreshes:                               0
    Number of Refresh Failures:                        1
    Number of Refreshes - Primary Master Server:       0
    Number of Refresh Failures - Primary Server:       0
    Number of Refreshes - Secondary Master Server:     0
    Number of Refresh Failures - Secondary Server:     0
    Number of Files Refreshed:                         249
    Date/Time of Last File Update:                     02/17/1999 01:00:36
    Date/Time of Last File Download:                   02/16/1999 15:57:05

Thin Server>
```

例:

```
Thin-Server> list pre-load-list
 <display of pre-load list raw file>
List of Pre-Load List File is Complete
```

例:

```
Thin-Server> list tftp-counters

TFTP Server Statistics/Counters
    Relay to Master File Server:                            Available
    Number of Total TFTP Requests:                            3
    Number of Current TFTP Requests:                          2
    Number of Files Served:                                  22
    Number of Files Served by Master Server:                 22
    Number of Files Served by Primary Master Server:         22
    Number of Files Served by Secondary Master Server:        0

Thin Server>
```

例: RFS の場合

```
Thin-Server>  list ts-counters

Thin Server Statistics/Counters
    Relay to Master File Server:                            Available
    Number of Total RFS Clients:                            0
    Number of Current RFS Clients:                          0
    Number of Files Served:                                 0
    Number of Files Served by Master Server:                0
    Number of NS Port Mapper socket accepts:                0
    Number of NS Port Mapper sockets currently active/open: 0
    Number of NS Server socket accepts:                     0
    Number of NS 8473 sockets currently active/open:        0
    Number of NS Login sock accepts:                        0
    Number of NS 8476 sockets currently active/open:        0
    Number of RFS writes to a Thin Server cached file:      0
Thin Server>
```

例: NFS の場合

```
Thin-Server>  list ts-counters

Thin Server Statistics/Counters
    Number of NFS Server Reads:                              13
    Number of NFS Server Read Directories:                    8
    Number of Unsupported NFS Requests:                       2
    Number of total NFS Mounts:                              22
    Number of current NFS Mounts:                             7
    Number of total NFS clients:                             15
    Number of current NFS Clients:                            4
```

Refresh

refresh コマンドは、キャッシュを強制的にリフレッシュするのに使用します。

構文:

refresh

例:

```
Thin-Server> refresh

Force a refresh of the cache (Y/N) [N]? y

Thin Server cache has been refreshed
```

Reset

reset コマンドは、カウンターを動的にリセットするのに使用します。

構文:

reset all
file-access-counters
file-refresh
tftp-counters
ts-counters

例:

```
Thin-Server> reset all

All Thin Server feature counters have been reset
```

Restart

restart コマンドは、TSF プロセスをリスタートするのに使用します。

構文:
restart

例:

```
Thin-Server> restart

Restart Thin Server? (Y/ [N]): y

Thin Server has been restarted
```

Set

set コマンドは、TSF キャッシュ・モードを設定するのに使用します。

構文:
set mode

mode TSF のモードを指定します。649ページの『Set』を参照してください。

有効値 :

- enable
- disable
- passthru
- disconnected

例:

```
Thin-Server> set mode disconnected

Thin Server caching is now disconnected
```

TSF 動的再構成サポート

このセクションでは、Talk 6 および Talk 5 コマンドに影響を与える場合の動的再構成 (DR) を説明します。

CONFIG (Talk 6) Delete Interface

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

GWCON (Talk 5) Activate Interface

GWCON (Talk 5) **activate interface** コマンドは、TSF には適用できません。インターフェースを活動化してもシン・サーバーに直接影響しません。しかし、これは、クライアントまたはマスター・ファイル・サーバーへの接続に影響する場合があります。

GWCON (Talk 5) Reset Interface

GWCON (Talk 5) **reset interface** コマンドは、TSF には適用できません。インターフェースをリセットしてもシン・サーバーに直接影響しません。しかし、これは、クライアントまたはマスター・ファイル・サーバーへの接続に影響する場合があります。

GWCON (Talk 5) 構成要素リセット・コマンド

シン・サーバー・フィーチャーは、次の TSF 固有 GWCON (Talk 5) **reset** コマンドをサポートします。

GWCON, Feature TSF, Restart コマンド

説明: シン・サーバーをリスタートします。

ネットワークへの影響:

シン・クライアントは、リスタートの間ファイルのシン・サーバーにアクセスできません。

制限事項:

マスター・ファイル・サーバーのタイプの変更 (rfs 対 nfs) は、お勧めしません。そうすると、ファイル・キャッシュとして使用される使用可能なメモリーの大きさに影響を与えますが、十分なメモリーが使用可能でなければ、リスタートは失敗します。

すべての TSF の構成変更は、以下を除いて自動的に活動化されます。

GWCON, feature tsf, restart コマンドによって変更が活動化されないコマンド
CONFIG, feature tsf, set memory-cache

GWCON (Talk 5) 一時変更コマンド

TSF は、装置の操作状態を一時変更する、次の GWCON コマンドをサポートします。これらの変更は、装置を再ロードしたり、リスタートしたり、動的に再構成可能なコマンドを実行すると、行われません。

コマンド
GWCON, feature tsf, set mode **注:** シン・サーバー・フィーチャーのモードは、変更されます。

非動的再構成可能コマンド

次の表には、動的に変更できない TSF 構成コマンドを記載します。これらのコマンドを活動化するには、装置を再ロードしたり、リスタートする必要があります。

コマンド
CONFIG, feature tsf, set memory-cache **注:** 指定したメモリー・キャッシュの大きさを大きくすると、ルーターのリスタートまたは再ロードが必要となります。

CONFIG, feature tsf, set mode
注: ルーターをリスタートまたは再ロードしたときにサーバー・モードが使用不可であった場合には、シン・サーバー・モードを使用可能に設定したあとでルーターのリスタートまたは再ロードが必要となります。シン・サーバー・モードは、シン・サーバー・パッケージを最初にロードしたとき、デフォルトで使用不可になります。

第37章 VCRM の構成と監視

バーチャル・サーキット・リソース・マネージャー (VCRM) は、リソース ReSerVation プロトコル (RSVP) をサポートするフィーチャーです。このプロトコルについては、*プロトコルの構成と監視 解説書 第 1 巻* の『RSVP の使用』および 『RSVP の構成および監視』の章で説明しています。RSVP からの予約要求に基づいて、VCRM は物理インターフェースを介したデータ・フローのための接続を作成します。その場合、最初に VCRM は予約を収容できる十分な帯域幅が得られるかどうかを調べることが必要です。

注: フレーム・リレーや X.25 のような WAN インターフェースを使用している場合、利用可能な帯域幅の量が VCRM に分かるようにするために、回線速度を設定する必要があります。回線速度の設定手順は、*Nways マルチプロトコル・アクセス・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および監視の章で説明しています。

インターフェースが ATM SVC の場合、VCRM は RSVP QoS 要求を SVC セットアップ要求にマップします。SVC のセットアップに成功すると、RSVP 予約要求は成功します。VCRM は、QoS パケット用の適切なバッファー・スペースが得られること、およびパケットが正しい SVC を介して伝送されることを確認します。

インターフェースが PPP リンク、LAN、または WAN の場合、VCRM は QoS のソフトウェア待ち行列化および最善的パケットを使用して、発信リンク上のパケットを優先順位付けします。

この章には、次の内容が記載されています。
- 『VCRM 構成環境へのアクセス』
- 『VCRM 監視環境へのアクセス』
- 662ページの『VCRM 監視コマンド』

VCRM 構成環境へのアクセス

VCRM 構成環境にアクセスするには、`Config>` プロンプトで、次のコマンドを入力します。

```
Config>  feature vcrm
VC & Resource Management config console
  --Currently no configurable objects.
Config>
```

表示されるメッセージの目的は、VCRM は別個には構成できないことを示すことです。RSVP を使用可能にすると VCRM も使用可能になり、そのパラメーターを RSVP 構成から入手します。

VCRM 監視環境へのアクセス

VCRM 監視環境にアクセスするには、次のように入力します。

```
* t 5
```

次に、**+** プロンプトで以下のコマンドを入力します。

```
+ feature VCRM
VCRM console
VCRM Console>
```

VCRM Console> プロンプトが表示されます。

VCRM 監視コマンド

ここでは、VCRM 監視コマンドについて説明します。次のコマンドは VCRM> プロンプトで入力します。

表 68. VCRM 監視コマンド

コマンド	機能
? (ヘルプ)	このコマンド・レベルで使用可能なすべてのコマンドを表示するか、または特定のコマンドのオプション (利用できる場合) を表示します。 xxxvページの『ヘルプの入手』を参照してください。
Clear	待ち行列統計をリセットします。
Queue	ATM 以外のソフトウェア待ち行列統計を表示します。
Exit	直前のコマンド・レベルに戻ります。 xxxvページの『下位レベル操作環境の終了』を参照してください。

Clear

clear コマンドは、ソフトウェア待ち行列統計をリセットするのに使用します。

構文:

clear

clear コマンドの例は、**queue** コマンドの項を参照してください。

Queue

queue コマンドは、ATM 以外の トラフィック・フローのソフトウェア待ち行列を表示するのに使用します。

構文:

queue

ATM 以外のソフトウェア待ち行列の表示に使用される用語の定義を次に示します。

Quota 予約された帯域幅の量。当初は、ベストエフォート (B.E.) がすべての quota (割り当て量) を所有します。予約されると、予約帯域幅 (b/w) が B.E. quota から QoS quota にシフトします。

Max-q パケットに記述されている最大待ち行列長さ

Curr-q
パケットに記述されている現行の待ち行列長さ

In quota
割り当てられた帯域幅内で送信されたパケット数または K バイト数

Outside quota
割り当てられた帯域幅外で送信されたパケット数または K バイト数 (アイドル帯域幅が利用可能の場合)

Packets/bytes dropped
ソフトウェア待ち行列によって廃棄されたパケット数またはバイト数

DLC packets/bytes dropped
パケットがソフトウェア待ち行列を通過した後で DLC によって廃棄されたパケット数またはバイト数

例:

```
*t 5

+feature vcrm
VCRM console
VCRM Console>?
CLEAR
QUEUE
EXIT
VCRM Console>queue
Flow-control Queues at sys-clock 346781 Second:
---------
Intf    B.E. Quota:       10000 Kbps            QoS Quota:        0     Kbps
0/Eth   B.E. Max-q        0                     QoS Max-q         0
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:        54169/   3926          in quota:            0/      0
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2048  Kbps            QoS Quota:        0     Kbps
2/PPP   B.E. Max-q        0                     QoS Max-q         0
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:           62/      6          in quota:            0/      0
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2032  Kbps            QoS Quota:        16    Kbps
3/FR    B.E. Max-q        1                     QoS Max-q         1
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:        53160/   4920          in quota:       346596/  31886
        outside quota:       0/      0          outside quota:       0/      0
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0
Intf    B.E. Quota:       2048  Kbps            QoS Quota:        0     Kbps
4/PPP   B.E. Max-q        1                     QoS Max-q         1
        B.E. curr-q       0                     QoS curr-q        0
        B.E. pkts/Kbytes sent:                  QoS pkts/Kbytes sent:
        in quota:           66/      6          in quota:          109/     1
        outside quota:       0/      0          outside quota:       0/
        B.E. pkts/bytes dropped: 0/0            QoS pkts/bytes dropped:  0/0
        DLC pkts/bytes dropped:  B.E.: 0/0      QoS: 0/0

Max total queue length=1;  current total length=0
VCRM Console>clear
Flow-control Queues cleared at sys-clock 346786 Second:
-------
VCRM Console>
```

VCRM の監視 (Talk 5)

付録. リモート AAA 属性

ここには、Radius、TACACS、および TACACS+ サーバーによって使用されるリモート AAA 属性を識別します。

Radius

IBM ベンダー ID: 211

認証属性

標準の草案

TUNNEL_TYPE	64
TUNNEL_MEDIUM_TYPE	65
TUNNEL_CLIEN_TYPE	66
TUNNEL_SERVER_EP	67
TUNNEL_CONN_ID	68
TUNNEL_PASSWORD	69

値

TUNNEL_TYPE		整数
	1	PPTP
	2	L2F
	3	L2TP
TUNNEL_MEDIUM_TYPE		整数
	1	IP
TUNNEL_SERVER_EP		文字列
		IP アドレス

IBM ベンダー特定

NAS_TUNNEL_PASSWORD	101
INBYTES_AH	110
INBYTES_ESP	111
OUTBYTES_AH	112
OUTBYTES_ESP	113
INPKTS_BAD	114
OUTPKTS_BAD	115
INPKTS_BAD_AH	116
INPKTS_BAD_ESP	117
OUTPKTS_BAD_AH	118
OUTPKTS_BAD_ESP	119
INPKTS_AH	120
AH INPKTS_ESP	121
OUTPKTS_AH	122

AH_OUTPKTS_ESP	123
INPKTS_BAD_AH_RPLY	124
INPKTS_BAD_ESP_RPLY	125
INBYTES_WRAP	128
OUTBYTES_WRAP	129
INB_AH_WRAP	130
INB_ESP_WRAP	131
OUB_AH_WRAP	132
OUB_ESP_WRAP	133
POLICY_NAME	135
P1_ID	136
TRANSFORMS	137
REFR_CNT	138
COMPR	139
ESP_ALGO	140
AH_ALGO	141
ESPAUTH_ALGO	142
P1_NAME	143
VC-ACTIVE	177
VC-IDLETIME	179
VC-SUSPENDTIME	180
CALLBACK_FLAGS	210
ENCRYPTION	211
HOSTNAME	213
SUBNETMASK	215
PRIVILEGE	216

キーワード

Radius サーバーでは、ベンダー特定のフィールド `<keyword>=<value>` に入力できるキーワードが使用されます。

KWD_VC_ACTIVE	VCN
KWD_VC_IDLETIME	VCI
KWD_VC_SUSPENDTIME	VCS
KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN
KWD_SUBNETMASK	SNM
KWD_PRIVILEGE	PRV

値

CALLBACK_FLAGS	
REQ	必須コールバック
ROAM	ローミング・コールバック

PRIVILEGE:
- ADMIN
- OPER
- MONITOR

RADIUS 構成ファイルの例

以下は、RADIUS 構成ファイルの例です。

```
VENDOR  IBM  211
ATTRIBUTE       User-Name               1       文字列
ATTRIBUTE       User-Password           2       文字列
ATTRIBUTE       CHAP-Password           3       文字列
ATTRIBUTE       NAS-IP-Address          4       ipaddr
ATTRIBUTE       NAS-Port                5       整数
ATTRIBUTE       Service-Type            6       整数
ATTRIBUTE       Framed-Protocol         7       整数
ATTRIBUTE       Framed-IP-Address       8       ipaddr
ATTRIBUTE       Framed-IP-Netmask       9       ipaddr
ATTRIBUTE       Framed-Routing          10      整数
ATTRIBUTE       Filter-Id               11      文字列
ATTRIBUTE       Framed-MTU              12      整数
ATTRIBUTE       Framed-Compression      13      整数
ATTRIBUTE       Login-IP-Host           14      ipaddr
ATTRIBUTE       Login-Service           15      整数
ATTRIBUTE       Login-TCP-Port          16      整数 #
ATTRIBUTE       Old-Password            17      文字列
ATTRIBUTE       Reply-Message           18      文字列
ATTRIBUTE       Callback-Number         19      文字列
ATTRIBUTE       Callback-Id             20      文字列 #
ATTRIBUTE       未割り当て              21      文字列
ATTRIBUTE       Framed-Route            22      文字列
ATTRIBUTE       Framed-IPX-Network      23      整数
ATTRIBUTE       State                   24      文字列
ATTRIBUTE       Class                   25      文字列
ATTRIBUTE       ベンダー特有            26      文字列
ATTRIBUTE       Session-Timeout         27      整数
ATTRIBUTE       Idle-Timeout            28      整数
ATTRIBUTE       Termination-Action      29      整数
ATTRIBUTE       Called-Station-Id       30      文字列
ATTRIBUTE       Calling-Station-Id      31      文字列
ATTRIBUTE       NAS-Identifier          32      文字列
ATTRIBUTE       Proxy-State             33      文字列
ATTRIBUTE       Login-LAT-Service       34      文字列
ATTRIBUTE       Login-LAT-Node          35      文字列
ATTRIBUTE       Login-LAT-Group         36      文字列
ATTRIBUTE       Framed-Appletalk-Link   37      整数
ATTRIBUTE       Framed-Appletalk-Net    38      整数
ATTRIBUTE       Framed-Appletalk-Zone   39      文字列
ATTRIBUTE       Acct-Status-Type        40      整数
ATTRIBUTE       Acct-Delay-Time         41      整数
ATTRIBUTE       Acct-Input-Octets       42      整数
ATTRIBUTE       Acct-Output-Octets      43      整数
ATTRIBUTE       Acct-Session-Id         44      文字列
ATTRIBUTE       Acct-Authentic          45      整数
ATTRIBUTE       Acct-Session-Time       46      整数
ATTRIBUTE       Acct-Input-Packets      47      整数
ATTRIBUTE       Acct-Output-Packets     48      整数
ATTRIBUTE       Acct-Terminate-Cause    49      整数
ATTRIBUTE       Acct-Multi-Session-Id   50      文字列
ATTRIBUTE       Acct-Link-Count         51      整数
```

```
ATTRIBUTE           CHAP-Challenge          60      文字列
ATTRIBUTE           NAS-Port-Type           61      整数
ATTRIBUTE           Port-Limit              62      整数
ATTRIBUTE           Login-LAT-Port          63      文字列
-------------------- START IBM ----------------------
ATTRIBUTE           Tunnel-Type             64      整数
ATTRIBUTE           Tunnel-Medium           65      整数
ATTRIBUTE           Tunnel-Client-EP        66      文字列
ATTRIBUTE           Tunnel-Server-EP        67      文字列
ATTRIBUTE           Tunnel-Conn-ID          68      文字列
ATTRIBUTE           Tunnel-Password         69      文字列
ATTRIBUTE           Tunnel-NAS-Password     101     文字列
ATTRIBUTE           VC-ACTIVE               177     整数
ATTRIBUTE           VC-IDLETIME             179     整数
ATTRIBUTE           VC-SUSPENDTIME          180     整数
ATTRIBUTE           IBM-Callback-Flags      210     文字列
ATTRIBUTE           IBM-Encryption          211     文字列
ATTRIBUTE           IBM-DialOut             214     文字列
ATTRIBUTE           IBM-Hostname            213     文字列
ATTRIBUTE           IBM-Subnetmask          215     文字列
ATTRIBUTE           IBM-Privilege           216     文字列
ATTRIBUTE           IBM-ipsec-inb-ah        110     整数
ATTRIBUTE           IBM-ipsec-inb-esp       111     整数
ATTRIBUTE           IBM-ipsec-ob-ah         112     整数
ATTRIBUTE           IBM-ipsec-ob-esp        113     整数
ATTRIBUTE           IBM-ipsec-ip-bad        114     整数
ATTRIBUTE           IBM-ipsec-op-bad        115     整数
ATTRIBUTE           IBM-ipsec-ip-bad-ah     116     整数
ATTRIBUTE           IBM-ipsec-ip-bad-esp    117     整数
ATTRIBUTE           IBM-ipsec-op-bad-ah     118     整数
ATTRIBUTE           IBM-ipsec-op-bad-esp    119     整数
ATTRIBUTE           IBM-ipsec-ip-ah         120     整数
ATTRIBUTE           IBM-ipsec-ip-esp        121     整数
ATTRIBUTE           IBM-ipsec-op-ah         122     整数
ATTRIBUTE           IBM-ipsec-op-esp        123     整数
ATTRIBUTE           IBM-ipsec-ip-bad-ah-r   124     整数
ATTRIBUTE           IBM-ipsec-ip-bad-esp-r  125     整数
ATTRIBUTE           IBM-ipsec-inb-wrap      128     整数
ATTRIBUTE           IBM-ipsec-ob-wrap       129     整数
ATTRIBUTE           IBM-ipsec-ib-ah-wrap    130     整数
ATTRIBUTE           IBM-ipsec-ib-esp-wrap   131     整数
ATTRIBUTE           IBM-ipsec-ob-ah-wrap    132     整数
ATTRIBUTE           IBM-ipsec-ob-esp-wrap   133     整数
ATTRIBUTE           IBM-ipsec-policy-name   135     文字列
ATTRIBUTE           IBM-ipsec-p1-id         136     文字列
ATTRIBUTE           IBM-ipsec-p1-name       143     文字列
ATTRIBUTE           IBM-ipsec-esp-algo      140     文字列
ATTRIBUTE           IBM-ipsec-ah-algo       141     文字列
ATTRIBUTE           IBM-ipsec-esp-algo      142     文字列

VALUE               Tunnel-Type             L2TP    3
VALUE               Tunnel-Type             L2F     2
VALUE               Tunnel-Type             PPTP    1
VALUE               Tunnel-Medium           IP      1
VALUE               VC-ACTIVE               YES     1
```

VALUE	VC-ACTIVE	NO	0
VALUE	IBM-Callback-Flags	Required	REQ
VALUE	IBM-Callback-Flags	Roaming	OAM
VALUE	IBM-Dialout	Enable	TRUE
VALUE	IBM-Dialout	Disable	FALSE
VALUE	IBM-Dialout	ONLY	ONLY
VALUE	IBM-Privilege	Administrator	ADMIN
VALUE	IBM-Privilege	Operator	OPER
VALUE	IBM-Privilege	Monitor	MONITOR

TACACS+

認証

承認

PPP service=ppp protocol=ip
LOGIN service=shell cmd=null pri_lvl*0

標準 TACACS+ 属性

service	
protocol	
cmd	
addr	
timeout	
priv_lvl	0 (monitor privilege), 1 (operator privilege), 15 (administrator privilege)
callback-dialstring	

IBM 特定の属性

encryption_key	16 進文字
dial_out	TRUE FALSE ONLY

会計

task_id
start_time
stop_time
elasped_time
timezone
event
reason
bytes
bytes_in
bytes_out
paks
paks_in
paks_out
status
err_msg

略語集

AAL ATM アダプテーション・レイヤー (ATM Adaptation Layer)

AAL-5 ATM アダプテーション・レイヤー 5 (ATM Adaptation Layer 5)

AARP AppleTalk アドレス解決プロトコル (AppleTalk Address Resolution Protocol)

ABR エリア・ボーダー・ルーター (area border router)

ack 確認応答 (acknowledgment)

AIX 拡張対話式エグゼクティブ (Advanced Interactive Executive)

AMA 任意 MAC アドレッシング (arbitrary MAC addressing)

AMP アクティブ・モニター・プレゼント (active monitor present)

ANSI 米国規格協会 (American National Standards Institute)

AP2 AppleTalk フェーズ 2 (AppleTalk Phase 2)

APPN 拡張ピアツーピア・ネットワーキング機能 (Advanced Peer-to-Peer Networking)

ARE 全ルート探索 (all-routes explorer)

ARI ATM 実インターフェース (ATM real interface)

ARI/FCI
アドレス認知標識 / フレーム複写標識 (address recognized indicator/frame copied indicator)

ARP アドレス解決プロトコル (Address Resolution Protocol)

AS 自律システム (autonomous system)

ASBR 自律システム境界ルーター (autonomous system boundary router)

ASCII 情報交換用米国標準コード (American National Standard Code for Information Interchange)

ASN.1 抽象構文表記法 1 (abstract syntax notation 1)

ASRT 適応ソース・ルーティング透過型 (adaptive source routing transparent)

ASYNC
非同期 (asynchronous)

ATCP AppleTalk 制御プロトコル (AppleTalk Control Protocol)

ATM 非同期転送モード (Asynchronous Transfer Mode)

ATMARP
クラシカル IP 中の ARP (ARP in Classical IP)

ATP AppleTalk トランザクション・プロトコル (AppleTalk Transaction Protocol)

AUI 接続ユニット・インターフェース (attachment unit interface)

AVI ATM バーチャル・インターフェース (ATM virtual interface)

ayt 相手確認 (are you there)

BAN 境界アクセス・ノード (Boundary Access Node)

BBCM ブリッジング・ブロードキャスト・マネージャー (Bridging Broadcast Manager)

BCM ブロードキャスト・マネージャー (BroadCast Manager)

BECN 逆方向明示的輻輳 (ふくそう)通知 (backward explicit congestion notification)

BGP ボーダー・ゲートウェイ・プロトコル (Border Gateway Protocol)

BGP ボーダー成長プロトコル (Border Growth Protocol)

BNC Bayonet Niell-Concelman

BNCP ブリッジング・ネットワーク制御プロトコル (Bridging Network Control Protocol)

BOOTP
BOOT プロトコル (BOOT protocol)

BPDU ブリッジ・プロトコル・データ単位 (bridge protocol data unit)

bps ビット / 秒 (bits per second)

BR ブリッジング / ルーティング (bridging/routing)

BRS 帯域幅予約システム (bandwidth reservation system)

BSD Berkeley ソフトウェア配布 (Berkeley software distribution)

BTP BOOTP リレー・エージェント (BOOTP relay agent)

BTU 基本伝送単位 (basic transmission unit)

CAM コンテンツ・アドレス可能メモリー (content-addressable memory)

CCITT 国際電信電話諮問委員会 (Consultative Committee on International Telegraph and Telephone)

CD 衝突検出 (collision detection)

CGWCON
ゲートウェイ・コンソール (Gateway Console)

CIDR 無クラス・ドメイン間ルーティング (Classless Inter-Domain Routing)

CIP クラシカル IP (Classical IP)

CIR 認定情報速度 (committed information rate)

CLNP コネクションレス型モード・ネットワーク・プロトコル (Connectionless-Mode Network Protocol)

CPU 中央演算処理装置 (central processing unit)

CRC 巡回冗長検査 (cyclic redundancy check)

CRS 構成報告書サーバー (configuration report server)

CTS 送信可 (clear to send)

CUD コール・ユーザー・データ (call user data)

DAF 宛先アドレス・フィルター (destination address filtering)

DB データベース (database)

DBsum
データベース要約 (database summary)

DCD データ・チャネル受信回線信号検出器 (data channel received line signal detector)

DCE データ回線終端装置 (data circuit-terminating equipment)

DCS 直接接続サーバー (Directly connected server)

DDLC デュアル・データ・リンク制御装置 (dual data-link controller)

DDN 防衛データ・ネットワーク (Defense Data Network)

DDP データグラム送達プロトコル (Datagram Delivery Protocol)

DDT 動的デバッグ・ツール (Dynamic Debugging Tool)

DHCP 動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)

dir 直接接続 (directly connected)

DL データ・リンク (data link)

DLC データ・リンク制御 (data link control)

DLCI データ・リンク接続識別子 (data link connection identifier)

DLS データ・リンク交換 (data link switching)

DLSw データ・リンク交換 (data link switching)

DMA 直接メモリー・アクセス (direct memory access)

DNA ディジタル・ネットワーク体系 (Digital Network Architecture)

DNCP DECnet プロトコル制御プロトコル (DECnet Protocol Control Protocol)

DNIC データ・ネットワーク識別コード (Data Network Identifier Code)

DoD 米国国防総省 (Department of Defense)

DOS ディスク・オペレーティング・システム (Disk Operating System)

DR 指定ルーター (designated router)

DRAM 動的ランダム・アクセス・メモリー (Dynamic Random Access Memory)

DSAP 宛先サービス・アクセス・ポイント (destination service access point)

DSE データ交換装置 (data switching equipment)

DSE データ交換機 (data switching exchange)

DSR データ・セット・レディー (data set ready)

DSU データ・サービス装置 (data service unit)

DTE データ端末装置 (data terminal equipment)

DTR データ端末レディー (data terminal ready)

Dtype 宛先タイプ (destination type)

DVMRP
距離ベクトル・マルチキャスト・ルーティング・プロトコル (Distance Vector Multicast Routing Protocol)

E&M Ear & Mouth

E1 2.048 Mbps 伝送速度 (2.048 Mbps transmission rate)

EDEL 終了区切り文字 (end delimiter)

EDI エラー検出標識 (error detected indicator)

EGP 外部ゲートウェイ・プロトコル (Exterior Gateway Protocol)

EIA 米国電子工業会 (Electronics Industries Association)

ELAN エミュレート LAN (Emulated LAN)

ELAP EtherTalk リンク・アクセス・プロトコル (EtherTalk Link Access Protocol)

ELS イベント・ログ・システム (Event Logging System)

ELSCon
2 次 ELS コンソール (Secondary ELS Console)

ESI エンド・システム識別子 (End system identifier)

EST 東部標準時 (Eastern Standard Time)

Eth イーサネット (Ethernet)

fa-ga 機能アドレス・グループ・アドレス (functional address-group address)

FCS フレーム検査シーケンス (frame check sequence)

FECN 順方向明示的輻輳 (ふくそう) 通知 (forward explicit congestion notification)

FIFO 先入れ先出し (first in, first out)

FLT フィルター・ライブラリー (filter library)

FR フレーム・リレー (Frame Relay)

FRL フレーム・リレー (Frame Relay)

FTP ファイル転送プロトコル (File Transfer Protocol)

FXO Foreign Exchange Office

FXS Foreign Exchange Station

GMT グリニッジ標準時 (Greenwich Mean Time)

GOSIP
米国政府 OSI 調達仕様 (Government Open Systems Interconnection Profile)

GTE 一般電話会社 (General Telephone Company)

GWCON
ゲートウェイ・コンソール (Gateway Console)

HDLC ハイレベル・データ・リンク制御 (high-level data link control)

HEX 16 進法 (hexadecimal)

HPR 高性能ルーティング (high-performance routing)

HST TCP/IP ホスト・サービス (TCP/IP host services)

HTF ホスト・テーブル形式 (host table format)

IBD 統合ブート装置 (Integrated Boot Device)

ICMP インターネット制御メッセージ・プロトコル (Internet Control Message Protocol)

ICP インターネット制御プロトコル (Internet Control Protocol)

ID 識別 (identification)

IDP イニシアル・ドメイン・パート (Initial Domain Part)

IDP インターネット・データグラム・プロトコル (Internet Datagram Protocol)

IEEE 米国電気電子学会 (Institute of Electrical and Electronics Engineers)

IETF インターネット技術特別調査委員会 (Internet Engineering Task Force)

Ifc# インターフェース番号 (interface number)

IGP 内部ゲートウェイ・プロトコル (interior gateway protocol)

ILMI インターリム・ローカル管理インターフェース (Interim Local Management Interface)

InARP 逆アドレス解決プロトコル (Inverse Address Resolution Protocol)

IP インターネット・プロトコル (Internet Protocol)

IPCP IP 制御プロトコル (IP Control Protocol)

IPPN IP プロトコル・ネットワーク (IP Protocol Network)

IPX インターネットワーク・パケット交換 (Internetwork Packet Exchange)

IPXCP IPX 制御プロトコル (IPX Control Protocol)

ISDN サービス総合ディジタル網 (integrated services digital network)

ISO 国際標準化機構 (International Organization for Standardization)

Kbps キロビット / 秒 (kilobits per second)

LAC L2TP ネットワーク・アクセス集線装置 (L2TP Network Access Concentrator)

LAN ローカル・エリア・ネットワーク (local area network)

LAPB 平衡型リンク・アクセス・プロトコル (link access protocol-balanced)

LAT ローカル・エリア・トランスポート (local area transport)

LCS LAN チャネル・ステーション (LAN Channel Station)

LCP リンク制御プロトコル (Link Control Protocol)

LE LAN エミュレーション (LAN Emulation)

LEC LAN エミュレーション・クライアント (LAN Emulation Client)

LED 発光ダイオード (light-emitting diode)

LECS LAN エミュレーション構成サーバー (LAN Emulation Configuration Server)

LES LAN エミュレーション・サーバー (LAN Emulation Server)

LES-BUS
LAN エミュレーション・サーバー - ブロードキャストおよび未知サーバー (LAN Emulation Server - Broadcast and Unknown Server)

LF 最大フレーム、改行 (largest frame; line feed)

LIS 論理 IP サブネット (Logical IP subnet)

LLC 論理リンク制御 (logical link control)

LLC2 論理リンク制御 2 (論理リンク制御 2)

LMI ローカル管理インターフェース (local management interface)

LNS L2TP ネットワーク・サーバー (L2TP Network Server)

LRM LAN 報告機構 (LAN reporting mechanism)

LS リンク状態 (link state)

LSA リンク状態公示 (link state advertisement)

LSA リンク・サービス体系 (Link Services Architecture)

LSB 最下位ビット (least significant bit)

LSI LAN ショートカット・インターフェース (LAN shortcuts interface)

LSreq リンク状態要求 (link state request)

LSrxl リンク状態再送リスト (link state retransmission list)

LU 論理装置 (logical unit)

MAC 媒体アクセス制御 (medium access control)

Mb メガビット (megabit)

MB メガバイト (megabyte)

Mbps メガビット / 秒 (megabits per second)

MBps メガバイト / 秒 (megabytes per second)

MC マルチキャスト (multicast)

MCF MAC フィルター (MAC filtering)

MIB 管理情報ベース (Management Information Base)

MIB II 管理情報ベース II (Management Information Base II)

MILNET
軍事ネットワーク (military network)

MOS マイクロ・オペレーティング・システム(Micro Operating System)

MOSDBG
マイクロ・オペレーティング・システム・デバッグ・ツール (Micro Operating System Debugging Tool)

MOSDDT
マイクロ・オペレーティング・システム動的デバッグ・ツール (Micro Operating System Dynamic Debugging Tool)

MOSPF
マルチキャスト拡張付き最短パス最優先オープン (Open Shortest Path First with multicast extensions)

MPC マルチパス・チャネル (Multi-Path Channel)

MPC+ ハイパフォーマンス・データ転送 (HPDT) マルチパス・チャネル (High performance data transfer (HPDT) Multi-Path Channel)

MSB 最上位ビット (most significant bit)

MSDU MAC サービス・データ単位 (MAC service data unit)

MSS マルチプロトコル・スイッチ・サービス (Multiprotocol Switched Services)

MRU 最大受信単位 (maximum receive unit)

MTU 最大伝送単位 (maximum transmission unit)

nak 否定応答 (not acknowledged)

NAS Nways スイッチ管理ステーション (Nways Switch Administration station)

NBMA 非ブロードキャスト・マルチアクセス (Non-Broadcast Multiple Access)

NBP ネーム・バインディング・プロトコル (Name Binding Protocol)

NBR 近隣、ネイバー (neighbor)

NCP ネットワーク制御プロトコル (Network Control Protocol)

NCP ネットワーク・コア・プロトコル (Network Core Protocol)

NDPS 非介入パス・スイッチ (non-disruptive path switching)

NetBIOS
ネットワーク基本入出力システム (Network Basic Input/Output System)

NHRP ネクスト・ホップ解決プロトコル (Next Hop Resolution Protocol)

NIST 米国連邦情報技術局 (National Institute of Standards and Technology)

NPDU ネットワーク・プロトコル・データ単位 (Network Protocol Data Unit)

NRZ 非ゼロ復帰 (non-return-to-zero)

NRZI 非ゼロ復帰反転 (non-return-to-zero inverted)

NSAP ネットワーク・サービス・アクセス・ポイント (Network Service Access Point)

NSF 国立科学財団 (National Science Foundation)

NSFNET
国立科学財団ネットワーク (National Science Foundation NETwork)

NVCNFG
不揮発性構成 (nonvolatile configuration)

OOS アウト・オブ・サービス (out of service)

OPCON
オペレーター・コンソール (Operator Console)

OSI 開放型システム間相互接続 (open systems interconnection)

OSICP
OSI 制御プロトコル (OSI Control Protocol)

OSPF 最短パス最優先オープン (Open Shortest Path First)

OUI 組織固有識別子 (organization unique identifier)

PC パーソナル・コンピューター (personal computer)

PCA 並列チャネル・アダプター (parallel channel adapter)

PCR ピーク・セル速度 (peak cell rate)

PDN 公衆データ網 (public data network)

PING パケット・インターネット・グローパー (Packet internet groper)

PDU プロトコル・データ単位 (protocol data unit)

PID プロセス識別子(process identification)

P-P ポイント・ポイント (Point-to-Point)

PPP ポイント・ポイント・プロトコル (Point-to-Point Protocol)

PROM プログラム式読み取り専用メモリー (programmable read-only memory)

PU 物理装置 (physical unit)

PVC パーマネント・バーチャル・サーキット (permanent virtual circuit)

Qos サービス品質 (Quality of Service)

RAM ランダム・アクセス・メモリー (random access memory)

RD ルート記述子 (route descriptor)

REM リング・エラー監視 (ring error monitor)

REV 受信 (receive)

RFC コメント要求 (Request for Comments)

RI リング標識、ルーティング情報 (ring indicator; routing information)

RIF ルーティング情報フィールド (routing information field)

RII ルーティング情報標識 (routing information indicator)

RIP ルーティング情報プロトコル (Routing Information Protocol)

RISC 縮小命令セット・コンピューター (reduced instruction-set computer)

RNR 受信不可 (receive not ready)

ROM 読み取り専用メモリー (read-only memory)

ROpcon
リモート・オペレーター・コンソール (Remote Operator Console)

RPS リング・パラメーター・サーバー (ring parameter server)

RTMP ルーティング・テーブル保守プロトコル (Routing Table Maintenance Protocol)

RTP ルーティング更新プロトコル (RouTing update Protocol)

RTS 送信要求 (request to send)

Rtype ルート・タイプ (route type)

rxmits 再送 (retransmissions)

rxmt 再送する (retransmit)

s 秒 (second)

SAF 発信元アドレス・フィルター (source address filtering)

SAP サービス・アクセス・ポイント (Service access point)

SAP サービス公示プロトコル (Service Advertising Protocol)

SCR 持続セル速度 (Sustained cell rate)

SCSP サーバー・キャッシュ同期プロトコル (Server Cache Synchronization Protocol)

sdel 開始区切り文字 (start delimiter)

SDLC SDLC リレー、同期データ・リンク制御 (SDLC relay, synchronous data link control)

SDU サービス・データ単位 (Service Data Unit)

seqno シーケンス番号 (sequence number)

SGID サーバー・グループ ID (sever group id)

SGMP シンプル・ゲートウェイ監視プロトコル (Simple Gateway Monitoring Protocol)

SL シリアル・ライン (serial line)

SLIP シリアル・ライン IP (Serial Line IP)

SMP 待機モニター・プレゼント (standby monitor present)

SMTP シンプル・メール転送プロトコル (Simple Mail Transfer Protocol)

SNA システム・ネットワーク体系 (Systems Network Architecture)

SNAP サブネットワーク・アクセス・プロトコル (Subnetwork Access Protocol)

SNMP シンプル・ネットワーク管理プロトコル (Simple Network Management Protocol)

SNPA サブネットワーク接続ポイント (subnetwork point of attachment)

SPF OSPF エリア内ルート (OSPF intra-area route)

SPE1 OSPF 外部ルート・タイプ 1 (OSPF external route type 1)

SPE2 OSPF 外部ルート・タイプ 2 (OSPF external route type 2)

SPIA OSPF エリア間ルート・タイプ (OSPF inter-area route type)

SPID サービス・プロファイル ID (service profile ID)

SPX 順次パケット交換 (Sequenced Packet Exchange)

SQE 信号品質エラー (signal quality error)

SRAM 静的ランダム・アクセス・メモリー (static random access memory)

SRB ソース・ルーティング・ブリッジ (source routing bridge)

SRF 特定ルート・フレーム (specifically routed frame)

SRLY SDLC リレー (SDLC relay)

SRT ソース・ルーティング透過型 (source routing transparent)

SR-TB
ソース・ルーティング - 透過型ブリッジ (source routing-transparent bridge)

STA 静的 (static)

STB スパンニング・ツリー・ブリッジ (spanning tree bridge)

STE スパンニング・ツリー探索 (spanning-tree explorer)

STP シールド付き対より線、スパンニング・ツリー・プロトコル (shielded twisted pair; spanning tree protocol)

SVC スイッチド・バーチャル・サーキット (switched virtual circuit)

SVN スイッチド・バーチャル・ネットワーキング (Switched Virtual Networking)

TB 透過型ブリッジ (transparent bridge)

TCN トポロジー変更通知 (topology change notification)

TCP 伝送制御プロトコル (Transmission Control Protocol)

TCP/IP 伝送制御プロトコル / インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)

TEI 端末終端点識別子 (terminal point identifier)

TFTP トリビアル・ファイル転送プロトコル (Trivial File Transfer Protocol)

TKR トークンリング (token ring)

TLV タイプ/長さ/値 (Type/Length/Value)

TMO タイムアウト (timeout)

TOS サービスのタイプ (type of service)

TSF 透過型スパンニング・フレーム (transparent spanning frames)

TTL 活動回数 (time to live)

TTY テレタイプライター (teletypewriter)

TX 送信 (transmit)

UA 非番号制確認 (unnumbered acknowledgment)

UDP ユーザー・データグラム・プロトコル (User Datagram Protocol)

UI 非番号制情報 (unnumbered information)

UNI ユーザー・ネットワーク・インターフェース (User-Network Interface)

UTP シールドなし対より線 (unshielded twisted pair)

VCC バーチャル・チャネル・コネクション (Virtual Channel Connection)

VINES バーチャル・ネットワーキング・システム (VIrtual NEtworking System)

VIR 可変情報速度 (variable information rate)

VL バーチャル・リンク (virtual link)

VNI バーチャル・ネットワーク・インターフェース (Virtual Network Interface)

VoFR ボイス・オーバー・フレーム・リレー (Voice over Frame Relay)

VR バーチャル・ルート (virtual route)

WAN 広域ネットワーク (wide area network)

WRS WAN レストラル / リルート (WAN restoral/reroute)

X.25 パケット交換網 (packet-switched networks)

X.251 X.25 物理レイヤー (X.25 physical layer)

X.252 X.25 フレーム・レイヤー (X.25 frame layer)

X.253 X.25 パケット・レイヤー (packet layer)

XID 交換 ID (exchange identification)

XNS Xerox ネットワーク・システム (Xerox Network Systems)

XSUM チェックサム (checksum)

ZIP AppleTalk ゾーン情報プロトコル (AppleTalk Zone Information Protocol)

ZIP2 AppleTalk ゾーン情報プロトコル 2 (AppleTalk Zone Information Protocol 2)

ZIT ゾーン情報テーブル (Zone Information Table)

用語集

この用語集には、以下からの用語および定義が含まれています。

- *American National Standard Dictionary for Information Systems*、ANSI X3.172-1990 (米国規格協会 (ANSI) が 1990 年に著作権を取得)。この複写版が米国規格協会 (ANSI: 11 West 42nd Street, New York, New York 10036)から発売されています。定義の後に記号 (A) を付けて出典を示してあります。
- ANSI/EIA Standard--440-A、*Fiber Optic Terminology*。この複写版が米国電子工業会 (2001 Pennsylvania Avenue, N.W., Washington, DC 20006) から発売されています。定義の後に記号 (E) を付けて出典を示してあります。
- *Information Technology Vocabulary*。国際標準化機構および国際電気標準会議の第 1 合同技術委員会第 1 分科会 (ISO/IEC JTC1/SC1) によって編さんされたものです。この語い集の刊行部分から転載した定義については、その後に記号 (I) を付けて示してあります。また、ISO/IEC JTC1/SC1 で編さん中の国際規格草案、分科会草案、および作業文書から採用した定義については、その後に記号 (T) を付けて、SC1 の加盟各国諸団体間で最終合意がなされていないことを示してあります。
- *IBM Dictionary of Computing* , New York: McGraw-Hill, 1994
- Internet Request for Comments: 1208、*Glossary of Networking Terms*
- Internet Request for Comments: 1392、*Internet Users' Glossary*
- *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

この用語集では、以下の形で相互参照しています。

と対比:
反対の意味または実質的に異なる意味をもつ用語を示します。

の同義語:
この用語集の該当箇所に記述されている、優先的に使用してほしい、同じ意味をもつ用語を示します。

と同義:
逆方向参照として、定義の対象となっている用語から、同じ意味をもつ他の用語をすべて参照します。

を参照:
一部の語 (特に最後の語) が同じ複数語からなる用語を参照します。

も参照:
関連する意味 (同義ではない) をもつ用語を参照します。

A

AAL. ATM アダプテーション・レイヤー (ATM Adaptation Layer)。ヘッダーを追加/除去し、セルへ/からのデータを細分化/再組み立てすることにより、ATM ネットワークへ/からのユーザー・データを適応させるレイヤー。

AAL-5. ATM アダプター・レイヤー 5 (ATM Adaptation Layer 5)。複数ある標準 AAL の 1 つ。AAL-5 はデータ通信用に設計されたもので、LAN エミュレーションおよびクラシカル IP によって使用される。

抽象構文 (abstract syntax). データ伝送に必要な特性はすべて含んでいるが、その他の明細 (たとえば、特定のコンピューター・アーキテクチャーに依存する明細など) は省略 (抽象化) されているデータ仕様。*抽象構文表記法 (ASN.1) (abstract syntax notation 1 (ASN.1))* および*基本符号化規則 (BER) (basic encoding rules (BER))* も参照。

抽象構文表記法 1 (ASN.1) (abstract syntax notation 1 (ASN.1)). 次の標準で指定されている抽象構文の開放型システム間相互接続 (OSI) 方式。

- ITU-T 勧告 X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T 勧告 X.680 (1994) | ISO/IEC 8824-1: 1994

基本符号化規則 (BER) (basic encoding rules (BER)) も参照。

ACCESS. シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理ノードがオブ

ジェクトに対して提供する最小レベルのサポートを定義する、管理情報ベース (MIB) モジュール内の文節。

確認応答 (acknowledgment). (1) 受信側が送信側に肯定応答として確認応答文字を伝送すること。 (T) (2) 送信された項目が受信されたことを示すこと。

アクティブ (active). (1) 運用可。 (2) 別のノードまたは装置に接続された、またはそれへの接続が利用可能なノードまたは装置に関する用語。

アクティブ・モニター (active monitor). トークンリング・ネットワークにおいて、一度に 1 つのリング・ステーションによって実行される機能で、トークンの伝送を開始し、トークン誤り回復機能を提供する。現在のアクティブ・モニターに障害が起こった場合、リング上の任意のアクティブ・アダプターが、アクティブ・モニター機能を提供することができる。

アドレス (address). データ通信において、通信ネットワークに接続された各装置、ワークステーション、またはユーザーに割り当てられる固有のコード。

アドレス・マッピング・テーブル (AMT) (address mapping table (AMT)). 現在のノード・アドレスとハードウェア・アドレスのマッピングを提供する、AppleTalk ルーター内に維持されているテーブル。

アドレス・マスク (address mask). インターネット・サブネットワークにおいて、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットを識別するために使用される、32 ビットのマスク。サブネット・マスク *(subnet mask)* およびサブネットワーク・マスク *(subnetwork mask)* と同義。

アドレス解決 (address resolution). (1) ネットワーク・レイヤー・アドレスを媒体特有アドレスにマッピングする方法。 (2) *アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP))* および *AppleTalk アドレス解決プロトコル (AARP) (AppleTalk Address Resolution Protocol (AARP))* も参照。

アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP)). (1) インターネット・プロトコルにおいて、サポートされる大都市圏ネットワークやローカル・エリア・ネットワーク (イーサネットやトークンリングなど) が使用するアドレスに、IP アドレスを動的にマップするプロトコル。 (2) *逆アドレス解決プロトコル (RARP) (Reverse Address Resolution Protocol (RARP))* も参照。

アドレッシング (addressing). データ通信において、端末局がデータの送信先の端末局を選択する方法。

隣接ノード (adjacent nodes). 他のノードとは接続していない少なくとも 1 つのパスによって相互に接続されている 2 つのノード。 (T)

管理ドメイン (Administrative Domain). 1 つの管理機関によって管理される、ホストとルーターおよび相互接続ネットワークの集合。

拡張ピアツーピア・ネットワーキング機能 (Advanced Peer-to-Peer Networking) (APPN). SNA の拡張機能で、次の特長を備えている。(a) 重大な階層間の依存関係を回避することによって、単一点の障害の影響を分離できるようにした、分散ネットワーク制御の機能強化。(b) 接続、再構成、および柔軟なルート選択を容易に実現できる、動的なネットワーク・トポロジー情報の交換。(c) ネットワークの資源の動的定義。(d) 資源の登録およびディレクトリー検索の自動化。 APPN は、エンド・ユーザー・サービス向けの LU 6.2 ピア間通信機能をネットワークの制御に拡張し、LU 2、LU 3、および LU 6.2 を含む複数の LU タイプをサポートする。

拡張ピアツーピア・ネットワーキング機能 (APPN) エンド・ノード (Advanced Peer-to-Peer Networking (APPN) end node). 広範囲のエンド・ユーザー・サービスを提供し、そのローカル・コントロール・ポイント (CP) と隣接するネットワーク・ノード内の CP との間のセッションをサポートするノード。このノードは、これらのセッションを使用して、隣接 CP (ネットワーク・ノード・サーバー) に資源を動的に登録し、ディレクトリー検索要求を送受信し、管理サービスを受ける。APPN エンド・ノードは、サブエリア・ネットワークに周辺ノードまたは他のエンド・ノードとして接続することもできる。

拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク (Advanced Peer-to-Peer Networking (APPN) network). 相互接続されたネットワーク・ノードとそれらのクライアント・エンド・ノードの集合。

拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node). 広範囲のエンド・ユーザー・サービスを提供するノードで、次のものを提供することができる。

- 分散ディレクトリー・サービス (中央ディレクトリー・サーバーへのドメインの資源の登録を含む)
- トポロジー・データベースは他の APPN ネットワーク・ノードと交換し、そのネットワーク内のネットワークが、要求されたサービス・クラスに基づいて LU-LU セッションの最適ルートを選択できるようにする。
- そのローカル LU とクライアント・エンド・ノードのセッション・サービス

- APPN ネットワークの中間ルーティング・サービス

拡張ピアツーピア・ネットワーキング機能 (APPN) ノード (Advanced Peer-to-Peer Networking (APPN) node). APPN ネットワーク・ノードまたは APPN エンド・ノード。

エージェント (agent). エージェントの役割を果たすシステム。

アラート (alert). 問題または切迫した問題を識別するためにネットワーク内の管理サービス中心拠点に送られるメッセージ。

全ステーション・アドレス (all-stations address). 通信において、*ブロードキャスト・アドレス (broadcast address)* の同義語。

米国規格協会 (ANSI) (American National Standards Institute (ANSI)). 認定組織が米国の自主業界標準を作成して維持するための手順を決める、生産者、消費者、および一般の関係団体から構成される組織。 (A)

アナログ (analog). (1) 連続的に変化する物理量から構成されるデータに関する用語。 (A) (2) *ディジタル (digital)* と対比。

AppleTalk. Apple Computer, Inc. によって開発されたネットワーク・プロトコル。このプロトコルは、ネットワーク上の装置を相互接続するために使用される。装置は、Apple 製品と非 Apple 製品を混合して使用できる。

AppleTalk アドレス解決プロトコル (AARP) (AppleTalk Address Resolution Protocol (AARP)). AppleTalk ネットワークにおいて、(a) AppleTalk ノード・アドレスをハードウェア・アドレスに変換し、(b) 複数のプロトコルをサポートするネットワーク内のアドレッシングの矛盾を調整するプロトコル。

AppleTalk トランザクション・プロトコル (ATP) (AppleTalk Transaction Protocol (ATP)). AppleTalk ネットワークにおいて、ゾーン情報を得るためにゾーン情報プロトコル (ZIP) にアクセスするホストに対して、クライアント/サーバー要求・応答機能を提供するプロトコル。

APPN ネットワーク (APPN network). *拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク (Advanced Peer-to-Peer Networking (APPN) network)* を参照。

APPN ネットワーク・ノード (APPN network node). *拡張ピアツーピア・ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node)* を参照。

任意 MAC アドレッシング (AMA) (arbitrary MAC addressing (AMA)). DECnet 体系において、出荷時設定アドレスとローカル管理アドレスをサポートする、DECnet フェーズ IV-Prime によって使用されるアドレッシング機構。

エリア、区域 (area). インターネットおよび DECnet ルーティング・プロトコルにおいて、ネットワークの通信事業者の定義によってグループ化された、ネットワークまたはゲートウェイのサブセット。各エリアは自己完結型で、あるエリアのトポロジーは他のエリアからは見えない。

非同期 (ASYNC) (asynchronous (ASYNC)). 共通タイミング信号のような特定の事象の発生に依存しない 2 つ以上のプロセス。 (T)

ATM. 非同期転送モード (Asynchronous Transfer Mode)。セル交換を基礎とした、コネクション型高速ネットワーキング・テクノロジー。

ATMARP. クラシカル IP 内の ARP。

接続ユニット・インターフェース (AUI) (attachment unit interface (AUI)). ローカル・エリア・ネットワークにおいて、媒体接続ユニットとデータ・ステーション内のデータ端末装置間のインターフェース。 (I) (A)

属性値ペア (AVP) (Attribute Value Pair (AVP)). メッセージ・タイプおよび本文をコード化する一律的な方法。この方式は、 L2TP のインターオペラビリティーを可能にすると同時に、拡張性を最大化する。

認証障害 (authentication failure). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、要求側クライアントが SNMP コミュニティーのメンバーでない場合に、認証エンティティーが生成するトラップ。

自律システム (autonomous system). TCP/IP において、1 つの管理機関の下にあるネットワークとルーターの集まり。このようなネットワークとルーターは緊密に協力し、自ら選択した内部ゲートウェイ・プロトコルを使用して、相互にネットワークの到達可能性とルーティングの情報を伝送する。

自律システム番号 (autonomous system number). TCP/IP において、IP アドレスの割り当てを行うのと同じ中央電気通信事業者が自律システムに割り当てる番

号。自律システム番号により、自動ルーティング・アルゴリズムは、自律システムを区別することができる。

B

BCM. ブロードキャスト・マネージャー (BroadCast Manager)。ブロードキャスト・フレームの効果を制限するために設計された、LAN エミュレーションの IBM 拡張版。

バックボーン (backbone). (1) ローカル・エリア・ネットワークのマルチ・ブリッジ・リング構成において、ブリッジまたはルーターを用いてリングが接続されている高速リンク。バックボーンは、バスまたはリングとして構成することができる。 (2) 広域ネットワークにおいて、ノードまたはデータ交換機 (DSE) が接続されている高速リンク。

バックボーン・ネットワーク (backbone network). より小規模の (通常は、より低速の) ネットワークを接続する中央のネットワーク。バックボーン・ネットワークは通常、相互接続するネットワークよりもはるかに高容量の通信ネットワーク、あるいは公用パケット交換データグラム・ネットワークのような広域ネットワーク (WAN) である。

バックボーン・ルーター (backbone router). (1) エリア間でデータを転送するのに使用されるルーター。 (2) ネットワークをより大規模なインターネットに接続するのに使用される、一連のルーターの中の 1 つ。

帯域幅 (Bandwidth). 光リンクの帯域幅は、リンクが情報を運ぶ容量を表し、光リンクがサポートできる最大ビット・レートを示す。

基本伝送単位 (BTU) (basic transmission unit (BTU)). SNA において、パス制御コンポーネント間で受け渡されるデータと制御情報の単位。 BTU は、1 つまたは複数のパス情報単位 (PIU) から構成される。

ボー (baud). 非同期伝送において、1 秒当りの変調速度の単位。つまり、サイクル間隔が 20 ミリ秒の場合、変調速度は 50 ボーになる。 (A)

ブートストラップ (bootstrap). (1) コンピューター・プログラムが完全に記憶装置に入り終わるまで、後に続く命令をロードして実行させる一連の命令。 (T) (2) それ自体の働きによって望ましい状態に到達するように設計された技法または装置。たとえば、最初の幾つかの命令が、残りの命令を入力装置からコンピューターに読み込むようになっている機械ルーチン。 (A)

ボーダー・ゲートウェイ・プロトコル (BGP) (Border Gateway Protocol (BGP)). ドメインと自律システムの間で使用されるインターネット・プロトコル (IP) ルーティング・プロトコル。

ボーダー・ルーター (border router). インターネット通信において、自律システムの端に位置し、別の自律システムの端にあるルーターと通信するルーター。

ブリッジ (bridge). 複数の LAN を (ローカルまたはリモート側で) 相互接続する機能を持った装置で、同じ論理リンク制御プロトコルを使用するが、異なる媒体アクセス制御プロトコルを使用することができる。ブリッジは、媒体アクセス制御 (MAC) アドレスに基づいてフレームを別のブリッジに転送する。

ブリッジ識別子 (bridge identifier). スパンニング・ツリー・プロトコルで使用される、最下位ポート識別子をもつポートの MAC アドレスとユーザー定義の値から構成される 8 バイトのフィールド。

ブリッジング (bridging). LAN では、フレームを 1 つの LAN セグメントから別のセグメントに転送すること。着側は、フレーム・ヘッダーの着信アドレス・フィールドに符号化された媒体アクセス制御 (MAC) サブレイヤー・アドレスによって指定される。

ブロードキャスト (broadcast). (1) すべての宛先に同じデータを伝送すること。 (T) (2) 複数の宛先に同時にデータを伝送すること。 (3) マルチキャスト *(multicast)* と対比。

ブロードキャスト・アドレス (broadcast address). 通信において、リンク上のすべてのステーションに共通のアドレスとして確保されているステーション・アドレス (8 桁の 1 で構成)。全ステーション・アドレス *(all-stations address)* と同義。

BUS. ブロードキャストおよび未知サーバー (Broadcast and Unknown Server)。マルチキャスト・フレームおよび不明ユニキャスト・フレームの送達を担当する LAN エミュレーション・サービス・コンポーネント。

C

キャッシュ (cache). (1) 主記憶装置から読み出した、プロセッサーが次に必要になる可能性がある命令とデータのコピーを入れておくために使用される、主記憶装置より小さくて高速の特殊用途バッファー記憶装置。 (T) (2) 頻繁にアクセスされる命令とデータを入れておくバッファー記憶装置。アクセス時間を短縮するために使用される。 (3) ディレクトリーの検索速度を上げるために、頻繁に使用されるディレクトリー情報を入れておくことができる、ネットワーク・ノード内のディレク

トリー・データベースのオプション部。 (4) キャッシュに入れる、または保管すること。

コール・リクエスト・パケット (call request packet). (1) コールのための接続を確立することを要求するために、データ端末装置 (DTE) がネットワーク全体に伝送するコール監視パケット。 (2) X.25 通信において、ネットワークを通してコール設定を要求するために、DTE によって伝送されるコール監視パケット。

標準アドレス (canonical address). LAN において、トークンリングまたはイーサネット・アダプターの媒体アクセス制御 (MAC) アドレスを伝送するための IEEE 802.1 形式。標準形式では、各アドレス・バイトの最下位 (右端) ビットが最初に伝送される。*非標準アドレス (noncanonical address)* と対比。

キャリア (carrier). 通信システムを介して伝送される情報を運ぶ信号によって変化する電波、電磁波、またはパルス列。 (T)

キャリア検出 (carrier detect). *受信回線信号検出器 (RLSD) (received line signal detector (RLSD))* の同義語。

キャリア・センス (carrier sense). ローカル・エリア・ネットワークにおいて、別のステーションが伝送中であるかどうかを検出する、データ・ステーションの機能。 (T)

搬送波検知多重アクセス/衝突検出 (CSMA/CD) (carrier sense multiple access with collision detection (CSMA/CD)). キャリア・センスを必要とするプロトコル。送信側データ・ステーションは、伝送中に別の信号を検出すると、送信を停止し、ジャム信号を送り、可変時間待ってから再試行する。 (T) (A)

CCITT. 国際電信電話諮問委員会 (International Telegraph and Telephone Consultative Committee)。 以前は国際電気通信連合 (ITU) の組織であったが、 1993 年 3 月 1 日に ITU は再編成され、標準化の任務は、電気通信連合の電気通信標準化部門 (ITU-TS) という名前の下部組織に移管された。 『CCITT』 という用語は、再編成の前に承認さた勧告を表すのに引き続き使用される。

チャネル (channel). (1) 信号を送ることができるパス。たとえば、データ・チャネル、出力チャネル。 (A) (2) 主記憶装置とローカル周辺装置との間のデータ転送を扱う、処理装置によって制御される装置。

チャネル・サービス・ユニット (CSU) (channel service unit (CSU)). ディジタル・ネットワークへのインターフェースを提供する装置。 CSU は、チャネル帯域幅内で信号の効率を一定に保つ伝送路調整 (等化) 機能、バイナリー・パルス・ストリームを構成する信号再編成機能、および CSU と通信事業体のオフィス・チャネル装置間のテスト信号伝送を含めたループバック・テスト機能を提供する。データ・サービス装置 *(DSU) (data service unit (DSU))* も参照。

チャネル化 (channelization). 通信回線上の帯域幅を多数のチャネル (サイズが異なる場合もある) に分割するプロセス。***時分割多重方式 (time division multiplexing)*** (TDM) とも呼ばれる。

チェックサム (checksum). (1) グループに関連し、検査目的で使用される、データのグループの合計。 (T) (2) 誤り検出において、ブロック内の全ビットを対象とする。書き込まれて計算された合計に一致しない場合は、誤りが指示される。 (3) ディスケットにおいて、誤り検出の目的でセクターに書き込まれるデータ。計算されたチェックサムが、セクターに書き込まれたデータのチェックサムに一致しない場合は、不良セクターを示している。データは、数字またはチェックサムの計算では数字とみなされる他の文字列のいずれかである。

CIP. クラシカル IP (Classical IP)。

CIPC. クラシカル IP クライアント (Classical IP Client)。

クラシカル IP (Classical IP). ATM 上で IP を使用して通信するための ATM 接続ホストの IETF 標準。

クラシカル IP クライアント (Classical IP Client). 論理 IP サブネットのユーザーを表すクラシカル IP コンポーネント。

サーキット交換 (circuit switching). (1) 必要に応じて、2 つ以上のデータ端末装置 (DTE) を接続し、その接続が解放されるまで、それらの装置間のデータ回線を専用に使用することができるプロセス。 (I) (A) (2) *回線交換 (line switching)* と同義。

クラス A ネットワーク (class A network). インターネット通信において、IP アドレスの上位 (最上位) ビットが 0 に設定され、ホスト ID が下位の 3 オクテットを占めるネットワーク。

クラス B ネットワーク (class B network). インターネット通信において、IP アドレスの 2 つの上位 (最上位と最上位の次の) ビットがそれぞれ 1 と 0 に設定され、ホスト ID が下位の 2 オクテットを占めるネットワーク。

サービス・クラス (COS) (class of service (COS)). セッションのパートナー間のルートを確立するために使用される一組の特性（ルートのセキュリティー、伝送の

優先順位、帯域幅など)。サービス・クラスは、セッションの開始プログラムによって指定されたモード名から導出される。

クライアント (client). (1) サーバーから共用サービスを受け取る機能単位。 (T) (2) ユーザーのこと。

クライアント/サーバー (client/server). 通信において、一方の側のプログラムが相手側のプログラムに要求を送信して応答を待つという、分散データ処理における対話のモデル。要求側プログラムをクライアントといい、応答側プログラムをサーバーという。

クロッキング、刻時 (clocking). (1) 2 進データ同期通信において、クロック・パルスを使用して、データおよび制御文字の同期を制御すること。 (2) 一定時間に通信回線上で送信するデータ・ビット数を制御する方法。

衝突 (collision). チャネル上の同時伝送によって生じる望ましくない状態。 (T)

衝突検出 (collision detection). 搬送波検知多重アクセス/衝突検出 (CSMA/CD) において、2 台以上のステーションが同時に伝送していることを示す信号。

認定情報速度 (Committed information rate). ネットワークが送達することに同意した、ビットで表されたデータの最大量。

コミュニティー (community). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、エンティティー間の管理関係。

コミュニティー名 (community name). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、コミュニティーを識別するオクテット列。

圧縮 (compression). (1) レコードまたはブロックの長さを短縮するために、ギャップ、空のフィールド、冗長要素、および不必要なデータを除去する処理。 (2) メッセージまたは記録を表すのに使用するビット数を減らすために符号化すること。

構成 (configuration). (1) 情報処理システムのハードウェアとソフトウェアを編成し、相互に接続する方法。 (T) (2) システム、サブシステム、またはネットワークを構成する装置とプログラム。

構成データベース (CDB) (configuration database (CDB)). 1 つまたは複数の装置の構成パラメーターを保管するデータベース。構成プログラムを使用して作成し、更新する。

構成ファイル (configuration file). システム装置またはネットワークの特性を指定するファイル。

構成パラメーター (configuration parameter). 構成定義内の変数で、その値により、あるプロダクトと同じネットワーク内の別のプロダクトの特性を表したり、プロダクト自体の特性を定義する。

構成報告書サーバー (CRS) (configuration report server (CRS)). IBM トークンリング・ネットワーク・ブリッジ・プログラムにおいて、 LAN ネットワーク・マネージャー (LNM) からのコマンドを受け入れて、ステーション情報を入手する、ステーション・パラメーターを設定する、およびステーションをリングから除去するサーバー。また、このサーバーは、リング上のステーションによって生成された構成報告書の収集および転送も行う。構成報告書には、新しいアクティブ・モニター報告書および最近隣アクティブ・アップストリーム (NAUN) 報告書が含まれる。

輻輳 (ふくそう) (congestion). *ネットワーク輻輳 (ふくそう) (network congestion)* を参照。

接続、コネクション (connection). データ通信において、情報を伝達するために装置間に設定される関係。 (I) (A)

コントロール・ポイント (CP) (control point (CP)). (1) ノードの資源を管理する、APPN ノードまたは LEN ノードのコンポーネント。 APPN ノードでは、CP は他の APPN ノードとの CP-CP セッションを行うことができる。 APPN ネットワーク・ノードでは、CP は APPN ネットワークの隣接エンド・ノードへのサービスも提供する。 (2) ノードの資源を管理し、オプションでネットワークの他のノードにサービスを提供する、該当ノードのコンポーネント。その例としては、タイプ 5 サブエリア・ノードのシステム・サービス・コントロール・ポイント (SSCP)、APPN ネットワーク・ノードのネットワーク・ノード・コントロール・ポイント (NNCP)、および APPN または LEN エンド・ノードのエンド・ノード・コントロール・ポイント (ENCP) がある。 SSCP および NNCP は、他のノードへのサービスを提供することができる。

コントロール・ポイント管理サービス (CPMS) (control point management services (CPMS)). 管理サービス機能から構成され、問題管理、効率および会計管理、変更管理、および構成管理を実行するのに役立つ機能を提供する、コントロール・ポイントの構成要素。 CPMS によって提供される機能には、システム資源をテストするために要求を物理装置管理サービス (PUMS) に送信する機能、システム資源に関する統計情報 (たとえば、誤りデータやパフォーマンス・データ) を PUMS から収集する機能、およびテスト結果と収集されたシステム資源に関する統計情報を分析および表示する機能が含ま

れる。問題判別およびパフォーマンス監視を分析および表示する機能は、複数の CPMS 間に分散することができる。

コントロール・ポイント管理サービス単位 (CP−MSU) (control point management services unit (CP-MSU)). 管理サービス機能セット間を流れる、管理サービス・データが入っているメッセージ単位。このメッセージ単位は、汎用データ・ストリーム (GDS) 形式である。*管理サービス単位 (MSU) (management services unit (MSU))* およびネットワーク管理ベクトル移送 *(NMVT) (network management vector transport (NMVT))* も参照。

CU 論理アドレス (CU Logical Address). 2216 に対してホストによって定義された制御装置アドレス。この値は、ホスト入出力構成プログラム (IOCP) の CNTLUNIT マクロ命令の CUADD ステートメントによって定義される。制御装置アドレスは、同じホスト上で定義された各論理区画ごとに固有でなければならない。

D

D ビット (D-bit). 送達確認ビット (Delivery-confirmation bit)。 X.25 通信において、受信側からのエンド・エンド確認 (送達確認) が必要な場合に 1 にセットされる、データ・パケットまたはコール・リクエスト・パケット内のビット。

デーモン (daemon). 標準サービスを行うために無人で実行されるプログラム。デーモンには、そのタスクを実行するために自動的に起動されるものと、定期的に動作するものがある。

データ・キャリア検出 (DCD) (data carrier detect (DCD)). *受信回線信号検出器 (RLSD) (received line signal detector (RLSD))* の同義語。

データ回線 (data circuit). (1) 両方向データ通信の手段を提供する、関連付けられた一対の送信チャネルと受信チャネル。 (I) (2) SNA においては、*リンク接続 (link connection)* の同義語。 (3) *物理回線 (physical circuit)* およびバーチャル・サーキット *(virtual circuit)* も参照。

注:

1. データ交換装置相互間では、データ回線は、データ交換装置で使用するインターフェースのタイプによって、データ回線終端装置 (DCE) を含むことがある。
2. データ端末とデータ交換装置またはデータ集線装置との間では、データ回線は、データ装置側のデータ回線終端装置を含み、またデータ交換装置またはデータ集線装置側の DCE と類似の装置を含むことがある。

データ回線終端装置 (DCE) (data circuit-terminating equipment (DCE)). データ端末において、データ端末装置 (DTE) と回線の間で信号変換および符号化を行う装置。 (I)

注:

1. DCE は、独立した機器であるか、DTE または中間装置に組み込まれている。
2. DCE は、伝送路のネットワーク側で一般的に必要とされる機能を果す。

データ・リンク接続識別子 (DLCI) (data link connection identifier (DLCI)). フレーム・リレー・サブポート、またはフレーム・リレー・ネットワークの PVC セグメントの数字識別子。 1 つのフレーム・リレー・ポート内の各サブポートは、固有の DLCI を持っている。下表 (米国規格協会 (ANSI) 標準 T1.618 および国際電信電話諮問委員会 (ITU-T/CCITT) 標準 Q.922 から抜粋) は、特定の DLCI 値に関連する機能を示している。

DLCI 値	機能
0	チャネル内信号
1-15	未使用
16-991	フレーム・リレー接続手順を用いて割り当て
992-1007	フレーム・リレー・ベアラー・サービスのレイヤー 2 管理
1008-1022	未使用
1023	チャネル内のレイヤー管理

データ・リンク制御 (DLC) (data link control (DLC)). データ・リンク (SDLC リンクまたはトークンリングなど) 上のノードが、情報を正確に交換するために使用する規則。

データ・リンク制御 (DLC) レイヤー (data link control (DLC) layer). SNA において、2 つのノード間のリンクを介するデータ転送をスケジュールし、そのリンクの誤り制御を行うリンク・ステーションから構成されるレイヤー。データ・リンク制御の例としては、ビット順次リンク接続の SDLC や、システム/370 チャネルのデータ・リンク制御がある。

注: 通常、DLC レイヤーは物理トランスポート機構から独立しており、上位レイヤーに送るデータの保全性が確保される。

データ・リンク・レイヤー (data link layer). 開放型システム間相互接続参照モデルにおいて、ネットワーク・レイヤー内のエンティティーが通信リンクを通して

相互にデータを転送するサービスを提供するレイヤー。データ・リンク・レイヤーは、物理レイヤーで発生した誤りを検出し、訂正する。 (T)

データ・リンク・レベル (data link level). (1) データ・ステーションの階層構造において、ハイレベル論理とデータ・リンクの制御を維持するデータ・リンクとの間の、制御または処理論理の概念的レベル。データ・リンク・レベルは、送信ビットの挿入および受信ビットの削除、アドレス・フィールドおよび制御フィールドの解釈、コマンドとレスポンスの生成、送信、および解釈、フレーム・チェック・シーケンスの計算と解釈といった機能を実行する。*パケット・レベル (packet level)* および*物理レベル (physical level)* も参照。 (2) X.25 通信において、*フレーム・レベル (frame level)* の同義語。

データ・リンク交換 (DLSw) (data link switching (DLSw)). IEEE 802.2 論理リンク制御 (LLC) タイプ 2 を使用する、ネットワーク・プロトコルの伝達方法。SNA および NetBIOS は、LLC タイプ 2 を使用する例である。*カプセル化 (encapsulation)* およびスプーフィング *(spoofing)* も参照。

データ・パケット (data packet). X.25 通信において、DTE/DCE インターフェースのバーチャル・サーキット上でユーザー・データを伝送するために使用されるパケット。

データ・サービス装置 (DSU) (data service unit (DSU)). データ端末装置にディジタル・データ・サービス・インターフェースを直接提供する装置。 DSU は、ループ等化機能、リモートおよびローカル・テスト機能、および標準 EIA/CCITT インターフェース機構を提供する。

データ・セット・レディー (DSR) (data set ready (DSR)). *DCE レディー (DCE ready)* の同義語。

データ交換機 (DSE) (data switching exchange (DSE)). 1 つの場所に設置され、回線交換、メッセージ交換、およびパケット交換などの交換機能を提供する装置。 (I)

データ端末装置 (DTE) (data terminal equipment (DTE)). データ・ステーションにおいて、データ送信側、データ受信側、またはその両方として動作する部分。 (I) (A)

データ端末レディー (DTR) (data terminal ready (DTR)). EIA 232 プロトコルで使用されるモデムへの信号。

データ転送速度 (data transfer rate). データ伝送システムの通信している装置の間を単位時間に通過するビット、文字、またはブロックの数の平均値。 (I)

注:

1. 速度は、秒、分、または時間当たりのビット数、文字数、またはブロック数で表す。
2. 通信する装置、たとえば、モデム、中間装置、または送信側と受信側を示す必要がある。

データグラム (datagram). (1) パケット交換において、発信データ端末装置 (DTE) から着信 DTE までのルーティングに必要な十分な情報を伝達し、前もって DTE とネットワーク・ノード間で情報交換をする必要がない、他のパケットから独立した自己完結型パケット。 (I) (2) TCP/IP においては、インターネット環境で受け渡される情報の基本単位。データグラムには、データの他に発信元アドレスと宛先アドレスが入っている。インターネット・プロトコル (IP) データグラムは、IP ヘッダーと後続のトランスポート・レイヤー・データによって構成される。 (3) *パケット (packet)* および *セグメント (segment)* も参照。

データグラム送達プロトコル (DDP) (Datagram Delivery Protocol (DDP)). AppleTalk ネットワーク・ノードおいて、インターネット・レイヤーのコネクションレス・ソケット間送達サービスによってネットワークの接続性を提供するプロトコル。

DCE レディー (DCE ready). EIA 232 標準において、ローカル・データ回線終端装置 (DCE) が通信チャネルに接続され、データ送信が可能になっていることを、データ端末装置 (DTE) に知らせる信号。*データ・セット・レディー (DSR) (data set ready (DSR))* と同義。

DECnet. 通常は資源の共用、分散計算、またはリモート・システム構成の目的で、Digital Equipment Corporation のシステムを相互連結するのに使用される、一連のソフトウェア・モジュール、データベース、およびハードウェア・コンポーネント動作を定義するネットワーク体系。 DECnet ネットワークの実現方式は、ディジタル・ネットワーク体系 (DNA) モデルに準拠している。

デフォルト (default). 明示的に指定されていない場合に仮定される属性、状態、値、またはオプション。 (I)

従属 LU リクエスター (dependent LU requester) (DLUR). APPN エンド・ノードまたは APPN ネットワーク・ノードで、従属 LU を所有するが、従属 LU サーバーがそれらの従属 LU に SSCP サービスを提供することを要求する。

指定ルーター (designated router). 他のルーターの存在とアイデンティティーをエンド・ノードに知らせるル

ーター。指定ルーターの選択は、最高の優先順位をもつルーターに基づいて行われる。最高の優先順位をもつルーターが複数ある場合は、最高のステーション・アドレスをもつルーターが選択される。

宛先ノード (destination node). 要求またはデータの送信先のノード。

宛先ポート (destination port). 順次サービスを提供するコネクション・ポイントとして機能する 8 ポート非同期アダプター。

宛先サービス・アクセス・ポイント (DSAP) (destination service access point (DSAP)). SNA および TCP/IP において、システムがリモート装置からのデータを該当する通信サポートにルーティングするのに使用される論理アドレス。*発信元サービス・アクセス・ポイント (SSAP) (source service access point (SSAP)* と対比。

装置 (device). 特定の目的をもつ機械的、電気的、または電子的な仕組み。

装置アドレス (device address). 2216 装置を選択するためにチャネル・パスで伝送される装置アドレス。S/370 入出力アーキテクチャーでは、サブチャネル番号とも呼ばれる。この値は、ホストIOCP 内の実装置に対する CNTLUNIT マクロ命令の UNITADD ステートメントによって定義される。

ディジタル (digital). (1) 数字からなるデータを表わす用語。 (T) (2) 数字の形をしたデータを表わす用語。 (A) (3) *アナログ (analog)* と対比。

ディジタル・ネットワーク体系 (DNA) (Digital Network Architecture (DNA)). すべての DECnet ハードウェアおよびソフトウェア実現モデル。

直接メモリー・アクセス (DMA) (direct memory access (DMA)). マイクロチャネル・バス上の装置が、システム処理装置を介さずに、システムまたはバス・メモリーに直接アクセスできるシステム機能。

ディレクトリー (directory). 識別子およびそれに対応するデータ項目への参照からなるテーブル。 (I) (A)

ディレクトリー・サービス (DS) (directory service (DS)). アプリケーション・プロセスによって使用される記号名を、OSI 環境で使用される完全なネットワーク・アドレスに変換するアプリケーション・サービス要素。 (T)

ディレクトリー・サービス (DS) (directory services (DS)). ネットワーク・リソースの場所に関する情報を維持する、APPN ノードのコントロール・ポイント・コンポーネント。

使用不可 (disable). 機能しないようにすること。

使用不可の (disabled). (1) 特定のタイプの割り込みの発生を防止する処理装置の状態を表わす用語。 (2) 伝送制御装置または音声応答装置が線路上の着信コールを受け入れることができない状態を表わす用語。

定義域、ドメイン (domain). (1) データ処理資源が共通制御下に置かれているコンピューター・ネットワーク部分。 (T) (2) 開放型システム間相互接続 (OSI) において、共通のポリシーが適用される、分散システムの部分または管理オブジェクトの集合。 (3) *管理ドメイン (Administrative Domain)* および*ドメイン名 (domain name)* を参照。

ドメイン名 (domain name). インターネット・プロトコルにおける、ホスト・システムの名前。ドメイン名は、区切り文字によって区切られた一連のサブネームから構成される。たとえば、ホスト・システムの完全修飾ドメイン名 (FQDN) が `ralvm7.vnet.ibm.com` である場合、以下がそれぞれドメイン名である。

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

ドメイン名サーバー (domain name server). インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップすることにより名前からアドレスへの変換を行うサーバー・プログラム。ネーム・サーバー *(name server)* と同義。

ドメイン名システム (DNS) (Domain Name System (DNS)). インターネット・プロトコルにおいて、ドメイン名を IP アドレスにマップするために使用される分散データベース・システム。

ドット 10 進表記 (dotted decimal notation). 基底を 10 とし、ピリオド (ドット) で相互を分離して書かれた、4 つの 8 ビット数字からなる 32 ビット整数の構文表記。 IP アドレスを表すのに使用される。

ダンプ (dump). (1) ダンプしたデータ。 (T) (2) 誤り情報を収集するために、バーチャル記憶装置のコンテンツの全部または一部をコピーすること。

動的再構成 (DR) (dynamic reconfiguration (DR)). 完全な構成テーブルを再生成したり、影響を受けるメジャー・ノードを停止せずに、ネットワーク構成 (周辺 PU および LU) を変更するプロセス。

動的ルーティング (Dynamic Routing). 初期化時に静的に構成されたルートではなく、動的に確認されたルートを使用するルーティング。

E

エコー (echo). データ通信において、通信チャネル上の反射信号。たとえば、通信端末装置では各信号は 2 度表示される。ローカル端末に入ったときに一度表示され、通信リンクを経由して戻ってきたときに再度表示される。これにより、信号が正確であるかどうかを検査することができる。

EIA 232. データ通信において、順次 2 進データ交換を使用して、データ端末装置 (DTE) とデータ回線終端装置 (DTE) 間のインターフェースを定義する米国電子工業会 (EIA) の仕様。

ELAN. エミュレートされたローカル・エリア・ネットワーク (Emulated Local Area Network)。 ATM 技術で実施された LAN セグメント。

米国電子工業会 (EIA) (Electronic Industries Association (EIA)). 業界の技術成長を促進し、各メンバーの意見を代表し、業界標準を開発するために組織された電子機器製造業者の団体。

EIA 単位 (EIA unit). 米国電子工業会で確立された測定単位で、44.45 mm (1.7 インチ) に等しい。

カプセル化 (encapsulation). (1) 通信において、階層化されたプロトコルによって使用される技法で、これを用いて各レイヤーはサポートするレイヤーからのプロトコル・データ単位 (PDU) に制御情報を追加する。この場合、このレイヤーは、サポートするレイヤーからのデータをカプセル化する。インターネット・プロトコルでは、たとえば、パケットには、物理レイヤーからの制御情報が入り、その後にネットワーク・レイヤーからの制御情報が続き、その後にアプリケーション・プロトコル・データが入っている。 (2) *データ・リンク交換 (data link switching)* も参照。

コード化 (encode). 元の形に再び変換できるような方法で、規則を使用してデータを変換すること。 (T)

エンド・ノード (EN) (end node (EN)). (1) *拡張ピアツーピア・ネットワーキング (APPN) エンド・ノード (Advanced Peer-to-Peer Networking (APPN) end node)* および*ローエントリー・ネットワーキング (LEN) エンド・ノード (low-entry networking (LEN) end node)* を参照。 (2) 通信において、頻繁に 1 つのデータ・リンクに接続されるノードで、中間ルーティング機能を実行できないもの。

入り口点 (EP) (entry point (EP)). SNA において、分散ネットワーク管理サポートを提供する、タイプ 2.0、タイプ 2.1、タイプ 4、またはタイプ 5 ノード。それ自体に関するネットワーク管理データとそれが制御する資源を、集中処理のために中心拠点に送り、中心拠点が開始したコマンドを受け取って実行することによって、その資源を管理および制御する。

等価容量 (equivalent capacity). NBBS 体系において、パケット紛失率を限界値以下にするために、コネクションに必要な帯域幅の最少量。

ESI. エンド・システム識別子 (End System Identifier)。ATM アドレスの 6 バイトのコンポーネント。

イーサネット(Ethernet). 複数の端末が事前の調整なしに伝送媒体に自由にアクセスできる、10 Mbps のベースバンド・ローカル・エリア・ネットワーク。搬送波検知/延期を使用して競合を回避し、衝突検出/遅延再送を使用して競合を解決する。イーサネットは、搬送波検知多重アクセス/衝突検出 (CSMA/CD) を使用する。

例外 (exception). データ・セットまたはファイルの処理中に見付かった入出力誤りのような異常な状態。

例外応答 (ER) (exception response (ER)). SNA において、受信した要求が受付不能または処理不能の場合にのみ応答を戻すように受信側に指示する (つまり、否定応答は戻すことができるが肯定応答は戻せない)、要求ヘッダーの「要求された応答形式」フィールドで指定されたプロトコル。*固定応答 (definite response)* および*応答なし (no response)* と対比。

交換 ID (XID) (exchange identification (XID)). 隣接ノード間でノードおよびリンクの特性を伝達するために使用される、基本リンク単位の 1 つのタイプ。 XID は、リンク起動の前と起動中はリンクおよびノード特性の設定と交渉を行うためにリンク・ステーション間で交換され、またリンク起動後はそれらの特性の変更を通知する。

明示ルート (ER) (explicit route (ER)). SNA において、2 つのサブエリア・ノードを接続する 1 つまたは複数の伝送グループ。明示ルートは、発側サブエリア・アドレス、宛先サブエリア・アドレス、明示ルート番号、および逆明示ルート番号によって識別される。*バーチャル・ルート (VR) (virtual route (VR))* と対比。

探索フレーム (explorer frame). *探索パケット (explorer packet)* を参照。

探索パケット (explorer packet). LAN において、発信元ホストによって生成され、LAN のソース・ルーテ

ィング全体を探索して、ホストが利用可能なパスに関する情報を収集するパケット。

外部ゲートウェイ (exterior gateway). インターネット通信において、ある自律システム上の、別の自律システムと通信するゲートウェイ。*内部ゲートウェイ (interior gateway)* と対比。

外部ゲートウェイ・プロトコル (EGP) (Exterior Gateway Protocol (EGP)). インターネット・プロトコルにおいて、ドメインと自律システム間で使用され、ネットワーク到達可能性情報を公示および交換することができるプロトコル。ある自律システム内の IP ネットワーク・アドレスが、EGP に参加しているルーターによって、別の自律システムに公示される。 EGP の例としては、ボーダー・ゲートウェイ・プロトコル (BGP) がある。内部ゲートウェイ・プロトコル (IGP) (Interior Gateway Protocol (IGP)) と対比。

F

ファックス (fax). ファクシミリ機から受け取ったハードコピー。***テレコピー (telecopy)*** と同義。

ファイル転送プロトコル (FTP) (File Transfer Protocol (FTP)). インターネット・プロトコルにおいて、TCP および Telnet サービスを使用して、計算機間またはホスト間で大量データ・ファイルを転送する、アプリケーション・レイヤー・プロトコル。

フラッシュ・メモリー (flash memory). プログラム式で、消去可能で、連続的な電力を必要としない、データ記憶装置。他のプログラム式、消去可能データ記憶装置と比べたフラッシュ・メモリーの主な長所は、回路ボードから取り外さずに再プログラムできることである。

フロー制御 (flow control). (1) SNA において、データ・トラフィックがネットワークのコンポーネント間を通過する速度を管理するプロセス。フロー制御の目的は、メッセージの流れを最適化してネットワーク輻輳 (ふくそう) を最小にすることである。つまり、受信側または中間ルーティング・ノードのバッファーがオーバーフローせず、また受信側が追加メッセージ単位の到着を待つこともないようにする。 (2) *ペーシング (pacing)* も参照。

フラグメント (fragment). *分割 (fragmentation)* を参照。

断片化 (fragmentation). (1) 伝送する物理媒体の容量に合わせるために、データグラムをより小さい部分つまり断片に分割する処理。 (2) *分割 (segmenting)* も参照。

フレーム (frame). (1) ある特別な情報で構成されるデータ構造。特別な情報とは、いくつかのスロットで成り立ち、各スロット内の属性値を読むことにより適切な接続手順が決められる。 (T) (2) IBM トークンリング・ネットワークなどのローカル・エリア・ネットワークにおける伝送単位。区切り文字、制御文字、情報、および検査文字が含まれる。 (3) SDLC において、SDLC 手順を使用して伝送される、コマンド、レスポンス、およびすべての情報を運ぶ手段。

フレーム・レベル (frame level). *データ・リンク・レベル (data link level)* と同義。*リンク・レベル (link level)* を参照。

フレーム・リレー (frame relay). (1) ユーザーの装置と高速パケット・ネットワークの境界を記述したインターフェース標準。フレーム・リレー・システムでは、無効なフレームは廃棄される。回復はホップごとではなく、エンド・エンドで行われる。 (2) サービス総合ディジタル網 (ISDN) D チャネル標準から導出された技法。接続は高信頼性で、ネットワークの誤り検出と制御のオーバーヘッドはないものと想定している。

フロントエンド・プロセッサー (front-end processor). メインフレームの通信制御タスクを軽減する、IBM 3745 または 3174 のようなプロセッサー。

G

ゲートウェイ (gateway). (1) ネットワーク体系が異なる 2 つのコンピューター・ネットワークを相互に接続する機能単位。ゲートウェイは、異なる体系をもつネットワークまたはシステムを接続する。ブリッジは、同一または類似の体系をもつネットワークまたはシステムを接続する。 (T) (2) IBM トークンリング・ネットワークにおいて、ローカル・エリア・ネットワークを、異なる論理リンク・プロトコルを使用する別のローカル・エリア・ネットワークまたはホストに接続する、装置と関連ソフトウェア。 (3) TCP/IP においては、*ルーター (router)* の同義語。

汎用データ・ストリーム (GDS) (general data stream (GDS)). LU 6.2 セッション内の会話に使用されるデータ・ストリーム。

汎用データ・ストリーム (GDS) 変数 (general data stream (GDS) variable). 識別子と長さフィールドで始まり、アプリケーション・データ、ユーザー制御データ、または SNA 定義制御データのいずれかを持つ RU 副構造の 1 タイプ。

H

ヘッダー (header). (1) ユーザー・データの前に置かれるシステムが定めた制御情報。 (2) 1 つまたは複数の宛先フィールド、発信元ステーションの名前、入力シーケンス番号、メッセージのタイプを示す文字列、メッセージの優先順位レベルなどの制御情報が入っているメッセージの部分。

ヒープ・メモリー (heap memory). データ構造を動的に割り振るために使用される RAM の量。

ハロー (Hello). 協働する承認ルーターが最小遅延ルートを見付けるために使用するプロトコル。

ハロー・メッセージ (hello message). (1) ルーター相互間またはルーターとホスト間の到達可能性を設定し、テストするために定期的に送られるメッセージ。 (2) インターネット・プロトコルにおいて、ハロー・プロトコルによって内部ゲートウェイ・プロトコル (IGP) として定義されるメッセージ。

ヒューリスティック (heuristic). 最終結果に向けての進展状況を評価することによって解答を見付けるという、問題解決の探索的方法を表わす用語。

ハイレベル・データ・リンク制御 (HDLC) (high-level data link control (HDLC)). データ通信において、HDLC 国際規格 ISO 3309 フレーム構造および ISO 4335 手順要素に準拠して、指定された一連のビットを使用してデータ・リンクを制御すること。

高性能ルーティング (HPR) (high-performance routing (HPR)). 特に高速リンクの使用時に、データ・ルーティングの効率と信頼性を高める、拡張ピアツーピア・ネットワーキング機能 (APPN) 体系の追加機能。

ホップ (hop). (1) APPN において、中間ノードを含まないルート部分。隣接ノード間を接続する 1 つの伝送グループだけで構成される。 (2) ルーティング・レイヤーにおいては、ネットワークの 2 つのノード間の論理距離。

ホップ・カウント (hop count). (1) 2 点間の距離の尺度。 (2) インターネット通信において、宛先までの線路でデータグラムが通過するルーターの数。 (3) SNA において、宛先までのパスで通過するリンク数の尺度。

ホスト (host). インターネット・プロトコルにおいて、エンド・システムのこと。エンド・システムはどのワークステーションでも構わず、必ずしもメインフレームである必要はない。

ホット・プラグ可能、常時交換可能 (hot pluggable). 該当するコンポーネントに接続されていない、あるいは依存していない他のリソースの動作を妨害せずに、取り付けや取り外しを行うことができるハードウェア・コンポーネントを表す用語。

ハブ (インテリジェント) (hub (intelligent)). 異なるケーブルおよびプロトコルをもつ LAN に対してブリッジングおよびルーティング機能を提供する、IBM 8260 のような集線装置。

ヒステリシス (hysteresis). アラート条件がクリアされる前に、設定されたアラート限界値を超過して変化する必要がある温度の量。

I

I フレーム (I-frame). 情報フレーム (Information frame)。

IETF. インターネット技術特別調査委員会 (Internet Engineering Task Force)。インターネット仕様を作成する機関。

ILMI. インターリム・ローカル管理インターフェース (Interim Local Management Interface)。ユーザー・ネットワーク・インターフェース (UNI) を管理するための SNMP ベースの手順。

情報 (I) フレーム (information (I) frame). 番号制情報転送に使用される I フォーマットのフレーム。

入出力チャネル (input/output channel). データ処理システムにおいて、内部機器と周辺機器の間のデータ転送を扱う装置。 (I) (A)

統合ディジタル網交換機 (IDNX) (Integrated Digital Network Exchange (IDNX)). 音声、データ、および画像アプリケーションを統合する処理装置。伝送資源の管理や、マルチプレクサーおよびネットワーク管理支援システムへの接続も行う。異なるベンダーからの装置を統合することができる。

サービス総合ディジタル網 (ISDN) (integrated services digital network (ISDN)). 音声やデータも含めた多数のサービスをサポートするディジタル・エンド・エンド通信ネットワーク。

注: ISDN は公衆網および私設網体系で使用される。

インターフェース (interface). (1) 機能特性、信号特性、またはその他の該当する特性によって定義された、2 つの機能単位間の共有された境界。この概念には、異なる機能をもつ 2 つの装置を接続するための仕様も含

まれる。 (T)　(2) システム、プログラム、または装置をつなぐハードウェア、ソフトウェア、またはその両方。

内部ゲートウェイ (interior gateway). インターネット通信において、専用の自律システムとのみ通信するゲートウェイ。*外部ゲートウェイ (exterior gateway)* と対比。

内部ゲートウェイ・プロトコル (IGP) (Interior Gateway Protocol (IGP)). インターネット・プロトコルにおいて、自律システム内部でネットワーク到達可能性およびルーティングに関する情報を伝送するのに使用されるプロトコル。 IGP の例としては、ルーティング情報プロトコル (RIP) および最短パス最優先オープン (OSPF) がある。

インターリービング (interleaving). (1) いくつかのコンピューター設備を同時に使用して、複数の処理や機能を交互に実行すること。 (2) データ伝送において、あるデータ・ストリームからのパケットと別のデータ・ストリームからのパケットを交互に処理すること。

中間ノード (intermediate node). 複数の分岐の終端にあるノード。 (T)

中間セッション・ルーティング (ISR) (intermediate session routing (ISR)). そのノードを通過するが、エンドポイントは別の場所にあるすべてのセッションに対して、セッション・レベルのフロー制御と障害報告を提供する、APPN ネットワーク・ノード内のルーティング機能の 1 タイプ。

国際標準化機構 (ISO) (International Organization for Standardization (ISO)). 製品やサービスの国際的な交流を容易にするため、また知的、科学的、技術的、経済的活動の分野における相互協力を進めるための標準化を推進するために設立された国際的な組織。

国際電気通信連合 (ITU) (International Telecommunication Union (ITU)). 世界の周波数割り振りおよび無線規制を含めて、標準化された通信手順および実施要領を提供するために設立された米国の特殊通信機関。

インターネット (internet). 一組のルーターによって相互接続され、1 つの大規模ネットワークとして機能することができるネットワークの集合体。*インターネット (Internet)* も参照。

インターネット (Internet). 世界中の大規模な国営バックボーン・ネットワークと、多数の地域や構内のネットワークから構成される、インターネット体系委員会 (IAB) によって管理されるインターネット。インターネットでは、1 組のインターネット・プロトコルを使用する。

インターネット・アドレス (Internet address). *IP アドレス (IP address)* を参照。

インターネット体系委員会 (IAB) (Internet Architecture Board (IAB)). TCP/IP として知られるインターネット・プロトコルの開発を監督する技術団体。

インターネット制御メッセージ・プロトコル (ICMP) (Internet Control Message Protocol (ICMP)). インターネット・プロトコル (IP) レイヤーの誤りを処理し、メッセージを制御するために使用されるプロトコル。問題の報告と誤っているデータグラム宛先が、データグラムの発信元に戻される。 ICMP は、インターネット・プロトコルの一部である。

インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP)). 例外通知、メトリック通知、および PING サポートを提供するバーチャル・ネットワーキング・システム (VIrtual NEtworking System (VINES))。*ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP))* も参照。

インターネット技術特別調査委員会 (IETF) (Internet Engineering Task Force (IETF)). インターネットの短期的な技術問題の解決を担当する、インターネット体系委員会 (IAB) の特別調査委員会。

インターネットワーク・パケット交換機能 (IPX) (Internetwork Packet Exchange (IPX)). (1) Novell のサーバー、または IPX を実装したワークステーションまたはルーターと、他のワークステーションを接続するために使用される、ネットワーク・プロトコル。 IPX は、インターネット・プロトコル (IP) に類似しているが、異なるパケット・フォーマットおよび用語を採用している。 (2) *Xerox ネットワーク・システム (XNS) (Xerox Network Systems (XNS))*も参照。

インターネット・プロトコル (IP) (Internet Protocol (IP)). 1 つのネットワークまたは相互接続ネットワークを通してデータをルーティングするコネクションレス・プロトコル。 IP は、上位のプロトコル・レイヤーと物理ネットワークの間の中間層として働く。ただし、このプロトコルは、誤り回復やフロー制御は行わず、また物理ネットワークの信頼性も保証しない。

インターオペラビリティー (interoperability). ユーザーが装置固有の特性をほとんど (または、まったく) 知らなくても、種々の機能単位間で通信したり、プログラムを実行したり、あるいはデータを転送できること。 (T)

エリア内ルーティング (intra-area routing). インターネット通信において、エリア内部でデータをルーティングすること。

逆アドレス解決プロトコル (InARP) (Inverse Address Resolution Protocol (InARP)). インターネット・プロトコルにおいて、事前設定されたハードウェア・アドレスを使用してプロトコル・アドレスを見付けるために使用されるプロトコル。フレーム・リレー文脈において、データ・リンク・コネクション識別子 (DLCI) は、事前設定ハードウェア・アドレスと同義。

IPPN. 他のプロトコルが IP を通してデータをトランスポートする場合に使用するインターフェース。

IP アドレス (IP address). インターネット・プロトコル、標準 5、Request For Comments (RFC) 791 によって定義された 32 ビット・アドレス。通常は、ドット付き 10 進表記で示される。

IP データグラム (IP datagram). インターネット・プロトコルにおいて、インターネットを通して伝送される情報の基本単位。発信元とあて信先のアドレス、ユーザー・データ、および制御情報 (データグラムの長さ、ヘッダー・チェックサム、データグラムの分割が可能かどうか、あるいは分割されているかどうかを示すフラグなど) が入っている。

IP ルーター (IP router). ネットワーク上のトラフィックが流れるパスを決定する、IP インターネット内の装置。ルーティング・プロトコルを使用して、ネットワークに関する情報を収集し、データグラムを最終着側に転送する最善ルートを決める。データグラムは、IP 宛先アドレスに基づいてルーティングされる。

IPXWAN. 広域ネットワーク (WAN) を介してインターネットワーク・パケット交換機能 (IPX) ルーティング情報を交換する前に、ルーター相互間で情報を交換するために使用される Novell プロトコル。

J

ジッター (jitter). (1) ディジタル信号の有意瞬間における、その理想位置からの短時間の非累積的な変動。 (2) 伝送されたディジタル信号の好ましくない変動。 (3) ネットワーク遅延の変動。

L

L2TP アクセス集線装置 (LAC) (L2TP Access Concentrator (LAC)). PPP プロトコルと L2TP プロトコルの両方を扱うことができる 1 つまたは複数の公衆サービス電話網 (PSTN) 回線または ISDN 回線に接続される集線装置。装置には、L2TP が稼働するためのメディアをサポートする必要がある。L2TP はトラフィックを 1 つまたは複数の L2TP ネットワーク・サーバー (LNS) に渡す。L2TP は、PPP ネットワークによって搬送されたプロトコルをトンネルすることができる。

L2TP ネットワーク・サーバー (LNS) (L2TP Network Server (LNS)). LNS は PPP エンド・ステーションなど任意のプラットフォーム上で稼働する。 LNS は L2TP プロトコルのサーバー側を扱う。L2TP は、L2TP トンネルを通じて到着する単一の媒体にだけ依存しているので、LNS は単一の LAN または WAN インターフェースだけをもつが、LAC によってサポートされる全範囲の PPP インターフェースのうちどのインターフェースから到着する呼び出しも着信する。これらには、非同期 ISDN、同期 ISDN、V.120、およびその他のタイプの接続が含まれる。

LAN ブリッジ・サーバー (LBS) (LAN bridge server (LBS)). IBM トークンリング・ネットワーク・ブリッジ・プログラムにおいて、2 つ以上のリング間で (ブリッジを介して) 転送されたフレームに関する統計情報を保持しているサーバー。 LBS は、LAN 報告機構 (LRM) を通して、これらの統計を該当の LAN マネージャーに送信する。

LAN エミュレーション (LE) (LAN Emulation (LE)). ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

LAN エミュレーション・クライアント (LEC) (LAN Emulation Client (LEC)). エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

LAN エミュレーション構成サーバー (LECS) (LAN Emulation Configuration Server (LECS)). 構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

LAN エミュレーション・サーバー (LES) (LAN Emulation Server (LES)). LAN 宛先を ATM アドレスにする、LAN エミュレーション・サービス・コンポーネント。

LAN ネットワーク・マネージャー (LNM) (LAN Network Manager (LNM)). ユーザーが中央のワークステーションから LAN 資源を管理および監視できるようにする、IBM ライセンス・プログラム。

LAN セグメント (LAN segment). (1) 独立して動作することができるが、ブリッジによってネットワークの他の部分に接続されている LAN の部分 (たとえば、バ

スまたはリング)。 (2) ブリッジのない環状ネットワークまたはバス・ネットワーク。

レイヤー (layer). (1) ネットワーク体系において、階層式に配列された一組のグループのうちの 1 つで、ネットワーク体系に一致するすべてのシステム間にまたがっている、概念的に完全なサービス・グループ。 (T) (2) 開放型システム間相互接続参照モデルにおいて、7 つの概念的に完全な、階層式に配列されたサービス、機能、およびプロトコルのグループのうちの 1 つで、すべての開放型システム間にまたがっている。 (T) (3) SNA において、他のグループの機能からは論理的に分離されている、関連する機能の集まり。あるレイヤーの機能の実現方式を変更しても、他のレイヤーの機能には影響を与えない。

LE. LAN エミュレーション (LAN Emulation)。 ATM ネットワークの従来の LAN アプリケーションをサポートする ATM フォーラム標準。

LEC. LAN エミュレーション・クライアント (LAN Emulation Client)。エミュレートされた LAN のユーザーを表す LAN エミュレーション・コンポーネント。

LECS. LAN エミュレーション構成サーバー (LAN Emulation Configuration Server)。構成データを中央に集めて広く配布する、LAN エミュレーション・サービス・コンポーネント。

LES. LAN エミュレーション・サーバー (LAN Emulation Server)。 LAN 宛先を ATM アドレスにする、LAN エミュレーション・サービス・コンポーネント。

回線交換 (line switching). *サーキット交換 (circuit switching)* の同義語。

リンク (link). リンク接続機構 (伝送媒体) と、2 つのリンク局 (リンク接続機構の両側に 1 つずつ) の組み合わせ。多地点構成またはトークンリング構成では、1 つのリンク接続を複数のリンクで共用できる。

平衡型リンク・アクセス・プロトコル (LAPB) (link access protocol balanced (LAPB)). リンク・レベルで X.25 ネットワークにアクセスするのに使用されるプロトコル。 LAPB は、ポイント・ポイント通信に使用される全二重、非同期、対称プロトコルである。

リンク・アドレス (Link Address). ESCON チャネル・アダプター付きの 2216 の場合は、次のように決められたポート番号である。つまり、通信パスに ESCD が 1 つある場合は、ホストに接続された ESCON ディレクター (ESCD) ポート番号。通信パスに ESCD が 2 つある場合は、動的接続で定義された ESCD のホスト側ポート番号。通信パスに ESCD がない場合、この値は X'01' に設定する必要がある。

リンク接続 (link-attached). (1) データ・リンクによって制御装置に接続されている装置を表わす用語。 (2) *チャネル接続 (channel-attached)* と対比。 (3) *リモート (remote)* と同義。

リンク接続機構 (link connection). (1) 1 つのリンク局と他の 1 つまたは複数のリンク局の間で両方向通信を提供する物理装置。たとえば、通信回線およびデータ回線終端装置 (DCE)。 (2) SNA においては、*データ回線 (data circuit)* と同義。

リンク・レベル (link level). (1) 加入者の機械をネットワーク・ノードに接続する全二重リンクを通してネットワークとの間でデータを受け渡しするのに使用されるリンク・プロトコルを定義している X.25 勧告の部分。 LAP および LAPB は、CCITT によって推奨されているリンク・アクセス・プロトコルである。 (2) データ・リンク・レベル *(data link level)* も参照。

リンク状態 (link-state). ルーティング・プロトコルにおいて、ルーターまたはネットワークの使用可能なインターフェースおよび到達可能な近隣に関する、公示された情報。プロトコルのトポロジー・データベースは、収集されたリンク状態公示から作成される。

リンク・ステーション (link station). (1) 特定のリンクを介した隣接ノードへの接続を表す、ノード内のハードウェアおよびソフトウェア・コンポーネント。たとえば、ノード A が 3 つの隣接ノードに接続する多地点回線の 1 次エンドのとき、ノード A は隣接ノードへの接続を表す 3 つのリンク・ステーションをもつことになる。 (2) *隣接リンク・ステーション (ALS) (adjacent link station (ALS))* も参照。

LIS. 論理 IP サブネット (Logical IP Subnet)。ATM 技術のスイッチド・バーチャル・ネットワーキング (SVN) 構成で 実現された IP サブネット。

ローカル (local). (1) 通信回線を使用しないで直接アクセスされる装置を表わす用語。 (2) *リモート (remote)* と対比。 (3) *チャネル接続 (channel-attached)* の同義語。

ローカル・エリア・ネットワーク (LAN) (local area network (LAN)). (1) 地理的に限定された区域内にある、ユーザーの構内に置かれているコンピューター・ネットワーク。ローカル・エリア・ネットワーク内部の通信は、外部の規制の対象にはならないが、LAN の境界を越えた通信は、何らかの形で規制を受ける場合がある。 (T) (2) 1 組の装置が相互通信を目的として接続されているネットワークで、さらに大きなネットワーク

に接続することができる。 (3) *イーサネット (Ethernet)* およびトークンリング *(token ring)* も参照。 (4) *大都市圏ネットワーク (MAN) (metropolitan area network (MAN))* および*広域ネットワーク (WAN) (wide area network (WAN))* と対比。

ローカル・ブリッジング (local bridging). 通信リンクを使用せずに 1 つのブリッジが複数の LAN セグメントを接続することができるブリッジ・プログラムの機能。*リモート・ブリッジング (remote bridging)* と対比。

ローカル管理インターフェース (LMI) (local management interface (LMI)). *ローカル管理インターフェース (LMI) プロトコル (local management interface (LMI) protocol)* を参照。

ローカル管理インターフェース (LMI) プロトコル (local management interface (LMI) protocol). NCP において、DLCI X'00' を介して回線状況の情報を交換するために隣接フレーム・リレー・ノードが使用する、1 組のフレーム・リレー・ネットワーク管理手順とメッセージ。 NCP は、米国規格協会 (ANSI) と国際電信電話諮問委員会 (ITU-T/CCITT) の両方のバージョンの LMI プロトコルをサポートする。これらの標準では、LMI プロトコルを*リンク保全検査テスト (LIVT) (link integrity verification tests (LIVT))* として参照している。

ローカル管理アドレス (locally administered address). ローカル・エリア・ネットワークにおいて、出荷時設定アドレスを指定変更するためにユーザーが割り当てることができるアダプター・アドレス。*出荷時設定アドレス (universally administered address)* と対比。

論理チャネル (logical channel). パケット交換モードの動作において、データ・リンクを介して同時にデータの送信と受信を行うために一緒に使用される、送信チャネルと受信チャネル。パケットの伝送をインターリーブすることにより、同じデータ・リンク上に複数の論理チャネルを確立することができる。

論理リンク (logical link). 1 対のリンク・ステーション (2 つの隣接ノードのそれぞれに 1 つ) とその基礎になるリンク接続。2 つのノード間に 1 つのリンク・レイヤー接続機構を提供する。 2 つのノードを接続する同一の物理媒体を共用しながら、複数の論理リンクを区別することができる。その例としては、ローカル・エリア・ネットワーク (LAN) ファシリティーで使用される 802.2 論理リンクと、2 つのノード間の同じポイント・ポイント物理リンクを使用する LAP E 論理リンクがある。論理リンクという用語には、DTE から X.25 ネットワークへのアクセス・リンクを共用する複数の X.25 論理チャネルも含まれる。

論理リンク制御 (LLC) (logical link control (LLC)). 情報を正確に交換するために、2 種類のデータ・リンク制御 (DLC) 動作を提供するデータ・リンク制御 (DLC) LAN サブレイヤー。最初のタイプはコネクションレス・サービスで、リンクを確立せずに情報を送受信することができる。コネクションレス・サービスの場合、LLC サブレイヤーは誤り回復またはフロー制御を行わない。 2 番目のタイプはコネクション指向のサービスで、情報を交換する前にリンクを確立する必要がある。コネクション指向のサービスは、順序保存情報転送、フロー制御、および誤り回復を提供する。

論理リンク制御 (LLC) プロトコル (logical link control (LLC) protocol). ローカル・エリア・ネットワークにおいて、伝送媒体の共用方法からは独立して、データ・ステーション間の伝送フレームの交換を規定するプロトコル (T)　LLC プロトコルは IEEE 802 委員会によって開発されたもので、すべての LAN 標準に共通である。

論理リンク制御 (LLC) プロトコル・データ単位 (logical link control (LLC) protocol data unit). 異なるノードのリンク・ステーション間で交換される情報の単位。 LLC プロトコル・データ単位には、宛先サービス・アクセス・ポイント (DSAP)、発信元サービス・アクセス・ポイント (SSAP)、制御フィールド、およびユーザー・データが入っている。

論理区画 (logical partition). 論理区分 (LPAR) モードで動作できる、ホスト内の区画に割り当てられた番号。 LPAR モードでは、ESCON アダプターは複数のホスト区画と論理ファイバー接続を共用することができる。

論理区分 (LPAR) モード) (Logically Partitioned (LPAR) mode). 処理を論理区画 (LP) に分割して、複数のプロセッサーがあるように見せる、一部のホスト・プロセッサーの機能。 LPAR モードでは、ESCON アダプターは複数のホスト区画と論理ファイバー接続を共用することができる。

LP. 論理区画 (logical partition)

LP 番号 (LP number). 論理区画番号 (Logical partition number)。これによって、複数の論理ホスト区画 (LP) が 1 つの ESCON ファイバーを共用することができる。この値は、ホスト入出力構成プログラム (IOCP) の RESOURCE マクロ命令によって定義される。ホストで EMIF を使用していない場合は、 LP 番号としてデフォルト値 0 を使用する。

LPAR. 論理区分 (logically partitioned)。

LPAR モード (LPAR mode). 論理区分 (LPAR) モード。

論理装置 (LU) (logical unit (LU)). ユーザーがネットワーク・リソースにアクセスし、相互に通信することができる、ネットワーク・アクセス可能単位の一種。

ループバック・テスト (loopback test). テスターからの信号をモデムや他のネットワーク要素でループさせてテスターに戻し、それを計測して通信パスの品質を調べたり、確認したりするテスト。

ローエントリー・ネットワーキング (LEN) (low-entry networking (LEN)). 論理装置間の複数の並列セッションをサポートするために、基本ピア間プロトコルを使用して相互に直接接続することができるノードの機能。

ローエントリー・ネットワーキング (LEN) エンド・ノード (low-entry networking (LEN) end node). 隣接 APPN ネットワーク・ノードからネットワーク・サービスを受ける LEN ノード。

ローエントリー・ネットワーキング (LEN) ノード (low-entry networking (LEN) node). 一連のエンド・ユーザー・サービスを行い、ピア・プロトコルを使用して他のノードと直接接続し、隣接 APPN ネットワーク・ノードから暗黙に (すなわち、CP-CP セッションを直接使用せずに) ネットワーク・サービスを受けるノード。

M

管理アクセス (management access). ネットワーク管理ステーション、または変更制御サーバーを NBBS ネットワークに接続する Nways スイッチ。

管理情報ベース (MIB) (Management Information Base (MIB)). (1) ネットワーク管理プロトコルによってアクセスできるオブジェクトの集合。 (2) ホストやゲートウェイから入手できる情報および許容される動作を指定する管理情報の定義。 (3) OSI では、開放型システム内の管理情報の概念的リポジトリー。

管理ステーション (management station). インターネット通信において、ネットワーク全体 (または、一部) を管理するシステム。管理ステーションは、シンプル・ネットワーク・マネージメント・プロトコル (SNMP) のようなネットワーク管理プロトコルを使用して、被管理ノードに常駐するネットワーク管理エージェントと通信する。

マッピング (mapping). あるフォーマットで送信側から伝送されたデータを、受信側が受け入れられるデータ形式に変換するプロセス。

マスク (mask). (1) 他の文字パターンの一部を保持または削除することを制御するために使用する文字パターン。 (I) (A) (2) 他の文字パターンの一部を保持または削除することを制御するために、文字パターンを使用すること。 (I) (A)

最大伝送単位 (MTU) (maximum transmission unit (MTU)). LAN において、1 つのフレームに入れて所定の物理媒体で送信できる最大可能データ単位。たとえば、イーサネットの MTU は 1500 バイトである。

媒体アクセス制御 (MAC) (medium access control (MAC)). LAN において、媒体に依存する機能をサポートし、物理レイヤーのサービスを使用して論理リンク制御 (LLC) サブレイヤーにサービスを提供する、データ・リンク制御レイヤーのサブレイヤー。 MAC サブレイヤーには、装置が伝送媒体にアクセスできる時期を判別する方法が含まれている。

媒体アクセス制御 (MAC) プロトコル (medium access control (MAC) protocol). ローカル・エリア・ネットワークにおいて、データ・ステーション間でデータを交換できるようにするために、ネットワークのトポロジーを考慮に入れて、伝送媒体へのアクセスを規制するプロトコル。 (T)

媒体アクセス制御 (MAC) サブレイヤー (medium access control (MAC) sublayer). ローカル・エリア・ネットワークにおいて、媒体アクセス方式に適用されるデータ・リンク・レイヤーの部分。 MAC サブレイヤーは、トポロジー依存の機能をサポートし、物理レイヤーのサービスを使用して、論理リンク制御サブレイヤーにサービスを提供する。 (T)

メトリック (metric). インターネット通信において、同じ自律システムへの複数の出入口ポイントを区別するために使用される、ルートに関連する値。最低のメトリックをもつルートが優先される。

大都市圏ネットワーク (MAN) (metropolitan area network (MAN)). 2 つ以上のネットワークを相互接続して形成された通信ネットワーク。個々のネットワークより高速で動作すること、行政の境界にまたがること、および複数のアクセス方式を使用することが可能になる。 (T) *ローカル・エリア・ネットワーク (local area network (LAN))* および*広域ネットワーク (wide area network (WAN))* と対比。

MIB. (1) MIB モジュール。 (2) 管理情報ベース (Management Information Base)。

MIB オブジェクト (MIB object). *MIB 変数 (MIB variable)* の同義語。

MIB 変数 (MIB variable). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、MIB モジュールに定義されているデータの特定インスタンス。 *MIB オブジェクト (MIB object)* と同義。

MIB ビュー (MIB view). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、特定のコミュニティーに見える、エージェントと呼ばれる管理オブジェクトの集合。

MILNET. 本来は ARPANET の一部であった軍用ネットワーク。 1984 年に ARPANET から分割された。 MILNET は、軍用施設に高信頼性のネットワーク・サービスを提供している。

モデム (変復調装置) (modem (modulator/demodulator)). (1) 信号を変調および復調する装置。モデムの機能の 1 つは、ディジタル・データをアナログ伝送ファシリティーを介して伝送できるようにすることである。 (T) (A) (2) コンピューターからのディジタル・データを、通信回線上で伝送できるアナログ信号に変換し、また受信したアナログ信号をコンピューターのためのデータに変換する装置。

モジュール (module). Nways スイッチにおいて、論理カード、コネクター、およびライトが含まれている、パッケージされたハードウェア装置。モジュールは、アダプター、回線インターフェース・カプラー、音声サーバー拡張、およびその他のコンポーネントをパッケージするのに使用される。すべてのモジュールが論理サブラックに**ホット・プラグ可能**。

モジュロ (modulo). (1) モジュラスに関する用語。たとえば、9 は 4 モジュロ 5 と同等。 (2) モジュラス *(modulus)* も参照。

モジュラス (modulus). 剰余を残さずに 2 つの関連する数値の差を除算する関係式における、正整数のような数。たとえば、9 と 4 はモジュラス 5 をもつ (9 - 4 = 5、4 - 9 = -5、かつ 5 は 5 と -5 の両方とも割りきれる)。

モニター (monitor). (1) 分析するために、データ処理システムの中の選ばれた活動を監視し、記録する機能。基準から著しく逸脱していることを示すため、または特定の機能の利用度を測るために使用する。 (T) (2) システムの操作を観察、監視、制御、検査するソフトウェアまたはハードウェア。 (A) (3) リング上のトークンの伝送を開始し、トークンの紛失、フレームの循環、またはその他の問題が生じた場合にソフト誤り回復を提供するために必要な機能。この機能は、すべてのリング・ステーションに存在する。

MSS. マルチプロトコル交換サービス (Multiprotocol Switched Services)。IBM のスイッチド・バーチャル・ネットワーキング (SVN) 構成のコンポーネント。

マルチキャスト (multicast). (1) 選択された宛先グループに同じデータを伝送すること。 (T) (2) パケットのコピーが可能なすべての宛先のサブセットだけに伝達される、特殊な形式のブロードキャスト。

マルチパス・チャネル (multipath channel) (MPC). VTAM-VTAM 間両方向通信用として複数の単一方向サブチャネルを使用するチャネル・プロトコル。

マルチドメイン・サポート (MDS) (multiple-domain support (MDS)). LU-LU および CP-CP セッションを介して管理サービス機能セット相互間で管理サービス・データを伝達する手法。*マルチドメイン・サポート・メッセージ単位 (MDS-MU) (multiple-domain support message unit (MDS-MU))* も参照。

マルチドメイン・サポート・メッセージ単位 (MDS-MU) (multiple-domain support message unit (MDS-MU)). 管理サービス・データが入っているメッセージ単位で、マルチドメイン・サポートによって使用される LU-LU および CP-CP セッションを介して管理サービス機能セット相互間に流される。このメッセージ単位およびその中に入っている実際の管理サービス・データは、一般データ・ストリーム (GDS) 形式である。*コントロール・ポイント管理サービス単位 (CP−MSU) (control point management services unit (CP-MSU))*、*管理サービス単位 (MSU) (management services unit (MSU))*、およびネットワーク管理ベクトル伝達 *(NMVT) (network management vector transport (NMVT))* も参照。

N

ネーム・バインディング・プロトコル (NBP) (Name Binding Protocol (NBP)). AppleTalk ネットワークにおいて、AppleTalk エンティティー (資源) 名 (文字列) からトランスポート・レイヤーの AppleTalk IP アドレス (16 ビットの数字) へのネーム変換機能を提供するプロトコル。

ネーム・レゾリューション (name resolution). インターネット通信において、機械名を対応するインターネット・プロトコル (IP) アドレスにマップする処理。*ドメイン名システム (DNS) (Domain Name System (DNS))* も参照。

ネーム・サーバー (name server). インターネット・プロトコルにおいて、*ドメイン名サーバー (domain name server)* の同義語。

最近隣活動アップストリーム (NAUN) (nearest active upstream neighbor (NAUN)). IBM トークンリング・ネットワークにおいて、リング上の所定のステーションにデータを直接送信するステーション。

近隣 (neighbor). ネットワーク管理者によってルーティング情報を受信するように指定された、共通サブネットワーク上のルーター。

NetBIOS. ネットワーク基本入出力システム (Network Basic Input/Output System)。メッセージ、プリンター・サーバー、およびファイル・サーバーの機能を提供するために LAN 上で使用される、ネットワーク、IBM パーソナル・コンピューター (PC)、および互換 PC への標準インターフェース。 NetBIOS を使用するアプリケーション・プログラムは、LAN データ・リンク制御 (DLC) プロトコルの詳細を処理する必要がない。

網、ネットワーク (network). (1) 情報交換のために接続されたデータ処理装置とソフトウェアの構成。 (2) ノードとそれを相互接続するリンクの集合。

ネットワーク・アクセス・サーバー (Network Access Server) (NAS). ユーザーに一時的なオンデマンド・ネットワーク・アクセスを提供する装置。このアクセスは、PSTN または ISDN 伝送路を使用するポイント・ポイントです。

ネットワーク・アクセス可能単位 (NAU) (network accessible unit (NAU)). 論理装置 (LU)、物理装置 (PU)、コントロール・ポイント (CP)、またはシステム・サービス・コントロール・ポイント (SSCP)。パス制御ネットワークによって伝送される情報の発側または着側となる。 *ネットワーク・アドレス可能単位 (network addressable unit)* と同義。

ネットワーク・アドレス (network address). ISO 7498-3 によると、1 組のネットワーク・サービス・アクセス・ポイントを識別する、OSI 環境内であいまいさのない名前。

ネットワーク・アドレス可能単位 (NAU) (network addressable unit (NAU)). *ネットワーク・アクセス可能単位 (network accessible unit)* の同義語。

ネットワーク体系 (network architecture). コンピューター・ネットワークの論理構造と運用原則。 (T)

注: 運用原則には、サービス、機能、およびプロトコルが含まれる。

ネットワーク輻輳 (ふくそう) (network congestion). 通信量がネットワークで処理できる量を上回ったことによって起こる望ましくない過負荷状態。

ネットワーク制御 (network control). 以下の目的のために Nways スイッチのコントロール・ポイントによって実行される NBBS 体系の機能。
- Nways スイッチ資源の割り振りと制御
- トポロジーおよびディレクトリー・サービスの提供
- ルートの選択
- 輻輳 (ふくそう) の制御

ネットワーク識別子 (network identifier). (1) TCP/IP において、ネットワークを定義する IP アドレスの部分。ネットワーク ID の長さは、ネットワーク・クラス (A、B、または C) のタイプによって異なる。 (2) 特定のサブネットワークを固有に識別する、1〜8 バイトのユーザーが選択した名前、または 8 バイトの IBM 登録名。

ネットワーク情報センター(NIC) (Network Information Center (NIC)). インターネット通信において、ユーザーに援助、資料、訓練、およびその他のサービスを提供する、全世界の局所的、地域的、および国家的なグループ。

ネットワーク・レイヤー (network layer). 開放型システム間相互接続 (OSI) 体系において、OSI 環境全体のルーティング、交換、およびリンク・レイヤー・アクセス機能を提供するレイヤー。

ネットワーク管理 (network management). 通信用のデータ処理または情報システムを計画、組織、および制御するプロセス。

ネットワーク管理ステーション (NMS) (network management station (NMS)). NetView/AIX および Nways スイッチ管理プログラムを稼働するステーション。 NBBS ネットワーク・トポロジー、会計、効率、構成の更新、および問題分析を管理する。

ネットワーク管理ステーションは、イーサネット LAN を介して管理アクセス Nways スイッチに接続される。

ネットワーク管理ステーション (network management station). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、ネットワーク要素を監視、制御する管理アプリケーション・プログラムを実行する端末。

ネットワーク管理ベクトル転送 (NMVT) (network management vector transport (NMVT)). 物理装置管理サービスとコントロール・ポイント管理サービス間のアクティブ・セッション (SSCP-PU セッション) を介して流される、管理サービス要求応答単位 (RU)。

ネットワーク・マネージャー (network manager). ネットワーク・ノードの問題を監視、管理、および診断するプログラムまたはプログラムの集まり。

ネットワーク・ノード (NN) (network node (NN)). *拡張ピアツー・ピア・ネットワーキング機能 (APPN) ネットワーク・ノード (Advanced Peer-to-Peer Networking (APPN) network node)* を参照。

ネクスト・ホップ解決プロトコル (NHRP) (Next Hop Resolution Protocol (NHRP)). RFC としての認定を受けるために提出されている、インターネット草案バージョン 10 に指定されているルーティング・プロトコル。ネクスト・ホップ解決プロトコルでは、発信元ステーションが、宛先の方向にある『NBMA ネクスト・ホップ』の非ブロードキャスト・マルチアクセス (NBMA) アドレスを判別する方式を定義する。NBMA ネクスト・ホップは、宛先自体である場合もあれば、 NBMA ネットワーク内にあって、宛先に『最も近い』ルーターである場合もある。こうして、発信元ステーションは、宛先またはルーターとの間に直接 NBMA バーチャル・サーキットを確立し、NBMA ネットワーク上のルーティング・ホップの数を減らすことができる。

ネットワーク・サポート・センター (Network Support Center). IBM が NBBS ネットワークにリモート・サポートを提供する場所。

ネットワーク・サポート・ステーション (network support station). ローカルで動作し、Nways スイッチにサービスするために使用される処理装置。 Nways スイッチの管理者またはサービス担当者が使用する。

ネットワーク・ユーザー・アドレス (NUA) (network user address (NUA)). X.25 通信において、最大 15 桁の 2 進コード数字を含む X.121 アドレス。

ネットワーキング広帯域サービス (NBBS) (Networking BroadBand Services (NBBS)). ATM 標準を補完して以下の機能を提供する、高速ネットワーキング用の IBM 体系。
- アクセス・サービス
- トランスポート・サービス
- ネットワーク制御

NHRP. ネクスト・ホップ解決プロトコル (Next Hop Resolution Protocol)。

ノード (node). (1) ネットワーク・ノードにおいて、1 台または複数の装置がチャネルまたはデータ回線を接続する点。 (I) (2) ネットワークに接続された、データを送受信する装置。

非標準アドレス (noncanonical address). LAN において、トークンリング・アダプターの媒体アクセス制御 (MAC) アドレスを伝送するためのフォーマットの 1 つ。非標準フォーマットでは、各アドレス・バイトの最上位 (左端) ビットが最初に伝送される。*標準アドレス (canonical address)* と対比。

非ゼロ復帰 (1) 記録 (NRZ-1) (Non-Return-to-Zero Changes-on-Ones Recording (NRZ-1)). 磁化状態の変化が 1 を表し、変化しないことが 0 を表す記録方式。 1 の信号のみが明示的に記録される。 (以前は***非ゼロ復帰反転 (NRZI)*** 記録と呼ばれていた。)

非シード・ルーター (nonseed router). AppleTalk ネットワークにおいて、同じネットワークに接続されているシード・ルーターからネットワーク番号範囲とゾーン・リスト情報を獲得するルーター。

Nways スイッチ (Nways Switch). IBM 2220 Nways ブロードバンド・スイッチ (IBM 2220 Nways BroadBand Switch) と同義。

Nways スイッチ構成端末 (Nways Switch configuration station). Nways Switch 構成ツール (NCT) の独立バージョンを稼働している専用 OS/2 端末。ネットワーク構成データベースを生成するのに使用され、リモート・コンソールに導入する必要がある。

O

最短パス最優先オープン (OSPF) (Open Shortest Path First (OSPF)). インターネット・プロトコルにおいて、領域ドメイン内の情報転送を行う機能。ルーティング情報プロトコル (RIP) の代替として、OSPF は最低コストのルーティングが可能であり、大きい地域や企業ネットワークのルーティングを扱う。

開放型システム間相互接続 (OSI) (Open Systems Interconnection (OSI)). (1) 情報交換のための国際標準化機構 (ISO) の標準に準拠した開放型システムの相互接続。 (T) (A) (2) データ処理システムの相互接続を可能にする標準的手順の使用。

注: OSI 体系は、コンピューター・システムの相互接続のための現在および将来の標準の開発を統合するための枠組みを設定している。ネットワーク機能は 7 つのレイヤーに分けられている。各レイヤーは、異なるアプリケーションをサポートする標準的方法で実行できる、関連したデータ処理および通信機能の集まりを表している。

開放型システム間相互接続 (OSI) 体系 (Open Systems Interconnection (OSI) architecture). 開放型システム相互接続に関連する特定の一組の ISO 規格に準拠したネットワーク体系。 (T)

開放型システム間相互接続 (OSI) 参照モデル (Open Systems Interconnection (OSI)). 開放型システム相互接続、およびその 7 つのレイヤーの目的と階層式配列の一般原則を記述したモデル。 (T)

発信元 (origin). メッセージまたはその他のデータが発信された外部論理装置 (LU) またはアプリケーション・プログラム。*宛先 (destination)* も参照。

孤立回線 (orphan circuit). その利用可能性が動的に学習される未構成の回線。

P

ペーシング (pacing). (1) オーバーランまたは輻輳 (ふくそう) を防止するために、受信側コンポーネントが送信側コンポーネントの伝送速度を制御する方法。 (2) *フロー制御 (flow control)*、*受信ペーシング (receive pacing)*、*送信ペーシング (send pacing)*、*セッション・レベル・ペーシング (session-level pacing)*、および*バーチャル・ルート (VR) ペーシング (virtual route (VR) pacing)* も参照。

パケット (packet). データ通信において、1 つのまとまりとして送信および交換される、データと制御信号を含む 2 進数の列。データ、制御信号、および誤り制御情報が、特定の形式に配列されている。 (I)

パケット・インターネット・グローパー (PING) (packet internet groper (PING)). (1) インターネット通信において、インターネット制御メッセージ・プロトコル (ICMP) エコー要求を宛先に送って応答を待つことにより、宛先に到達できるかどうかをテストする、TCP/IP ネットワーク・ノードで使用されるプログラム。 (2) 通信における、到達可能性のテスト。

パケット損失率 (packet loss ratio). パケットが指定の宛先に到達しない、または指定された時間内に到達しない確率。

パケット・モード動作 (packet mode operation). *パケット交換 (packet switching)* の同義語。

パケット交換 (packet switching). (1) アドレス指定されたパケットを用いてデータのルーティングと転送を行うことによって、パケットの伝送中だけチャネルが占有されるようにする処理。伝送が完了すると、そのチャネルは他のパケットの伝送に利用可能になる。 (I) (2) *パケット・モード動作 (packet mode operation)* と同義。*回線交換 (circuit switching)* も参照。

並列ブリッジ (parallel bridges). 同じ LAN セグメントに接続され、そのセグメントへの冗長パスを形成する 1 対のブリッジ。

並列伝送グループ (parallel transmission groups). 各グループが異なるグループ番号をもつ、隣接ノード間の複数の伝送グループ。

パス (path). (1) 通信ネットワークにおける 2 つのノード間のルート。パスは複数の分岐を含むことができる。 (T) (2) 2 つのネットワーク・アクセス可能装置間で交換される情報が通る、一連の伝送ネットワーク・コンポーネント (パス制御およびデータ・リンク制御)。*明示ルート (ER) (explicit route (ER))*、*ルート拡張 (route extension)*、および*バーチャル・ルート (VR) (virtual route (VR))* も参照。

パス制御 (PC) (path control (PC)). 通信ネットワークのネットワーク・アクセス可能装置間でメッセージをルーティングし、相互間のパスを提供する機能。伝送制御からの基本情報単位 (BIU) を (場合によっては分割して) パス情報単位 (PIU) に変換し、1 つまたは複数の PIU を含む基本伝送単位をデータ・リンク制御と交換する。パス制御はノード・タイプによって異なる。あるノード (たとえば、APPN ノード) は、ローカルに生成されたセッション識別子をルーティングに使用し、あるノード (サブエリア・ノード) は、ネットワーク・アドレスをルーティングに使用する。

パス・コスト (path cost). リンク状態ルーティング・プロトコルにおいて、2 つのノードまたはネットワーク・ノード間のパス上のリンク・コストの合計。

パス情報単位 (PIU) (path information unit (PIU)). 伝送ヘッダー (TH) のみから成る、または TH の後に基本情報単位 (BIU) または BIU セグメントが続いているメッセージ単位。

パターン突き合わせ文字 (pattern-matching character). 1 文字または複数の文字を表すために使用できる、アスタリスク (*) や疑問符 (?) のような特殊文字。任意の 1 文字または一組の文字を、パターン突き合わせ文字と置き換えることができる。*グローバル文字 (global character)* および*ワイルドカード文字 (wildcard character)* と同義。

パーマネント・バーチャル・サーキット (PVC) (permanent virtual circuit (PVC)). X.25 およびフレーム・リレー通信で、各データ端末装置 (DTE) に論理チャネルが固定的に割り当てられているバーチャル・サーキット。コール設定プロトコルは不要である。*スイッチド・バーチャル・サーキット (SVC) (switched virtual circuit (SVC))* と対比。

物理回線 (physical circuit). 多重化なしで確立されている回路。*データ回線 (data circuit)* も参照。*バーチャル・サーキット (virtual circuit)* と対比。

物理レイヤー (physical layer). 開放型システム間相互接続参照モデルにおいて、伝送媒体を介して物理接続を確立、維持、および解放するための機械的、電気的、機能的、および手順的な手段を提供するレイヤー。 (T)

物理装置 (PU) (physical unit (PU)). (1) SSCP-PU セッションを介した SSCP の要求に応じて、ノードに関連する資源 (接続リンクや隣接リンク・ステーションなど) を管理および監視するコンポーネント。 SSCP は、接続リンクのようなノードの資源を PU を介して間接的に管理するために、物理装置をもつセッションを起動する。この用語は、タイプ 2.0, タイプ 4, およびタイプ 5 ノードにのみ適用される。 (2) *周辺 PU (peripheral PU)* およびサブエリア *PU (subarea PU)* も参照。

PING コマンド (ping command). インターネット制御メッセージ・プロトコル (ICMP) エコー要求パケットをゲートウェイ、ルーター、またはホストに送信し、その応答を待つコマンド。

ポイント・ポイント・プロトコル (PPP) (Point-to-Point Protocol (PPP)). パケットをカプセル化し、シリアル・ポイント・ポイント・リンクを介して伝送する方法を提供するプロトコル。

ポーリング (polling). (1) 多地点接続またはポイント・ポイント接続において、データ・ステーションに対して一度に 1 台ずつ送信するように促す処理。 (I) (2) 競合を避けるため、動作状況を調べるため、またはデータの送信または受信が可能であるかどうかを調べるための、装置に対する問い合わせ。 (A)

ポート (port). (1) データを入出力するためのアクセス・ポイント。 (2) 他の装置 (ディスプレイ、プリンターなど) のケーブルが接続される装置上のコネクター。 (3) リンク・ハードウェアへの物理接続の表現。ポートはアダプターと呼ばれることもあるが、アダプターは 2 つ以上のポートをもつことができる。単一の DLC プロセスで、1 つまたは複数のポートを制御することができる。 (4) インターネット・プロトコルにおいて、TCP またはユーザー・データグラム・プロトコル （UDP) と、上位レベルのプロトコルまたはアプリケーションの間の通信に使用される 16 ビットの番号。ファイル転送プロトコル (FTP) やシンプル・メール転送プロトコル (SMTP) など一部のプロトコルでは、すべての TCP/IP 実装に同一の割り当て済みポート番号が使用される。 (5) ホスト計算機内の複数の宛先を区別するために、トランスポート・プロトコルが使用する抽象概念。 (6) *ソケット (socket)* と同義。

ポート・アダプター (port adapter). ポート回線に NBBS 体系のアクセス・サービスを提供するコードを実行している、Nways スイッチの 2216 以外の型式のモジュール。 2216 では、ポート・アダプターとトランク・アダプターの機能が結合された多重化ポート/トランク・アダプター (MPTA) が使用されている。

ポート回線 (port line). 外部ユーザー装置を Nways スイッチに接続し、それにより NBBS ネットワークへの接続を可能にする通信回線。回線エミュレーション・サービス (CES)、パルス符号変調 (PCM)、ハイレベル・データ・リンク制御 (HDLC)、またはフレーム・リレー (FR) など、各種のアクセス・サービスおよびインターフェースを使用できる。

Nways スイッチでは、各ポート回線は 1 つの (または、複数の) NBBS ポートに関連付けられている。

ポート番号 (port number). インターネット通信において、トランスポート・サービスに対してアプリケーション・エンティティーを識別するもの。

ポテンシャル接続 (potential connection). NBBS 体系において、NBBS ネットワークの外部の 2 つの装置間の事前定義された接続。エンドポイント Nways スイッチの 1 つに保管されている構成パラメーターによって定義される。

構内交換機 (PBX) (private branch exchange (PBX)). 公衆電話網と相互に呼を伝送する構内電話交換機。

問題判別 (problem determination). プログラムのコンポーネント、機械の障害、通信設備、ユーザー所有または外注のプログラムや機器、停電などの環境障害、あるいはユーザーの誤りなど、問題の原因を判別するプロセス。

プログラム一時修正 (PTF) (program temporary fix (PTF)). プログラムの未変更の現行リリースに含まれる、IBM によって診断された問題の一時的な解決策または迂回策。

プロトコル (protocol). (1) 機能単位が通信する方法を規定する、意味上および構文上の一組の規則。 (I) (2) 開放型システム間相互接続体系において、同じレイヤー内のエンティティーが通信機能を実行する方法を規定する、1 組の意味上および構文上の規則。 (T) (3) SNA において、ネットワーク管理、データ伝送、およびネットワーク・コンポーネントの状態の同期化を行うために使用する要求とレスポンスの意味と順序の規則。*回線制御規則 (line control discipline)* および*伝送制御手順 (line discipline)* と同義。*ブラケット・プロトコル (bracket protocol)* および*リンク・プロトコル (link protocol)* を参照。

プロトコル・データ単位 (PDU) (protocol data unit (PDU)). 特定のレイヤーのプロトコルに指定されており、このレイヤーのプロトコル制御情報 (および、この

レイヤーのユーザー・データが含まれる場合もある) から構成されるデータの単位。 (T)

パルス符号変調 (PCM) (pulse code modulation (PCM)). アナログ音声信号のディジタル化のために採用された標準。 PCM では、音声は 8 kHz の速度でサンプリングされ、各サンプルは 8 ビット・フレームに符号化される。

Q

サービス品質 (QOS) (quality of service (QoS)). NBBS 体系では、サービス品質でネットワーク接続の特性を保証する。これは、エンド・エンド遅延、ジッター、およびパケット紛失率などを表わす。

サービス品質 (QoS) (Quality of Service (QoS)). 性能パラメーターを使用してアクセスされる、エンド・エンド・サービスのユーザー指向の性能。ATM ネットワークでは、セル損失比率、セル伝送遅延、およびセル遅延変動といった性能パラメーターによって、エンド・エンド ATM 接続の QoS が決まる。

R

高速トランスポート・プロトコル (RTP) コネクション (Rapid Transport Protocol (RTP) connection). 高性能ルーティング (HPR) において、セッション・トラフィックを伝達するためにルートのエンドポイント間に確立される接続。

到達可能性 (reachability). ノードまたは資源が、別のノードまたは資源と通信できること。

読み取り専用メモリー (ROM) (read-only memory (ROM)). 特殊な条件下を除いて、保管されたデータをユーザーが変更できないメモリー。

リアルタイム処理 (real-time processing). 処理操作中に、ある処理が必要とするデータまたは生成するデータを処理すること。通常はその結果が、実行中の処理 (および、おそらく関連の処理にも) 使用され、それに影響を与える。

再組み立て (reassembly). 通信において、分割されたパケットを受信後に相互に結合して元に戻すプロセス。

受信不可 (RNR) (receive not ready (RNR)). 通信において、着信フレームを受け入れることができないという一時的な状態を示す、データ・リンク・コマンドまたはレスポンス。

受信不可 (RNR) パケット (receive not ready (RNR) packet). *RNR パケット (RNR packet)* を参照。

受信回線信号検出器 (RLSD) (received line signal detector (RLSD)). EIA 232 標準において、リモート・データ回線終端装置 (DCE) からの信号を受信中であることをデータ端末装置 (DTE) に示す信号。*キャリア検出 (carrier detect)* およびデータ・キャリア検出 *(DCD) (data carrier detect (DCD))* と同義。

認定私企業 (RPOA) (Recognized Private Operating Agency (RPOA)). 電気通信サービスを提供し、国際電信電話諮問委員会の定める義務と規則に従う、政府省庁や機関以外の個人、会社、または組織。たとえば、通信事業者。

縮小命令セット・コンピューター (RISC) (reduced instruction-set computer (RISC)). 実行速度を上げるために、少数の単純化された頻繁に使用される命令セットを使用するコンピューター。

リモート (remote). (1) 通信回線を介してアクセスされるシステム、プログラム、または装置を表わす。 (2) *リンク接続 (link-attached)* と同義。 (3) *ローカル (local)* と対比。

リモート・ブリッジング (remote bridging). 2 つのブリッジが通信リンクを使用して複数の LAN を接続することができる、ブリッジの機能。*ローカル・ブリッジング (local bridging)* と対比。

リモート・コンソール (remote console). OS/2、TCP/IP、およびリモート Nways スイッチ資源制御プログラムを実行しているステーション。任意のネットワーク・サポート・ステーションに接続し、リモートから Nways スイッチの操作と保守を行うことができる。

接続は、以下を介して行う。
- モデムを使用する交換回線を介して

任意のネットワーク・サポート・ステーションを、別のネットワーク・サポート・ステーションのリモート・コンソールとして使用することができる。

リモート実行プロトコル (REXEC) (Remote Execution Protocol (REXEC)). ネットワーク・ノード内の任意のホストからコマンドまたはプログラムを実行することができるプロトコル。ローカル・ホストは、コマンドの実行結果を受け取る。

コメント要求 (RFC)(Request for Comments (RFC)). インターネット通信において、インターネット・プロトコルの一部とそれに関連する実験を記述した文書シリーズ。すべてのインターネット標準は、RFC として文書化されている。

リセット (reset). バーチャル・サーキットにおいて、データ・フロー制御を再初期化すること。リセットすると、転送中のデータはすべて削除される。

リセット要求パケット (reset request packet). X.25 通信において、バーチャル・コールまたはパーマネント・バーチャル・サーキットのリセットを要求するために、データ端末装置 (DTE) またはデータ回線終端装置 (DCE) に送信するパケット。要求の理由もパケットに指定することができる。

資源 (resource). Nways スイッチにおいて、ハードウェア要素または制御プログラムによって作成される論理エンティティー。たとえば、アダプター、LIC、および伝送路は物理資源である。コントロール・ポイント、およびコネクションは論理資源である。

リング (ring). *環状ネットワーク (ring network)* を参照。

環状ネットワーク (ring network). (1) 各ノードに正確に 2 本の分岐が接続されており、任意の 2 つのノード間には正確に 2 つのパスがあるネットワーク・ノード。 (T) (2) 装置が単方向伝送リンクで接続されて閉じたパスを形成しているネットワーク構成。

リング・セグメント (ring segment). リングの残りの部分から分離することができる (コネクターを引き抜くことによって) リングの区間。 *LAN セグメント (LAN segment)* を参照。

rlogin (リモート・ログイン) (rlogin (remote login)). Berkeley UNIX ベースのシステムによって提供されるサービス。ある機械の許可ユーザーがインターネットを介して他の UNIX システムに接続し、相互の端末が直接接続されているかのようにして対話することができる。rlogin ソフトウェアは、ユーザーの環境に関する情報 (たとえば、端末タイプ) をリモートの機械に渡す。

RNR パケット (RNR packet). データ端末装置 (DTE) またはデータ回線終端装置 (DCE) が、バーチャル・コールまたはパーマネント・バーチャル・サーキットに対する追加パケットを一時的に受付不能であることを示すために使用するパケット。

ルート (根) ブリッジ (root bridge). ブリッジ・ネットワークにおいて、他のアクティブ・ブリッジとの間に形成されたスパンニング・ツリーのルート (根) となるブリッジ。ルート (根) ブリッジは、スパンニング・ツリー・トポロジーを維持するために、ブリッジ・プロトコル・データ単位 (BPDU) を発信し、他のアクティブ・ブリッジに転送する。これは、ネットワーク内の最高の優先順位をもつブリッジである。

ルート (route). (1) 発信ノードから着信ノードまでのパスを表し、相互間で交換されるトラフィックが通る、正しいシーケンスのノードと伝送グループ (TG)。 (2) ネットワークのトラフィックが発信元から宛先に達するために使用するパス。

ルート (経路) ブリッジ (route bridge). 2 つのブリッジ・コンピューターが通信リンクを使用して 2 つの LAN を接続することができる、IBM ブリッジ・プログラムの機能。各ブリッジ・コンピューターは LAN の 1 つに直接接続されており、通信リンクが 2 つのブリッジ・コンピューターを接続する。

ルート拡張機能 (REX) (route extension (REX)). SNA において、サブエリア・ノードと隣接周辺ノード内のネットワーク・アドレス可能単位 (NAU) 間のパス部分を形成する、周辺リンクを含めたパス制御ネットワーク・コンポーネント。*明示ルート (ER) (explicit route (ER))*、*パス (path)*、および*バーチャル・ルート (VR) (virtual route (VR))* も参照。

ルート選択制御ベクトル (RSCV) (Route Selection control vector (RSCV)). APPN ネットワーク内のルートを記述する制御ベクトル。 RSCV は、発信元ノードから宛先ノードまでのパスを形成する TG とノードを識別する、正しいシーケンスの制御ベクトルから構成される。

ルーター (router). (1) ネットワークのトラフィックの流れのパスを決めるコンピューター。パスの選択は、特定のプロトコル、最短または最善パスを識別するアルゴリズム、およびその他の基準 (メトリックやプロトコル特有の宛先アドレスなど) から得られた情報に基づいて、複数のパスから選ばれる。 (2) 参照モデル・ネットワーク・レイヤーにおいて、類似または異なる体系を使用する 2 つの LAN セグメントを接続する装置。 (3) OSI 用語では、エンティティーに到達できるパスを判別する機能。 (4) TCP/IP では、*ゲートウェイ (gateway)* と同義。 (5) *ブリッジ (bridge)* と対比。

ルーティング (routing). (1) メッセージを宛先に到達させるためのパスを割り当てること。 (2) SNA において、メッセージ単位で運ばれるパラメーター (伝送ヘッダー内の宛先ネットワーク・アドレスなど) によって決められた、ネットワークの特定パスを通ってメッセージ単位を転送すること。

ルーティング・ドメイン (routing domain). インターネット通信において、ルーティング・プロトコルを使用してネットワーク全体の表示が各中間システム内で同一になるようにしている、中間システムのグループ。ルーティング・ドメインは、外部リンクによって相互に接続されている。

ルーティング情報プロトコル (RIP) (Routing Information Protocol (RIP)). インターネット・プロトコルにおいて、領域間のルーティング情報を交換し、インターネット・ホスト間の最適ルートを決めるために使用される、内部ゲートウェイ・プロトコル。 RIP は、リンク伝送速度ではなく、ルート・メトリックに基づいて最適ルートを決める。

ルーティング・ループ (routing loop). コンバージェンスが起こるまで、あるいは関係のネットワークが到達不能とみなされるまで、ルーターが相互間で情報を循環するときに発生する状態。

ルーティング・プロトコル (routing protocol). ルーターが他のルーターを見付け、到達可能なネットワークに達する最善ルートに関する情報を最新に保つために使用される技法。

ルーティング・テーブル (routing table). データグラムを転送したり、接続を確立するために使用されるルートの集まり。この情報は、ネットワーク・トポロジーと着側への到達可能性を識別するために、ルーター間で受け渡される。

ルーティング・テーブル保守プロトコル (RTMP) (Routing Table Maintenance Protocol (RTMP)). AppleTalk ネットワークにおいて、AppleTalk ルーティング・テーブルを用いて、トランスポート・レイヤーでルーティング情報を生成し、保守する機能を提供するプロトコル。 AppleTalk ルーティング・テーブルは、インターネットを通して、発信元ソケットから宛先ソケットにパケットを伝送する。

ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP)). ルーティング・データベースを維持しているバーチャル・ネットワーキング・システム (VIrtual NEtworking System (VINES)) プロトコルで、VINES ノード間でのルーティング情報の交換を可能にする。*インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP))* も参照。

rsh. ログイン・ステップを完全に飛ばして、リモート UNIX 機械上のコマンド解釈プログラムを呼び出し、そのコマンド解釈プログラムにコマンド行引き数を渡す、rlogin コマンドの変数。

S

SAP. サービス・アクセス・ポイント (service access point) を参照。

シード・ルーター (seed router). AppleTalk ネットワークにおいて、ネットワーク構成データ (たとえば、ネットワーク範囲の数やゾーン・リスト) を維持するルーター。各ネットワークには、少なくとも 1 つのシード・ルーターがある。シード・ルーターは、構成ツールを使用して、最初に設定する必要がある。*非シード・ルーター (nonseed router)* と対比。

セグメント (segment). (1) コンポーネント間または装置の相互間のケーブル区間。セグメントは、1 本のパッチ・ケーブル、相互接続された複数のパッチ・ケーブル、または相互接続された建物ケーブルとパッチ・ケーブルの組み合わせから成る。 (2) インターネット通信において、異なる機械にある TCP 機能の間の転送単位。各セグメントには、制御フィールドとデータ・フィールドが入っており、現在のバイト・ストリーム位置、実際のデータ・バイト、および受信データを妥当性検査するためのチェックサムが付加されている。

分割 (segmenting). OSI において、サポートするレイヤーからの 1 つのプロトコル・データ単位 (PDU) を複数の PDU にマップするためにレイヤーが実行する機能。

シーケンス番号 (sequence number). 通信において、伝送の流れやデータの受信を制御するために、フレームまたはパケットに割り当てられる番号。

シリアル・ライン・インターネット・プロトコル (Serial Line Internet Protocol) (SLIP). シリアル・ライン (たとえば、シリアル・ケーブルまたは電話回線を介したモデムへの RS232 接続) を介した 2 つの IP ホスト間のポイント・ポイント接続上で使用されるプロトコル。

NBBS ネットワークでは、SLIP は、ネットワーク・サポート・ステーションと IBM ネットワーク・サポート・センター (NSC) の間の接続にまたがって使用される。

サーバー (server). 通信ネットワークを通してワークステーションに共用サービスを提供する機能。たとえば、ファイル・サーバー、プリント・サーバー、メール・サーバー。 (T)

サービス・アクセス・ポイント (SAP) (service access point (SAP)). (1) 開放型システム間相互接続 (OSI) 体系において、あるレイヤーのサービスが、そのレイヤーのエンティティーによって、すぐ上のレイヤーのエンティティーに提供されるポイント。 (T) (2) アダプターによって提供される、情報を送受信することができる論理ポイント。 1 つのサービス・アクセス・ポイントで、多数のリンクを終端させることができる。

サービス公示プロトコル (SAP) (Service Advertising Protocol (SAP)). インターネットワーク・パケット交換機能 (IPX) において、以下を提供するプロトコル。

- インターネット上の IPX サーバーが、そのサービスの名前とタイプを公示することができる機構。このプロトコルを使用するサーバーの名前、サービス・タイプ、およびアドレスは、NetWare を稼働するすべてのファイル・サーバーに記録されている。
- ワークステーションが、すべてのタイプのすべてのサーバー、特定タイプのすべてのサーバー、または特定タイプの最近隣サーバーのアイデンティティーを見付けるために、照会をブロードキャストできる機構。
- ワークステーションが、特定タイプのすべてのサーバーの名前とアドレスを見付けるために、NetWare を稼働するすべてのファイル・サーバーを照会することができる機構。

セッション (session). (1) ネットワーク体系において、装置間のデータ通信を目的として、接続の確立、維持、および解放の過程で生じるすべての活動。 (T) (2) 要求に応じて、活動化し、さまざまのプロトコルを提供するように調整し、非活動化することができる、ネットワーク・アクセス可能単位 (NAU) 間の論理結合。各セッションは、セッション中に交換されるすべての伝送を伴う伝送ヘッダー (TH) の中で固有に識別される。(3) L2TP において、ダイヤル・ユーザーと LNS 間でエンドツーエンド PPP 接続が試行されるとき、ユーザーがセッションを開始したか、 LNS がアウトバウンド・コールを開始したかどうかにかかわらず、L2TP はセッションを生成する。そのセッション用のデータグラムは、LAC と LNS 間のトンネルを通じて送信される。LNS および LAC は、LAC に接続された各ユーザーについての状態情報を保持する。

シンプル・ネットワーク管理プロトコル (SNMP) (Simple Network Management Protocol (SNMP)). インターネット・プロトコルにおいて、ルーターと接続ネットワークを監視するのに使用されるネットワーク管理プロトコル。 SNMP は、アダプテーション・レイヤー・プロトコルである。管理される装置に関する情報が定義され、そのアプリケーションの管理情報ベース (MIB) に保管される。

SLIP. シリアル・ライン IP (Serial Line IP)。シリアル通信リンク上で実行中の IP に関する IETF 標準。

SNA 管理サービス (SNA/MS) (SNA management services (SNA/MS)). SNA ネットワークの管理を援助するために提供されるサービス。

SNAP. (1) サブネットワーク・アクセス・プロトコル (SubNetwork Access Protocol)。 (2) サブネットワーク接続点 (SubNetwork Attachment Point)。

ソケット (socket). (1) 処理間またはアプリケーション・プログラム間の通信のエンドポイント。 (2) カリフォルニア大学の Berkeley ソフトウェア配布 (一般には、 Berkeley UNIX または BSD UNIX と呼ばれる) によって提供される抽象概念で、プロセスまたはアプリケーション間の通信のエンドポイントとして働く。

ソース・ルート・ブリッジング (source route bridging). LAN において、フレームの IEEE 802.5 媒体アクセス制御 (MAC) ヘッダー内のルーティング情報を使用して、フレームが送信する必要があるリングまたはトークンリング・セグメントを判別するブリッジング方式。ルーティング情報は、発信元ノードによって MAC ヘッダーに挿入される。ルーティング情報フィールド内の情報は、発信元ホストが生成する探索パケットから取り出される。

ソース・ルーティング (source routing). LAN において、発信元ステーションがフレームの通るルートを決めて、そのルーティング情報をフレームに組み込む方式。ブリッジは、そのルーティング情報を読み取り、フレームを転送するかどうかを判別する。

発信元サービス・アクセス・ポイント (SSAP) (source service access point (SSAP)). SNA および TCP/IP において、システムがリモート装置にデータを送信することを可能にする論理アドレス。*宛先サービス・アクセス・ポイント (DSAP) (destination service access point (DSAP))* と対比。

スパンニング・ツリー (spanning tree). LAN において、ブリッジが自動的にルーティング・テーブルを作成し、トポロジーの変更に応じてそのテーブルを更新することによって、ブリッジ・ネットワーク内の任意の 2 つの LAN 間に 1 つしかルートが存在しないようにする方式。この方式により、パケットがルートを循環して送信元ルーターに戻るというパケットのループを防止することができる。

制御範囲 (SOC) (sphere of control (SOC)). 1 つの管理サービス中心拠点によってサービスされるコントロール・ポイント・ドメインの集合。

制御範囲 (SOC) ノード (sphere of control (SOC) node). 中心拠点の制御範囲内にあるノード。 SOC ノードは、その中心拠点と管理サービス機能を交換している。 APPN エンド・ノードは、管理サービス機能を交換する機能をサポートする場合は、SOC ノードになれる。

水平分割 (split horizon). ネットワークのコンバージェンスを達成する時間を最小化するための技法。ルーターは特定のルート (経路) を受信したインターフェースを記録し、そのルートに関する情報は再び同じインターフェースに伝送しないようにする。

スプーフィング (spoofing). データ・リンクにおいて、エンド・ステーションから開始されたプロトコルが、最終宛先の代わりに中間ノードによって確認応答されて処理される技法。たとえば、IBM 6611 データ・リンク交換では、SNA フレームはカプセル化して TCP/IP パケットに入れられ、非 SNA 広域ネットワーク・ノードを通って伝送され、別の IBM 6611 によってアンパックされて、最終宛先に渡される。スプーフィングの利点は、エンド・エンド・セッションのタイムアウトを防止できることである。

標準 MIB (standard MIB). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理情報構造 (SMI) の管理の下に置かれ、インターネット技術作業部会 (IETF) によって標準とみなされている MIB モジュール。

静的ルート (static route). ルーティング・テーブルに手入力される、ホスト間、ネットワーク・ノード間、またはその両方のルート。

ステーション (station). 通信機能を使用するシステムの入力または出力ポイント。たとえば、通信回線を通してデータを送信または受信することができる、ある特定の場所にある 1 台または複数のシステム、コンピューター、端末、装置、および関連のプログラム。

StreetTalk. バーチャル・ネットワーキング・システム (VINES) において、利用者がネットワークのトポロジーを知らなくても、ネットワーク上の任意のリソースを見付けてアクセスすることができる、ネットワーク全体の固有のネーミング/アドレッシング・システム。*インターネット制御プロトコル (ICP) (Internet Control Protocol (ICP))* および *ルーティング更新プロトコル (RTP) (RouTing update Protocol (RTP))* も参照。

管理情報構造 (SMI) (Structure of Management Information (SMI)). (1) シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、ネットワーク管理プロトコルを用いてアクセスできるオブジェクトを定義するのに使用される規則。 (2) OSI において、情報の管理に関連する標準の集合。この集合には、*管理情報モデル (Management Information Model)*および *管理オブジェクト定義の指針 (Guidelines for the Definition of Managed Objects)*が含まれる。

サブエリア (subarea). サブエリア・ノード、接続された周辺ノード、および関連の資源から構成される SNA ネットワークの部分。サブエリア・ノード内では、すべてのネットワーク・アクセス可能単位 (NAU)、リンク、およびサブエリア内のアドレス可能な隣接リンク端末 (接続された周辺ノードまたはサブエリア・ノード内の) は、共通のサブエリア・アドレスを共用し、異なる要素アドレスを持っている。

サブネット (subnet). (1) TCP/IP において、IP アドレスの一部によって識別されるネットワークの部分。 (2) サブネットワーク *(subnetwork)* の同義語。

サブネット・アドレス (subnet address). インターネット通信において、ホスト・アドレスの一部がローカル・ネットワーク・アドレスとして解釈される、基本 IP アドレッシング機構の拡張。

サブネット・マスク (subnet mask). *アドレス・マスク (address mask)* の同義語。

サブネットワーク (subnetwork). (1) 1 組の共通特性 (同一ネットワーク ID など) を持つノードの集まり。 (2) サブネット *(subnet)* の同義語。

サブネットワーク・アクセス・プロトコル (SNAP) (Subnetwork Access Protocol (SNAP)). LAN において、パケットが属している非 IEEE 標準プロトコル・ファミリーを識別する、5 バイトのプロトコル識別子。SNAP 値を使用して、`$AA` をサービス・アクセス・ポイント (SAP) 値として使用する各プロトコルを区別する。

サブネットワーク接続点 (SubNetwork Attachment Point). フレームのプロトコル・タイプを識別する LLC ヘッダー拡張部。

サブネットワーク・マスク (subnetwork mask). *アドレス・マスク (address mask)* の同義語。

サブシステム (subsystem). 制御システムから独立して、または非同期で、動作することができる、2 次的または従属的なシステム。 (T)

スイッチド・バーチャル・サーキット (SVC) (switched virtual circuit (SVC)). 必要に応じて動的に確立される X.25 回線。交換回線と同等の X.25 回線。パーマネント・バーチャル・サーキット *(PVC) (permanent virtual circuit (PVC))* と対比。

同期 (synchronous). (1) 共通タイミング信号のような特定の事象の発生に依存する 2 つ以上のプロセス。 (T) (2) 規則的または予測可能な時間的関係をもって起こること。

同期データ・リンク制御 (SDLC) (Synchronous Data Link Control (SDLC)). (1) リンク接続上で同期、コード透過、ビット直列情報伝送を管理するための、米国規格協会 (ANSI) のアドバンスト・データ通信制御手順 (ADCCP) および国際規格のハイレベル・データ・リンク制御 (HDLC) のサブセットに従う規則。伝送交換は、交換回線または非交換回線上で、全二重または半二重で行われる。リンク接続の構成は、ポイント・ポイント、多地点、またはループのいずれかである。 (I) (2) *2*

進データ同期通信 (BSC) (binary synchronous communication (BSC)) と対比。

同期光ネットワーク (synchronous optical network) (SONET). 光インターフェースを介してディジタル情報を伝送するための米国標準。これは、同期ディジタル階層 (SDH) 勧告と密接な関連がある。

SYNTAX. シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、管理オブジェクトに対応する抽象データ構造を定義する、MIB モジュール内の文節。

システム (system). データ処理において、特定の機能を達成するために組織された人間、機械、および方式の集まり。(I) (A)

システム構成 (system configuration). 特定のデータ処理システムを形成する装置とプログラムを指定するプロセス。

システム・サービス・コントロール・ポイント (SSCP) (system services control point (SSCP)). 構成の管理、ネットワーク運用者および問題判別の要求の調整、およびネットワーク利用者にディレクトリー・サービスやその他のセッション・サービスを提供するめの、サブエリア・ネットワーク内のコンポーネント。相互に対等の立場で協働する複数の SSCP は、ネットワークを複数の制御領域に分割し、各 SSCP が自身の領域内の物理装置および論理装置に対して階層的な制御関係を持つようにすることができる。

システム・ネットワーク体系 (SNA) (Systems Network Architecture (SNA)). ネットワークを通して情報単位を伝送し、ネットワークの構成と運用を制御するための、論理構造、フォーマット、プロトコル、および動作手順の記述。 SNA の階層化された構造により、情報の最終的な発信元と宛先 (つまり、利用者) が、情報交換に使用される SNA ネットワークの特定のサービスや機能から独立し、その影響を受けなくすることができる。

T

TCP/IP. (1) 伝送制御プロトコル/インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)。 (2) 本来は米国国防総省によって開発された UNIX に似ている、イーサネットを基礎にしたシステム相互接続プロトコル。 TCP/IP により、レイヤー 4 が TCP でレイヤー 3 が IP のパケット交換方式リサーチ・ネットワークである ARPANET (拡張研究プログラム機関ネットワーク (Advanced Research Projects Agency Network)) の便利性が向上した。

Telnet. インターネット・プロトコルにおいて、リモート端末接続サービスを提供するプロトコル。このプロトコルによって、あるホストのユーザーがリモート・ホストにログオンし、そのホストに直接接続されている端末ユーザーとして対話することができる。

しきい値 (threshold). (1) IBM ブリッジ・プログラムにおいて、『しきい値超過』 オカレンスがカウントされてネットワーク管理プログラムに通知される前に、誤りのためにブリッジを通過して転送されないフレームの最大数として設定される値。 (2) そこからカウンターが 0 まで減分される初期値、または初期値からカウンターが増分または減分されて到達する値。

スループット・クラス (throughput class). パケット交換において、データ端末装置 (DTE) パケットがパケット交換ネットワークを通過する速度。

時分割多重 (TDM) (time division multiplexing (TDM)). ***チャネル化 (channelization)*** を参照。

活動回数 (TTL) (time to live (TTL)). ベストエフォート送達プロトコルが、パケットの無限ループを禁止するために使用する技法。 TTL カウンターが 0 に達すると、パケットは廃棄される。

タイムアウト (timeout). (1) 指定された事象の発生時から始まる事前定義された時間間隔の終了前に起こる別の事象。 (I) (2) システム操作を中断してリスタートすることが必要になる前の、ポーリングまたはアドレッシングに対するレスポンスのような、特定の動作を起こすために割り当てられた時間。

TLV. タイプ/長さ/値 (Type/Length/Value)。LAN エミュレーション・パケットの中の汎用情報要素。

トークン (token). (1) ローカル・エリア・ネットワークにおいて、あるデータ装置が一時的に伝送媒体を制御していることを示すために、そのデータ装置から別のデータ装置に連続的に渡される許可信号。各データ装置には、媒体を制御するためにトークンを獲得して使用する機会が与えられる。トークンというのは、伝送許可を示す特別のメッセージまたはビット・パターンである。 (T) (2) LAN において、伝送媒体上を、ある装置から別の装置に渡される一連のビット。トークンにデータが付加されるとフレームになる。

トークンリング (token ring). (1) IEEE 802.5 では、媒体に接続されたステーション間でトークン (特殊なパケットまたはフレーム) を渡すことによって媒体アクセスを制御するネットワーク技術。 (2) ある接続リング・ステーション (ノード) から別のノードにトークンを渡すリング・トポロジーを持つ、FDDI または IEEE 802.5

ネットワーク。 (3) *ローカル・エリア・ネットワーク (LAN) (local area network (LAN))* も参照。

トークンリング・ネットワーク (token-ring network). (1) トークン・パッシング手順により、データ・ステーション間で単方向のデータ伝送を行い、伝送されたデータが送信元ステーションに戻ってくる構造の環状ネットワーク。 (T) (2) ノードからノードへ順にトークンを渡すリング・トポロジーを使用するネットワーク。送信の準備ができているノードは、トークンを取り込み、伝送するデータを挿入することができる。

トポロジー (topology). 通信において、ネットワーク・ノード内のノードの物理的または論理的な配置。特に、ノードとそれを結ぶリンクの関係を表す。

トポロジー・データベース更新 (TDU) (topology database update (TDU)). ネットワーク・トポロジー・データベースを維持するために、APPN ネットワーク・ノード間にブロードキャストされ、各ネットワーク・ノードに完全に複写される、新規または変更されたリンクまたはノードに関するメッセージ。 TDU には、以下のものを識別する情報が入っている。

- 送信元ノード
- ネットワークの各種資源のノード特性およびリンク特性
- 記述されている各資源の最新の更新のシーケンス番号

トレース (trace). (1) コンピューター・プログラムの実行の記録。命令が実行された順序を表す。 (A) (2) データ・リンクの場合は、送信または受信されたフレームとバイトの記録。

トランシーバー (送受信装置) (transceiver (transmitter-receiver)). LAN において、ホスト・インターフェースをイーサネットのようなローカル・エリア・ネットワークに接続する物理装置。イーサネット・トランシーバーには、ケーブルに信号を送って衝突を検出する電子機器が内蔵されている。

伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP)). インターネット、およびインターネットワーク・プロトコルに関する米国国防総省の規格に準拠するその他のすべての通信ネットワークで使用されている通信プロトコル。 TCP は、パケット交換通信網のホストとそのネットワークの相互接続システムのホストとの間に、高信頼性ホスト間プロトコルを提供する。基礎となるプロトコルとして、インターネット・プロトコル (IP) を使用している。

伝送制御プロトコル/インターネット・プロトコル (TCP/IP) (Transmission Control Protocol/Internet Protocol (TCP/IP)). ローカル・エリア・ネットワークと広域ネットワーク・ノードの両方で、ピア間接続機能をサポートする一組の通信プロトコル。

伝送グループ (TG) (transmission group (TG)). (1) 伝送グループ番号によって識別された隣接ノード間の接続。 (2) サブエリア・ネットワークにおいて、隣接ノード間の単一リンクまたはリンク群。伝送群がリンク群で構成される場合、リンクは単一の論理リンクと見なされ、伝送群は*マルチリンク伝送群 (MLTG)* と呼ばれる。*混合媒体マルチリンク伝送群 (MMMLTG)* とは、異なる媒体タイプのリンク (たとえば、トークンリング、交換 SDLC、非交換 SDLC、およびフレーム・リレー・リンク) を含むものを言う。 (3) APPN ネットワークにおいて、隣接ノード間の 1 つのリンク。 (4) *並列伝送群 (parallel transmission groups)* も参照。

伝送ヘッダー (transmission header) (TH). パス制御が、メッセージ単位をルーティングし、ネットワークの中の流れを制御するために作成して使用する制御情報。オプションでその後に基本情報単位 (BIU) または BIU セグメントを続けることができる。*パス情報単位 (path information unit)* も参照。

透過ブリッジング (transparent bridging). LAN において、媒体アクセス制御 (MAC) レベルを通して、個々のローカル・エリア・ネットワークを相互に結合する方式。透過型ブリッジには MAC アドレスが入ったテーブルが保管されており、テーブルに指示されている場合は、ブリッジが検出したフレームを別の LAN に転送することができる。

トランスポート・レイヤー (transport layer). 開放型システム間相互接続参照モデルにおいて、高信頼性エンド・エンド・データ転送サービスを提供するレイヤー。パス内に中継開放型システムが存在する場合もある。 (T) *開放型システム間相互接続参照モデル (Open Systems Interconnection reference model)*も参照。

トランスポート・サービス (transport services). 以下の目的のために Nways スイッチのコントロール・ポイントによって実行される NBBS 体系の機能。

- トランク・ラインと Nways スイッチの接続サポート
- 帯域幅の使用率の最大化
- サービス品質の保証
- Nways スイッチ間のパケット転送
- 論理待ち行列の管理と、伝送のスケジューリング

トラップ (trap). シンプル・ネットワーク・マネージメント・プロトコル (SNMP) において、例外条件を報告するために、管理ノード (エージェント機能) が管理ステーションに送るメッセージ。

トランク・アダプター (trunk adapter). トランク・ラインに NBBS 体系のトランスポート・サービスを提供するコードを実行する、Nways スイッチの 2216 以外の型式のモジュール。 2216 では、ポート・アダプターとトランク・アダプターの機能が結合された多重化ポート/トランク・アダプター (MPTA) が使用されている。

トランク・ライン (trunk line). 2 つの Nways スイッチを接続する高速伝送路。同軸ケーブル、ファイバー・ケーブル、または無線を使用でき、通信会社からリースすることもできる。

Nways スイッチでは、各トランク・ラインは 1 つの NBBS トランクに関連付けられている。

トンネル (Tunnel). トンネルとは、LNS-LAC の対によって定義されるもので、 LAC と LNS の間で PPP データグラムを伝える。単一のトンネル で多くのセッションを多重化することができる。制御接続が同じトンネルを介して作動する場合は、すべてのセッションおよびトンネル自体の設定、解放、および保守を制御する。

トンネル伝送 (tunneling). トランスポート・ネットワークを、単一の通信リンクまたは LAN のように扱うこと。*カプセル化 (encapsulation)* も参照。

T1. 米国では、1.544-Mbps の公衆アクセス回線。 24 個の 64 Kbps チャネルで利用可能。欧州方式 (E1) は 2.048 Mbps で伝送する。

U

出荷時設定アドレス (universally administered address). ローカル・エリア・ネットワークにおいて、製造時にアダプターに永久的に符号化されるアドレス。出荷時設定アドレスは固有である。*ローカル管理アドレス (locally administered address)* と対比。

ユーザー・データグラム・プロトコル (UDP) (User Datagram Protocol (UDP)). インターネット・プロトコルにおいて、低信頼性のコネクションレス・データグラム・サービスを提供するプロトコル。このプロトコルを使用して、ある計算機またはプロセス上のアプリケーション・プログラムが、別の計算機またはプロセス上のアプリケーション・プログラムに、データグラムを送信することができる。 UDP では、インターネット・プロトコル (IP) を使用してデータグラムを送達する。

V

V.24. データ通信において、データ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

V.25. データ通信において、手動および自動で設定されたコールのエコー制御装置を使用禁止にする手順を含めた、一般交換電話ネットワークの自動応答装置および並列自動コール装置を定義する CCITT の仕様。

V.34. 標準の市販の音声グレードの 33.6 Kbps (およびそれより低速の) チャネルを介してのモデム通信に関する ITU-T 勧告。

V.35. データ通信において、種々のデータ転送速度のデータ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

V.36. データ通信において、48, 56, 64, または 72 キロビット/秒のデータ転送速度のデータ端末装置 (DTE) とデータ回線終端装置 (DCE) 間の交換回線の一連の定義を規定した CCITT の仕様。

VCC. バーチャル・チャネル・コネクション (Virtual Channel Connection)。当事者 (通話者) 間の接続。

バージョン (version). 通常は重要な新しいコードまたは新しい機能を含む、別個のライセンス・プログラム。

VINES. バーチャル・ネットワーキング・システム (VIrtual NEtworking System)。

バーチャル・サーキット (virtual circuit). (1) パケット交換で、実際の接続箇所をユーザーに見えるようにする、ネットワークによって提供される機能。 (T) *データ回線 (data circuit)* も参照。*物理回線 (physical circuit)* と対比。 (2) 2 台の DTE 間に確立された論理接続。

バーチャル・コネクション (virtual connection). フレーム・リレーにおいて、ポテンシャル接続の戻りパス。

バーチャル・リンク (virtual link). 最短パス最優先オープン (OSPF) において、非バックボーン中継エリアによって分離されたボーダー・ルーターに接続する、ポイント・ポイント・インターフェース。エリア・ルーターは OSPF バックボーンの一部なので、バーチャル・リンクはバックボーンに接続する。バーチャル・リンクは、OSPF バックボーンが不連続にならないようにする。

バーチャル・ローカル・エリア・ネットワーク (VLAN) (Virtual Local Area Network (VLAN)). プロトコルおよびサブネットに基づく、1 つまたは複数の LAN の論理的グループ化で、ネットワーク・トラフィックを、こうしてできるグループ内に分離する場合に使用される。

バーチャル・ネットワーキング・システム (VINES) (VIrtual NEtworking System (VINES)). Banyan Systems, Inc. からのネットワーク運用システムとネットワーク・ソフトウェア。VINES ネットワークにおける

バーチャル・リンクでは、たとえ実際には数百マイル離れていても、すべての装置およびサービスが相互に直接接続されているように見える。 *StreetTalk* も参照。

バーチャル・ルート (VR) (virtual route (VR)). (1) SNA において、次のような論理接続。(a) 特定の明示ルートとして物理的に実現されている 2 つのサブエリア・ノード間の論理接続。または (b) ノード内のセッション用のサブエリア・ノード内に完全に収まっている論理接続。別個のサブエリア・ノードの間のバーチャル・ルートは、使用する明示ルートに伝送優先順位を定め、バーチャル・ルート・ペーシングよってフロー制御を行い、パス情報単位 (PIU) にシーケンス番号を付けることによりデータ保全性を確保する。 (2) *明示ルート (ER) (explicit route (ER))* と対比。*パス (path)* および*ルート拡張 (REX) (route extension (REX))* も参照。

W

広域ネットワーク (WAN) (wide area network (WAN)). (1) ローカル・エリア・ネットワークや大都市圏ネットワークよりも広い地域に通信サービスを提供し、公衆通信施設を使用または提供することができるネットワーク。 (T) (2) 何百キロあるいは何千キロも離れた区域にサービスを行うように設計されたデータ通信ネットワーク。たとえば、公衆および私用パケット交換ネットワークや各国の電話網など。 (3) *ローカル・エリア・ネットワーク (local area network (LAN))* および*大都市圏ネットワーク (metropolitan area network (MAN))* と対比。

ワイルドカード文字 (wildcard character). *パターン突き合わせ文字 (pattern-matching character)* の同義語。

X

X.21. 公衆データ網上の同期動作のための、データ端末装置とデータ回線終端装置の間の汎用インターフェースに関する、国際電信電話諮問委員会 (CCITT) の勧告。

X.25. (1) データ端末装置とパケット交換データ網間のインターフェースに関する、国際電信電話諮問委員会 (CCITT) の勧告。 (2) *パケット交換 (packet switching)* も参照。

Xerox ネットワーク・システム (XNS) (Xerox Network Systems (XNS)). Xerox Corporation によって開発された一組のインターネット・プロトコル。TCP/IP プロトコルに類似しているが、XNS は異なるパケット・フォーマットと用語を使用している。*インターネットワーク・パケット交換機能 (IPX) (Internetwork Packet Exchange (IPX))* も参照。

Z

ゾーン (zone). AppleTalk ネットワークにおいて、インターネット内部のノードのサブセット。

ゾーン情報プロトコル (ZIP) (Zone Information Protocol (ZIP)). AppleTalk プロトコルにおいて、セッション・レイヤーのインターネット全体のゾーン名とネットワーク番号のマッピングを維持してゾーン管理サービスを提供するプロトコル。

ゾーン情報テーブル (ZIT) (zone information table (ZIT)). インターネットのネットワーク番号と対応ゾーン・ネームのマッピングをリストしたもの。このリストは、AppleTalk インターネットの各インターネット・ルーターによって維持される。

特殊文字 (Special Characters)

2216 Nways ブロードバンド・スイッチ (2216 Nways BroadBand Switch). NBBS ネットワークでの高速通信を可能にする高速パケット交換機。 2220 Nways ブロードバンド・スイッチでは、ネットワーキング・ブロードバンド・サービス体系で定義されている機能を実装している。 ***Nways スイッチ (Nways Switch)*** と同義。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

［サ行］

［タ行］

［ナ行］

［ハ行］

［マ行］

［ヤ行］

［ラ行］

A

B

C

D

E

F

H

I

L

M

N

P

Q

R

S

T

U

V

W

Printed in Japan

SD88-6112-02

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12

Spine information:

IBM

Nways
マルチプロトコル・アクセス・
サービス

MAS V3.4 フィーチャーの使用