ネットワーク・ユーティリティー

設置、入門、使用者の手引き

GA88-6548-01
(英文原典：GA27-4167-02)

ネットワーク・ユーティリティー

設置、入門、使用者の手引き

GA88-6548-01
(英文原典：GA27-4167-02)

お願い

本書の情報および本書に記載されている製品をご使用になる前に、 401ページの『付録A. 特記事項』および403ページの『付録B. 安全上の注意』の安全に関する注意を必ずお読みください。

第 3 版 (1999 年 6 月)

本書は、ネットワーク・ユーティリティー モデル TN1 および TX1 と、マルチプロトコル・アクセス・サービス (MAS) V3.3 に適用されます。

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： GA27-4167-02
Network Utility
Installation,
Getting Started,
and User's Guide

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 1999.9

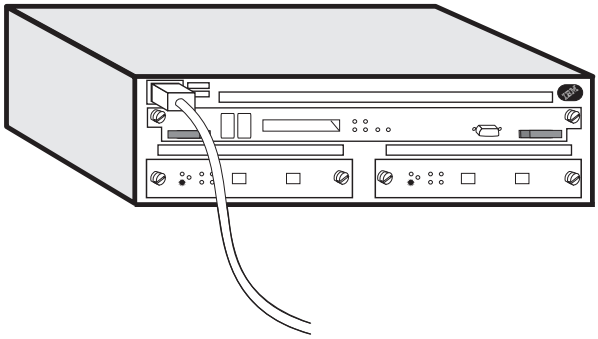
この文書では、平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

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

目次

本書について

本書では、IBM ネットワーク・ユーティリティーをセットアップし、初期構成を実行し、設置時に発生する恐れがある問題を訂正し、ネットワーク・ユーティリティーを使用する方法について説明します また、本書には、一部の一般的なネットワーク・ユーティリティーのネットワーク構成を示す詳細な構成例も示してあります



IBM ネットワーク・ユーティリティーには、ネットワーク・ユーティリティー TN3270E サーバー (モデル TN1) とネットワーク・ユーティリティー・トランスポート (モデル TX1) という、2 種類のモデルがあります 特に明示的に断らない限り、ネットワーク・ユーティリティー という用語を使用する場合は、モデル TN1 とモデル TX1 の両方を指すものとします

本書は、xiiページの『ライブラリーの概説』 に記載されているネットワーク・ユーティリティーに関する資料の一環をなすものです。本書は、他の資料に記載されている詳細な参照情報をお読みいただくにあたって、入門書の役割を果たすものです。

本書の対象読者

本書は、ネットワーク・ユーティリティーの設置、構成、および管理を担当される方々を対象としています

作業の進め方

設置と初期構成

1. 製品に付属の *設置と初期構成の手引き* を使用して、シャシーとケーブルを取り付けます (『第1章 ハードウェアのセットアップ』 を参照) (あるいは、IBM サービス技術員による設置をご利用いただけます。 追加情報については、IBM 担当員にお問い合わせください)。

   注: パラレル・チャネル・アダプター (FC 2299) 用のケーブルの敷設は、IBM サービス技術員またはチャネルについて研修を積んだ担当者が行う必要があります。

2. 製品の構成と操作ができるようにするために、ローカル接続の場合は、端末かワークステーションを接続し (『第2章 ユーザー・コンソールの始

動』 を参照)、リモート接続の場合は、システム・カードにプラグが差し込まれている PCMCIA モデムを電話回線に接続します。

3. 使用したい構成方式を決めて、2216 モデル 400 またはネットワーク・ユーティリティー ネットワーク・ユーティリティーの初期構成を実行します (『第3章 初期構成の実行』を参照)。

習得

- IBM ルーティング製品のコマンド行インターフェースを扱った経験が多少なりともある場合、またはチュートリアルに従って学習するよりも、タスクを試みてみたいと考える場合は、『第4章 ユーザー・インターフェースのクィック・リファレンス』を使用して、コマンド行インターフェースのナビゲーションの基本の一部を検討します。 第2部 ネットワーク・ユーティリティーについての学習の他の章を通読して、必要になる追加情報が記載されている個所を確認しておきます。

  IBM ルーティング製品のコマンド行インターフェースに未経験の場合は、『第5章 コマンド行インターフェースの解説』をチュートリアルとして使用して、基本概念とナビゲーションについて学習します。
- 基本的な構成および操作の機能に詳しい場合は、 第3部 構成および管理の詳細に挙げてある構成事例の中から選択を行います。 ご使用のネットワーク特性に似ている構成を選択します。
  - モデル TN1 のユーザーの場合 -- 145ページの『第12章 TN3270E サーバー』 を参照してください。
  - モデル TX1 のユーザーの場合 -- 229ページの『第14章 チャネル・ゲートウェイ』、 271ページの『第16章 データ・リンク交換』、または 313ページの『第19章 VPN (仮想私設ネットワーク)』 を参照してください。
  - すべてのユーザー -- IBM ホスト・ネットワーキング製品を伴う構成の場合は、 295ページの『第18章 サンプル・ホスト定義』 を参照してください。

最終的な構成と操作

1. 第2部 ネットワーク・ユーティリティーについての学習 に記載されている操作と管理のタスク、および 第3部 構成および管理の詳細 に記載されている事例を使用して、デバッグを行い、初期構成を完了します。
2. 最終構成を実行します。 *構成プログラム使用者の手引き* および、*ソフトウェア使用者の手引き* を参照してください。

ライブラリーの概説

ネットワーク・ユーティリティーと IBM 2216 モデル 400 には、共通の資料が少なくありません 次の図には、ライブラリーに収められている資料を作業別にまとめて示してあります。

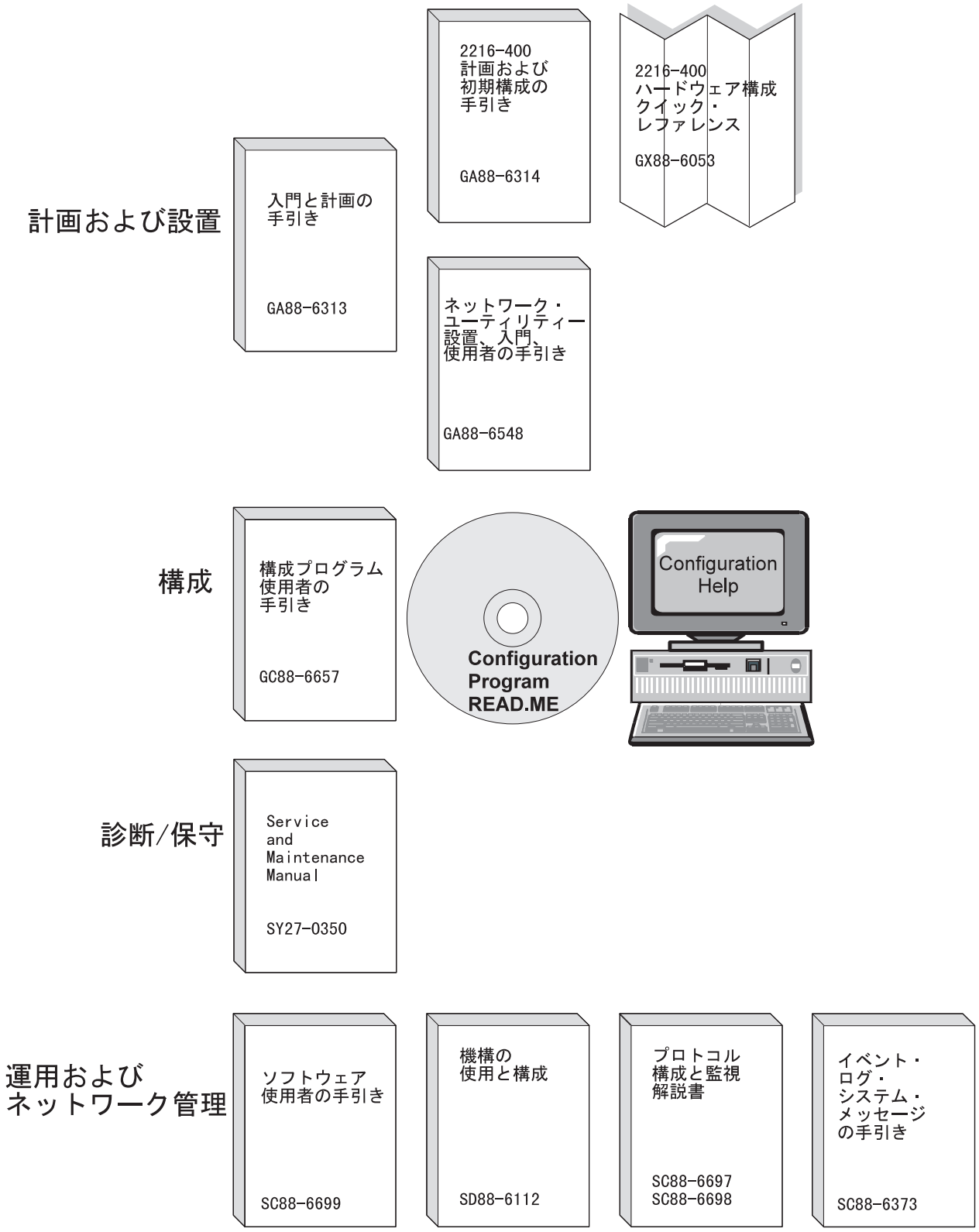


図 1. IBM 2216 モデル 400 とネットワーク・ユーティリティーに共通の作業とライブラリー

製品に付属して出荷されるハードコピー資料

これらの資料 (英語版のみ) はハードコピーで出荷されますが、この製品の Documentation CD-ROM (SK2T-0405) にも入っています。

計画

GA88-6313

2216 Nways マルチアクセス・コネクターおよびネットワーク・ユーティリティー 入門と計画の手引き

この資料では、設置のための準備方法、購入したいハードウェアの選択方法について説明しています。ユーザーのネットワーク用のハードウェアおよびソフトウェアの仕様が記載されています。また、この資料では、ルーティング・ネットワークの管理に関する情報も提供します。

設置と習得

GA88-6548

ネットワーク・ユーティリティー の専用資料

ネットワーク・ユーティリティー 設置、入門、使用者の手引き

この資料 (本書) では、ネットワーク・ユーティリティーの設置方法と設置後の検査方法について説明しています。さらに、製品の使用法についても説明し、製品のサンプル構成も示してあります。

GA88-6314

2216 モデル 400 の専用資料

2216 Nways マルチアクセス・コネクター モデル 400 設置および初期構成の手引き

この資料では、2216 モデル 400 の設置方法と設置後の検査方法について説明しています。

GX88-6053

2216 モデル 400 の専用資料

2216 Nways マルチアクセス・コネクター ハードウェア構成 クィック・リファレンス

この資料は、IBM 2216 モデル 400 の正しい状態の判別に使用するハードウェア構成情報を入力および保管する場合に使用します。

診断と保守

SY27-0350

2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual

この資料には、モデル 400 およびネットワーク・ユーティリティーに問題が生じた場合の診断、および修理に関する手順が記載されています

安全

SD21-0030

Caution: Safety Information--Read This First

この資料には、装置の取り付けおよび保守に適用される注意および危険通報を翻訳した内容が記載されています。

構成

GC88-6657

構成プログラム 使用者の手引き

この資料では、Nways マルチプロトコル・アクセス・サービス構成プログラムの使用法について説明します。

CD-ROM に収めてソフトコピーとして出荷される資料

これらの資料は、別途にハードコピーを発注していただくこともできます。

運用およびネットワーク管理

SC88-6699

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

この資料では、次のことを行う方法を説明しています。

- Nways マルチプロトコル・アクセス・サービスのソフトウェアおよびマイクロコードを構成、監視、および使用する。
- Nways 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、2216 基本と一緒に出荷されるネットワーク・インターフェースおよびリンク・レイヤー・プロトコルを構成および監視する。

SD88-6112

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

この資料では、マルチプロトコル・アクセス・サービス (MAS) 機能について記述し、それらの機能を使用するためのコマンドについて説明しています。これらの機能には、プロトコルを拡張する機能も独立型の機能もあります。例として、フレームの MAC アドレスに基づいてフレームをフィルターする MAC フィルター機能、PPP またはフレーム・リレー・シリアル・インターフェースを通るトラフィックのタイプを選択して、選択したトラフィック・タイプ用として帯域幅の予約を可能にする帯域幅予約システム、 IP の実行時に IP アドレスを別の IP アドレスで表すことができるようにするネットワーク・アドレス変換機能などがあります。

SC88-6697

Nways マルチプロトコル・アクセス・サービス プロトコル構成と監視 解説書 第 1 巻

SC88-6698

Nways マルチプロトコル・アクセス・サービス プロトコル構成と監視 解説書 第 2 巻

これらの資料では、Nways マルチプロトコル・アクセス・サービスのコマンド行ユーザー・インターフェースを使用して、製品とともに出荷されるルーティング・プロトコル・ソフトウェアを構成および監視する方法を説明します。

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

SC88-6373

Nways イベント・ログ・システム・メッセージの手引き

この資料では、発生しうるエラー・コードのリストが、説明、およびエラーを訂正するための推奨処置とともに記載されています。

IBM 資料の発注方法

IBM 資料は、ワールド・ワイド・ウェブ (WWW) 上で下記のアドレスの IBM Publications Direct Catalog にアクセスして、発注することができます。

`http://www.elink.ibmlink.ibm.com/pbl/pbl`

IBM では、多くの資料をさまざまな言語に翻訳しています。したがって、必要な資料が自国語で入手できる場合が少なくありません。

Web サイトへのアクセス

下記の IBM Web ページで、製品情報を提供しています。

ネットワーク・ユーティリティー関係 :
`http://www.networking.ibm.com/networkutility`
モデル 400 関係 : `http://www.networking.ibm.com/216/216prod.html`

下記の IBM Web ページでは、2216 基本およびネットワーク・ユーティリティーの資料をオンラインで提供しています。

`http://www.networking.ibm.com/did/2216bks.html`

情報、更新、および訂正

このページでは、資料が印刷された後にインプリメントされた技術変更、説明、および修正に関する情報を提供します。

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

製品サポート

下記のページでは、ダウンロードおよび追加サポート情報を提供しています。

ネットワーク・ユーティリティー関係 :
`http://www.networking.ibm.com/support/networkutility`
モデル 400 関係 : `http://www.networking.ibm.com/support/2216`

第1部 始めに

第1章 ハードウェアのセットアップ

この章では、以下のトピックについて説明します。
- ネットワーク・ユーティリティーの設置および構成に必要な要件の定義
- ネットワーク・ユーティリティー・シャシーのラック取り付けまたは床据え付け
- PCMCIA カードの挿入
- ネットワーク・ユーティリティーの初回電源オン
- システムが正常であることが LED によって示されていることの確認

ネットワーク・ユーティリティーの設置

始める前に： 本書の図では、アダプター・スロットは、すべてが埋まっている場合を想定しています。ネットワーク・ユーティリティーが完全に装備されている場合の重量は約 15 kg です。

設置前の要件 -- 次のものがそろっている必要があります。
- ASCII 端末またはワークステーション (PC)
- ワークステーションの場合は、Telnet クライアントと ASCII 端末エミュレーション・ソフトウェア (例えば、ProComm) のどちらか
- ネットワーク・ユーティリティー PCMCIA モデムにダイヤルインする場合は、リモート・ワークステーション用のモデム
- 構成ファイルまたはコードをネットワーク・ユーティリティー内に転送する (Xmodem 経由以外の方法で) 場合は、ワークステーション用の LAN アダプター
- ネットワーク・ユーティリティー PCMCIA EtherJet カードを使用する場合は、小さいイーサネット・ハブ、またはイーサネット対応可能ワークステーションを直接接続するためのクロス・ケーブル

ラック取り付け要件 -- EIA 標準 19 インチのラックであれば、どれでも使用できます。ラックは開放型でも閉鎖型でも構いません。ただし、閉鎖型のラックを選んだ場合は、ネットワーク・ユーティリティー内の通気を十分に確保する必要があります。ラックの前面にカバーがあると、ネットワーク・ユーティリティーに空気の流れが届かないことがあるので、取り外すなり修正を施すなりして、通気を確保する必要があります。同様に、背面に通気口がないラック・カバーは、ネットワーク・ユーティリティーの内部から空気を逃がすことができなかったり、幾つかのマシンからの背圧が蓄積される原因となる可能性があるので、使用しないようにする必要があります。

1. 内容の確認

次の品目がネットワーク・ユーティリティーに同梱されていることを確認します。

資料

本書のほかに、次の資料が付属している必要があります。

- *Caution: Safety Information-Read This First*、 SD21-0030
- *2216 Nways マルチアクセス・コネクターおよびネットワーク・ユーティリティー 入門と計画の手引き*、GA88-6313
- *2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual*, SY27-0350
- *構成プログラム 使用者の手引き*、 GC88-6657
- *2216 Documentation CD-ROM*, SK2T-0405

ハードウェア

- アダプター類をすでに取り付け済みのネットワーク・ユーティリティー
- 発注したすべてのケーブル類
- ラック取り付け補助具
- 電源コード
- PCMCIA モデム (PCMCIA モデムが使用できない国の場合を除く)
- IBM EtherJet PC カード
- ラック取り付け用ケーブル・ブラケット (ネットワーク・ユーティリティーに FC 2299 (パラレル・チャネル・アダプター) がある場合)
- ヌル・モデムおよび 2 本の 9 〜 25 ピン・シリアル通信ケーブル

ソフトウェア

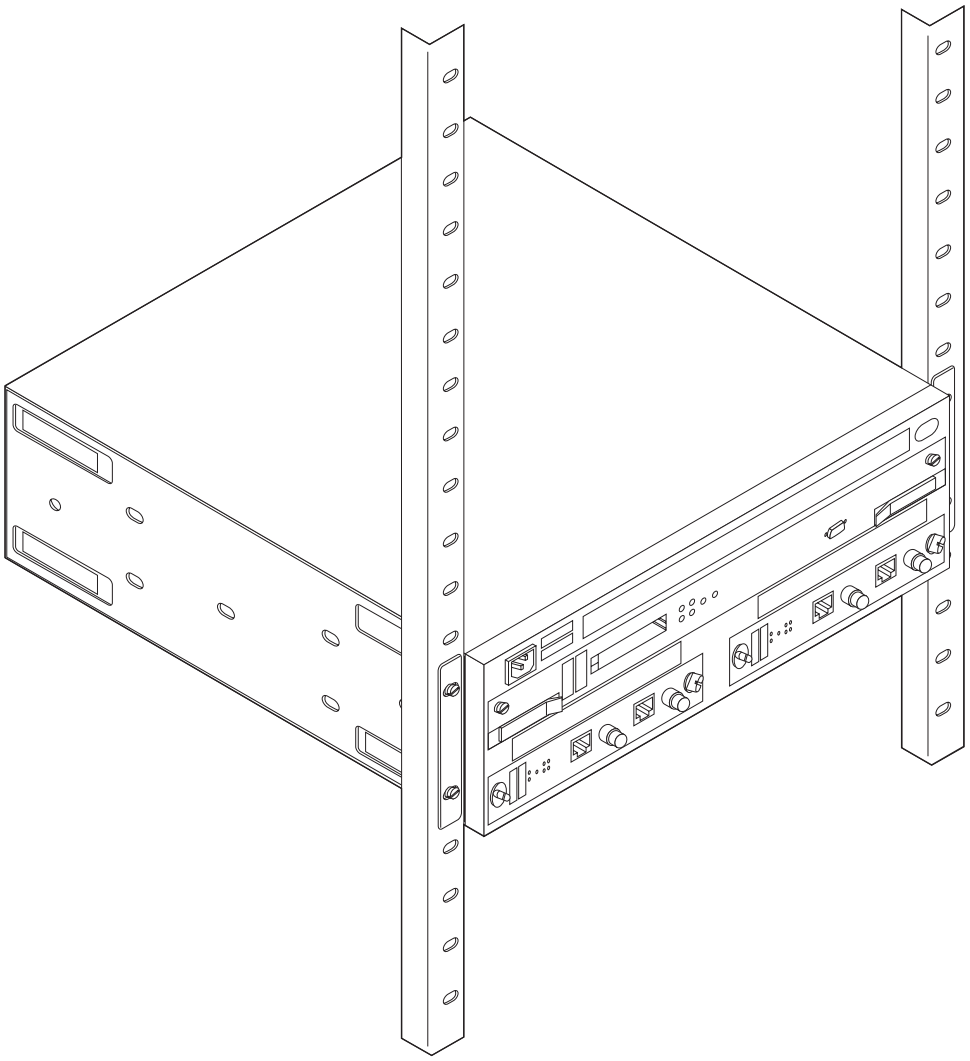
- IBM 2216 モデル 400 および ネットワーク・ユーティリティー構成プログラム CD-ROM
- 命令コードはネットワーク・ユーティリティーにプリロードされています。

次に進んでください。

床据え付けの場合 - 9 ページのステップ 7

ラック取り付けの場合 - 5 ページのステップ 2

2. ネットワーク・ユーティリティーのラック取り付け



次の品目が必要です。

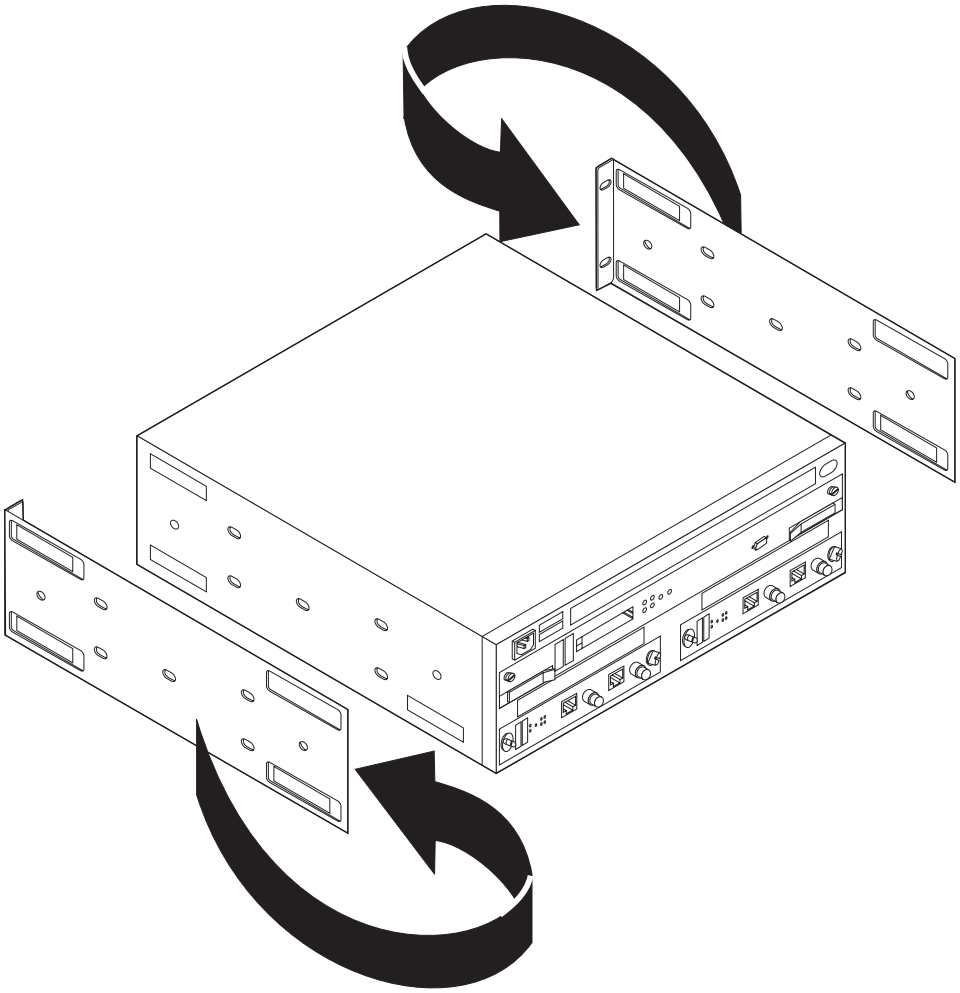
- ケーブル (必要に応じて)
- 4 本のラック取り付けねじ
- ねじ回し

注:

1. ラック用の棚がある場合は、それを取り付けてから続けてください。
2. 棚が取り付けてある場合は、取り付け補助具を使用しないでください。

6 ページのステップ 3 に進んでください。

3. ラック取り付け (床据え付けの場合は任意選択)

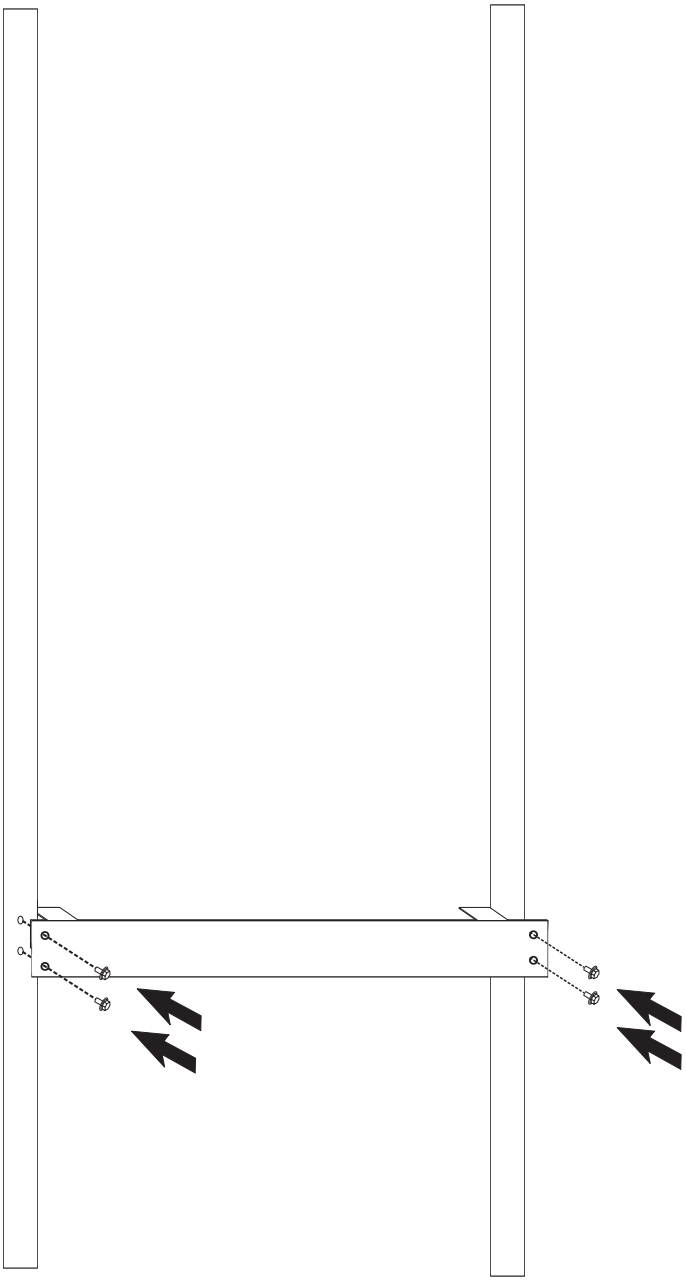


ネットワーク・ユーティリティー取り付け金具には、出荷時に、背面に面してフランジが取り付けられています。

1. それぞれの取り付け金具から 2 本のねじ (1 本は前面に、1 本は背面にあります) を抜きます。
2. それぞれの取り付け金具を裏返して、ネットワーク・ユーティリティーがラックに取り付けられるようにします。
3. 4 本のねじを再び取り付けます。

取り付け金具が正しく取り付けられると、それぞれの金具に施されている浮き彫り文字が後ろ側の端にきます。 A が右側で、B が左側になります。

4. ラック取り付け



取り付け補助具は金属製の棒で、ネットワーク・ユーティリティーをラック内に取り付けるときにそれを支持するものです。この取り付け補助具によって、ネットワーク・ユーティリティーとラックを正しくそろえることができます。

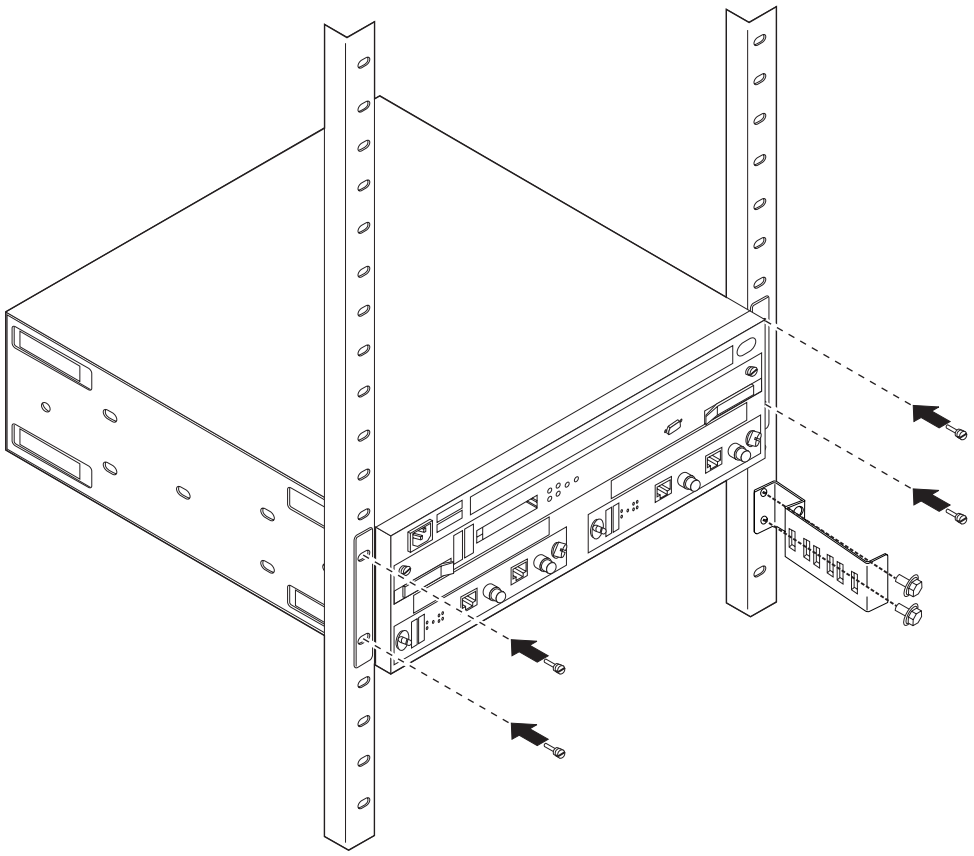
取り付け補助具の穴をラックとそろえ、すべてのねじを取り付けてください。

5. ラック取り付け

ネットワーク・ユーティリティーを IBM 2216 取り付け補助具または棚の上に置きます。取り付け金具によって、取り付け作業中にネットワーク・ユーティリティーがラック内に落下するのを防ぐことができます。

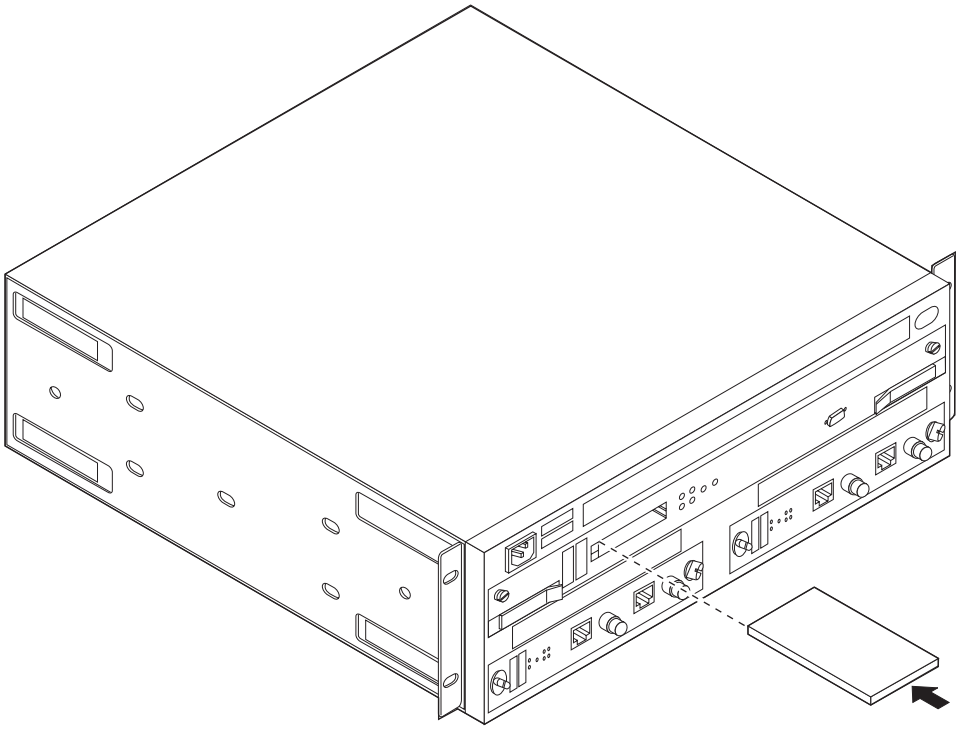
取り付け補助具が取り付けられているので、次のステップが完了するまで、ネットワーク・ユーティリティーがぐらつくことはありません。

6. ラック取り付け



1. ねじを下側のねじから取り付けます。
2. FC 2299 の場合 : 2 本のねじを使用して、ラック前面のネットワーク・ユーティリティーの下側にラック取り付け用ケーブル・ブラケットを取り付けます。

7. ラック取り付けまたは床据え付け

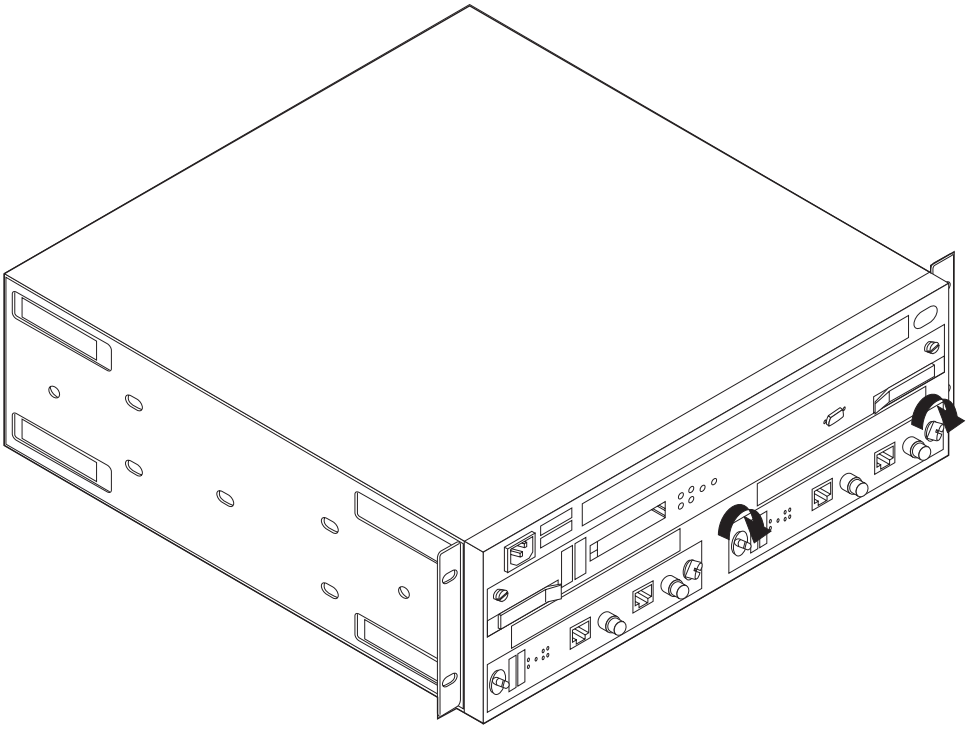


PCMCIA モデムや PCMCIA EtherJet LAN アダプターを取り付ける場合は、システム・カード上のいずれかの PCMCIA スロットに滑り込ませます。電話ケーブルをモデムに接続します (三角形がケーブルの左側を示します)。

注:

1. ネットワーク・ユーティリティーの出荷時に付属している EtherJet LAN アダプターの代わりに別のイーサネット PCMCIA カードを使用することはできません。
2. ネットワーク・ユーティリティーに PCMCIA モデムや PCMCIA イーサネット・アダプターを 2 つ取り付けると、システムは立ち上がらなくなります。

8. ラック取り付けまたは床据え付け



1. **すべての**つまみねじがきつく締まっていることを確認します (取り付け中にねじを緩めなかった場合でも)。
2. 電源コードをネットワーク・ユーティリティーと電源コンセント (ユニットの電源用) に接続します 4 〜 5 分後、正しい LED がオンになっているか確認します (11ページの表1 を参照してください)。 12ページの図2 に示されている LED の状態を監視します。

   ユニットがブートし、アダプターのテストが行われている間に、以下の状態が認められれば、正常です。

   - 緑色と黄色のシステム・カード LED が両方とも短い時間オンになっている。
   - 緑色と黄色のアダプター・カード LED が両方とも短い時間オンになっている。
   - ハード・ディスクおよびアダプター・スロット誤り黄色 LED が短い時間オンになっている。
3. 問題が認められた場合は、14ページの『問題解決』 の表と手順を使用して、問題を解決または報告してください。

9. セットアップ (ラック取り付けまたは床据え付け) の完了

1. ケーブルを接続します (パラレル・チャネル・アダプター、FC 2299 を除きます)。
   注: FC 2299 を使用している場合は、チャネルについて研修を積んだ IBM サービス技術員または担当者がケーブルの敷設にあたる必要があります。

   FC 2299 用のケーブルを取り付ける場合は、IBM サービス技術員に連絡してください。パラレル・チャネルおよびその接続装置の場合は、ケーブルの取り付けが正しく行われていないと、障害が生じることになります。
2. 15ページの『第2章 ユーザー・コンソールの始動』 に進んで、ユーザー端末コンソールをセットアップします。

10. IBM サービス技術員が行う FC 2299 の作業

1. アダプター・ケーブルを FC 2299 に接続します (*Service and Maintenance Manual* の『Installing Channel Adapters』の項に記載されている手順を使用します)。まだ、ホスト・チャネル・ケーブルには接続しないでください。
2. 折り返しテストを実行して、すべてのアダプター・ケーブルが正しく動作することを確認します。
3. ホスト・チャネル・ケーブルをアダプター・ケーブルに接続します。

ハードウェア・セットアップの検査

表1 には、ブートの完了後 (**電源オンの 4 ～ 5 分後)**の、ユニットの前面にある LED の正しい状態が示してあります。 LED がすべて正しい状態にあれば、ユニットの構成を始めることができます。ネットワーク・ユーティリティー上の LED の位置については、 12ページの図2 をごらんください。

表 1. 作動可能時のマシンの LED の状態

カード	LED 名	色	状態
システム・カード	PCMCIA 1 (装置取り付け済み)	黄色	オフ
	PCMCIA 2 (装置取り付け済み)	黄色	オフ
	OK	緑色	オン
	Not OK	黄色	オフ
全アダプター・カード	OK	緑色	オン
	Not OK	黄色	オフ
	スロット誤り	黄色	オフ
	入出力ポート (ユニットへの構成のロード前)	緑色	オフ
	入出力ポート	黄色	オフ

LED インディケーター

ネットワーク・ユーティリティーには、ユニットの機能状況を示す発光ダイオード (LED) が多数備えられています。

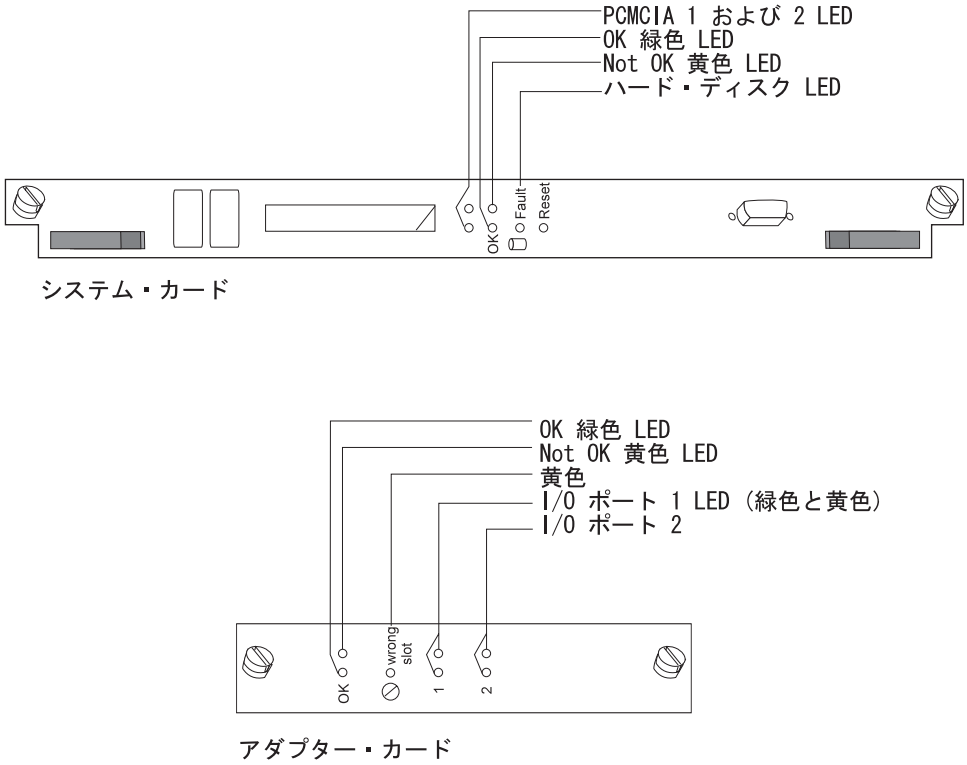


図 2. システム・カードおよびアダプター・カードの LED

システム・カードの状況

LED	意味
PCMCIA 1 または PCMCIA 2 (黄色)	オン - PCMCIA デバイスに障害があるか、取り付けられていないか、または正しくはまっていません。 オフ - 装置は自己テストに合格しました。
OK (緑色)	オン - カード・ハードウェアが正常に稼働しています。 明滅 - ハード・ディスクからロード中です。
(黄色)	オン - カード・ハードウェアに障害があります。
障害ハード・ディスク (黄色)	オン - ハード・ディスクが故障しました。

アダプター・カードの状況

LED	意味
OK (緑色)	オン - アダプターが作動可能です。
(黄色)	オン - アダプターに障害があります。
スロット誤り (黄色)	オン - サービス技術員に連絡してください。

LED	意味
緑色のポート [1]	オン - ポートは正常に稼働しています (使用可能にされ、構成済みです)。 オフ - ポートは構成されていないか、または使用不可です。 明滅 (ESCON アダプターのみ) - 光学式電力測定テストを実行中です。
黄色のポート [1]	オン - 1 つまたは複数のポートにハードウェア障害があります。 明滅 - 1 つまたは複数のポートにポート入出力またはネットワークの障害があります。 *2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual* に記載されている保守分析手順 (MAP) を使用して分離します。 オフ - 問題が検出されません。

重要な電話番号

連絡先の名前	電話番号
システム管理者:	
サービス技術員:	

1. マルチポート WAN アダプター (FC 2282、FC 2290、および FC 2291) のポート LED の場合は、1 つまたは複数のポートの状況が反映されます。

問題解決

セットアップ中に発生する問題を識別し、訂正するには、質問に答え、以下に示されているように適切な処置をとってください。

システム・カードについて、黄色の Not OK LED がオンになっていますか ?

はい: カードに障害があります。

1. システムをその給電部から切り離します。
2. カードを取り付け直します。
3. システムをその給電部に再接続します。
4. 4 〜 5 分待ってから、LED の状態を調べます。

問題が訂正されない場合は、サービス技術員に連絡してください。

いいえ: 次の質問に進んでください。

システム・カードについて、緑色の OK LED がオフになっていますか?

はい: 緑色の LED は、命令コードによってオンにされます。

緑色の LED がオンにならない場合は、サービス技術員に連絡してください。

いいえ: 次の質問に進んでください。

システム・カードについて、PCMCIA ポート LED がオンになっていますか?

はい: PCMCIA カード・スロットが空か、カードが電源オン自己テストを行いませんでした。 カードを取り付け直します。

問題が訂正されない場合は、サービス技術員に連絡してください。

いいえ: 次の質問に進んでください。

スロット 1 および 2 の入出力カードについて、黄色の Not OK LED がオンになっていますか ?

はい: カードに障害があります。 アダプターを取り付け直します。

問題が訂正されない場合は、サービス技術員に連絡してください。

いいえ : 次の質問に進んでください。

スロット 1 および 2 の入出力カードについて、緑色の OK LED がオンになっていますか ?

はい : ネットワーク・ユーティリティーの状態は OK のようです。

いいえ : カードを取り付け直します。それでも緑色の OK LED がオンにならない場合は、カードが不良です。サービス技術員に連絡してください。

第2章 ユーザー・コンソールの始動

ネットワーク・ユーティリティーに構成および操作の目的でアクセスするため、端末をセットアップする必要があります。この章に記載されている情報は、以下の作業を行う場合に役立ちます。

- 端末をセットアップする方法の習得
- 環境に最適の方式の選択
- デフォルト設定値の使用による端末の接続と起動

この章の説明に従って作業を完了すると、端末は動作可能な状態となり、初期コマンド・プロンプトが表示されて、構成に取りかかる準備が整っているはずです。

アクセス方式

ネットワーク・ユーティリティーにアクセスして接続できる方法は、 表2 に要約してあるように、幾つもあります

表 2. ユーザー・コンソール接続オプション

物理的な接続機構	回線プロトコル	アクセス・プロトコル	デフォルトの IP アドレス
サービス・ポート + ヌル・モデム・サービス・ポート + 外付けモデム PCMCIA モデム	非同期文字	ASCII 端末エミュレーション	該当しない
	SLIP	Telnet	ネットワーク・ユーティリティー = 10.1.1.2 ワークステーション = 10.1.1.3
PCMCIA EtherJet	IP	Telnet	ネットワーク・ユーティリティー = 10.1.0.2 ワークステーション = 10.1.0.3
任意の IP ネットワーク・インターフェース	IP	Telnet	デフォルト値なし

以下のものを使用したい場合は、次のいずれか 1 つの方法で物理接続を行います。

1. **ASCII 端末**、または端末エミュレーション・ソフトウェアが稼働している**ワークステーション**：
   - ヌル・モデム・ケーブルを EIA 232 サービス・ポートに接続して行うローカル接続 (16ページの図3 を参照)。このタイプの接続では、ヌル・モデム・アダプターと、この製品に付属の 2 本の 9 〜 25 ピン・シリアル・ケーブルが使用されます。
   - PCMCIA モデムを介するリモート・ダイヤルイン (電話回線を使用) (17ページの図4 を参照)
   - EIA 232 サービス・ポートに外付けモデム (図示されていない) を接続したリモート・ダイヤルイン (電話回線を使用)。この構成が使用されるのは、 PCMCIA モデムが承認されていない国々の場合です。Hayes AT コマンド・セットをサポートする非同期モデムを使用してください。サポートされるモデムの判別については、`http://www.networking.ibm.com/networkutility` の「Product Literature Sales」ページを参照してください。

2. TCP/IP ソフトウェアが稼働しているワークステーション上の **Telnet プロトコル** :
   - 上記の 15ページの1 に挙げた方式の中で記述されている物理接続のいずれか。

     これらの物理接続の場合は、Telnet ワークステーションでは、シリアル・ライン・インターネット・プロトコル (SLIP) をサポートする TCP/IP が稼働しています。SLIP は、非同期回線を通して IP パケットを送信する方式の 1 つです。

     「Telnet over SLIP」によってアクセスすることができるのは、命令コード・コマンド行インターフェースだけであって、ファームウェア・メニュー・インターフェースにはアクセスできません。
   - ローカル・イーサネット・ハブを使用した、ネットワーク・ユーティリティー PCMCIA LAN アダプター (IBM EtherJet PC カード) からワークステーションへのローカル・ケーブル 17ページの図5 に、この構成のバージョンの 1 つが図示してあります。

     クロス・ケーブル経由で、ワークステーション・イーサネット・アダプターを EtherJet カードに直接接続したり、イーサネット LAN と Telnet ワークステーションの間に広域ネットワークをはさむこともできます。

     ネットワーク・ユーティリティー IBM EtherJet PC カードは、ユーザー・コンソールの提供やファイルの転送など、サービスおよび操作の目的に供されるものです。通常のネットワーク・ルーティング・インターフェースとして使用することはできません。
   - アダプター・スロット内のアダプターの IP 対応可能ネットワーク・インターフェースのいずれかに接続した、ネットワーク接続ワークステーション。

     この構成は、ここには図示してありません。ネットワーク・インターフェースは、トークンリング、10/100 Mbps イーサネット、FDDI などの LAN アダプター上が可能です。また、いずれも IP ルーティングをサポートするので、他のどんなアダプター上でも構いません。Telnet ワークステーションの場合は、ローカルでもリモートでも接続可能です。

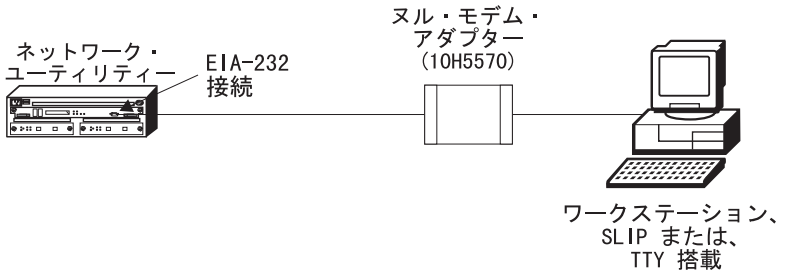


図 3. EIA 232 ポートへのワークステーションのローカル・シリアル接続

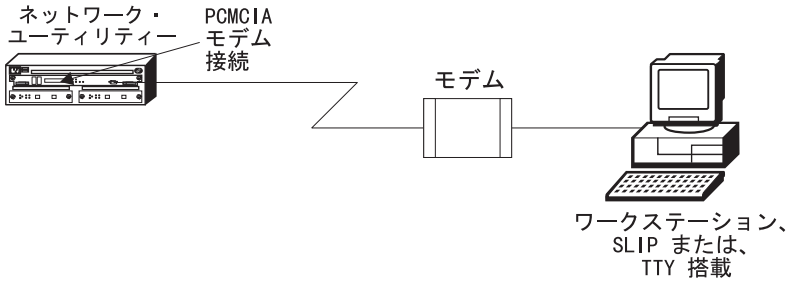


図 4. PCMCIA モデムへのリモート・シリアル接続

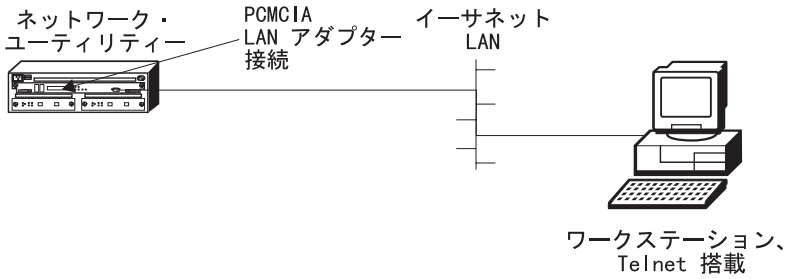


図 5. PCMCIA LAN アダプターを介する LAN 接続

どのアクセス方式を使用したらよいか ?

- **新規ユーザーで、 ネットワーク・ユーティリティー** に物理的に隣接している場合は、ASCII 端末エミュレーションを端末コンソールとして使用して (18ページの『ASCII 端末のセットアップと使用』を参照)、ワークステーションをユニットに直接接続します (16ページの図3 を参照)。この方式の主要な利点には、次のようなものがあります。
  - セットアップが簡単にできる。
  - 基本的な端末エミュレーション・ソフトウェアの使用で良好に作動する。
  - ユニットの構成が不要である。
  - 製品の使用法の習得時に構成とリブートを繰り返して行った場合でも、接続が安定している。
  - 習得や使用の対象としたいファームウェア・ユーザー・インターフェースにアクセスできる。
- **新規ユーザーで、 ネットワーク・ユーティリティー** から隔たっている場合は、物理的にユニットに隣接している新規ユーザーの場合と同じ理由が幾つかあるので、Telnet よりもダイヤルアップ端末エミュレーションがお勧めです。
- **構成した ネットワーク・ユーティリティー を実動ネットワーク内に入れる場合は、** ネットワーク構成に最適なだけでなく、サービスと運用の戦略にも最適の端末コンソール・アクセス方式を選択します。 Telnet を「日常」端末コンソール・アクセス方式として使用し、ネットワークが利用不能か、ファームウェア・アクセスが必要か、いずれかの場合にダイヤルアップ端末エミュレーションをバックアップ・サービス方式として使用することができます。IBM サービス技術員が構成およびネットワークの問題のデバッグにあたる場合は、いずれかの方式を使用します。

ASCII 端末のセットアップと使用

ASCII 端末、または端末エミュレーションを搭載したワークステーションをセットアップする場合は、この節を使用します。ASCII 端末エミュレーションを使用すれば、構成が行われているかどうかに関係なく、ネットワーク・ユーティリティーにアクセスすることができます

ASCII 端末コンソールでは、メイン命令コード (コマンド行インターフェース) と、ファームウェア・ユーザー・インターフェース (76ページの『ファームウェア』 を参照) の両方にアクセスすることができます。 PCMCIA または外付けモデムにリモートでダイヤルインし、ユニットをリブートすると、コンソール接続が失われ、リダイヤルが必要になります[2]。ローカル接続の場合は、コンソール接続は、リブート中維持されます。

ASCII 端末への接続

ASCII 端末またはエミュレーター (該当するエミュレーション・ソフトウェアを搭載) を接続すると、17ページの図4 および 16ページの図3 に示してあるように、ローカルまたはリモート・アクセスが得られます。DEC VT100 および DEC VT220 ASCII 端末、ならびにそれをサポートするように構成されているパーソナル・コンピューター・システムなどの装置がサポートされます。

シリアル・ポートおよび PCMCIA モデムのデフォルト設定

以下は、シリアル・ポート用のデフォルト設定です。

速度	19.2 Kbps
パリティー	なし
データ・ビット	8
ストップ・ビット	1
端末タイプ	VT220、モノクローム

シリアル・ポートに関する設定を変更する場合は、以下の手順に従います。

1. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されているタスクの 1 つを使用して、ネットワーク・ユーティリティーをリブートしてファームウェア・メインメニューを表示させます。
2. オプション 1 「**Manage Configuration**」を選択します。
3. COM1 シリアル・ポートの行にカーソルを移動して、 **Enter**を押します。
4. 変更したい特性 (例えば、ボー・レート) にカーソルを移動して、 **Enter** を押します。
5. 新しい値を選択して、**Enter** を押します。
6. ファームウェア・メインメニューに戻る場合は、**Esc** を押します。
7. 現行ブート・シーケンスを続行し、命令コードに新しい設定の使用を開始させたい場合は、**F9** (OS 開始) を押します。

2. 外付けモデムを使用している場合は、ネットワーク・ユーティリティーからの DTR での廃棄を外付けモデムが無視する設定にできれば、ネットワーク・ユーティリティーのリブート時にコンソール接続が失われることはありません。使用しているモデムの資料を参照してください。

リブートしてファームウェアに入り、ファームウェアに新しい設定の使用を開始させたい場合は、**F3** (リブート) を押します。

8. 端末または端末エミュレーション・ソフトウェアの設定を変更して、ネットワーク・ユーティリティー シリアル・ポートの新しい設定に一致させます。

PCMCIA モデムは、ほとんどの国の場合に、ネットワーク・ユーティリティーの出荷時に付属している標準品目です。33.6 Kbps V.34 データ・モデムであり、電話網の相手側のパートナー・モデムとの間で使用するデータ速度の交渉を行います。データ圧縮を使用すれば、このモデムで 33.6 Kbps を超えるデータ・スループットを達成することができます。

ネットワーク・ユーティリティー・システムとその PCMCIA モデムの間のデータ速度は、デフォルトで 19.2 Kbps ですが、それを引き上げて、2 つのモデムが相互間で達成できるさらに高いスループットに対処することができます。例えば、このデータ速度を 57.6 Kbps に設定して、2 つの 33.6 Kbps モデムがデータ圧縮を実行した場合の有効データ速度よりも高くすることができます。使用するモデムが両方とも 19.2 Kbps より高速の場合は、この速度を上げると、Xmodem ファイル転送時間が短縮されます。

PCMCIA モデムのデータ速度やその他の設定のいずれかを変更する場合は、シリアル・ポートの設定を変更する場合に説明した上記の手順と同じ手順に従いますが、シリアル・ポートではなく、COM2 の PCMCIA モデムを選択します。

ASCII 端末セットアップ属性

ネットワーク・ユーティリティー・サービス・ポートに接続されている端末または端末エミュレーターをセットアップする場合に必要なすべてのオプションが、下にリストしてあります。あらゆる端末 (特に 3151 および 3161) がこれらすべてのオプションをもつわけではありません。端末で設定できるオプションを設定するにはこの情報を使用する必要があります。

端末設定値および機能キー

ボー・レート: 19200 ビット/秒

注: ボー・レートは、ネットワーク・ユーティリティー・シリアル・サービス・ポートの速度に一致する必要があります。

パリティー: なし
データ・ビット : 8
ストップ・ビット: 1

二重: 全二重
フロー制御: XON/XOFF および RTS/CTS (注 1 を参照)

画面制御: ANSI 全画面
画面の幅: 80 文字
画面の高さ: 24 行
行ラップ: オン
画面スクロール: オン

改行キー変換: CR (0Dx)
バックスペース・キー変換: 復元不可

注:

1. 端末および端末エミュレーター・プログラムにフロー制御オプションがない場合は、『永続送信要求』に設定する必要があります。
2. 端末エミュレーターが端末タイプ選択を必要とする場合は、VT-220 に設定します。

機能キー

ファームウェアにアクセスする場合は、機能キー F1、F2、F3、F4、F6、および F9 の使用が必要になります。すべての端末や端末エミュレーターで、これらの機能キーに対するサポートが標準になっているとは限りません (例えば、 VT100 タイプの場合)。

これらの機能キーを最も簡単にシミュレートする方法は、次の順序で下記のキーをたたくことですが、それぞれのキーをたたく間隔が 2 秒を超えないようにする必要があります。

1. **Ctrl-a**
2. 必要な機能キーの番号を表す数字 (機能キー自体ではない)
3. **Enter**

機能キーを押すと、次のようなエスケープ・キー・シーケンスが生成されるように、端末エミュレーターをセットアップすることもできます。

```
Function 1 (F1):  <Esc> O P         Hex: 1B 4F 50
Function 2 (F2):  <Esc> O Q         Hex: 1B 4F 51
Function 3 (F3):  <Esc> O R         Hex: 1B 4F 52
Function 4 (F4):  <Esc> O S         Hex: 1B 4F 53
Function 6 (F6):  <Esc> [ 0 0 6 q   Hex: 1B 5B 30 30 36 71
Function 9 (F9):  <Esc> [ 0 0 9 q   Hex: 1B 5B 30 30 39 71
```

注: 機能キーの定義の中で、次の文字にはそれぞれ次の意味があります。

O = 英大文字の O
0 = 数字のゼロ
すべての文字に大文字小文字の区別がある

複数の端末ユーザー

システム・カード・シリアル・ポートまたは PCMCIA モデム・インターフェースを介して、アクティブ端末コンソールを使用できるのは、一度には一人のユーザーだけです。ワークステーションがシリアル・ポートにローカルで接続されており、コールが PCMCIA モデムを介して着信する場合、そのコールに優先度が与えられます。そのコールの後で、ローカル・ワークステーションのユーザーは再接続することが必要になります。

Telnet のセットアップと使用

Telnet 端末コンソール・アクセスをセットアップする場合は、この節を使用します。

Telnet によってアクセスすることができるのは、メイン命令コード (コマンド行インターフェース) だけであって、ファームウェア・ユーザー・インターフェースにはアクセスできません。コマンド行インターフェースからユニットをリブートした場合は、Telnet 接続が失われるので、ユニットのリブート後、再確立することが必要になります。

構成がまったく行われていないユニットの場合は、ユニットに Telnet でログインするには、デフォルトの SLIP または PCMCIA EtherJet IP アドレスを使用する以外に方法がありません。

SLIP アドレス

PCMCIA モデムまたは外付けモデムで使用するためのデフォルトの SLIP IP アドレスは、次のとおりです。

ワークステーションの場合:
10.1.1.3

ネットワーク・ユーティリティー の場合 :
10.1.1.2

SLIP のインストールに関する説明については、ご使用のバージョンの TCP/IP PC ソフトウェアに関する資料を参照してください。

PCMCIA LAN IP アドレス

PCMCIA EtherJet PC カードで使用するためのデフォルトの IP アドレスは、次のとおりです。

ワークステーションの場合:
10.1.0.3

ネットワーク・ユーティリティー の場合 :
10.1.0.2

これらのアドレスについては、命令コード・コマンド行インターフェースからでも、ファームウェアからでも変更することができます (46ページの『IP の基本的な構成と操作』 に記載されている手順を使用します)。ASCII 端末エミュレーションを使用するか、デフォルトの IP アドレスに Telnet でログインすることによって、まず最初に初期ユーザー・コンソールを始動する必要があります。

ネットワーク・インターフェース IP アドレス

ネットワーク・インターフェース (アダプター・スロットに入っているアダプター上のもの) には、デフォルトの IP アドレスはありません。コマンド行インターフェースと構成プログラムのどちらかを使用して、ネットワーク・インターフェースの IP アドレスを設定します。135ページの『第3部 構成および管理の詳細』 に例として挙げてある構成テーブルのすべてに、インターフェースに対して IP アドレスを設定する方法が示してあります。IP アドレス構成変更をアクティブにしてからでないと、ネットワーク・インターフェースを通して Telnet でログインすることはできません。

IP アドレスは、インターフェースに割り当てるだけでなく、ユニット全体にも割り当てることができます。この IP アドレスは、*内部* IP アドレスと呼ばれているもので、個々のネットワーク・インターフェースの状態とは関係なく、アクティブであり続けます。

モデル TN1 を使用し、TN3270 サーバー機能を使用しようとしている場合は、TN3270 が使用する IP アドレスと TCP ポート番号を構成する必要があります。TN3270 のデフォルトの Telnet ポート番号 23 を受け入れる場合は、TN3270 サーバー用として構成した IP アドレスとは異なる IP アドレスにコンソール Telnet セッションを接続する必要があります。そうすることによって、ユニットではコンソール Telnet セッションと TN3270 クライアント・セッションを区別することができます。

複数の Telnet ユーザー

同時に 2 人のユーザーが、ネットワーク・インターフェースを通して、 Telnet コンソールを始動することができます。 3 人目のユーザーによる Telnet 試行は、最初の 2 人のユーザーのいずれか一方が切断するまでは、リジェクトされることになります。システム・カード・サービス・ポートまたは PCMCIA インターフェースを介して、アクティブ端末コンソールを使用できるのは、SLIP または PCMCIA LAN カードを介する Telnet の場合も含めて、一度には一人のユーザーだけです。

コマンド・プロンプトへのアクセス

ユーザー・コンソールのセットアップが終わったら、メッセージがないかどうか調べ、ここで説明されているコマンド・プロンプトのいずれかにアクセスします。

表示される内容

ネットワーク・ユーティリティーの電源をオンにしてから最初のコマンド・プロンプトが表示されるまで、ユーザー・コンソールがアクティブであれば、次のことに関する一連の通知状況メッセージが表示されます。

- 端末タイプを変更するためのエスケープ
- メモリー初期化
- システム・ボード診断
- その他の診断
- ブートの進行状況 (ファームウェア・メニューを表示させるためにブートを中断する方法を含む)
- ディスクからの命令コードのロード (次のメッセージが表示されて終了)

```
Please press the space bar to obtain the console.

Loading /hd0/sys0/LMX.ld from disk ...
Loading /hd0/sys0/LML.ld from disk ...
Loading /hd0/sys0/sysext.ld from disk ...
Loading /hd0/sys0/diags.ld from disk ...
Loading /hd0/sys0/snmp.ld from disk ...
Loading /hd0/sys0/router.ld from disk ...
Loading /hd0/sys0/appn.ld from disk ...
Loading /hd0/sys0/tn3270e.ld from disk ...

<you press the space bar>
Console granted to this interface
Config (only)>
```

プロンプト Please press the space bar to obtain the console が表示されたら、いつでもスペース・バーを押せば、ネットワーク・ユーティリティー・コンソール・プロセスがセッションに接続されます。システムでは、メッセージ Console granted to this interface によってこのアクションを確認し、コードのロードが完了すると、コマンド・プロンプトを表示します。

まったく構成が行われていないネットワーク・ユーティリティーの場合は、システムが表示するコマンド・プロンプトは Config (only)> になります。したがって、 第3章 初期構成の実行 に記載されている説明どおりに手順を進めれば、ネットワーク・ユーティリティーを構成することができます。構成が十分行われていて、ネットワーク・ユーティリティーが完全に作動可能な状態になっている場合は、システムが表示するコマンド・プロンプトは、アスタリスク (*) になります。

ブート・シーケンス全体からのメッセージをすべて表示できるのは、ASCII 装置が直接接続されている場合だけです。 PCMCIA モデムを介するダイヤルインや Telnet によるログインによってユーザー・コンソールを始動する場合は、少なくとも部分的にブートされるまでは、ネットワーク・ユーティリティーが接続の試みに対して応答することはできません。接続した時点では、ブート・プロセスは後半の段階のいずれかにあるか、完了している可能性があります。ブート・プロセスが完了すると、システムでは即時にコンソール権限を付与し、コマンド・プロンプトを表示します。

ASCII 端末の問題の解決

不要情報やランダム文字が表示されたり、端末がネットワーク・ユーティリティーに接続できなかったりする場合は、サービス・ポートに原因がある可能性があります。不要情報やランダム文字が表示される場合は、最も一般的な原因として、端末のボー・レートがネットワーク・ユーティリティーに同期していないことが考えられます。

ネットワーク・ユーティリティーは、常に特定のボー・レート (デフォルトでは、 19.2 Kbps) に設定されています。このボー・レートを変更する方法は、ファームウェアの使用以外にないので、その変更には、コンソールが正しく作動していることが必要です。したがって、コンソールの画面が読み取れない場合は、読み取れる状況メッセージやコマンド・プロンプトが表示されるようになるまで、ボー・レートを端末側で変更して試行してみます。

その他に接続の問題の原因としては、次のようなことが考えられます。
- シリアル・ケーブル上にヌル・モデムがない。
- 端末またはネットワーク・ユーティリティーの AC 接地に欠陥がある。
- 端末とネットワーク・ユーティリティーの間のケーブルに欠陥やシールド不良があるか、または誤った接地が行われている。
- 端末または端末エミュレーターに欠陥がある。
- ネットワーク・ユーティリティーのシステム・ボードに欠陥がある。

このような問題の処理について詳しくは、*2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual* の「Service Terminal Display Unreadable」の項を参照してください。

Telnet の問題の解決

Telnet の問題として最も一般的なのは、IP ネットワークを通してネットワーク・ユーティリティーに到達できない場合が生じることです。標準的なデバッグ・ツール (PING とトレース・ルート) を使用して、発生している事態を判別できます。ネットワーク・ユーティリティーの内部 IP アドレスへの PING を試みる場合は、そのアドレスへのホスト・ルートを、ネットワーク・ユーティリティーに入る場合に使用するインターフェース IP アドレスをネクスト・ホップとして、ワークステーション内で設定する必要があります。

また、ネットワーク・ユーティリティーからワークステーションへ逆に PING を試みることもできます。ファームウェアには、これを EtherJet または SLIP ポートから行う手段があり、命令コードのコンソール・プロセスには、これをネットワーク・インターフェースから行う手段があります。これらの手順の概要については、46ページの『IP の基本的な構成と操作』 を参照してください。

第3章 初期構成の実行

この章では、ネットワーク・ユーティリティーの構成の基本について説明し、ネットワーク・ユーティリティーを新たに構成する場合の特定の手順を示します。このような手順を実行すると、ネットワーク・ユーティリティーは受動的な状態、つまり構成を待っている状態から、能動的な状態、つまりネットワーク・インターフェースおよびプロトコルがアクティブな状態に移行します。

このような手順を使用するにあたっては、その前に 15ページの『第2章 ユーザー・コンソールの始動』の説明に従って、ユーザー・コンソールを接続しておく必要があります。

構成の基本

ネットワーク・ユーティリティーの構成とは、以下のような要素も含めて、ソフトウェアの動作を制御するデータ項目を集めたものです。

- 起動したいインターフェース
- 始動させたいリンク
- アクティブにしたいプロトコルおよびフィーチャー
- 特定のプロトコルまたはフィーチャーの中でアクティブにしたい機能
- 使用したいネットワークのアドレスと名前

ネットワーク・ユーティリティーをブートすると、システムでは、その構成情報をハード・ディスク上のファイルから読み取り、そのファイルに収められている情報に従って、インターフェースおよびプロトコルを起動します。なお、ファイルの作成は、次のいずれかの方法で行うことができます。

- ユーザー端末コンソールでコマンド行インターフェースを使用する。

  コマンドを入力して、メモリー内に構成データ項目を作成した上で、ネットワーク・ユーティリティーのハード・ディスクに構成を書き込みます。
- 独立型ワークステーションで稼働するグラフィック構成プログラムを使用する。

  ワークステーションで構成を作成してから、それをネットワーク・ユーティリティーのハード・ディスクに転送します。

  ネットワーク・ユーティリティーの構成プログラムは、新しいネットワーク・ユーティリティーのすべてと共に CD-ROM に収め、包装して出荷されますが、Web でのダウンロードも可能です。Windows 95 および Windows NT 用、 AIX 用、および OS/2 用のバージョンが用意されています。ワークステーション要件については、ハードコピーがネットワーク・ユーティリティーに同梱して出荷されている *構成プログラム使用者の手引き* に記載されています。

構成方式の選択

IBM ルーティング製品の場合、構成プログラムを優先するユーザーもあれば、コマンド行インターフェースを選択するユーザーもあり、両方の組み合わせを採用したいと希望するユーザーもあります。どの方法を採用するかは、ユーザーの選択に任されています。

以下は、構成プログラムの選択を優先するユーザーが挙げる要因の一部です。
- 複数のネットワーク・ユーティリティーおよび 2216 用の構成ファイルの集中保守ができる。
- テーブル指向の、直観的なデータ項目の編成が得られる。
- コマンド行方式の場合に比べて、パラメーターの入力妥当性検査および相互チェックが多く行われる。
- 個々のデータ項目に関するオンライン・ヘルプが組み込まれている。

次は、コマンド行インターフェースの選択を優先するユーザーが挙げる要因の一部です。
- 構成、動的再構成、および監視を行うための単一統合方式が得られる。
- 製品資料および IBM 「レッドブック」に記載が豊富である。
- クィック構成変更の実施および試行が簡単である。
- 構成プログラムをインストールする場合に比べて、ユーザー・コンソールのセットアップに必要なワークステーション資源も時間も少なくて済む。

Config-only モードからの開始

ネットワーク・ユーティリティーをブートして、ユーザー・コンソールに `Config (only)>` プロンプトが表示された場合は、config-only モードです。ネットワーク・ユーティリティーがブートして config-only モードになるのは、ハード・ディスク上の現行構成ファイルに、有用な機能を実行する (例えば、データ・パケットを転送する) ことができるデータ項目がない場合です[3]。 ネットワーク・ユーティリティーが始動して通常の作業モードに入るためには、少なくとも 1 つのアダプターと 1 つのプロトコル (例えば、IP、DLSw、または APPN) を構成して、リブートする必要があります。

ネットワーク・ユーティリティーで `Config (only)>` プロンプトが表示されている場合は、以下の処置を実行します。

1. 初期構成にあたってコマンド行を使用するのか、構成プログラムを使用するのかの選択を行います。両方式を試みたければ、方式間の切り替えは後で簡単に行えます。
2. どちらを選択したかに応じて、次の手順のどちらかに従います。
   - 『手順 A: 初期構成用コマンド行手順』
   - 30ページの『手順 B: 構成プログラム 初期構成』

手順 A: 初期構成用コマンド行手順

ネットワーク・ユーティリティーの初めての構成を `Config (only)>` コマンド行プロンプトから開始する場合は、この手順を使用します。

パート 1: 最小基本構成の作成

1. **add device** コマンドを使用して、少なくとも 1 つのネットワーク・インターフェースを次のようにして構成します。

3. また、構成が CORRUPT の場合も同様です。

a. **add dev ?** と入力して、サポートされるアダプターのタイプのリストを表示させます。

b. **add dev** *type* を入力します。ただし、*type* は、アダプター・リスト中のある行の最初の何文字かで構成されます。例えば、**add dev tok** と入力すれば、トークンリング・アダプターが選択されます。構成したいアダプターを固有に識別できる十分な文字数を入力します。

c. スロット番号の入力を指示するプロンプトが出たら、ネットワーク・ユーティリティーの左アダプター・スロットの場合は **1** を、右アダプター・スロットの場合は **2** を入力します。

d. マルチポート・アダプターを追加する場合は、システムではプロンプトを出して、構成したいインターフェースのポート番号の入力を指示します。アダプター上のポート番号は、次のように固定されています。
   - マルチポート LAN アダプター上のポートには、1 および 2 の番号が付けられ、アダプターの表面にラベルがはってあります。
   - マルチポート WAN アダプター上のポートには、0 から始まる番号が付けられ、アダプター・ケーブル端のコネクターにラベルがはってあります。

e. システムでは、次に、論理 *インターフェース番号* (*ネット番号* とも呼ばれる) を割り当てます。これは重要な番号であり、システム内の他のどのコマンドでも、この番号でこのインターフェースを指します。 例えば、このインターフェースの構成を削除したい場合であれば、 **delete interface** と入力した上で、この論理インターフェース番号を指定します。

f. 必要な場合は、デフォルトの入出力装置構成に次のような調整を行います。

   追加したのがトークンリング・ポートで、これをデフォルトの 4 Mbps ではなく、 16 Mbps で稼働させたい場合は、次のようにコマンドを入力します。

   net *interface number*
   speed 16
   exit

   追加したのが 10 Mbps (10/100 ではない) イーサネット・ポートで、デフォルトの RJ45 (10BASET) コネクターではなく、BNC (10BASE2) コネクターを使用したい場合は、次のようにコマンドを入力します。

   net *interface number*
   conn bnc
   exit

以上のステップ 1 は、構成したい各インターフェースごとにそれぞれ繰り返します。

2. 将来、インターフェースを動的に追加する場合に、ネットワーク・ユーティリティーをリブートしなくても済むようにしたければ、`Config (only)>` プロンプトで **set spare** *number* を入力します。ただし、*number* は、リブートをしないで追加できる必要があるインターフェースの最大数です。

3. ″Quick Config″ プログラムを開始する場合は、 **qconfig** コマンドを使用します。このプログラムは、ネットワーク・ユーティリティーへの IP および SNMP アクセスを構成する場合に、次のように使用します。

   Quick Config は、コマンド行構成プロセスのフィーチャーの 1 つです。ユーザーによるコマンドの入力を待つのではなく、ユーザーに質問し、ユーザーの応答に応じて構成データを作成します。 Quick Config の質問の例を下に示します。

```
Configure Bridging? (Yes, No, Quit): [Yes]
```

小括弧で囲まれている値は、応答として使用できる値です。大括弧内の値はデフォルトの応答です。デフォルト値を受け入れる場合は、**Enter** を押します。

Quick Config の質問には、次のように応答します (応答の一部はデフォルトの応答になっています)。

a. `Configure Bridging?` に **no** と応答して、ブリッジングを構成します。

b. `Configure Protocols?` に **yes** と応答して、プロトコルを構成します。

c. 次のようにして、IP を構成します。

   1) `Configure IP?` に対して **yes** と入力する。

   2) IP アドレスを割り当てたいインターフェースの場合は、 `Configure IP on this interface?` に **yes** と応答する。 PCMCIA EtherJet カードを唯一の IP インターフェースとして使用する予定の場合は、構成済みネットワーク・インターフェースのいずれについても、すべて **no** と応答します。

   3) `IP Address` プロンプトに、IP アドレスを入力します。

   4) `Address Mask` プロンプトに、IP マスクを入力します。

   5) RIP または OSPF を使用可能にしたい場合は、`Enable Dynamic Routing?` に **yes** と応答し、後続の関連質問に応答します。

   6) ある時点で、構成プログラムからこのネットワーク・ユーティリティーに構成を直接送信したいと考える可能性がある場合は、`Define Community with Read_Write_Trap Access?` に対して **yes** と応答し、コミュニティー名にしたい任意の 1 ワードの名前を入力します。

      構成プログラムの使用をまったく予定していない場合は、**no** と応答します。

   7) `Save this configuration?` に **yes** と応答します。こうすれば、構成の IP 部分がメモリーに保管されます。

d. `Do you want to write this configuration?` に対して **yes** と応答して、構成ファイルを保管します。

パート 2: 新規構成の起動

以上で、少なくとも 1 つのインターフェースと 1 つのプロトコル (IP、および SNMP) が構成されました。これはわずかな構成ですが、config-only モードを終了するにはこれで十分です。

1. `Config (only)>` プロンプトで **reload** と入力し、確認プロンプトに対して **yes** と応答します。ネットワーク・ユーティリティーがリブートし、新規構成が起動します。

   構成変更の保管に関するプロンプトがここで表示されたとしたら、この手順のパート 1 の完了時に構成ファイルを保管した後で、構成変更を行ったことを意味します。したがって、**yes** と入力して、リブートが行われる前に、このような変更を新規構成の一部として保管します。

2. ネットワーク・ユーティリティーのリブートを確認します。

ユーザー・コンソールでダイヤル接続や Telnet 接続を使用している場合は、リブートによって接続が失われます。したがって、数分後に再接続してください。それ以外の場合は、コンソールからのブート・メッセージに注意します。

リブートが完了すると、コンソールには * コマンド・プロンプトが表示されるはずです。これは、通常の操作モードに入っており、config-only モードではなくなっていることを示しています。この手順のパート 1 で作成した構成は、これでアクティブになりました。

パート 3 - 追加のプロトコル情報の追加

以上で、インターフェースが構成されて、通常の操作モードに入り、 IP だけが稼働しています。

この製品を使用するのが初めてで、他の機能 (例えば、TN3270 や DLSw など) を構成する前に、この製品に精通しておきたいと考える場合は、この手順の残りの部分を飛ばして、34ページの『次に行うこと』に記載されているガイドラインをごらんください。

すべての機能をここで構成してしまいたい場合は、以下を続けます。

1. ユーザーがこのネットワーク・ユーティリティーを使用しようとしている場合に最もよく似た構成事例を 135ページの『第3部 構成および管理の詳細』から選択します。
   - モデル TN1 のユーザーの場合 - 145ページの『第12章 TN3270E サーバー』を参照してください。
   - モデル TX1 のユーザーの場合 - 229ページの『第14章 チャネル・ゲートウェイ』、 271ページの『第16章 データ・リンク交換』、または 313ページの『第19章 VPN (仮想私設ネットワーク)』 をごらんください。

   これらの事例のいずれも適切でない場合は、*MAS プロトコル構成と監視解説書*、*MAS フィーチャーの使用と構成*、および *MAS ソフトウェア使用者の手引き* を使用して、構成の必要があるものを判別してください。
2. 選択した事例の後の「構成例の詳細」の章で、その事例に対応する構成パラメーター表を探します。[4] 「コマンド行コマンド」欄を指針として、その事例を構成し、ユーザーの場合に特定のアダプターおよびネットワークに応じて値を変更します。

   コマンド行のナビゲーションおよびコマンドの入力が円滑に行えなかったりすると、先に進む前に、一般的なコマンド行構成にさらに詳しくなる必要性を感じる場合があります。そのような場合は、34ページの『次に行うこと』を参照して、ヒントをつかんでください。
3. 構成コマンドの入力が完了したら、28ページの『パート 2: 新規構成の起動』の手順を繰り返します。ただし、**reload** コマンドは、`Config (only)>` プロンプトではなく、 * プロンプトから出します。

4. 対応する表がない場合は、その事例に関する「構成のかぎ」の項を使用して開始します。

手順 B: 構成プログラム 初期構成

ネットワーク・ユーティリティー 構成プログラムを使用して初めてネットワーク・ユーティリティーを構成する場合は、この手順を使用します。

パート 1: 構成プログラムでの構成の作成

1. 構成プログラム CD-ROM から、該当するバージョンの構成プログラムをワークステーションにインストールします。

   インストールの方法については、下記のものを参照してください。
   - CD-ROM に入っている ネットワーク・ユーティリティー README ファイル
   - CD-ROM と一緒に出荷されている *構成プログラム使用者の手引き*

   構成プログラムを開始します。スクラッチから新規構成を行うことによってプログラムを試行したい場合は、ナビゲーション・ウィンドウのメニュー・バーの **Configure** オプションから **New configuration** と **Network Utility** を選択します。
2. ユーザーがこのネットワーク・ユーティリティーを使用しようとしている場合に最もよく似た構成事例を 135ページの『第3部 構成および管理の詳細』から選択します。

   - モデル TN1 のユーザーの場合 - 145ページの『第12章 TN3270E サーバー』を参照してください。

   - モデル TX1 のユーザーの場合 - 229ページの『第14章 チャネル・ゲートウェイ』、 271ページの『第16章 データ・リンク交換』、または 313ページの『第19章 VPN (仮想私設ネットワーク)』をごらんください。

   これらの事例のいずれも適切でない場合は、*MAS プロトコル構成と監視解説書*、*MAS フィーチャーの使用と構成*、および *MAS ソフトウェア使用者の手引き* の資料を使用して、構成の必要があるものを判別してください。コマンド行コマンドと構成プログラムのパネルとのマッピングの例として、 135ページの『第3部 構成および管理の詳細』の構成パラメーター表のいずれかを使用します。構成が完了したら、31ページの7 に跳びます。
3. 選択した事例の後の「構成例の詳細」の章で、その事例に対応する構成パラメーター表を探します。[4]
4. Web ブラウザーで、メイン・ネットワーク・ユーティリティー Web ページ

   `http://www.networking.ibm.com/networkutility`

   からの `Support and Downloads` リンクに従い、選択した事例にマッチする構成ファイル例を探します。このファイルをバイナリーでダウンロードし、構成プログラムが稼働しているワークステーションに転送します。
5. ナビゲーション・ウィンドウから「**Open Configuration ...**」を選択し、ダウンロードした構成ファイル例のパス名とファイル名を選択します。
6. ステップ 3 の表の「″構成プログラム・ナビゲーション」および「構成プログラム値」の欄を指針として使用し、構成全般にわたって移動し、ユーザーの場合に特定のアダプターおよびネットワークに応じて値を変更します。

7. 構成がネットワーク・ユーティリティーに送信できる準備ができたら、「**Save configuration as ...**」を選択して、ワークステーションに構成を保管します。 新しい名前を選択して、元の構成ファイル例は変更しないでおくこともできます。

パート 2: ネットワーク・ユーティリティーへの構成の転送とその起動

以上で初期構成は作成されました。後は、構成をネットワーク・ユーティリティーのハード・ディスクに転送し、ネットワーク・ユーティリティーをリブートして構成を起動するだけです。この転送方法は、次のように、接続の設定によって異なります。

- 構成プログラム・ワークステーションが TCP/IP をサポートし、ネットワーク・ユーティリティーの PCMCIA EtherJet カードとネットワーク・アダプター (スロット 1 または 2 の) のどちらかへの物理接続がある場合は、手順 A を使用します。
- ユーザー・コンソールで ASCII 端末エミュレーションが使用され、上記の IP 接続を設定するよりも、Xmodem の使用を優先する場合は、手順 B を使用します。

91ページの『新規構成ファイルのロード』をごらんになれば、構成をネットワーク・ユーティリティーに転送する方法を網羅したリストが記載されています。手順 A にも B にも従わない方法を選択した場合は、 TCP/IP ワークステーションに TFTP サーバー・ソフトウェアが必要になります。

手順 A: ネットワーク・ユーティリティー PCMCIA EtherJet またはネットワーク・アダプターによる直接転送

構成プログラム・ワークステーションが TCP/IP をサポートし、ネットワーク・ユーティリティーの PCMCIA EtherJet カードとネットワーク・アダプター (スロット 1 または 2 の) のどちらかへの物理接続がある場合は、この手順を使用します。

1. コマンド行からネットワーク・ユーティリティーをクィック構成して、少なくとも 1 つのインターフェース上には IP アドレスがあり、IP および SNMP が使用可能になっているようにします。
   a. ユーザー・コンソールで 26ページの『パート 1: 最小基本構成の作成』のステップを実行します。必ず次のようにしてください。
      1) **add device** を使用して、スロット 1 または 2 に少なくとも 1 つのインターフェースを定義する。
      2) Quick Config で、`Define Community with Read_Write_Trap Access?` に **yes** と応答する。
   b. 構成プログラムの中で、送信しようとしている構成で、SNMP が使用可能にされ、同じコミュニティー名が「読み取り/書き込みトラップ」アクセスで定義されていることを確認します。この構成を起動した後で、この手順のステップ 32ページの3 を繰り返して別の構成を送信できるようにするには、こうなっていることが必要です。
   c. 28ページの『パート 2: 新規構成の起動』のステップを実行して、ネットワーク・ユーティリティーをリブートし、この一時コマンド行構成を起動します。
2. PCMCIA EtherJet カードの使用を計画している場合は、ネットワーク・ユーティリティーのリブートの完了後に、次のようにしてその IP アドレスを設定します。

* プロンプトで、**talk 6** と入力します。Config> プロンプトで、**system set ip** と入力し、プロンプトの指示に従って次の値を入力します。
- IP アドレス : EtherJet カード用として使用したい IP アドレス
- ネットマスク : EtherJet カードに接続されているサブネット用のマスク
- ゲートウェイ・アドレス : 構成プログラム・ワークステーションの IP アドレス、またはネットワーク・ユーティリティーがあるルーターに到達する場合に使用できるそのルーターの IP アドレス

それぞれのプロンプトの横には、システムによって、現行値がデフォルト値として表示されます。デフォルト値を受け入れる場合は、**Enter** を押します。値をすべて入力し終えると、指定したアドレス変更はいずれも即時に有効となります。値はネットワーク・ユーティリティーの NVRAM に保管されますが、どの構成ファイルの一部ともなりません。

3. 次のようにして、構成プログラムから構成を送信します (SNMP を使用)。
   a. 「**Configure**」ドロップダウン・メニューで、「**Communications**」と「**Single router**」を選択します。
   b. 「Communicate」パネルで、次の入力を行います。
      - IP アドレスまたは名前 : 構成の送信に使用したいネットワーク・ユーティリティー・インターフェースの IP アドレス。PCMCIA EtherJet IP アドレスと、Quick Config で割り当てたネットワーク・インターフェース IP アドレスのどちらかです。
      - コミュニティー : Quick Config で割り当てたコミュニティー名
   c. 「**Send configuration**」と「**Restart router**」を選択します。現在の日付と時刻を受け入れるか、または入力して、ネットワーク・ユーティリティーが新規構成の受信後ただちに新規構成でリブートするようにします。
   d. **OK** をクリックします。構成プログラムは、SNMP を使用して、指定されたルーターへの構成データ項目の送信を即時に開始します。

      構成プログラムでは、転送に関する状況メッセージおよび結果メッセージを出します。送信動作が正常に行われなかった場合は、考えられる理由が、構成プログラムによって示されるので、それを調べて訂正します。

   構成プログラムがその構成の転送を完了すると、ネットワーク・ユーティリティーはハード・ディスクに構成を保管し、指示に従って自動的にリブートします。
4. ネットワーク・ユーティリティーのリブートを確認します。

   ユーザー・コンソールでダイヤル接続や Telnet 接続を使用している場合は、リブートによって接続が失われます。したがって、数分後に再接続してください。それ以外の場合は、ユーザー・コンソールからのブート・メッセージに注意します。

   リブートが完了すると、コンソールには * コマンド・プロンプトが表示されるはずです。これは、通常の操作モードに入っており、config-only モードではなくなっていることを示しています。この手順のパート 1 で作成した構成は、これでアクティブになりました。

手順 B: ユーザー・コンソール・セッションを介する間接 Xmodem 転送

コンソールで ASCII 端末エミュレーションが使用され、構成プログラム・ワークステーションからの IP 接続を設定するよりも、Xmodem の使用を優先する場合は、この手順を使用します。

1. 構成プログラムから、構成をネットワーク・ユーティリティーが理解しているファイル形式にエクスポートします。

   Configure ドロップダウン・メニューで、「**Create router configuration**」を選択し、.CFG ファイルのパス名とファイル名を指定します。**OK** をクリックして、ファイルに書き込みます。

2. 必要な場合は、構成プログラム・ワークステーションから端末エミュレーション・ワークステーションに .CFG ファイルを転送します。

3. コンソールの `Config (only)>` プロンプトで、以下の順序に従います。

   ```
   Config (only)>boot
   Boot configuration
   Boot config>dis auto
   Select the duration to disable autoboot: (once, always): [always] once
   AutoBoot mode is now disabled once.

   Operation completed successfully.
   Boot config>exit
   Config (only)>rel y
   ```

   構成変更の保管に関するプロンプトが出た場合は、 **no** と応答します。ネットワーク・ユーティリティーがリブートし、ファームウェア・メニューが表示されたところで停止します。

   ユーザー・コンソールでダイヤル接続を使用している場合は、リブートによって接続が失われます。数分後に再接続すると、ファームウェア・メニューが表示されます。

4. 次の順序で一連のファームウェア・メニュー選択を行います。
   a. システム管理サービス (メインメニュー) : オプション 4 「**Utilities**」
   b. システム管理ユーティリティー : オプション 12 「**Change Management**」
   c. 変更管理ソフトウェア制御 : オプション 12 「**Xmodem software**」
   d. タイプ選択 : 「**Config**」
   e. バンク選択 : 「**Bank A**」(アクティブ・バンク) を選択
   f. Config を選択 : 位置「**1**」を選択[5]

   ファームウェアによって、ファイル転送の開始時点が通知されます。

5. 端末エミュレーション・パッケージを表示し、任意の名前を使用して、ワークステーション・サーバーからファイルの転送を開始します。ネットワーク・ユーティリティーが構成ファイルを受信すると、ファイル位置の状況が CORRUPT から AVAIL に変更されます。この確認は、ファームウェアの「Change Management」メニューでオプション 7 の「**List Software**」を使用して行うことができます。

6. ロードしたばかりの構成を使用するネットワーク・ユーティリティーをブートします。
   a. オプション 9 の「**Set Boot Information**」を使用して、現行命令コード・バンクおよび新規構成を選択します。
   b. **Esc** を押して、メインメニューが表示されたら、 **F9** (OS 開始) を押して、新規構成のネットワーク・ユーティリティーをブートします。

7. ネットワーク・ユーティリティーのブートを確認します。

---

5. このようにバンクと構成ファイル位置を選択するのは、このネットワーク・ユーティリティーの初回のブートであることが前提になっています。このトピックの詳細な背景については、 80ページの『ディスク上の構成ファイル』 を参照してください。

ユーザー・コンソールでダイヤル接続を使用している場合でも、「OS 開始」オプションを使用すれば、接続が失われることはありません。コンソールからのブート・メッセージに注意します。

ブートが完了すると、コンソールには * コマンド・プロンプトが表示されるはずです。これは、通常の操作モードに入っており、config-only モードではなくなっていることを示しています。この手順のパート 1 で作成した構成は、これでアクティブになりました。

次に行うこと

この章の手順に従ってここまで来ると、ネットワーク・ユーティリティーは作成した構成を備えて、完全な操作モードに入っています。ユーザー・コンソールには * プロンプトが表示されているので、コマンド行インターフェースを使用して、次のことを行える状態になっています。

- インターフェースおよびプロトコルの状況を照会する。
- イベントの起動およびイベント・ログの監視を行う。
- オペレーター・コマンドを発行して状況変更を実施する。
- リブートを伴わないで動的変更を実行する。

これらは、新規構成が適正に働いているかどうかを確認し、新規構成に細かい調整を施すための手段です。

コマンド行インターフェースを使用するのが初めてである場合は、 57ページの『第5章 コマンド行インターフェースの解説』 を使用すれば、その概念および使用法に詳しくなることができます。

IBM ルーティング製品に多少なりとも経験があり、チュートリアルどおりに学習するよりもタスクを試みたいと考える場合は、37ページの『第4章 ユーザー・インターフェースのクィック・リファレンス』 は、コマンド行ナビゲーションおよび一部の一般的なタスクに関する概要情報として使用することができます。

第 6 章 ～ 第 10 章を使用すれば、下記に関する詳細な背景情報が得られます。

- 構成ファイルの管理
- 動的再構成
- ネットワーク・ユーティリティーによって行われることをローカルで、またはリモート・ネットワーク管理プロダクトを使用して管理
- ソフトウェアおよびファームウェアの更新
- サービスおよびサポートの要求

135ページの『第3部 構成および管理の詳細』 の構成例情報をすでにご使用になっている場合もあると思われます。 その各章には、次の機能の構成および管理に関する紹介情報も記載されています。

- TN3270E サーバー
- チャネル・ゲートウェイ
- データ・リンク交換
- 仮想私設ネットワーク

初期構成ですでにこれらの機能のいずれかの構成を行っている場合は、該当する章の「管理」の項を使用して、その構成の監視およびデバッグを行います。

第4章 ユーザー・インターフェースのクィック・リファレンス

この章には、コマンド行インターフェースのナビゲーション、コマンドの入力、および一般的なタスクの実行に関する概要情報が記載してあります。例示による詳細な説明については、57ページの『第5章 コマンド行インターフェースの解説』を参照してください。

ナビゲーション

コマンド行インターフェースは、アスタリスク (*) プロンプトをルートとするメニューのツリーで構成されています。コマンドの入力および制御キーの使用によってツリー内のさまざまな個所に移動した上で、コマンドを入力して実際にタスクを実行します。

プロセスとプロンプト

* プロンプトで、 **talk** コマンド (**t** と略記する) を使用して、プロセス、つまりシステムを表示させて見る方法の 1 つに接続します。コマンドを入力できる各プロセスは、それぞれ異なるコマンド・プロンプトで識別されています。

表 3. 主要プロセス

名前	アクセスするためのコマンド	目的	最上位プロンプト
構成	**t 6** または **config**	構成の表示および変更	`Config>`
コンソール	**t 5** または **console**	稼働状況の表示および制御、構成変更の実施	+ (正符号)
モニター	**t 2** または **event**	リアルタイム・イベント・メッセージ・ログの表示	(なし)

t *n* を入力して、 **Enter** を 2 回押すと、コマンド・プロンプトが表示されます。どのプロセスに入っている場合でも、その中で **Ctrl-p** を押せば、* プロンプトに戻ります。

モニター・プロセスにはコマンド・プロンプトはありません。このプロセスでは、コマンドは出さないで、イベント・メッセージの実行ログを監視するからです。 **Ctrl-s** を押せば、スクロールが一時停止し、 **Ctrl-q** を押せば、再開されます。

サブプロセス

talk 6 または talk 5 プロセス内での作業時に、コマンドによっては、入力プロンプトが変わり、ある機能エリアに特有の新しいコマンド・メニューが表示される場合があります。次にその例を挙げます。

- talk 6 のもとで **protocol dlsw** と入力すると、データ・リンク交換を構成するための Config サブプロセスに移動し、コマンド・プロンプトが `DLSw config>` になります。

- talk 5 のもとで **perf** と入力すると、CPU 使用状況統計を表示するためのコンソール・サブプロセスに移動し、コマンド・プロンプトが PERF Console> になります。

また、サブプロセス間で移動することもできます。例えば、 DLSw Config サブプロセスで **ban** と入力すると、境界アクセス・ノード構成サブプロセスに移動します。この場合は、メニュー・システム内でネスト・レベルが 1 つ深くなりましたので、戻る場合は、DLSw サブプロセスを経由する必要があります。

次のようなナビゲーション・ルールが適用されます。

- サブプロセスに入る場合は、そこに導いてくれる特定のコマンドを入力します。どのメニューでも **?** を入力すれば、使用可能コマンドを表示させて見ることができます。コマンド・プロンプトが変われば、サブプロセスに入ったことが分かります。
- どのサブプロセスにある場合でも、そこを終了して、レベルが一段高い次のメニューに戻るには、**exit** と入力します。
- また、どのサブプロセスにある場合でも、そこを終了して、* プロンプトに直接移動するには、**Ctrl-p** を押します。この場合は、現行プロセスからも出ることになります。
- **Ctrl-p** を押した後でサブプロセスを再開する場合は、**t** *n* (ただし、*n* は、終了したプロセスの番号) を入力した上で、**Enter** を 2 回押します。これで、 **Ctrl-p** を押した時点で入っていたサブプロセス内でプロセスが再開されます。

コマンドの入力

プロセスに入る場合、サブプロセスに入る場合とそこから出る場合、およびタスクを実行する場合は、コマンドを入力します。タスク・コマンドの場合は、プロンプトが出てパラメーター値の入力を指示されるものもあれば、コマンド名以外の入力は必要としないものもあります。

コマンドの形成

コマンドとは、1 つまたは複数のキーワードを並べたもので、コマンド行に入力したパラメーター値が、その後に続く場合も続かない場合もあります。コマンドの形成には、以下のガイドラインが適用されます。

- 完全なコマンドを入力してからでないと、システムがアクションを起こしたり、入力パラメーターの入力を指示するプロンプトを出すことはありません。有効なコマンドの一部しか入力しなかった (キーワードが十分でない) 場合は、システムが Command not fully specified と応答します。
- どのプロセス・プロンプトやサブプロセス・プロンプトに対しても、あるいはどんなに不完全なコマンドの後にでも、**?** を入力すれば、それぞれそこで使用可能なコマンド・キーワードのメニューが表示されます。したがって、これを使用すれば、下に省略して示してある例のように、コマンドを見付けたり完成したりすることができます。

```
Config>?
ADD (device, user)
BOOT and load file functions
CHANGE (device, password, user)
  ...             < other commands not shown>
```

```
Config>add
Command not fully specified
Config>add ?
DEVICE
NAMED-PROFILE
PPP-USER
TUNNEL-PROFILE
USER
Config>add user
Enter user name:  []?  <enter>
No user was added
Config>
```

上の例で、**add** では、完全なコマンドではありませんでしたが、**add user** で完全になりました。ユーザーが完全なコマンドを入力すると、システムがプロンプトを出して入力パラメーター値の入力を指示しています。

- ほとんどのコマンド・キーワードについては、表示されているメニューでそれが固有に選択できる最小文字数まで略記できます。例えば、 **talk 6** の代わりに **t 6** と入力したり、**protocol appn** の代わりに **p appn** と入力することができます。上記の例では、ユーザーは、**add user** と入力していますが、その代わりに **a u** と入力してもよかったのです。
- talk 6 と talk 5 の両方で、前に入力してあったコマンドについては、下記のキーを使用して次のように処理することができます。

  Ctrl-B 前に入力したコマンドを後方にスクロールする。

  Ctrl-F 前に入力したコマンドのリストを前方にスクロールする。

  Ctrl-U コマンドを検索してコマンド行から消去する。

  Backspace
  コマンドを検索して末尾から編集する。

  コマンド履歴バッファーは、talk 6 と talk 5 の共用になっています。

自動コマンド完成機能

ネットワーク・ユーティリティーでは、MAS V3.3 以降、ユーザーがキーワードを入力すると、それを自動的にコマンドとして完成し、選択可能なメニュー・オプションを表示することで、ユーザーによるコマンドの形成を補助できるようになりました。この自動コマンド完成機能は、コマンド行と構成プログラムのどちらかを使用して、使用不可または使用可能か使用不可に構成します。自動コマンド完成機能は、新規 MAS V3.3 構成の開始時には、デフォルトで使用可能になっていますが、既存の構成をアップグレードした場合は、デフォルトでは使用不可です。新規ユーザーの場合は、自動コマンド完成機能を使用可能にして使用する (**Config (only)>** プロンプトと **Config>** プロンプトのどちらかで、**enable command** と入力する) ことをお勧めします。

自動コマンド完成機能の振る舞いを理解するために、次のコマンドが下に示すメニュー・コンテキストで使用できるものとします (ただし、これはメニュー例に過ぎません)。

enable auto-refresh

caching

| **set** cache-size
| cache-timeout
| priority

- **ena** と入力して、スペース・バーを押すと、コマンドが完全な形で **ENABLE** と表示されます。そこで、**?** を入力すると、使用可能にできる項目 (**auto-refresh** と **caching**) が一覧表示され、コマンド **ENABLE**はコマンド行にそのまま表示されています。
- **ena** と入力して、**Enter** を押した場合は、コマンドの指定が不完全であることを示すメッセージが出力され、使用可能にできる項目 (**auto-refresh** と **caching**) が一覧表示され、コマンド **ENABLE** はコマンド行にそのまま表示されています。
- **ENABLE** コマンドでは、使用可能にできる項目が 1 つ必要であるため、コマンド完成候補の一覧表の左側欄外に『...』を付けて表示され、そのコマンドについてさらに入力が必要であることが示されます。
- 入力が複数のコマンドに一致する場合は、完成候補の一覧表が表示されます。改行後のコマンド行での入力は、最も長い共通接頭部に拡張されます。例えば、**set ca** と入力して、スペース・バーを押すと、**CACHE-SIZE** と **CACHE-TIMEOUT** が表示され、『cache-』が両方の完成候補に共通なので、改行後のコマンド行は **SET cache-** に拡張されます。そこで、英字『s』か英字『t』を入力して、完成候補が ″size″ なのか ″timeout″ なのかを区別する必要があります。
- 共通コマンドでは、表示される形式が代替できる場合があります (**SHOW**、**DISPLAY**、**LIST**)。共通コマンドの 1 つ (例えば、**SHOW**) で、自動コマンド完成機能が一致を見つけられない場合は、代替コマンド **DISPLAY** か **LIST** (もし見つかれば) が表示されます。
- 1 つのコマンド (および、代替コマンド) の検索によって一致が見つからない場合は、入力の一部を使用して、完成候補の一覧表が表示されます。例えば、**enable** と入力し、その後に続けてスペース・バーを押した場合は、**ena** によって置き換えられ、**ENABLE** が完成候補として表示されます。
- コマンド候補の一覧表が表示されたら、現行コマンド行でタブ・キーを使用してコマンドを一度に 1 つずつ順繰りに検討できます。表示されているコマンドから選択する場合は、スペース・バーか Enter キーを使用します。

自動コマンド完成機能に関する包括的なオンライン・ヘルプが必要な場合は、コマンド・プロンプトで **<esc> ?** と入力します。

コマンドのパラメーター値の入力

タスクを実行するコマンドの一部には、入力パラメーターの値を指定する必要があるものがあります。このような入力パラメーター値については、システムにプロンプトを出させてから入力してもよいし、(ほとんどの場合) 前もってコマンド名の後に続けて、コマンド行に入力しておくこともできます。

前もってパラメーター値を入力しない場合 :

- コマンド名だけを入力して、**Enter** を押します。

- システムがそれぞれのパラメーターごとにプロンプトを出し、そのパラメーターのデフォルト値を大括弧で囲んで示します。デフォルト値は、固定されているものもありますが、大部分は該当のパラメーターに対してユーザーが直前に割り当てた値です。
  - デフォルト値を受け入れる場合は、**Enter** を押します。
  - 新しい値を指定する場合は、その値を入力して、**Enter** を押します。
  - 左右の大括弧が [] のようにくっついている場合は、デフォルト値がないので、値を指定する必要があります。

  システムでは、ユーザーの応答について妥当性検査を実行してから、次の値の入力を指示するプロンプトを出します。
- 最終のパラメーター・プロンプトに対するユーザーの応答が終わると、システムはコマンドで指定されたアクションを実行します。

前もってパラメーター値を入力する場合 :

- コマンド名と、その後に続けて 1 つまたは複数のパラメーター値をブランクで区切って入力して、**Enter** を押します。
- システムでは、コマンド行を解析して、最初の値は最初のパラメーターに、 2 番目の値は 2 番目のパラメーターにというように割り当てていきます。したがって、値を指定するにあたっては、この予測に応じた順序で指定する必要があります。

  システムでは、それぞれの値を対応するパラメーターに割り当てながら、妥当性検査を実行します。
- ユーザーが値を指定したパラメーターより多くのパラメーターが必要なコマンドの場合は、上記の場合と同じように、システムはプロンプトを出して、追加の値の入力を指示します。
- システムでは、各パラメーターにそれぞれ値を割り当てると、コマンドによって指定されたアクションを実行します。

経験の豊かなユーザーであれば、前もって値を入力しておく方が手っ取り早く便利です。ただし、有効なパラメーターを正しい順序で指定するよう注意する必要があります。

警戒が必要な場合として、完全なコマンドの後に続けて **?** を入力し、コマンドがこれを最初の入力パラメーターの値として前もって入力された値として扱う場合があります。このような事態が生じた場合は、コマンドを打ち切るか取り消して、あらためて試みます。

一般的なエラー・メッセージ

42ページの表4 には、コマンド行インターフェースからの標準的なエラー・メッセージが説明してあります。

表 4. エラー・メッセージと訂正処置

エラー・メッセージ	説明および訂正処置
`Command error`	入力したコマンドが、現行メニューにありません。入力したコマンドが、タイプミスであったか、ここでは出せないコマンドであったか、文字数の不足でメニューの中から識別できなかったかいずれかです。 プロンプトを調べて現在の場所を確認し、**?** と入力して、使用可能コマンドを表示させて見ます。コマンドを訂正するか、正しい場所に移動します。
`Command not fully specified`	入力したコマンド・キーワードでは、完全なコマンドが形成されていません。 **Ctrl-b** を押してコマンドを検索した上で、その末尾に「 **?**」を追加して、次のキーワードとしての選択対象を調べます。追加する次のキーワードを選択したら、 **?** をそのキーワードで置き換えて、コマンドを発行し直します。 入力を試みているコマンドについて、該当する MAS コマンド行の解説書を参照することもお勧めです。
`Command syntax error`	コマンドは有効でも、入力の形式に誤りがありました。指定したパラメーターが無効または予期しないものであった可能性があります。 パラメーター値を指定しないで、あらためてコマンドを試行してみるか、 MAS コマンド行の解説書の該当する項目を参照してください。
`Feature <name> available but not enabled`	talk 5 のもとにあって、コンソール・サブプロセスに入ろうと試みたフィーチャーが、ソフトウェア・ロードではサポートされているが、アクティブな状態で稼働していません。現行構成で該当のフィーチャーが使用可能にされていないか、そのフィーチャーを起動するために必要なキー値が欠落しているかいずれかです。 構成プログラムを使用している場合は、必要なパラメーターが設定されていないことを示す **?** がナビゲーション・パネル上にないかどうか探します。設定されていないフィールド名が赤く表示されているパネル (複数の場合もある) が表示されるまで、**?** 証跡を追跡します。 構成をコマンド行から行っている場合は、本書に記載されている構成例、および MAS の解説書の該当のフィーチャーに関する章に示されている構成例を参照してください。機能を使用可能にするための基本パラメーターとして示されているキー・パラメーターを探します。
`Protocol <name> available but not configured`	上記の `Feature available but not enabled` の場合と同じですが、対象がフィーチャーでなくプロトコルです。

主要なユーザー・タスク

ここでは、一般的なユーザー・タスクをグループ別に編成し、それぞれのタスクを実行するためのコマンドのクィック・リファレンスを表にして示してあります。

物理アダプターおよびインターフェースの構成

表5 には、物理アダプターおよびインターフェースの構成に関連するタスクの実行方法が記載してあります。

表 5. 物理アダプターおよびインターフェースの構成方法

タスク	タスクの実行方法
初期構成でインターフェースを追加する。	1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. **add dev ?** と入力して、サポートされるアダプターのタイプのリストを表示させます。 3. **add dev** *type* を入力します。ただし、*type* は、リストの中にあって必要なアダプター・タイプを表すキーワードです。 4. 構成しようとしているインターフェースの物理スロットおよびポート番号 (ただし、ある場合) を入力します。スロットは、左から 1 と 2 という番号が付いています。LAN ポートの番号は、アダプター表面に示されており、 WAN ポートの番号は、ケーブル・コネクター上に示されています。 5. ネットワーク・ユーティリティーがこのインターフェースに割り当てる論理インターフェース (ネットワーク) 番号を書き留めておきます。 6. **net** *logical interface number* を入力して、特定のインターフェース・タイプに関する Config (構成) サブプロセスに入ります。そのサブプロセスでのコマンドを使用して、該当のインターフェースに関するデフォルト設定を確認または変更します。 7. **exit** と入力して、Config> プロンプトに戻ります。 8. **write** と入力してこの構成を保管した上で、 **reload** に続けて **yes** と入力して、その構成でリブートします。
初期構成後にインターフェースの動的追加を使用可能にする。	インターフェースを動的に追加する場合は、アクティブ ネットワーク・ユーティリティー構成であらかじめ「スペア・インターフェース」が定義されている必要があります。 1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. **set spare** と入力し、必要なスペア・インターフェースの数を入力します。 3. **write** と入力してこの構成を保管した上で、 **reload** に続けて **yes** と入力して、その構成でリブートします。

表 5. 物理アダプターおよびインターフェースの構成方法 (続き)

タスク	タスクの実行方法
初期構成後にインターフェースを動的に追加する。	1. スペア・インターフェースがアクティブになっていることを確認します。 a. * プロンプトで **talk 5** と入力し、**Enter** を 2 回押して、+ プロンプトにアクセスします。 b. **int** と入力し、NULL インターフェースがあることを確認します。 c. **Ctrl-p** を押して、* プロンプトに戻ります。 スペア・インターフェースがない場合は、上記の手順に従ってスペア・インターフェースを構成に追加し、リブートします。 2. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 3. **add dev** および **net** コマンドを使用して、初期構成手順に記載されているように、新しいインターフェースを構成します。 **add dev** コマンドによって割り当てられた新しい論理インターフェース番号を書き留めておきます。 4. **protocol** および **feature** コマンドを使用して、 Config (構成) サブプロセスに移動し、新しいインターフェースに関するプロトコル情報を構成します。 5. **Ctrl-p** を押し、**talk 5** と入力し、**Enter** を 2 回押して + プロンプトにアクセスします。 6. **activate int** と入力し、新しい論理インターフェース番号を指定します。システムによって新しいインターフェースが動的に起動されます。 7. 新しいインターフェース構成を保管して、リブートしても消えないようにしたい場合は、talk 6 に戻り、**write** と入力して、変更後の構成をディスクに書き込みます。または、対応する変更を構成プログラムで行い、改訂後の構成をネットワーク・ユーティリティーにダウンロードします。
インターフェース構成を動的に変更する。	1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. **list dev** と入力して、変更したいインターフェースのインターフェース番号を表示させます。 3. **net** *logical interface number* を入力して、特定のインターフェースに関する Config (構成) サブプロセスに入ります。インターフェースの構成を変更するためのコマンドを入力します。**exit** と入力して、Config> プロンプトに戻ります。 4. **protocol** および **feature** コマンドを使用して、プロトコルおよびフィーチャー構成サブプロセスにアクセスします。インターフェースに関連するパラメーターを変更するためのコマンドを入力します。 5. **Ctrl-p** を押し、**talk 5** と入力し、**Enter** を 2 回押して + プロンプトにアクセスします。 6. **reset** と入力し、再構成したばかりのインターフェースの論理番号を入力します。 ネットワーク・ユーティリティーがインターフェースをいったんダウンにし、変更後の構成を使用してアップに戻します。 7. これらの構成を保管して、リブートしても消えないようにしたい場合は、talk 6 に戻り、**write** と入力して、変更後の構成をディスクに書き込みます。または、対応する変更を構成プログラムで行い、改訂後の構成をネットワーク・ユーティリティーにダウンロードします。

物理アダプターおよびインターフェースの管理

表6 には、物理アダプターおよびインターフェースの管理に関連するタスクの実行方法が記載してあります。

表 6. 物理アダプターおよびインターフェースの管理方法

タスク	タスクの実行方法
インターフェースの状況を調べる。	1. * プロンプトで **talk 5** と入力し、**Enter** を 2 回押して、+ プロンプトにアクセスします。 2. **config** と入力して、ソフトウェアに関する情報を表示させ、末尾にすべてのインターフェースの現在の状態を表示させます。表示出力が一時停止して、`--More--` が表示された場合は、スペース・バーを押して、次の画面の出力を表示させて見ます。 3. **int** と入力して、スロット番号およびポート番号と、インターフェースの起動カウントを表示させて見ます。 4. **stat** と入力して、インターフェースに関するパケットおよびバイトの統計を表示させて見ます。 5. **err** と入力して、インターフェースに関するエラー件数を表示させて見ます。 6. **queue** および **buff** と入力して、インターフェースに関するバッファー・カウントを表示させて見ます。 7. **net** *logical interface number* を入力して、特定のインターフェース・タイプに関する Console (構成) サブプロセスに入ります。そのサブプロセスでのコマンドを使用して、タイプ固有のインターフェース状況情報を表示させます。
インターフェースをリサイクルさせる (使用不可/使用可能にする)。	1. * プロンプトで **talk 5** と入力し、**Enter** を 2 回押して、+ プロンプトにアクセスします。 2. **int** と入力して、リサイクルさせたいインターフェースの論理「ネットワーク」番号を表示させて見ます。 3. **disable int** *logical interface number* を入力して、インターフェースを動的にオフラインにします。 4. **test** *logical interface number* を入力して、インターフェースをアップに戻します。
アダプターをリサイクルさせる (使用不可/使用可能にする)。	**注**: アダプターが使用不可になっている間にアダプターを取り外す (標準的な「ホット・プラグ」手順) 予定の場合は、 *2216 Nways Multiaccess Connector and Network Utility Service and Maintenance Manual* の「取り外しおよび取り付けの手順」の章も参照する必要があります。 1. * プロンプトで **talk 5** と入力し、**Enter** を 2 回押して、+ プロンプトにアクセスします。 2. **disable slot** *slot number* を入力します。ただし、1 が左スロット、2 が右スロットになります。これで、そのスロット内のアダプター上のインターフェースすべてが使用不可にされます。 3. **enable slot** *slot number* を入力して、そのスロット内のアダプター上のインターフェースすべてを起動します。

IP の基本的な構成と操作

表7 には、IP アダプターおよびインターフェースに関する基本的な構成および操作のタスクが記載してあります。

表 7. IP の基本的な構成と操作

タスク	タスクの実行方法
ネットワーク・アダプターに IP アドレスを追加する。	1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. **prot ip** と入力して、IP Config (構成) サブプロセスにアクセスします。 3. **li addr** と入力して、現在構成されている IP アドレスを表示させて見ます。 4. **add addr** と入力して、IP アドレスを追加します。インターフェースの論理インターフェース (ネットワーク) 番号、 IP アドレス、およびアドレス・マスクを指定します。 5. 稼働しているネットワーク・ユーティリティー内でこの IP 構成変更およびその他の IP 構成変更をアクティブにしたい場合は、次のようにします。 a. **Ctrl-p** を押し、**talk 5** と入力し、**Enter** を 2 回押して + プロンプトにアクセスします。 b. **prot ip** と入力して、IP コンソール・サブプロセスにアクセスします。 c. **int** と入力して、現在アクティブのインターフェース IP アドレスを表示させて見ます。 d. **reset ip** と入力して、新規アドレスをアクティブにします。 e. **int** と入力して、新規アドレスを確認します。
PCMCIA EtherJet アダプターの IP アドレスを設定する。	1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. **system set ip** と入力し、次の情報を指定します (これらのパラメーターの現行値がデフォルト値です)。 • IP アドレス - EtherJet アダプター用として使用されるアドレス • IP ネットマスク - そのアドレスのネットワーク・マスク • IP ゲートウェイ・アドレス - ユーザーが通信する可能性が高い IP ワークステーション、またはそのワークステーションにアクセスする場合に使用するルーターのアドレス 変更を加えた場合は、いずれも即時に有効となり、ネットワーク・ユーティリティーの不揮発性メモリーに保管されます。これらのアドレスは、ネットワーク・ユーティリティーの構成の一部にはなりません。 ファームウェアからも EtherJet IP アドレスを設定することができます。下記の EtherJet PING に関する手順に従いますが、オプション 3 の **Ping** ではなく、オプション 1 の **IP Parameters** を選択します。
静的ルートを追加する。	1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. **prot ip** と入力して、IP Config (構成) サブプロセスにアクセスします。 3. **li route** と入力して、現在構成されているルートを表示させて見ます。 4. **add route** と入力して、静的ルートを追加します。要求された情報を指定します。

表 7. IP の基本的な構成と操作 (続き)

タスク	タスクの実行方法
ネットワーク・アダプターからの PING およびトレース・ルートを行う。	1. * プロンプトで **talk 5** と入力し、**Enter** を 2 回押して、+ プロンプトにアクセスします。 2. **prot ip** と入力して、IP コンソール・サブプロセスにアクセスします。 3. デフォルト・パラメーターでアドレスを PING する場合は、**ping** *ip address* を入力します。パラメーターを変更する場合は、**ping** とだけ入力して、プロンプトに応答します。 **Ctrl-c** を押して、PING を終了します。 4. デフォルト・パラメーターでアドレスへのルートをトレースする場合は、**trace** *ip address* を入力します。パラメーターを変更する場合は、**trace** とだけ入力して、プロンプトに応答します。 **Ctrl-c** を押して、トレース・ルートを終了します。
PCMCIA EtherJet アダプターからの PING を行う。	1. 51ページの『ブート・オプション：高速ブートとファームウェアへのアクセス』 に記載されている手順の 1 つを使用して、ファームウェア・メインメニューにアクセスします。 2. PING を行う元のパネルをアップにします。 a. オプション 4 の **Utilities** を選択します。 b. オプション 11 の **Remote Initial Program Load Setup** を選択します。 c. オプション 3 の **Ping** を選択します。 d. PCMCIA Ethernet インターフェースを選択します。 3. PING を行うために使用したい IP アドレスを入力して (これらのアドレスによって、構成済みアドレスが一時的にオーバーライドされます)、**Enter** を押します。

コマンド行構成の管理

表8 には、コマンド行構成の管理方法が記載してあります。

表 8. コマンド行構成の管理方法

タスク	タスクの実行方法
1 つのプロトコルまたはすべてのプロトコルの構成を消去する。	1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. **clear ?** と入力して、単一のコマンドを用いて消去することができる構成情報のセットのリストを表示させて見ます。 3. **clear** *protocol name* を入力して、特定のプロトコルに関する情報を消去するか、または **clear all** と入力して、すべてのプロトコルに関する情報 (ただし、装置情報ではない) を消去します。 これらのコマンドによってメモリーに入っている現行構成は変更されますが、ネットワーク・ユーティリティーの動作状態が影響を受けることはありません。
1 つのインターフェースまたはすべてのインターフェースの構成を消去する。	1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. 特定のインターフェースに関して、そのインターフェースに関連するすべてのプロトコル構成も含めて、構成を削除したい場合は、 **del int** と入力します。 3. すべてのインターフェースの構成を削除したい場合は、 **clear dev** と入力します。このコマンドでは、関連プロトコル情報は消去されないので、構成を完全に消去する場合は、通常、 **clear all** と併用することになります。 これらのコマンドによってメモリーに入っている現行構成は変更されますが、ネットワーク・ユーティリティーの動作状態が影響を受けることはありません。
現行の talk 6 構成全体を起動する。	1. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 2. **write** と入力して、メモリーに入っている現行構成をディスク内でアクティブ・バンクの次に使用可能な構成ファイル位置に書き込みます。 3. **reload** と入力し、次に **yes** と入力して、ネットワーク・ユーティリティーをリブートし、構成を起動します。 プロトコルも装置情報もなしで構成を起動した場合は、ネットワーク・ユーティリティーは config-only モードに入ることになります。1 つのプロトコルおよび 1 つのインターフェースを定義し、リブートしてからでないと、ネットワーク・ユーティリティーが完全に作動可能になることはできません。

一般的な状況の監視

表9 には、一般的な状況の監視タスクの実行方法が記載してあります。

表 9. 一般的な状況の監視の実行方法

タスク	タスクの実行方法
CPU 使用状況を調べる。	1. * プロンプトで **talk 5** と入力し、**Enter** を 2 回押して、+ プロンプトにアクセスします。 2. **perf** と入力して、パフォーマンス監視コンソール・サブプロセスにアクセスします。 3. **list** と入力して、CPU モニター状態が ENABLED であることを確認します。これがネットワーク・ユーティリティーのデフォルト設定です。状態が ENABLED でない場合は、**enable cpu** と入力します。 4. **report** と入力して、最新の CPU 使用状況統計を表示させて見ます。最新スナップショットでは、値が ″Most recent short window″ です。 5. CPU 使用状況が、talk 2で監視できるイベント・メッセージが出されるつど、それと同じ頻度で報告されるようにしたい場合は、**enable t2** と入力します。**Ctrl-p** を押し、**talk 2** と入力して、生成される CPU 使用状況メッセージを監視します。**Ctrl-p** を押して、 talk 2 を終了します。 6. talk 2 CPU 報告が次のリブート後も継続されるようにしたい場合は、 talk 6 に移動し、上記のコマンドを繰り返します。あるいは、構成プログラムの「CPU Utilization」パネル上で同じ設定を構成し、更新後の構成をネットワーク・ユーティリティーに転送します。
メモリー使用状況を調べる。	1. * プロンプトで **talk 5** と入力し、**Enter** を 2 回押して、+ プロンプトにアクセスします。 2. **mem** と入力して、現在のグローバル・メモリー統計を表示させて見ます。 このコマンドでは、取り付けられている物理メモリーの合計、およびルーティング機能が使用しているメモリー部分に関する詳細が報告されます。ルーティング機能には、APPN および TN3270 サーバーを除いて、ネットワーク・プロトコルおよびフィーチャーがすべて含まれます。 3. APPN または TN3270 サーバーを実行している場合は、 **p appn** と入力して、APPN コンソール・サブプロセスにアクセスします。 **mem** と入力して、現在の APPN メモリー統計およびしきい値状態を表示させて見ます。稼働しているのがサブエリア TN3270 ホスト処理装置接続機構だけであっても、これらの統計には TN3270 サーバーの使用量が含まれます。

表 9. 一般的な状況の監視の実行方法 (続き)

タスク	タスクの実行方法
デフォルトの ELS メッセージをオンにする。	1. * プロンプトで **talk 5** と入力し、**Enter** を 2 回押して、+ プロンプトにアクセスします。 2. **event** と入力して、イベント・ログ・コンソール・サブプロセスにアクセスします。 3. **disp sub all** と入力して、すべての定義済みサブシステムに関する STANDARD レベルのログ記録をアクティブにします。これには、エラー・メッセージと一般的でない通知メッセージが含まれます。 4. **Ctrl-p** を押し、**talk 2** と入力して、生成されるメッセージをいずれも監視し、 **Ctrl-p** を押して talk 2 を終了します。 5. これらの設定が次のリブート後も維持されるようにしたい場合は、talk 6 に移動し、上記のコマンドを繰り返します。こうすることによって、設定が構成の一部になります。

ブート・オプション : 高速ブートとファームウェアへのアクセス

表10 には、高速ブートとファームウェアへのアクセスのためにブート・オプションを実行する方法が記載してあります。

表 10. ブート・オプション : 高速ブートとファームウェアへのアクセス

タスク	タスクの実行方法
テスト環境でブート時間を最小化する。	1. **talk 6** と入力した上で、**boot** と入力して、ブート Config (構成) サブプロセスにアクセスします。 2. **en fast** と入力して、高速ブート・オプションを使用可能にします。 ネットワーク・ユーティリティーの次回リブート時には、電源オン診断の一部が飛ばされて、さらに迅速にブートするようになります。ただし、このオプションは実稼働環境では推奨できません。**dis fast** を使用すれば、通常の全診断モードに戻ります。
直接接続端末コンソールを使用している場合に、ファームウェアにアクセスする。	1. 端末エミュレーション画面サイズが 24 行 80 桁に設定されていることを確認するか、端末エミュレーターで自動折り返しを設定します。 2. * プロンプトで **reload** と入力し、確認メッセージに **yes** と応答します。ブート状況メッセージの入念な監視を開始します。 3. メッセージ `Starting Boot Sequence` に続けて、メッセージ `Strike F1 key now to prematurely terminate Boot` が表示されたら、すぐに **Ctrl-c** または **F1** を押します。このメッセージを見落とさないようにするために、システム・ボード診断の開始後であれば、いつでも **Ctrl-c** を押したままの状態を開始して構いません。ファームウェア・メインメニューが表示されるか、監視パスワードの入力を指示するプロンプトが表示されるまで、 **Ctrl-c** を押したままにします。 4. メッセージ `Strike F1 key now to prematurely terminate Boot` が表示されてから数秒以内に、ファームウェア・メインメニューと監視パスワード入力指示プロンプトのどちらかが表示されるはずです。 このどちらも表示されず、ディスク・ロード・メッセージが表示された場合は、長く待ち過ぎ、**Ctrl-c** または **F1** を押す時刻ウィンドウを見落としたことになります。 ブート・シーケンスが完了するのを待って、この手順のステップ 2 および 3 を繰り返します。 あるいは、ダイヤルイン手順を使用して、正しい時点でキーを押さなくても、確実にファームウェア内で停止するようにします。 5. システムによって監視パスワードの入力を指示するプロンプトが出された場合は、元もと工場で「2216」に設定されている現行パスワードを入力します。そうすると、システムによってファームウェア・メインメニューが表示されます。

表 10. ブート・オプション : 高速ブートとファームウェアへのアクセス (続き)

タスク	タスクの実行方法
ダイヤルアップ端末コンソールを使用している場合に、ファームウェアにアクセスする。	1. 端末エミュレーション画面サイズが 24 行 80 桁に設定されていることを確認するか、端末エミュレーターで自動折り返しを設定します。 2. * プロンプトで **talk 6** と入力し、**Enter** を 2 回押して、 Config> プロンプトにアクセスします。 3. **boot** と入力して、ブート Config (構成) サブプロセスにアクセスします。 4. **disable auto-boot** と入力して、ブート・シーケンスがファームウェア内で常に停止することになるモードを選択します。持続期間 (once/always) プロンプトが表示された場合は、ファームウェア内での停止を次回のリブート時だけにしたいか、以後のすべてのリブート時にしたいかを選択します。 5. **Ctrl-p** を押して * プロンプトにアクセスし、**reload yes** と入力してネットワーク・ユーティリティーをリブートします。リブートによって、ダイヤル接続は失われることになります。 6. 数分後、逆にダイヤルインすると、ファームウェア・メインメニューと監視パスワード入力指示プロンプトのどちらかが表示されます。 7. システムによって監視パスワードの入力を指示するプロンプトが出された場合は、元もと工場で「2216」に設定されている現行パスワードを入力します。そうすると、システムによってファームウェア・メインメニューが表示されます。 持続期間 (once/always) プロンプトが表示され、always (毎回) を選択した場合や、このプロンプトが表示されなかった場合は、次回命令コードにアクセスしたとき、 **enable auto-boot** を実行します。
ファームウェアから命令コード内にブートする。	1. ファームウェア・メニュー構造内で、必要に応じて **Esc** を押して、ファームウェア・メインメニューにアクセスします。 2. 現行ブート・シーケンスのアップを命令コード内まで続けたい場合は、 **F9** (OS 開始) を押します。 電源オン診断から始めて完全にリブートしたい場合は、 **F3** (リブート) を押します。こうすると、ネットワーク・ユーティリティーの PCMCIA モデムやシステム・カード・サービス・ポートにダイヤルインしている場合は、接続が失われることになります。 3. 必要なら、逆にダイヤルインし、そうでなければ、ディスク・ロード・メッセージを監視するだけにします。システムから要求された場合は、スペース・バーを押してコマンド・プロンプトを表示させます。

第2部 ネットワーク・ユーティリティーについての学習

第5章 コマンド行インターフェースの解説

この章では、IBM ルーティング製品を初めて使用されるユーザーを対象に、ネットワーク・ユーティリティーのコマンド行インターフェースの概念と基本的なナビゲーションについて解説します。この章には、下記の内容が網羅されています。

- アダプター番号およびポート番号の基本概念
- システムの各部への移動方法とそれぞれの目的
- 各プロセスでのタスクおよびコマンドの例
- メニュー・ナビゲーションの方法およびコマンドの発行方法
- 構成方法、状況の照会方法、およびシステム・ログの監視方法
- 構成変更の保管および起動の方法
- ファームウェアとは何か、ファームウェアにアクセスする方法、ファームウェアでできること
- 自動コマンド完成機能によるユーザー補助の方法と、コマンド行に入力するコマンドの構文

この章の解説を最大限に理解していただくためには、始めから終わりまで同じネットワーク・ユーティリティーについて習得していただくことが大切です。

すでに IBM 2216 の使用経験があるユーザーの場合は、ネットワーク・ユーティリティーのインターフェースもほとんど変わりがないことに気付かれるはずです。IBM 2212 のユーザーの場合も、ファームウェア・インターフェースを除けば、同じことが言えます。IBM 2210 のユーザーにとっては、プロンプトやメニュー・ナビゲーションはなじみ深いものでしょうが、アダプターの構成、構成の保管、製品のリブートなどの分野では違いに気付かれるはずです。

プロンプトとプロセス

25ページの『第3章 初期構成の実行』 に記載されている初期構成手順の 1 つに従って作業を行っていれば、ネットワーク・ユーティリティーは構成を終え、ブートが行われて、通常の操作モードに入っているはずです。したがって、ユーザー・コンソールには、アスタリスク (*) コマンド・プロンプトが表示されているはずです。

通常の操作モードでは、ネットワーク・ユーティリティーのルーティング機能が稼働しています。したがって、オペレーターとしてコマンド行インターフェースを使用して、構成の表示および変更、アクティブ・システム状況の表示、メッセージ・ログの表示など、さまざまなことができます。コマンド行インターフェースの各部にナビゲートして、さまざまなタスクを実行することになりますが、ナビゲーション・ツリーのルートにあるのが * プロンプトです。

* プロンプトで **?** を入力すると、ここで使用可能なコマンドが表示されます。

```
  *?
CONFIGURATION        (Talk 6)
CONSOLE              (Talk 5)
EVENT Logging System (Talk 2)
ELS Console          (Talk 7)
LOGOUT
PING   <IP Address>
RELOAD
TELNET to IP-Address <this terminal type>
```

```
-------------------------------------------------
DIAGS hardware diagnostics
DIVERT output from process
FLUSH output from process
HALT output from process
INTERCEPT character is
MEMORY statistics
STATUS of process(es)
SUSPEND command completion
TALK to process
*
```

これらのコマンドには、それぞれに独自の用途がありますが、特に高頻度で使用されるものに次の 2 つのコマンドがあります。

talk システムを表示させて見るさまざまな方法、つまりさまざまなプロセスのうちの 1 つにコンソールを接続します。

reload ネットワーク・ユーティリティーをリブートします。

talk コマンドを使用する場合は、**t** *n* を入力します。ただし、*n* (*プロセス ID*) は、通常、次の値のいずれか 1 つになります。

6 構成の表示および変更を行う場合 (*Config (構成)* プロセス)

5 現在のシステム状況の表示、実行システムの状態の能動的制御、および動的構成変更の起動を行う場合 (コンソール・プロセス)

2 通知メッセージおよび状況メッセージのローリング・ログの表示を行う場合 (*監視* プロセス)

talk コマンドを取り消して、プロセス内から直接 * プロンプトに戻る場合は、どのプロセスでも **Ctrl-p** を押します。

MAS V3.3 では、自然言語に近いコマンドを導入して、**talk** コマンドと同じ機能が実行できるようにしました。したがって、**talk 6** ではなく、**config** と入力するだけで済みます。同様に、**console** と入力して、**talk 5** に代え、**event** と入力して、**talk 2** に代えることもできます。

以下の 3 節では、主要プロセスのそれぞれについて記述し、それぞれのプロセス内で実行できるタスクの一部について説明します。その過程で、プロセス間およびメニュー間を自在に移動することができるようになり、コマンドの入力にも精通していただけるはずです。

構成 (talk 6、Config (構成) プロセスの使用)

* プロンプトで **t 6** か **config** と入力すると、ネットワーク・ユーティリティーを構成するためのコマンド行プロセスに入ります。

```
*         <Enter>
*t 6
Gateway user configuration
Config>   <Enter>
Config>
```

これで Config (構成) プロセスの中に入ったので、コマンド・プロンプトが * から Config> に変わっています。 Config (構成) プロセスおよびコンソール・プロセスに

は、いずれも固有のプロンプトがあるので、一目見ただけで、どちらのプロセスに入っているかが分かります。状況メッセージ Gateway user configuration が表示されるのは、リブート後に初めて Config (構成) プロセスに入ったときだけです (システム内のさまざまな個所で、「ゲートウェイ」が「ルーター」の同義語として使用されています)。

前にあるプロセスに入っていて、**talk** コマンドを使用してそのプロセスに再度入ると、システムでは、即時コマンド・プロンプトではなく、ブランク行を表示します。**Enter** を押すと、前回そのプロセス内にいたときに表示されていた個所に戻ります。

```
Config>   <Ctrl-p>        <---- leave Config and go back to *
*         <Enter>
*t 6                      <---- go back into Config
          <Enter>
Config>                   <---- we're back at the main Config prompt
```

Config (構成) プロセス内での作業時には、ネットワーク・ユーティリティーが動作するための構成を変更します。このような変更は、わずかな例外を除いて、ルーターの実行状態に影響を与えることはありません。talk 6 での変更をアクティブにするには、次のどちらかを行う必要があります。

- 一連の変更をアクティブにするためのコマンドの 1 つを発行する。
- 変更をハード・ディスクに保管して、システムをリブートする。

この章での学習の過程で、上記の 2 つの方法の例が示されます。

コマンドの概説

メイン Config> プロンプトで **?** と入力すると、使用可能なコマンドがアルファベット順にリストされて表示されます。

```
Config>?
ADD (device, user)
BOOT and load file functions
CHANGE (device, password, user)
CLEAR configuration information
DELETE (interface, user)
DISABLE (interface, console-login, etc)
ENABLE (interface, console-login, etc)
EVENT logging system and messages
FEATURE (non-protocol and network features)
LIST (devices, configuration, patches, users)
LOAD (add, delete, list)
NETWORK interface configuration
PATCH global configuration parameters
PERFORMANCE monitor
PROTOCOL configuration
QCONFIG (quick configuration)
SET system-wide parameters
SYSTEM
TIME of day parameters
UNPATCH global configuration parameters
UPDATE
WRITE
Config>
```

これらのコマンドには、ボックスの機能を実際に構成するためのものもあれば、構成管理およびシステム管理を行うためのものもあります。 talk 6 のもとで行われるこ

との種類について感触をつかんでいただくために、主要なコマンドをユーザー・タスク別にグループにまとめて以下にリストしておきます。

- アダプターおよびポートの構成

  add device
  単一のアダプター・スロットおよびポートを構成します。

  change device
  スロット構成を別のスロットに移動またはコピーします。

  delete interface
  単一のインターフェース (アダプター・ポート) および関連プロトコル情報を削除します。

  disable/enable interface
  特定のインターフェースを起動するかどうかを制御します。

  list device
  構成済みインターフェースすべてを表示します。

  net *interface number*
  プロトコル・レベルより下で、指定されたインターフェースを構成するためのサブプロセスに進みます。

  set data-link
  新たに追加された WAN アダプター・ポートをデフォルトの PPP からフレーム・リレー、SDLC、SDLC リレー、または X.25 に変更します。

  system set/display ip
  PCMCIA LAN アダプターの IP パラメーターの設定または表示、あるいはその両方を行います。

- プロトコルおよびフィーチャーの構成

  protocol *name*
  指定されたプロトコルを構成するためのサブプロセスに進みます。

  feature *name*
  指定されたフィーチャーを構成するためのサブプロセスに進みます。

- 構成およびソフトウェア・ロードの管理

  boot ディスク上の構成ファイルおよびソフトウェア・ロードの転送および使用を管理するためのサブプロセスに進みます。

  clear RAM 内の現行構成の全デバイス、全プロトコル、または特定部分を消し去ることができます。

  write RAM 内の現行構成をハード・ディスクに保管します。

- ボックスを監視するための構成

  event アクティブなイベント・ログ・システム (ELS) メッセージを構成するためのサブプロセスに進みます。

  performance
  CPU 使用状況監視を構成するためのサブプロセスに進みます。

- システムの管理

  add/change/delete/list user, change password
  制御下でのコンソール・アクセス用 ID を管理します。

  disable/enable console-login
  コンソールへのリモート・アクセスを制御します。

  set host/prompt/contact/location
  ホスト名、プロンプト接頭部、連絡相手、または場所を設定します。

time 時刻と時刻形式、またはリモート・ホストから時刻を入手するかどうかを設定します。

- ソフトウェアのサービス

disable/enable/set dump, reboot
ネットワーク・ユーティリティー・ボックスが動作を異常終了した場合に、ダンプとリブートを制御します。

patch, unpatch
特定のユーザー環境で問題を回避するための特殊化ソフトウェア機能を制御します。

system retrieve
ルーターの圧縮システム・ダンプをサーバーに送信します。

system view
現行ダンプ・ファイルに関する情報を表示します。

以下の例では、これらの talk 6 コマンドの一部について、その使用によって基本的な構成タスクを実行する方法を示します。これらの例について学習するにつれ、例示されているタスクについて経験を積むだけでなく、一般的に、メニュー間の自在な移動やコマンドの発行にも習熟できるはずです。なお、初期構成でコマンド行を使用していれば、すでになじみになっているはずのタスクから例示を始めることにします。

例 : アダプター上のポートの構成

ここで採用しているいずれの例でも、ユーザーが初めてネットワーク・ユーティリティーをブートするときの構成は、次のようになっています。

- ESCON がスロット 1 に入っており、IP は構成されていない。
- トークンリング・アダプターがスロット 2 に入っており、ポート 2 は IP アドレス 192.1.1.8 で構成されている。

この例に従う場合は、**clear dev** を使用してユーザー独自の入出力装置構成を消去し[6]、次に **add dev** と **del int** を使用して、下に示すように、 ESCON/TR 入出力装置構成に入ります。

Config> プロンプトで **list device** (または省略形の **li dev**) を入力すると、現行構成の中で定義されているアダプターおよびポートが表示されます。構成もアダプター・ポートも定義していない場合は、**li dev** では、出力はまったく表示されず、ユーザー・プロンプトが再度表示されるだけです。装置はすべて消去してしまったので、装置を追加することはできます。**add dev ?** と入力すると、追加できるアダプターのタイプすべてのリストが表示されます。

```
Config>clear dev
You are about to clear all Device configuration information.
Are you sure you want to do this? ? [No]: yes
Device configuration cleared
Config>li dev
Config>add dev ?
ATM            1-port 155 Mbps ATM adapter
EIA-232E       8-port EIA-232E/V.24 adapter
ESCON Channel  1-port ESCON Channel adapter
ETHERNET       2-port Ethernet adapter
```

6. 通常、**clear dev** は、プロトコル情報を消し去る **clear all** と一緒にしか使用しません。

```
ETH100          1-port 10/100 Mb Ethernet adapter
FDDI            1-port FDDI adapter
HSSI            1-port HSSI adapter
PCA             1-port Parallel Channel adapter
TOKEN-RING      2-port Token-Ring adapter
V35/V36         6-port V.35/V.36 adapter
X21             8-port X.21 adapter
Config>
```

add dev コマンドを使用して、単一アダプター上に単一のポートを構成します。マルチポート・アダプターの場合は、構成に追加するポートを指定し、アクティブにしたい各ポートごとに、それぞれコマンドを出し直す必要があります。ここでは、1 ポート ESCON アダプター、および 2 ポート・トークンリング・アダプターの両ポートを追加します。

```
Config>add dev esc
Device Slot #(1-2) [1]? 1
Adding ESCON Channel device in slot 1  port 1 as interface #0
Use "net 0" to configure ESCON Channel parameters
Config>add dev tok
Device Slot #(1-2) [1]? 2
Device Port #(1-2) [1]? 1
Adding Token-Ring device in slot 2  port 1 as interface #1
Use "net 1" to configure Token-Ring parameters
Config>add dev tok
Device Slot #(1-2) [1]? 2
Device Port #(1-2) [2]? 2
Adding Token-Ring device in slot 2  port 2 as interface #2
Use "net 2" to configure Token-Ring parameters
Config>li dev
Ifc 0     ESCON Channel                     Slot: 1   Port: 1
Ifc 1     Token-Ring                        Slot: 2   Port: 1
Ifc 2     Token-Ring                        Slot: 2   Port: 2
Config>
```

アダプター・タイプを指定する場合は、**add dev** と同じ行に、**add dev ?** の出力リストの左端欄のワードの最初の数文字 (追加したいアダプター・タイプを区別できる十分な文字数) を入力します。プロンプトによる指示が出たら、スロットおよび (マルチポート・アダプターの場合のみ) ポート番号を指定する必要があります。スロットおよびポートの番号は、次のように固定されています。

- ネットワーク・ユーティリティー上の 2 つのアダプター・スロットには、ボックスの前から見て、左から右へ 1 および 2 と番号が付けられています。
- マルチポート LAN アダプター上のポートには、1 および 2 の番号が付けられ、アダプターの表面にラベルがはってあります。
- マルチポート WAN アダプター上のポートには、0 から始まる番号が付けられ、アダプター・ケーブル端のコネクターにラベルがはってあります。

add dev コマンドを使用すれば、同一スロット内に 2 つの異なるアダプターの追加を試みたり、存在しないスロットにアダプターの追加を試みたり、特定のアダプター上に存在しないポート番号の指定を試みたりすることがなくなります。このコマンドでは、選択した装置タイプをネットワーク・ユーティリティーに物理的に取り付けられているアダプターと突き合わせて、妥当性検査を行うことは ***ありません***。したがって、まだ取り付けていないアダプターを構成したり、別のネットワーク・ユーティリティー用の構成を作成したりすることができます。システムで入出力装置構成の妥当性検査を行うのは、特定の構成でブートアップしたり、インターフェースの動的起動を試みたりした場合だけです。システムではミスマッチの報告は、ロ

ーカルで表示可能なイベント・ログによるだけでなく、アダプターの前面の LED によっても行います。後でこの章で扱いますが、アダプター状況を表示させるコマンドを入力することもできます。

論理インターフェース番号

add dev コマンドに対する応答として、ネットワーク・ユーティリティーは、ユーザーが追加したばかりのポートに論理 インターフェース番号、つまり論理 ネットワーク番号 を割り当てます。これは重要な番号であり、システム内の他のどのコマンドでも、この番号でこのインターフェースを指します。物理スロットおよびポートの番号を使用するのは、 **add dev** コマンドだけであり、他のコマンドでは、すべて論理インターフェース番号を使用します。物理 (「基本」) ポート (例えば、 ESCON など) を複数のバーチャル・インターフェースに細分すると、各バーチャル・インターフェースにもそれぞれインターフェース番号が付きます。上記で示したように、**li dev** コマンドを使用すると、すべての物理インターフェースおよびバーチャル・インターフェースのそれぞれのインターフェース番号を表示させて見ることができます。

例 : インターフェースの削除

間違いを犯してしまい、**add dev** コマンドを取り消したい場合や、何らかの理由でアダプターまたはポート、あるいはその両方の構成を削除したい場合は、**delete interface** コマンドを使用します (これは名前を指定した「delete device」ではありません。論理インターフェース番号が対象であり、アダプター・スロット番号が対象ではないからです)。例を続行したい場合は、使用したいのがトークンリング・アダプターのポート 2 だけであるものとします。次のようにして、ポート 1 (偶然インターフェース 1 でもある) を削除します。

```
Config>li dev
Ifc 0     ESCON Channel                     Slot: 1   Port: 1
Ifc 1     Token-Ring                        Slot: 2   Port: 1
Ifc 2     Token-Ring                        Slot: 2   Port: 2
Config>del int
Interface number? 1
Interface being deleted... please be patient.
The router must be restarted
Interface 1 deleted successfully
Config>li dev
Ifc 0     ESCON Channel                     Slot: 1   Port: 1
Ifc 1     Token-Ring                        Slot: 2   Port: 2
Config>
```

これでトークンリング・ポート 2 がインターフェース 1 になったことに注意してください。番号が 1 より大きいインターフェースが他にあった場合は、それらの番号も 1 つずつ小さくなったはずです。構成内のインターフェースをすべて削除したい場合は、インターフェースがなくなるまで、もっぱらインターフェース 0 を繰り返し削除します。

入出力装置構成自体に加えて、特定のインターフェースに対応するプロトコル構成があるのが通常です。ユーザーが **del int** コマンドを使用してインターフェースを削除すると、システムでも、そのインターフェースに対応するプロトコル構成をすべて削除し、番号が付け直されたインターフェースに対応するプロトコル構成すべて

の番号を付け直します[7]。 **del int** 操作が実行システムで有効になるためには、ネットワーク・ユーティリティーをリブートする必要があります。

例 : メニューの使用によるホスト名の設定

一般的にコマンドを出す方法をさらに綿密に検討する場合は、 **set** コマンドの使用によるこのネットワーク・ユーティリティーの名前 (「ホスト名」) の設定など、単純な作業を試みてみます。

注: この例では、自動コマンド完成機能を使用不可にしてしていることを前提にしています。ネットワーク・ユーティリティーで自動コマンド完成機能を使用する方法については、39ページの『自動コマンド完成機能』 をごらんください。

まず最初にコマンド自体だけで試行します。

```
Config>set
Command not fully specified
```

このエラー・メッセージでは、**set** コマンドには、それに伴うキーワードのメニューがあり、したがって、アクションを実行する完全なコマンドが形成されるまで、キーワードを追加入力する必要があることが報告されています。 メニューが表示されている場合はいつでも (すでにこれまでに見てきたように)、**?** と入力して、入力の対象として使用できるコマンドやキーワードを表示させて見ることができます。コマンド・キーワードの記憶にさえ努めておけば、資料で該当のコマンドを調べるよりも、 **?** と入力するだけで済ます方が、通常ははるかに時間がかかりません。この場合は、オプションは次のようになります。

```
Config>set ?
CONTACT-PERSON
DATA-LINK
DOWN-NOTIFY
GLOBAL-BUFFERS
HOSTNAME
INACTIVITY-TIMER
INPUT-LOW-WATER
LOCATION
PACKET-SIZE
PROMPT
RECEIVE-BUFFERS
SPARE-INTERFACES
```

これでごらんいただけるように、**set** メニューには、データ項目が混在しています。つまり、システム管理用のものもあれば、ノード・チューニング用のものもあれば、その他のものもあるという具合です。ネットワーク・ユーティリティーでは、ノード・チューニング・オプションにはデフォルト値が取られるので、変更する必要はありません。

話をタスクに戻すと、必要なキーワードが「hostname」であることは明らかです。メニュー項目 (コマンド名やキーワード) については、いずれも固有であるために必要な文字数まで省略できるので、「hostname」についても少し短縮します。

---

7. **clear dev** コマンドではこの機能は実行されないので、それを使用するのは、手作業でプロトコル情報の消去も行う場合だけにする必要があります。

```
Config>set host
Host name for this node []? rtp01
Host name updated successfully
rtp01 Config>
```

デフォルトでは、システムは新しいホスト名をすべてのコマンド・プロンプトの前に挿入します。これを好むユーザーが多いのは、単一のワークステーションから多数のルーター内に Telnet でログインし、ルーター・コンソール間の区別を簡単に行うことができるからです。別のプロンプト接頭部を選択したい場合は、 **set prompt** コマンドを使用してそうすることができます。ホストとプロンプトのどちらかをヌル値にリセットする場合は、**clear host** または **clear prompt** コマンドを使用し、ネットワーク・ユーティリティーをリブートします。現行値を表示させて見る場合は、**list config** を使用します。

set host は、通常の talk 6 ルールの例外であることに注意してください。即時に有効になり、何らかの種類の「起動」コマンドを発行する必要もなければ、ネットワーク・ユーティリティーをリブートする必要もありません。このように振る舞う talk 6 コマンドはほとんどありませんが、ユーザー・プロンプトに対する影響を即時に確認できるので、これは非常に有用です。

例 : 前入力

新たにプロンプトが表示されるのは好まないが、ホスト名は ″rtp01″ から ″RTP01″ に変更したいものとします。 この場合は、次のようにして、1 つのコマンドで済ますことができます。

```
rtp01 Config>set host RTP01
Host name updated successfully
RTP01 Config>
```

元のコマンド行にホスト名を入力したので、システムがプロンプトを出してその入力を指示することはありません。この例に示されているのが、もう 1 つの一般的なルールです。つまり、コマンドが完全であれば、入力パラメーターの入力を指示するプロンプトが出ますが、この場合に、元のコマンド行に入力パラメーターを入力しておき、プロンプトが出ないように飛ばすことができます。ただし、このようにプロンプトを飛ばしたい場合は、パラメーターを正しい順序で入力するよう注意する必要があります。

例 : ″net″ の使用によるポート・パラメーターの設定

これでホスト名を構成したので、次はもう少し複雑なことをやってみることにします。 Config-only モードからのリブート時に、新たに構成したトークンリング・アダプター・ポート 2 がアップしないことに気付いた場合を想定します。構成されているリング速度を表示させて見て、その値を変更することができます。この種の下位レベル装置固有構成パラメーターが、次のようにして、**net** コマンドを使用する対象となります。

```
RTP01 Config>li dev           <------ what were those i/f numbers again?
Ifc 0     ESCON Channel                    Slot: 1   Port: 1
Ifc 1     Token-Ring                       Slot: 2   Port: 2
RTP01 Config>       <Enter>
RTP01 Config>net 1            <------ I configure interface 1
Token-Ring interface configuration
RTP01 TKR config>   <Enter>   <------ note the new subprocess prompt
```

```
RTP01 TKR config>?            <------ what are the commands here?
EXIT
FRAME
LIST
LLC
MEDIA
SET
PACKET-SIZE bytes
SOURCE-ROUTING
SPEED Mb/sec
RTP01 TKR config>li           <------ show me what I have now
Token-Ring configuration:
Packet size (INFO field): 2052
Speed:                    4 Mb/sec       <----- It should be 16Mb/sec
Media:                    Shielded
RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
RTP01 TKR config>speed
Speed (4 or 16) [4]? 16       <------ change the speed here
RTP01 TKR config>li           <------ verify the new value
Token-Ring configuration:
Packet size (INFO field): 2052
Speed:                    16 Mb/sec       <----- looks good now
Media:                    Shielded
RIF Aging Timer:          120
Source Routing:           Enabled
MAC Address:              000000000000
RTP01 TKR config>ex           <------ exit the subprocess
RTP01 Config>                 <------ you are back at the main T 6 menu
```

リング速度に加えたこの変更は、即時には有効にならないので、talk 5 コマンドの 1 つを実行するか、リブートしてアクティブにする必要があります。リブートを行わないで構成変更をアクティブにする方法の基本については、 84ページの『動的再構成』 で説明します。通常は、**add dev** の直後に **net** コマンドを使用して、新規インターフェースのデフォルト設定を表示させて見て、必要な変更があれば、そのポートを最初に起動する前に、すべて行っておきます。

この例では、**net 1** と入力して、トークンリング・インターフェースを構成するためのサブプロセス内に移動しました。基本メニューが変わり、プロンプトも変わったことで、すでにメイン Config> メニューではなく、1 つ低いレベルに入っていることが分かります。どのサブプロセスの場合でも、そこを終了して、レベルが 1 つ高い次のメニューに戻るには、 **exit** と入力します。また、**Ctrl-p** を押すと、即時に一足跳びで * プロンプトが表示され、そのプロセスに戻ると、最後にいた所に再び入ります。

```
RTP01 Config>       <Enter>     <------ start here
RTP01 Config>net 1              <------ enter a Config subprocess
Token-Ring interface configuration
RTP01 TKR config>   <Ctrl-p>    <------ jump out
RTP01 *   <Enter>
RTP01 *t 6                      <------ go back to Config
               <Enter>
RTP01 TKR config>   <Enter>     <------ you are back in the subprocess
RTP01 TKR config>ex             <------ exit the subprocess
RTP01 Config>                   <------ You are back where you started
```

もう 2 つ Config (構成) プロセスでの例を試みて、その後はコンソール・プロセスに移ることにします。最初の例では、ボックスを再ロードする時間を短縮する方法を示し、2 番目の例では、ボックス・プロトコルに関連するパラメーターを変更する方法を示しいます。

例 : 「fast-boot (高速ブート)」の使用可能化

Config> プロンプトで **boot** と入力すると、構成、コード・ロード、およびブート・オプションを管理するためのサブシステムにアクセスします。このサブシステムの完全な背景については、87ページの『第7章 構成ファイルの取り扱い』 に記載してありますから、ここではすべてのコマンドについて表示させて見る必要はありません。**enable** コマンドの下だけにして、「fastboot」オプションを試してみます。

```
RTP01 Config>boot                       <----- enter subprocess
Boot configuration
RTP01 Boot config>   <Enter>            <----- note new prompt
RTP01 Boot config>en ?                  <----- list "enable" options
AUTO-BOOT-- set Unattended mode
FAST-BOOT-- bypass diags
RTP01 Boot config>en fast               <----- try out "fast-boot"
FastBoot mode is now enabled.

Operation completed successfully.
RTP01 Boot config>ex                    <----- exit the boot subprocess
RTP01 Config>
```

ネットワーク・ユーティリティーの電源をオンにしたとき、または **reload** コマンドを入力したとき、コンソールのブートアップ・メッセージを監視していれば、システムがブート時に数多くの電源オン診断を行っていることに気付いたはずです。実動ルーターの場合は、リブートの頻度が低く、ハードウェアの妥当性検査が必要であるため、これは望ましいことには違いありませんが、ブート時間が長引くことになります。特定のルーターについて、能動的に構成を行い、リブートを繰り返している場合は、このような診断をはしょって、ブート時間を短縮したいと考えることがあります。そこで、**enable fast-boot** コマンドを用いてこれを行ったのが、この例です。これで、次回の **reload** では、その進行が迅速になります。この変更は、ネットワーク・ユーティリティーを実動に移す前に、**disable fast-boot** を使用して取り消すことができます。

高速ブート・モードを制御できるのは、コマンド行だけであり、構成プログラムではできないことに注意してください。システムのブート・モードは、非揮発性メモリーに保管されるもので、構成ファイルの一部にはなりません。

例 : インターフェース IP アドレスの変更

Config (構成) プロセスの最終例では、IP プロトコル・サブプロセスのメニューとコマンドを使用して、インターフェース IP アドレスを変更します。 61 ページで指摘したように、ここで扱う例の開始時には、ネットワーク・ユーティリティー は、 IP アドレスがインターフェース 1 (スロット 2 のトークンリング・アダプター上のポート 2) に構成されていました。

```
RTP01 Config>li dev             <----- what are the intfcs again?
Ifc 0     ESCON Channel                   Slot: 1   Port: 1
Ifc 1     Token-Ring                      Slot: 2   Port: 2
RTP01 Config>p ip               <----- short for "protocol ip"
Internet protocol user configuration
RTP01 IP config>   <enter>      <----- now in IP Config subprocess
RTP01 IP config>li addr         <----- list configured IP addresses
IP addresses for each interface:
   intf     0                              IP disabled on this interface

   intf     1   192.1.1.8        255.255.255.0    Local wire broadcast, fill 1
RTP01 IP config>change addr
```

```
Enter the address to be changed []? 192.1.1.8
New address [192.1.1.8]? 192.7.7.7
Address mask [255.255.255.0]?   <enter>
RTP01 IP config>li addr        <----- verify the change
IP addresses for each interface:
   intf     0                                IP disabled on this interface

   intf     1   192.7.7.7        255.255.255.0    Local wire broadcast, fill 1
RTP01 IP config>ex             <----- exit IP config
RTP01 Config>
```

これは、個々のプロトコルを対象とするサブプロセスに入るのに **protocol** コマンドを使用する最初の例です。 IP は、選択できたプロトコルのうちの 1 つであり、**feature** コマンドを使用してアクセスできるフィーチャーにも、似たようなリストがあります。 Config> で **list config** と入力して、構成できるプロトコルおよびフィーチャーの完全なリストを表示させるか、**p ?** または **f ?** とだけ入力して、クィック・メモを表示させます。プロトコルおよびフィーチャーはすべて同じように動作します。1 つのプロトコルまたはフィーチャーを対象とするサブプロセスに入り、そのプロトコルまたはフィーチャーに固有のコマンドを使用してその構成を行ったら、 **exit** でメイン Config> プロンプトが表示されます。

特定のプロトコルの構成に関する詳細なコマンド解説資料については、 2 巻の *MAS プロトコル構成と監視解説書* のどちらかの巻のそのプロトコルに関連する章を参照してください。このような章のそれぞれには、プロトコルについての入門となる解説、およびそのプロトコルに関する構成コマンドおよび監視コンソール・コマンドのそれぞれの説明が記載されています。MAS フィーチャーに関する同様な情報については、*MAS フィーチャーの使用と構成* を参照してください。

以上で Config (構成) プロセスとそのコマンドの概説が終わりました。これで talk 5 のコンソール・プロセスに移動することができます。どのプロセスにあっても、終了するために **Ctrl-p** を押せば、* プロンプトが表示されるので、 **talk** コマンドを使用して、別のプロセスに入ることができます。

```
RTP01 Config>   <Ctrl-p>
RTP01 *
```

操作 (talk 5、コンソール・プロセスの使用)

* プロンプトで **t 5** か **console** と入力すると、ネットワーク・ユーティリティーのアクティブ状態の監視と制御を行うためのコマンド行プロセスに入ります。

```
RTP01 *   <Enter>
RTP01 *t 5


CGW Operator Console

RTP01 +   <Enter>
RTP01 +
```

これでコンソール・プロセスの中に入ったので、コマンド・プロンプトが * から + に変わっています。Config (構成) プロセスとコンソール・プロセス、およびそれらのサブプロセスにはそれぞれ固有のプロンプトがあるので、どこにあっても現在の位置は一目瞭然 (りょうぜん) です。状況メッセージ CGW Operator Console が表示されるのは、リブート後に初めてコンソール・プロセスに入ったときだけです。talk 6 の

場合に説明したように、**t 5** と入力したとき、システムがブランク行を表示した場合は、前に talk 5 に入っていたので、**Enter** を押すだけ、最後にいた所から再開できることを意味します。

コンソール・プロセスでの作業中は、コマンドを入力して、ネットワーク・ユーティリティーのアクティブの実行状態を表示および変更することができます。ただし、このプロセスでは、ネットワーク・ユーティリティーの構成ファイルを変更することはできません。talk 5 コマンドによっては、構成パラメーターを動的に変更できるものもありますが、こうして行った変更は、ネットワーク・ユーティリティーのリブート時には消失します。ただし、talk 6 のもとで行った構成変更には、ネットワーク・ユーティリティーをリブートしなくても、talk 5 から動的に起動することができるものもあります。

コマンドの概説

メイン + プロンプトで **?** と入力すると、使用可能なコマンドがアルファベット順にリストされて表示されます。

```
RTP01 +?
ACTIVATE interface
BUFFER statistics
CLEAR statistics
CONFIGURATION of router
DISABLE interface or slot
ENABLE slot
ERROR counts
EVENT logging
FEATURE commands
INTERFACE statistics
MEMORY statistics
NETWORK commands
PERFORMANCE monitor
PROTOCOL commands
QUEUE lengths
RESET interface
STATISTICS of network
TEST network
UPTIME
RTP01 +
```

これらのコマンドには、ボックスの状況を表示させて見るためのものもあれば、その状況を能動的に変更するためのオペレーター・コマンドもあります。さらに、それぞれのプロトコルおよびフィーチャーのもとには、これら 2 種類のコマンドが混在して含まれるコンソール・サブプロセスがあります。主要な talk 5 コマンドをユーザー・タスク別にグループにまとめて、下に一覧表にしてあります。

- ボックス状況の表示

  buffer インターフェース・バッファー割り振りおよび使用中カウントを表示します。

  configuration
  ソフトウェア ID、プロトコル/フィーチャー、およびインターフェース状況を表示します。

  error 1 つまたは複数のインターフェースに関するフレーム・エラー件数を表示します。

interface
インターフェース番号のスロット/ポート・マッピング (talk 5 で talk 6 の **list dev** に相当するもの) に加えて、自己テスト合格/不合格カウントを表示します。

memory
取り付けられているメモリー、およびメモリーとグローバル (非インターフェース) バッファーに関する使用中統計を表示します。

queue 1 つまたは複数のインターフェースに関する入出力待ち行列カウントを表示します。

statistics
1 つまたは複数のインターフェースに関するパケット・カウントおよびバイト・カウントを表示します。

uptime
直前のリブート以降の経過時間を表示します。

- ボックス状況の制御

  activate
  talk 6 のもとで構成したばかりのスペア・インターフェースを使用可能にします。

  clear 1 つまたは複数のインターフェースに関するカウンターをリセットします。

  disable
  単一のインターフェースとスロット内のすべてのインターフェースのどちらかをオフラインにします。

  enable
  指定されたスロット内のすべてのインターフェースをオンラインにします。

  reset インターフェースを使用不可にし、talk 6 のもとで変更した新しい構成パラメーターを使用して再度使用可能にします。

  test 単一のインターフェースを検査し、オンラインにします。

- 他のサブプロセスへのアクセス

  event カウントの表示に進み、ログに記録される ELS メッセージを一時的に変更します。

  feature *name*
  指定されたフィーチャーに関する状況の表示および変更に進みます。

  network *interface number*
  指定されたフィーチャーに関する状況の表示および変更に進みます。

  performance
  CPU 統計の表示に進み、その収集および表示の方法を一時的に変更します。

  protocol *name*
  指定されたプロトコルに関する状況の表示および変更に進みます。

例 : ボックス状況の表示

talk 6 の場合と同様に、これらの talk 5 コマンドの一部を試行してみます。ボックス状況を表示するためのコマンドは、いずれも非常に単純です。1 ワードのコマンドを単に入力するだけで、出力が表示されます。

```
RTP01 +mem
Physical installed memory:       256 MB
Total routing (heap) memory:     228 MB
Routing memory in use:             3 %
                  Total  Reserve    Never     Perm     Temp     Prev
                                    Alloc    Alloc    Alloc    Alloc
Heap memory    239390720    26616 232309212  7029792    49828     1888
Number of global buffers: Total = 1000, Free = 1000, Fair = 194, Low = 200
Global buff size: Data = 4478, Hdr = 82, Wrap = 72, Trail = 7, Total = 4644
RTP01 +   <Enter>
RTP01 +buff
                   Input Buffers        Buffer sizes                    Bytes
Net   Interface     Req Alloc Low Curr   Hdr  Wrap  Data Trail Total    Alloc
0     ESCON/0       255   255  20    0    86    72  4478     0  4636  1182180
1     TKR/0         250   250   7    0    85    72  2052     7  2216   554000
```

ごらんいただけるように、**mem** ではボックス・レベルの状況が表示され、**buff** ではインターフェース・レベルの情報が示されます。 インターフェース単位の情報が示されるコマンド (**buff**、**config**、 **error**、**int**、 **queue**、**stat**) の場合はすべて、インターフェース番号の範囲をリストにして指定することができます。

```
RTP01 +int 0-1
                                                Self-Test  Self-Test Maintenance
Net   Net'   Interface   Slot-Port              Passed     Failed      Failed
0     0      ESCON/0     Slot: 1   Port: 1          0          0           0
1     1      TKR/0       Slot: 2   Port: 2          0          0           0
RTP01 +stat 1
Net   Interface      Unicast  Multicast      Bytes    Packets      Bytes
                    Pkts Rcv   Pkts Rcv   Received      Trans      Trans
1     TKR/0                0          0          0          0          0
```

各コマンドの出力のフィールドの説明については、*MAS ソフトウェア使用者の手引き*の「操作/監視プロセス」の章を参照してください。

例 : インターフェース状況の表示

config コマンドが特に重要なのは、出力の末尾に、指定されたインターフェースすべての状況が表示されるからです (この例では、編集によってブランク行は取り除かれています)。

```
RTP01 +c
Multiprotocol Access Services
NetU-TX1 Feature 1001 V3.1 Mod 0 PTF 1 RPQ 0 MAS.DE1 netu_38PB

Num Name  Protocol
0   IP     DOD-IP
3   ARP    Address Resolution
11  SNMP   Simple Network Management Protocol
29  NHRP   Next Hop Resolution Protocol
Num Name  Feature
2   MCF    MAC Filtering
7   CMPRS  Data Compression Subsystem
8   NDR    Network Dispatching Router
10  AUTH   Authentication

2 Total Networks:
Net  Interface   MAC/Data-Link        Hardware                    State
0    ESCON/0     ESCON               ESCON Channel               Not present

1    TKR/0       Token-Ring/802.5    Token-Ring                  HW Mismatch
RTP01 +
```

この例の出力が実際に得られたネットワーク・ユーティリティーの場合は、スロット 1 は空きで、イーサネット・アダプターがスロット 2 に入っていました。talk 6 では、構成したものが取り付けられていたアダプターに一致しなくても、問題になりませんが、その構成でリブートすると、talk 5 では、構成したインターフェースがアップにならないことが示されます。

構成が正しく行われていれば、このインターフェース状態は「Testing」で始まり、「Up」に移ったはずであり、**net** コマンドを使用して、アダプター固有のコンソール・サブプロセスに入り、詳細な状況情報が得られたはずです。しかし、現在の状態では、次のように表示されています。

```
RTP01 +net 0
 Network interface is not available.
RTP01 +
```

例 : 未構成プロトコルへのアクセス

特定のプロトコルで現在行われていることの表示および制御を行う場合は、 **protocol** コマンドを使用して、そのプロトコルに関するコンソール・サブプロセスに入ります。前に説明した場合と同様、 **p ?** と入力すると、特定のソフトウェア・ロード内でサポートされるプロトコルのクィック・リストが表示されます。例えば、データ・リンク交換 (DLSw) を選択します。

```
RTP01 +p dls                      <----- short for "protocol dlsw"
 Protocol DLSW is available but not configured
RTP01 +
```

DLSw が ***使用可能*** なのは、このソフトウェア・ロードでサポートされているからであり[8]、 ***構成されていない*** のは、talk 6 に入ったことがなかったし、DLSw を使用可能にするためのコマンドを入力したことがないからです。 DLSw が構成に入っていないままでボックスをブートしたので、DLSw は実行されていないし、talk 5 で表示したり変更したりする DLSw 状況はありません。

例 : 構成済みプロトコルへのアクセス

61 ページに記載されているように、この例を開始したネットワーク・ユーティリティーは、ブート時にすでに IP 構成を備えていました。したがって、IP はアクティブに稼働中であり、そのコンソール・サブプロセスに入って、使用可能なコマンドを表示させて見ることができます。

```
RTP01 +p ip                     <----- short for "protocol ip"
RTP01 IP>?
ACCESS controls
CACHE
COUNTERS
DUMP routing tables
INTERFACE addresses
PACKET-FILTER summary
PARAMETERS
PING dest_addr [src_addr size ttl rate]
REDUNDANT Default Gateways
RESET
RIP
```

8. もしサポートされていなかったら、**p ?** のもとで表示されることはなかったはずであり、システムが値 ″dls″ を認識することはなかったはずです。

```
ROUTE given address
ROUTE-TABLE-FILTERING
SIZES
STATIC routes
TRACEROUTE dest_addr [src_addr size probes wait ttl]
UDP-FORWARDING
VRID
VRRP
EXIT
RTP01 IP>
```

このコマンド・リストを、talk 6 で **IP config>** プロンプトに **?** と入力したときに表示されたコマンド・リストと比較してみれば、 talk 5 コマンドと talk 6 コマンドがまったく異なっていることが分かります。 talk 5 では、例えば、**ping** を開始して、ネットワーク・ユーティリティーから特定の IP アドレスにアクセスできるかどうか確認することができます。 これはアクティブ・ネットワーク・インターフェースに対して即時に働くアクティブ・コマンドであるため、talk 6 には属しません。同様にアクティブ状況を表示させて見るためのその他のコマンドも talk 5 コマンドであって、talk 6 コマンドではありません。

例 : 動的再構成

talk 6 で、トークンリング・ポート 2 の IP アドレスを 192.1.1.8 から 192.7.7.7 に変更しました。そこで、talk 5 のもとで表示される値を見てみます。

```
RTP01 IP>int                          <----- short for "interface"
Interface  IP Address(es)   Mask(s)
  TKR/0    192.1.1.8        255.255.255.0
```

talk 6 での変更がネットワーク・ユーティリティーの動作状態にまったく影響を与えなかったのは、明示コマンドにせよリブートにせよ、その変更をまだアクティブにしていなかったからです。コマンド **reset ip** を使用して、現行の talk 6 IP 構成を再読み取りし、実行システム内でそれを動的にアクティブにします。

```
RTP01 IP>reset ip
RTP01 IP>int
Interface  IP Address(es)   Mask(s)
  TKR/0    192.7.7.7        255.255.255.0
RTP01 IP>ex
RTP01 +
```

ごらんになればお分かりのように、IP アドレス変更 (および、talk 6 のもとで行ったその他の IP 変更すべても) これでアクティブになっています。 ほとんどのプロトコルには、動的再構成のための何らかのメカニズムがありますが、すべてのプロトコルに talk 5 のもとでの **reset** コマンドがあるわけではありません。動的再構成を行うための手段の詳細な背景については、 84ページの『動的再構成』 を参照してください。

以上で、talk 5 コマンドを発行して、システムの状況を能動的に照会する方法が分かりました。それとは別に、受動的なメカニズムとして、ネットワーク・ユーティリティーが生成するイベント・メッセージの表示も使用可能です。この場合は、**talk 2** を使用します。例によって、**Ctrl-p** を押して、現行プロセスを終了します。

```
RTP01 +   <ctrl-p>
RTP01 *
```

イベント・ログ (talk 2、モニター・プロセスの使用)

* プロンプトで **t 2** か **event** と入力して、ネットワーク・ユーティリティーのローカル・メッセージ・ログを表示させるためのプロセスにコンソールを接続します。

```
RTP01 *   <Enter>
RTP01 *t 2
00:00:50   GW.001:

Copyright 1984 Massachusetts Institute of Technology,
Copyright 1989 The Regents of the University of California


00:00:50   GW.002: Portable CGW RTP01 Rel NetU-TX1 Feature 1001 V3.1 Mod 0 PTF 1
 RPQ 0 MAS.DE1 netu_38PB
 strtd
00:00:50   GW.005: Bffrs: 1000 avail 1000 idle   fair 194 low 200
00:00:50  DOLOG: .....Remote Logging Facility is now available.....
```

この例では、ネットワーク・ユーティリティーの前回のブート以降にログに記録されたメッセージは、 4 つだけです。それぞれのメッセージの形式は、次のとおりです。

- タイム・スタンプの形式は *HH:MM:SS*

  上記のメッセージは 4 つすべてが同時刻、つまりクロック開始の 50 秒後
- メッセージ ID の形式は *SUBSYSTEM.ID*

  GW.001、GW.002、および GW.005 は GW (GateWay) サブシステム内の ELS メッセージ。 DOLOG は非標準、無条件タイプのメッセージ で、時々表示されます。
- メッセージ本体

  GW.001 の本体は 2 つの著作権表明。GW.002 の本体はソフトウェア・バージョン表明。特定の ELS メッセージの意味を調べたい場合は、 Web または CD-ROM 形式の *イベント・ログ・システム・メッセージの手引き* を参照してください。

talk 6 や talk 5 のプロセスの場合とは異なり、talk 2 プロセスにはユーザー・コマンド・プロンプトはありません。talk 2 にいるときは、コマンドを入力することはなく、ネットワーク・ユーティリティーによるメッセージの生成に応じて、それがローリングするのを監視するだけであるからです。talk 6 と talk 5 のどちらかの **event** サブプロセスのもとで、個々のメッセージまたはメッセージ・グループを使用可能または使用不可にすることによって、表示されるメッセージを制御します。ELS の概念および ELS メッセージの制御の概要については、100ページの『イベント・メッセージの監視』を参照してください。

次に、talk 2 のもとでは、入力としては、通常、* プロンプトに戻り、talk 5 または talk 6 に移動する場合に **Ctrl-p** を押すという形で行うものがあるだけです。メッセージのスクロールが速過ぎて読み取れない場合は、**Ctrl-s** を使用してスクロールを一時停止させ、**Ctrl-q** を使用してスクロールを再開させることができます。高速で移動するイベント・メッセージを捕えるためのオプションとしては、その他に次のような方法があります。

- コンソールで使用している PC 端末エミュレーション・プログラムの内部から、ログ・ファイルを起動する。

- UNIX または AIX ワークステーションから、ネットワーク・ユーティリティーに Telnet でログインして、コンソール接続にアクセスし、ローカル・ワークステーション・ファイル内への Telnet セッションの *tee* を行う。
- ELS メッセージをローカル talk 2 プロセスにではなく、ネットワークを通してリモート・ホストのログに記録できる、ネットワーク・ユーティリティーの機能を使用する。

これらのオプションについては、*MAS ソフトウェア使用者の手引き* の「イベント・ログ・システム (ELS)」の章に詳述してあります。

talk 2 に入ると、talk 2 の前回終了以降にバッファーに入れられたメッセージが、システムによってすべて表示されます。メッセージ・バッファーがオーバーランしたり、システムが現在メッセージを生成している速度が速過ぎて、メッセージを表示しきれない場合は、talk 2 の出力がスクロールする間、随所に「フラッシュされたメッセージ」に関する行が配されて表示されます。

talk 2 に入ろうとしているとき、現在のメッセージを表示させて見る前に、表示させたい古いメッセージのバックログがあることが分かっている場合は、 **talk 2** に入る前に、* プロンプトでコマンド **flush 2** を使用します。システムではバックログ全体を廃棄し、**flush** コマンドを入力した後で生成されたメッセージだけが talk 2 で表示されます。

Ctrl-p を押し、talk 2 を終了して、* プロンプトに戻ります。

構成の保管とリブート

この章の説明どおりに例をすべて実行した場合は、以下の talk 6 構成変更が開始以後に行われているはずです。
- 2 つのインターフェースの追加
- ホスト名の設定
- インターフェースのトークンリング速度の変更
- インターフェースの IP アドレスの変更

注 : 「fast-boot (高速ブート)」オプションも使用可能にしましたが、この変更は NVRAM に保管されているので、ここでは無関係です。

ネットワーク・ユーティリティー上では、talk 6 での変更は、実際には構成の RAM コピー内で行われます。したがって、これらの変更が永続的変更となり、ネットワーク・ユーティリティーの次回リブートに伴って使用されるようにしたい場合は、それをハード・ディスクに書き込む必要があります。このタスクを実行するには、2 つの異なるコマンド・シーケンスが使用できます。

```
RTP01 *t 6
                <Enter>
RTP01 Config>write
Config Save: Using bank A and config number 3

<boot messages start to appear>

RTP01 Config>   <Ctrl-p>
```

```
RTP01 *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes

<boot messages start to appear>
```

..... または .....

```
RTP01 *reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
The configuration has been changed, save it? (Yes or [No] or Abort):yes
Config Save: Using bank A and config number 3

<boot messages start to appear>
```

最初のシーケンスでは、ユーザーは、**reload** の前に、 **write** コマンドを使用して、変更をディスクにコミットします。2 番目のシーケンスでは、ユーザーが **write** コマンドを使用することはなく、システムが、**reload** に進む前に、変更をディスクに保管するかどうか尋ねてきます。

どちらの方式を使用するかは、ユーザー次第です。2 番目の方式を採用したがるユーザーが多いのは、考えたり入力したりする手間が少なくて済むからですが、 talk 6 での変更後間もなく **write** コマンドを出さないと、自分で行った変更を忘れやすい可能性もあります。

ファームウェア

以上では、ネットワーク・ユーティリティーのブートが操作ソフトウェアまで行われて、`Config (only)>` と `*` のどちらかのプロンプトが表示される例ばかりでした。したがって、まだアクセスしていない主要なコンソール・ユーザー・インターフェースがもう 1 つ残されています。つまり ファームウェア の場合です。 確かにファームウェアとの対話が必要になることは多くありませんが、ファームウェアによって、コードおよび構成ファイルをハード・ディスクにロードする代替手段が得られ、困難な問題の解消手段が得られる場合もあることを考えれば、ファームウェアについて知っておく必要があります。

ネットワーク・ユーティリティーのファームウェアは、システムの電源オンおよびブート論理を駆動する下位レベルのソフトウェアです。ハード・ディスクにではなく、フラッシュ・メモリーに常駐しているので、ディスク上のオペレーショナル・ソフトウェア・ロードの破壊などの障害が発生した場合は、新しいソフトウェアまたは構成ファイルを検索して、バックアップおよび実行ができます。

ファームウェア・ユーザー・インターフェースにアクセスするためには、ユーザー・コンソールでローカルまたはダイヤルイン ASCII 端末エミュレーションが使用されている必要があります。ファームウェア・ユーザー・インターフェースに Telnet でログインすることはできません。メイン・ファームウェア・メニューにアクセスする場合は、`*` プロンプトから **reload** を実行し、次のようなメッセージが表示されるのを待ちます。

```
Starting Boot Sequence...
Strike F1 key now to prematurely terminate Boot
```

これらのメッセージは、それぞれが数秒しか表示されないので、注視が必要です。プロンプトが表示されたら、**F1** を押すか、または、メッセージの表示前も表示中も **Ctrl-c** を押さえたままにして、通常のブート・シーケンスを中断し、ファームウェアに入ります。

ブート・シーケンスの中断後は、システムがプロンプトを出して監視パスワードの入力を指示し、それに従わないと、ファームウェア・メイン・メニューを表示させることができない場合があります。このパスワードによって、機密の下位レベル・ファームウェア機能へのアクセスが制御されます。工場出荷時のその初期値は「2216」です。これは、「Utilities」メニューのもとで、ファームウェア自体からからでない限り変更できません。

ネットワーク・ユーティリティーにモデム経由でダイヤルインして、コンソールにアクセスし、**再ロード**時に接続が失われた場合は、元どおり再接続しても、**F1** を押すタイミングに間に合わない可能性があります。この場合は、Config (構成) プロセスの**ブート**・サブシステムに進み、 **disable auto-boot** コマンドを出します。

```
*t 6
Gateway user configuration
Config>boot
Boot configuration
Boot config>dis auto             <----- short for "disable auto-boot"
Select the duration to disable autoboot: (once, always) [always] once
AutoBoot mode is now disabled once.

Operation completed successfully.
Boot config>   <Ctrl-p>
*rel y                           <----- short for "reload, yes"

<boot messages appear>
```

AutoBoot モードが使用不可にしてあれば、システムが**再ロード**・プロセスをファームウェアで停止するので、ユーザーが **F1** を押す必要はありません。そうすれば、元どおり再接続すると、メインメニューが表示されるか、監視パスワードの入力を要求するプロンプトが表示されます。

いつも talk 6 で自動ブートを使用不可にしてファームウェアにアクセスしている場合や、持続期間 (once/always) プロンプトが表示されなかった場合は、命令コードにアクセスするときに使用可能に戻しておくことを忘れないようにしないと、**再ロード**のたびに、ファームウェア内で停止することになります。

ファームウェアにアクセスすると、次のようなテキスト・メニューがユーザー・コンソールに表示されます。

```
Nways System Firmware
Version 3.00 built on 04/21/98 at 22:18:42 in cc3:paws_netu6e:cc3_6e
(C)Copyright IBM Corporation, 1996, 1998.  All rights reserved.
                          System Management Services
 Select one:
  1. Manage Configuration
  2. Boot Sequence Selection
  3. Select Device to Test
  4. Utilities



    Enter    -    Esc=Quit   -     F1=Help   -    F3=Reboot  -   F9=Start OS
  ------------   ------------   ------------   -------------   ------------
```

ファームウェアのメニュー構造とそのオプションについては、*2216 and Network Utility Service and Maintenance Manual* の「Using 2216 Firmware」で説明されています。入力するコマンドはありませんが、オプションを選択して一連のメニュー間を移動します。 ファームウェアから実行する必要がある主要なタスクには、以下のものがあります。

- ディスクへの構成ファイルおよびオペレーション・ソフトウェアの転送

  これらの機能は、talk 6 のもとでの**ブート**・サブシステム機能と同等です。ファームウェア・メニューの「″Utilities」と、次は「Change Management」のもとにあります。
- ファームウェア自体のアップグレード

  この場合は、メインメニューの「Utilities」から始め、次に「Update System Firmware」に進みます。

メニュー間を少し移動してみれば、メニューになれることができます。ファームウェア・タスクのいずれかを完了したら、**Esc** を押せば、メインメニューに戻ります。継続する場合は、次のオプションのいずれか 1 つを使用します。

F3=Reboot - ブート・プロセス全般を開始します。自動ブートが使用不可にしてある場合は、再度ファームウェア内で停止することになります。ダイヤルインしている場合は、再度接続が失われます。

F9=Start OS - ファームウェアを越えて命令コードに入るまでブート・プロセスが継続します。

以上でこのネットワーク・ユーティリティーのユーザー・インターフェースの学習が終了しました。以下の各章では、この章で記述した必要な背景知識を身につけていることを前提にして、その他にも数多くあるネットワーク・ユーティリティーの重要な概念および方式について説明します。

第6章 構成の概念と方式

この章には、ネットワーク・ユーティリティーの構成について、以下のことも含めて背景情報が記載してあります。
- ネットワーク・ユーティリティーを構成することの意味
- 構成情報を保管および転送するさまざまな手段
- 構成の作成および変更に使用できるさまざまな方式

25ページの『第3章 初期構成の実行』では、ネットワーク・ユーティリティーを構成する基本的な方式について説明し、その選択について指針を示しました (25ページの『構成方式の選択』を参照)。この章では、それぞれの方式について詳述し、両方式を合わせて使用する方法について説明します。

構成ファイルを処理する特定の手順およびコマンドについては、 87ページの『第7章 構成ファイルの取り扱い』を参照してください。一般的な構成タスクには、 37ページの『第4章 ユーザー・インターフェースのクィック・リファレンス』で説明されているものもあります。

構成の基本

ネットワーク・ユーティリティーの構成とは、以下のような要素も含めて、ソフトウェアの動作を制御するデータ項目を集めたものです。
- 起動したいインターフェース
- 始動させたいリンク
- アクティブにしたいプロトコルおよびフィーチャー
- 特定のプロトコルまたはフィーチャーの中でアクティブにしたい機能
- 使用したいネットワークのアドレスと名前

ネットワーク・ユーティリティーをブートすると、システムでは、その構成をハード・ディスク上のファイルから読み取り、そのファイルに収められている情報に従って、インターフェースおよびプロトコルを起動します。 なお、ファイルの作成は、次のいずれかの方法で行うことができます。
- ユーザー端末コンソールでコマンド行インターフェースを使用する。

  コマンドを入力して、メモリー内に構成データ項目を作成した上で、ネットワーク・ユーティリティーのハード・ディスクに構成を書き込みます。
- PC またはワークステーションで稼働するグラフィック構成プログラムを使用する。

  ワークステーションで構成を作成してから、それをネットワーク・ユーティリティーのハード・ディスクに転送します。

システムがアップし稼働すれば、コマンド行インターフェースを使用して、次のような種類の構成変更を加えることができます。
- 実行システム内で有効になるが、ファイルに保管されないので、リブートすると消失する変更
- 実行システムで有効になり、ファイルにも保管されるので、リブートしても消失しないで保持される変更

- 実行システムでは有効にならないが、ファイルに保管され、リブートして初めてアクティブになる変更

ディスク上の構成ファイル

ネットワーク・ユーティリティーのハード・ディスクは、2 つの命令コード (ソフトウェア) ロードのそれぞれに 1 つずつ、合計 2 つの論理 バンク を含むように編成されています。したがって、アクティブ・コード・ロードを一方のバンクに収容し、新規ロードをもう一方のバンクに転送してテストし、必要なら、元のロードに戻すことができます。 2 つのバンクは、それぞれバンク A およびバンク B と呼んでいます。

2 つのバンクのそれぞれに、構成ファイルが 4 つずつ収まります。バンク A 内のコード・ロードは、バンク A 内の 4 つの構成ファイルのいずれとでも一緒にブートアップすることができます。バンク B の場合も同様です。バンク A の構成ファイルをバンク B のコード・ロードで使用する場合は、まず最初に、バンク A の構成ファイルをバンク B 内の 4 つのファイル位置のいずれか 1 つにコピーする必要があります。

ハード・ディスク上のバンクに構成ファイルを転送する方法には、次の 4 つがあります。

1. talk 6 コマンド **write** を使用して、RAM 内の現行構成を書き出し、ディスク・ファイルとして保管する。

   このコマンドを使用するのは、ネットワーク・ユーティリティーの構成に、構成プログラムではなく、コマンド行 talk 6 プロセスを使用する場合です。

   注：「talk 6」という用語になじみがない場合は、 57ページの『第5章 コマンド行インターフェースの解説』でコマンド行インターフェースについて習得してください。
2. TFTP または Xmodem を使用して、構成ファイルをローカル・サーバー (PC またはワークステーション) から直接ハード・ディスク上に転送する。

   構成ファイルは、構成プログラムから作成したものでも、このネットワーク・ユーティリティーや別のネットワーク・ユーティリティーから以前転送されたものでも、転送することができます。
3. SNMP を使用して、構成データを構成プログラムから RAM 内に転送した上で、ハード・ディスク上に転送する。

   ファイル転送は、構成プログラムから開始します。この方式が使用できるのは、構成プログラムから転送する場合だけです。
4. 構成ファイルをバンク間でコピーする。

   コピーおよびその他の構成ファイル管理操作は、ネットワーク・ユーティリティー・コンソールで、 talk 6 のもとの **boot** サブプロセスから開始します。

これらの操作の詳細については、87ページの『第7章 構成ファイルの取り扱い』の中の 91ページの『新規構成ファイルのロード』を参照してください。

構成方式

コマンド行インターフェース

コマンド行インターフェースを使用する場合は、まず最初にローカル・コンソールまたはリモート・コンソールでネットワーク・ユーティリティーを立ち上げます。このための方法、および * または Config (only)> プロンプトにアクセスする方法については、 15ページの『第2章 ユーザー・コンソールの始動』を参照してください。

アクティブ・コンソールで * プロンプトが表示されている場合は、**talk 6** を使用して Config (構成) プロセスにアクセスします。Config (only)> が表示されている場合は、使用できるのは Config (構成) プロセスだけです。Config (構成) プロセスから、メニュー間をナビゲートし、コマンドを発行してインターフェースおよびプロトコルを構成し、こうして行った変更をネットワーク・ユーティリティーのハード・ディスク上の構成ファイルに書き込みます。

ほとんどの場合、コマンド行インターフェースを使用して構成するのは、ユーザーが接続されているネットワーク・ユーティリティーだけです。しかし、1 台のネットワーク・ユーティリティーを使用して、他のネットワーク・ユーティリティーに転送される構成ファイルを簡単に作成することができます。 talk 6 のもとで **write** コマンドを使用して、構成をディスク・ファイルに保管してから、ブート・サブプロセスのもとで **tftp put** を使用して、ファイルをネットワーク・ユーティリティー外に転送するだけです。これで、構成プログラムを使用した場合と同じように、ターゲット・ネットワーク・ユーティリティーにロードできるファイルになります。

コマンド行からしか使用できないオプションとして、Quick Config (クィック構成) があります。ステップ 27ページの3 で説明されているように、 Quick Config では、ネットワーク・ユーティリティーのプロトコルのサブセットの初期構成が行われます。この場合、システムでは、ユーザーによるコマンドの入力を待つ通常のモードとは異なり、ユーザーに質問する形を取ります。

ネットワーク・ユーティリティーをリブートしなくても構成変更を動的にアクティブにすることができる機能も、コマンド行インターフェースだけのものです。73ページの『例 : 動的再構成』では、talk 5 を使用して、talk 6 のもとで行われた IP アドレス変更をアクティブにする方法を説明しました。84ページの『動的再構成』では、ネットワーク・ユーティリティーの動的再構成機能の詳細な背景について説明しています。

構成プログラム

ネットワーク・ユーティリティーは、2216-400 を構成する場合に使用できるグラフィック構成プログラムと同じ構成プログラムでサポートされています。このプログラムを PC またはワークステーションで実行し、作成した構成を 1 台または複数台の 2216 またはネットワーク・ユーティリティーに送信します。 2216/ネットワーク・ユーティリティーの構成プログラムには、次のオペレーティング・システムのそれぞれで使用できるバージョンがあります。

- Microsoft™ Windows 95 または Windows NT
- IBM AIX
- IBM OS/2

IBM では、主要なリリースの構成プログラムを CD-ROM および Web で配布しています。ただし、正規保守 PTF は、Web でご利用いただくしかありません。*構成プログラム使用者の手引き* には、システム要件が示され、プログラムのインストールおよび使用の方法が記載されています。

ネットワーク・ユーティリティーおよび 2216-400 に対するサポート

構成プログラムを使用して新規構成を開始すると、ドロップダウン・リストが表示されるので、新規構成が 2216-400 用であるか、ネットワーク・ユーティリティー用であるかの選択を行うことができます。どちらを選択するかによって、次のものが変わります。

- 構成できるアダプター・スロットの数
- 構成できるアダプターのタイプ (ネットワーク・ユーティリティーがサポートするのは、2216 アダプターの全リストのうちの一部です)
- 構成できるプロトコルおよびフィーチャー (ネットワーク・ユーティリティーがサポートするのは、全 MAS 機能の一部です)
- さまざまなチューニング・パラメーターのデフォルト値 (ネットワーク・ユーティリティーは、予定のアプリケーションに応じて事前設定されています)

2216-400 用とネットワーク・ユーティリティー用の構成を交換することはできません。

構成ファイルの形式

構成プログラムでは、次の 3 つの異なる形式の構成ファイルを処理します。

- .CSF ファイル : 構成プログラムに固有の形式のデータが入ります。

  この形式は、*構成* プルダウン・コマンド **Open**、**Save**、**Save as**、および **Delete** で使用します。内容は、ソフトウェアのリリースに応じて異なります。**Open** を実行すると、構成プログラムが自動的にデータ項目を移行します。
- .CFG ファイル : ルーターに固有の形式のデータが入ります。

  この形式を使用するのは、ルーターに転送するファイルを作成したいとき、またはルーターから転送されたファイルを読み込みたいときです。
- .ACF ファイル : ASCII フラット・ファイル形式のデータが入ります。

  構成を ASCII フラット・ファイルに書き出し、テキスト・エディターを用いて変更を加え、読み込んで戻すことができます。

構成の転送と起動

構成プログラムからネットワーク・ユーティリティーに構成を転送する方法には、次の 2 通りがあります。

1. ルーター形式 (.CFG) ファイルを作成し、ネットワーク・ユーティリティーの近くのサーバーに転送し (FTP を使用すると考えられる)、Xmodem または TFTP を用いてネットワーク・ユーティリティーのハード・ディスク上にリトリーブする。構成がアクティブになるのは、構成を選択して、ネットワーク・ユーティリティーをリブートした時点です。
2. 構成プログラムの ″send″ 操作を開始します。構成プログラムでは、SNMP を使用して、ネットワーク・ユーティリティー内に個々のデータ項目 (実際のファイルではない) を送信します。ネットワーク・ユーティリティーでは、その現行構成のア

クティブ・メモリー・コピーを消去し、データ項目を受信してから、ディスクに新規ファイルとして書き込みます。″send″ を実行する前に、ネットワーク・ユーティリティーは新規構成でリブートする必要があるかどうか、必要があるとすれば、いつにするかの選択を、構成プログラムで行っておきます。送信した構成がアクティブになるのは、リブート後です。

それぞれの方式で、転送および起動の対象となるのは、ネットワーク・ユーティリティーの構成全体であることに注意してください。構成プログラムには、わずかな構成変更でも、それを動的に送信して、ネットワーク・ユーティリティーのリブートを必要としないでネットワーク・ユーティリティーでそれをアクティブにすることができるメカニズムはありません。この種の動的再構成が実行できるのは、コマンド行インターフェースを使用する場合だけです。

その他の構成プログラム・フィーチャー

構成プログラムには、次のようなフィーチャーがあります。

- 時限再始動

  構成プログラムの機能を使用して、構成をルーターに送信する場合は、ルーターに再始動と構成の使用を行わせたい日時を指定することができます。

- 複数ルーター送信

  構成ファイルを受信するターゲット・ルーターのリストを作成し、それぞれのルーターごとに、構成ファイル、再始動時刻、その他について、同じか別かを指定することができます。

- コマンド行機能

  構成プログラムを開始したワークステーションのオペレーティング・システム・コマンド行を使用して、プログラム内で使用可能な構成操作を自動化することができます。元のコマンド行または引き数ファイルに引き数を入れれば、構成プログラムがそのような引き数を使用してその操作を誘導します。

  AIX からの場合は、この機能を使用するのに、オペレーティング・システムのグラフィック環境 (例えば、Xwindows) がインストールされている必要はありません。**headless** コマンドを使用して、構成プログラムを開始することができます。

- ASCII ファイル・サポート

  構成プログラムを使用して、ASCII 形式の構成ファイルの作成および読み取りを行うことができます。 また、構成ファイルを形式間で変換することもできます。ASCII 構成ファイルが有用なのは、構成を構成プログラムにロードしないで、一度に多くの構成を更新したい場合です。このフィーチャーは、新規構成を作成したり、既存の構成に大きな変更を加える場合の使用は考えられていません。

- オンライン・ヘルプ

  構成プログラムは、広範囲に及ぶヘルプ・ファイルのセットをサポートします。どのデータ項目に位置している場合でも、**F1** を押すと、そのデータ項目を記述し、そのデフォルト値および許容範囲を示すポップアップ・ウィンドウが表示されます。

動的再構成

ネットワーク・ユーティリティーをリブートしなくても構成パラメーターを動的に変更することができる機能は、コマンド行インターフェースからしか使用できません。表11 には、コマンド行から構成パラメーターを変更できる方法が、変更によってリブート前の実行システムに影響が生じるかどうかにも、変更がアクティブになるのがリブート後であるかどうかにも関係なく要約してあります。「ディスクへの書き込みの選択」欄では、メイン talk 6 メニューから **write** コマンドを出して、構成をディスクに保管することにしたか、**reload** コマンドの発行後のディスクへの保管を要求したかを示します。

表 11. 動的再構成オプション

方式	ディスクへの書き込みの選択	実行システムへの影響	リブート後アクティブ
talk 6 での変更	はい	なし (注 1)	はい
	いいえ	なし (注 1)	いいえ
talk 5 での変更	該当しない	あり	いいえ
talk 6 で変更、talk 5 で起動 (注 3)	はい	あり (注 2)	はい
	いいえ	あり (注 2)	いいえ

注:

1. ネットワーク・ディスパッチャー・フィーチャーはこのルールの例外で、talk 6 での変更は即時に有効になります。
2. 変更が有効になるのは、起動コマンドを出した時点であり、パラメーターを変更した時点ではありません (talk 5 での直接変更の場合とは異なります)。
3. APPN プロトコルはこのルールの例外で、talk 6 での変更を起動するのは、 talk 5 からではなく、talk 6 からです。

これで分かるように、一般的なルールとしては、talk 6 での変更がアクティブになるのは、リブートの後か、talk 5 コマンドによる起動の後ということになります。 talk 5 コマンドは即時にアクティブになりますが、リブートと同時に消失します。

すべての構成データ項目が上記の方法のいずれでも変更できるとは限りません。該当のデータ項目がシステムのどの部分に (プロトコルかインターフェースかなど) 属するかによって異なります。例えば、DLSw、SNMP、および ELS 構成では、すべてが talk 6 および talk 5 で同じコマンドのほとんどをサポートします。したがって、変更の永続性を必要とするかどうかに応じて、どちらで変更を行っても構いません。talk 6 での変更を起動するための talk 5 コマンドはありません。同じ変更を行うための talk 5 コマンドが存在するからです。

しかし、IP では、talk 6 コマンドに対応する talk 5 コマンドはありません。現行 talk 6 構成をアクティブにする場合は、 talk 5 で **reset ip** を使用します。インターフェース再構成も、単一の talk 5 コマンドを使用してアクティブにします。インターフェースのダウンおよびアップを伴うからです。

アダプターおよびインターフェースにかかわる一般的な動的再構成の例については、 43ページの『物理アダプターおよびインターフェースの構成』を参照してください。

構成方式の結合

構成にコマンド行インターフェースしか使用しないと決めている場合は、構成プログラムを使用する必要はまったくありません。しかし、構成プログラムを使用する場合は、次のような理由が幾つかあるため、やはりコマンド行 Config (構成) プロセスを使用する必要があります。

- プロトコルによっては、アクティブネットワーク・ユーティリティー上の構成プログラム構成を表示させて見る方法は、talk 6 以外にはない場合があります。
- 構成項目には、ELS メッセージや PCMCIA EtherJet アドレスなどのように、アクセスできるのは talk 6 による場合だけで、構成プログラムからはアクセスできないものがあります。
- コマンド行が、動的構成変更を行う唯一の手段です。

構成プログラムと talk 6 の結合を使用する場合は、構成プログラムの .CSF ファイルは、ネットワーク・ユーティリティーの構成情報と同期に保持する必要があります。一般的な事例を挙げれば、次のようになります。

1. 初期構成を構成プログラムで行います。
2. SNMP を使用するか、または .CFG ファイルを作成して手動で転送することによって、この構成をネットワーク・ユーティリティーに転送します。
3. コマンド行インターフェースを使用して、ネットワーク・ユーティリティーで構成の起動、デバッグ、およびチューニングを行います。
4. SNMP を使用するか、.CFG ファイルに読み込むことによって、構成をリトリーブして構成プログラム内に戻します。
5. 動的構成変更を加える必要に応じて、ネットワーク・ユーティリティーから構成を規則的にリトリーブします。
6. 計画したネットワーク変更を構成プログラムから行い、新規構成をネットワーク・ユーティリティーに送信します。

構成ファイルを転送するための特定の手順については、87ページの『第7章 構成ファイルの取り扱い』を参照してください。

新しい MAS リリースへの構成の移行

保守目的にせよ、新規機能を採用するためにせよ、時折は、ネットワーク・ユーティリティーを新しいリリースの MAS に移行する必要が生じます。[9] ネットワーク・ユーティリティー構成にはリリース固有の情報が含まれるため、構成についても、インストールする MAS のリリースのレベルにアップグレードする必要があります。

コマンド行インターフェース ***だけ*** を使用してネットワーク・ユーティリティーを構成している場合は、119ページの『第10章 ソフトウェアの保守』に記載されている手順の 1 つを使用して、新しいリリースの MAS のロードおよびブートを行うだけで済みます。新しいリリースの MAS がブートすると、構成は新しいリリース・レベルに合わせて自動的に調整されます。このような調整はメモリーで行われ、構成のデ

9. コード・アップグレードに関する背景情報および手順については、119ページの『第10章 ソフトウェアの保守』を参照してください。

ィスク・コピーには影響が及びません。 Config> プロンプトで **write** コマンドを発行して、アップグレード後の構成をディスクに保管できます。以前のリリースからのブートが必要になる場合に備えて、以前のレベルのコードが入っているディスク・バンクに以前のリリースの構成のコピーを残しておくことができます。

たとえ時折だけでも ***もっぱら*** 構成プログラムを使用している場合は、構成プログラムを使用して構成をアップグレードする ***必要があります***。新規リリースの MAS には、新規リリースの構成プログラムが必ず付いています。構成のアップグレードは、以下の手順に従って行います。

1. 旧リリース・バージョンの構成プログラムの使用
   a. 必要なら、ネットワーク・ユーティリティーから構成をリトリーブして構成プログラムに入れます。これを行う必要があるのは、前回構成プログラムからネットワーク・ユーティリティーに構成を送信した後で、コマンド行変更を構成に加えたことがある場合だけです。
   b. **Configure** ドロップダウン・メニューの **Save** または **Save as** を使用して、構成を .CSF ファイル (内部構成プログラム形式) として保管します。
2. 新リリース・バージョンの構成プログラムの使用
   a. **Configure** ドロップダウン・メニューの **Open** を使用して、構成をオープンします。新しいバージョンの構成プログラムでは、構成を読み込みながら、新しいリリースのレベルに自動的にアップグレードしていきます。
   b. 新しいリリース・バージョンの構成を保管します。
   c. 新しいリリース・バージョンの構成がネットワーク・ユーティリティーに転送され、新しいリリースの MAS をブートすると、自動的にアクティブになります。

第7章 構成ファイルの取り扱い

この章では、次のことを行うための特定の手順について説明します。
- ネットワーク・ユーティリティー のハード・ディスク上の構成ファイルの表示と管理
- ネットワーク・ユーティリティーの外部からそのハード・ディスクへの構成の転送
- ネットワーク・ユーティリティーのハード・ディスクからの構成ファイルの転送

ネットワーク・ユーティリティーの構成に関する背景情報については、25ページの『第3章 初期構成の実行』および 79ページの『第6章 構成の概念と方式』を参照してください。

この章で扱う個々のコマンドについての詳細は、 *MAS ソフトウェア使用者の手引き* の中の下記の章を参照してください。

- 「BOOT Config の使用による変更管理の実行」
- 「変更管理の構成」

ディスク上の構成ファイルの管理

ネットワーク・ユーティリティーのハード・ディスク上の構成ファイルをリストおよび管理するためのコマンドは、すべてがブート Config (構成) サブプロセス内にあります。次の例には、このサブプロセスにアクセスして、使用可能コマンドをリストさせる方法が示してあります。

```
*t 6
                <Enter>
Config>boot
Boot configuration
Boot config>?
ADD description
COPY software
DESCRIBE software VPD
DISABLE boot choices
ENABLE boot choices
ERASE software
LIST software status
LOCK Config File
SET boot information
TFTP software
TIMEDLOAD software
UNLOCK Config File
UPDATE Firmware
EXIT
Boot config>
```

構成のリスト表示

list コマンドは、2 つのコード・ロード・バンクのそれぞれの 4 つの位置に入っている、構成ファイルを表示させるための開始点になります。ここに示す同じ表示が、メニュー上の多くのコマンドに組み込まれています。

```
Boot config>li
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 03 Aug 1998 10:04 |
| CONFIG 1 - AVAIL       |                                 | 04 Aug 1998 13:50 |
| CONFIG 2 - ACTIVE  *   | example config 1                | 04 Aug 1998 13:52 |
| CONFIG 3 - AVAIL       |                                 | 04 Aug 1998 06:41 |
| CONFIG 4 - AVAIL       |                                 | 04 Aug 1998 09:43 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - PENDING        |                                 | 05 Aug 1998 03:41 |
| CONFIG 1 - PENDING *   |                                 | 31 Jul 1998 12:59 |
| CONFIG 2 - AVAIL       |                                 | 31 Jul 1998 09:50 |
| CONFIG 3 - AVAIL       |                                 | 31 Jul 1998 09:52 |
| CONFIG 4 - AVAIL       |                                 | 31 Jul 1998 12:50 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

 Auto-boot mode is enabled.   Fast-boot mode is enabled.

Time Activated Load Schedule Information...

The load timer is not currently activated.
Boot config>
```

イメージ (コード・ロード) および構成の状態の定義は、以下のとおりです。

ACTIVE (アクティブ)
ファイルがネットワーク・ユーティリティーの現行ブートに使用されました。

AVAIL (使用可能)
ACTIVE にすることができる有効なファイルです。

CORRUPT (破壊)
ファイルは使用不能です。その理由は、通常、この位置へのファイル転送が正常に完了しなかったことにあります。

LOCAL (ローカル)
ファイルが使用されるのは、次回のロードまたはリセット時になります。使用後、ファイルは AVAIL 状態に入ります。

NONE (なし)
該当の位置にファイルがありません (初期状態)。

PENDING (保留)
ファイルが使用されるのは、ネットワーク・ユーティリティーの次回の再ロード、リセット、または電源オン時になります。

特定の構成ファイルの内容を思い出す必要がある場合は、 **add** コマンドを使用して、簡単な記述を入力します。

構成をアクティブにする方法

特定の構成ファイルをアクティブにする場合は、ACTIVE または PENDING コード・ロードが入っているバンク内の PENDING 構成ファイルにした上で、ネットワーク・ユーティリティーをリブートします。ファイルがすでに存在している場合、またはファイルを作成する場合に、次のようにしてこれを行います。

- ファイルがすでにディスク上にある場合は、 **set** コマンドを使用して、次回のブートに使用するバンクおよび構成ファイル位置を指定します。

ソース・バンクおよび構成の新規設定については、単に次回のブートだけのためである (状態は LOCAL になる) のか、今後のブートすべてのためである (状態は PENDING になる) のかを指定することができます。

通常、**set** コマンドを使用するのは、 TFTP または Xmodem の使用によるファイルの転送後になります。

- talk 6 **write** コマンドの使用による新規ファイルの作成である場合は、自動的に ACTIVE バンク内の PENDING 構成になります。

  write を実行すると、システムでは、アクティブ・メモリー内の構成を ACTIVE バンク内の次のロック解除位置 (順次交替する) に書き込みます。ファイル位置を選出することはありません。特定のファイルが上書きされないようにしたい場合は、 **lock** コマンドを使用します。

  新規ファイルが PENDING になっているため、**write** の後に続けて **reload** を実行することができます。使用されている特定の位置に注意する必要もなければ、 **set** コマンドを発行する必要もありません。

- **reload** と入力し、構成変更の保管を選択して、ファイルを暗黙的に作成する場合は、新規ファイルは、リブートが始まる前に PENDING 構成になります。

  次のシーケンスの働きは、**write** コマンドを発行した場合と同じになります。

  ```
  *rel y
  The configuration has been changed, save it? (Yes or [No] or Abort):yes
  ```

- 構成プログラムで構成を直接転送するための **Communicate** オプションを使用してファイルを作成する場合は、新規ファイルは PENDING 構成になります。

  この場合も、働きは **write** コマンドを発行した場合と同じになります。 構成プログラムからリブートを要求した場合は、この構成がアクティブになるのは、リブートが行われてからになります。

遅延起動

構成の時限起動 (不在で行われると想定される) を行わせる方法には、次の 2 通りがあります。

- 構成プログラムを使用し、構成の転送に **Communicate** オプションを使用する場合は、ネットワーク・ユーティリティーがリブートし、構成をアクティブにする日時を指定することができます。
- どんな方式を使用して、ネットワーク・ユーティリティーのハード・ディスク上に構成ファイルを作成した場合でも、ブート Config (構成) サブプロセスで **timedload** コマンドを使用して、ネットワーク・ユーティリティーがリブートし、指定されたコード・ロードおよび構成をアクティブにする日時をスケジュールすることができます。

  現行のコード・ロードと構成を選択した場合は、この機能は単にスケジュールによるリブート操作になります。

ファイル・ユーティリティー

ブート Config (構成) サブプロセスには、ディスク上の構成ファイル (およびコード・ロード) を管理するためのユーティリティー・コマンドが数多く用意されています。

add　構成の簡単な記述を入力するためのものです。

copy バンク間またはファイル位置間、あるいはその両者間で構成をコピーするためのものです。

erase 構成ファイルを除去し、位置の状況を NONE に戻すためのものです。

lock ファイル作成方式のいずれかによってファイルが上書きされることがないようにするためのものです。

unlock
ファイル位置が新規ファイル用としてあらためて使用できるようにするためのものです。

ファームウェア変更管理

ブート Config (構成) サブプロセスの構成管理機能のほとんどは、ネットワーク・ユーティリティーのファームウェア・メニューからでも使用可能です。アクセスする場合は、ファームウェア・メインメニューから始めて、次のシーケンスを使用します。

- オプション 4 「Utilities」
- オプション 12 「Change Management」

新規構成ファイルのロード

表12 には、ネットワーク・ユーティリティーの外部からそのハード・ディスクに構成を転送できる方法が要約してあります。SNMP の場合は、構成プログラムからネットワーク・ユーティリティーへの直接転送になりますが、TFTP および Xmodem の場合は、構成ファイルがネットワーク・ユーティリティーへのファイル・サーバーの役割を果たすワークステーション上にあることが必要です。

ネットワーク・ユーティリティーへの転送にどちらの方式を選択するかは、ネットワーク・ユーティリティーに接続できる方法、構成プログラムを使用しているかどうか、ワークステーションで使用しているソフトウェア、およびユーザーの好みによって決まります。ネットワーク・ユーティリティーの構成ファイルは、一般的に非常に小さいので、低速モデムを介する転送で時間が不当にかかるということはありません。

表 12. 構成のロード

物理接続機構	回線 プロトコル	転送 プロトコル	ツール	デフォルトの IP アドレス
サービス・ポート + ヌル・モデム	非同期 端末	Xmodem	ファームウェア	該当しない
サービス・ポート + 外付けモデム PCMCIA モデム	SLIP	TFTP	命令コード	ネットワーク・ユーティリティー = 10.1.1.2 ワークステーション = 10.1.1.3
		SNMP	構成プログラム	
PCMCIA EtherJet イーサネット LIC (10 Mbps) トークンリング LIC	IP	TFTP	命令コード ファームウェア	ネットワーク・ユーティリティー = 10.1.0.2 ワークステーション = 10.1.0.3
		SNMP	構成プログラム	
任意の IP ネットワーク・インターフェース	IP	TFTP	命令コード	デフォルト値なし
		SNMP	構成プログラム	

以下の各項では、使用できる構成転送手順を転送を開始するツール別にグループにまとめ、それぞれについて要約しています。

構成プログラムの使用

構成プログラムからネットワーク・ユーティリティーに構成を転送する方法には、次の 2 通りがあります。

1. ルーター構成ファイルを作成した上で、ネットワーク・ユーティリティーの命令コードまたはファームウェアを転送を行う元のツールとして使用する。
2. SNMP を使用して、ネットワーク・ユーティリティーのメモリーまたはハード・ディスクに構成を転送する。

ルーター構成ファイルのエクスポート

構成プログラムを開始し、ネットワーク・ユーティリティーの構成を作成したら、ナビゲーション・ウィンドウに移動して、次のようにします。

1. **Configure** ドロップダウン・メニューをアップにして、 **Create router configuration** を選択する。

2. 構成プログラムを実行しているワークステーション上で、ルーター構成ファイル (.cfg) を保管させたいディレクトリー・パスおよびファイル名を選択する。
3. **OK** をクリックする。構成プログラムがこのファイルをディスクに書き込みます。
4. **Configure** のもとで **Save as** を選択して、アーカイブする場合の優先形式である .csf 形式でも構成を保管する。

次に、ユーザーの責任でファイルをネットワーク・ユーティリティーにロードします。ロードの実行には、命令コードとファームウェアのどちらかを使用します。93ページの『命令コードの使用』または 95ページの『ファームウェアの使用』に記載されている手順のいずれを使用しても構いません。

構成プログラムを実行している PC またはワークステーションが、これらの手順でのファイル転送用の TFTP または Xmodem サーバーとして使用できない場合は、サーバーになることができるワークステーションに、まず .cfg ファイルを移動しておく必要があります。ワークステーション間でのファイルの移動には、任意のファイル転送方式 (例えば、FTP など) を使用することができます。

SNMP の使用による直接送信

SNMP 転送を使用するため、IP アドレスがあるネットワーク・ユーティリティーを構成し、読み取り/書き込みコミュニティー名をもつ SNMP を使用可能にする必要があります。53ページの『第2部 ネットワーク・ユーティリティーについての学習』に示してあるサンプル構成のそれぞれに、構成プログラムと talk 6 の両方で、この通信用の IP アドレスおよび SNMP を構成する方法が示してあります。

SNMP を使用してネットワーク・ユーティリティーのまさに最初の構成をダウンロードしたい場合は、 30ページの『手順 B: 構成プログラム 初期構成』を参照してください。

これが最初の構成でない場合は、ハード・ディスク上の現在アクティブのコード・バンクに、ロック解除構成ファイル位置が (アクティブのもの以外に) 少なくとも 1 つあることを確認します (詳しくは、 87ページの『構成のリスト表示』を参照してください)。

ネットワーク・ユーティリティーの構成を構成プログラムで作成し終えたら、以下の手順を使用して、その構成をネットワーク・ユーティリティーに SNMP を使用して転送します。

1. **Configure** ドロップダウン・メニューをアップにして、 **Communications** を選択する。
2. 現行構成を 1 台のネットワーク・ユーティリティーに送信したい場合は、ポップアップから **Single router** を選択し、任意の保管済み構成を任意の台数のターゲット・ルーターに送信したい場合は、 **Multiple routers** を選択する。
3. 次に表示される単一ルーターのパネルまたは複数ルーター・リストのパネルで、**Send** オプションを選択し、ルーターに関する必要なアドレッシング情報を入力する。

   この構成でルーターを再始動させたい日時についても、指定したければ、入力することができます。これには、次の 2 通りの方法があります。

a. **Send** および **Restart router** を選択する。[10]

ルーターには揮発性メモリーに再始動時刻が保管されているので、ネットワーク・ユーティリティーがスケジュールによる予定の時刻より前にリブートした場合は、構成は早期に起動されます。

過去の日時を入力すると、ルーターは新規構成を即時に起動します。

b. **Timed config** を選択する。

ルーターには揮発性メモリーに再始動時刻が保管されているので、ネットワーク・ユーティリティーがスケジュールによる予定の時刻より前にリブートした場合は、その現行構成を使用します。新たにダウンロードされた構成は、スケジュールによる予定の時刻にならないと起動されません。

過去の日時を入力した場合は、ルーターは、新規構成をディスクに保管しますが、それを起動することはありません。以前の「timed config」再始動操作が保留になっていた場合は、取り消されます。

これらの方式のいずれで日時を設定する場合も、この日時をネットワーク・ユーティリティーと同期する必要はありませんし、ネットワーク・ユーティリティーで日時を設定する必要さえありません。構成プログラムがユーザーの設定した日時を時間間隔に変換し、その値をネットワーク・ユーティリティーに送信します。

4. **OK** (複数ルーター・リストの場合は、**Run**) クリックする。構成プログラムが SNMP を使用して、指定されたルーター (または、複数のルーター) への構成データ項目の送信を開始します。ターゲット・ルーターの再始動の日時をもっと後に指定したかどうかに関係なく、送信は即時に開始されます。
5. 構成プログラムが転送に関する状況メッセージおよび結果メッセージを出します。問題を検出し、送信先が 1 つのルーターである場合は、**Send** ではなく、**Query router information** ボタンを試行することもできます。このオプションでは、ルーターから少量の情報が取り出されます。これを使用して、ルーターへの SNMP 通信パスがあるかどうか確認することができます。

ルーターが SNMP を介してルーターの受信を始めると、前回のリブート以降に行われた talk 6 での変更があれば、すべてこの構成で置き換えられます。転送が完了すると、ネットワーク・ユーティリティーでは、受信した構成をディスクに書き込み、送信操作の開始時に選択した内容に基づいて、その起動を行います。

命令コードの使用

命令コードを使用して、次のいずれかの方法で作成されていた構成ファイルを取り込むことができます。

- ステップ 91ページの1 の使用による構成プログラムからのエクスポート
- このネットワーク・ユーティリティーまたは別のネットワーク・ユーティリティーからの以前の転送

91ページの表12 に示されているように、命令コードから開始することができる構成転送手順の場合は、いずれも TFTP をファイル転送プロトコルとして使用します。

10. **Send** を行い、後で手動による **Restart router (ルーター再始動)** 操作を行っても構いません。

TFTP の使用

TFTP を使用して構成ファイルをネットワーク・ユーティリティーのハード・ディスクに転送するための命令コード手順は、次のとおりです。

1. TFTP サーバー・ソフトウェアがインストールされ、ネットワーク・ユーティリティーへの IP ネットワーク物理接続があるワークステーションに構成ファイルを入れる。
2. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されている手順を使用して、ファームウェア・メインメニューにアクセスする。
3. 使用する IP アドレスを構成する。

   イーサネットまたはトークンリング・アダプターを含めて、標準ネットワーク・インターフェースを使用している場合は、構成プログラムまたは talk 6 を使用して、通常の方法でインターフェースの IP アドレスを構成します (talk 6 では、 IP サブプロセスで **add address** を使用します)。この構成変更は、先に進む前にアクティブにします。

   PCMCIA EtherJet カードを使用している場合は、 **system set ip** を使用して、次のアドレスを設定します。
   - IP アドレス : EtherJet カードの IP アドレス
   - ネットマスク : EtherJet カードに接続されているサブネット用のマスク
   - ゲートウェイ・アドレス : TFTP サーバー・ワークステーションの IP アドレス

   SLIP を使用している場合は、IP アドレスは変更できませんが、 91ページの表12に示されているものを使用する必要があります。
4. ファイルを転送する。

   * プロンプトで、以下のシーケンスに従います。

   ```
   *t 6
   Config>boot
   Boot configuration
   Boot config>tftp get config
   ```

   次のようにプロンプトに応答します。
   - サーバー IP アドレス : TFTP サーバー・ワークステーションのアドレスを書き込みます。
   - リモート・ディレクトリー : 構成ファイルがあるサーバー・ワークステーション上のディレクトリーへのパス名を書き込みます。サーバーで予測されている向きのスラッシュを使用します。 大文字小文字の区別が意味をもつのは、それがサーバーで意味をもっている場合だけです。
   - あて先バンク : バンク A またはバンク B を選択します。
   - あて先構成 : 1 と 4 の間にロック解除位置を選択します。

   サーバーの IP アドレスおよび構成済みネットワーク・ユーティリティー・インターフェースの IP アドレスに基づいて、ネットワーク・ユーティリティーでは、サーバーにアクセスする場合に使用するそのインターフェースを選択します。ネットワーク・ユーティリティーでは、適宜、成功または失敗状況メッセージを表示します。
5. リブートして、またはリブートをスケジュールして、構成を使用する。

新規構成を即時にアクティブにする場合は、 Boot Config> プロンプトで次の手順を使用します。

a. **set** コマンドを使用して、新規構成が次回のリブートで使用されるように選択する。
b. **Ctrl-p** を押し、**reload** と入力してネットワーク・ユーティリティーをリブートする。

新規構成を後でアクティブにする場合は、 Boot config> プロンプトで **timedload activate** と入力して、バンクおよび新規構成を選択し、ネットワーク・ユーティリティーがリブートする日時を指定します。ロードするかという質問に対しては「NO」と答えることができます。このステップはすでに行ったからです。

上記の手順で使用されているコマンドについて詳しくは、*MAS ソフトウェア使用者の手引き* の「変更管理の構成」の章を参照してください。

ファームウェアの使用

ファームウェアを使用して、次のいずれかの方法で作成されていた構成ファイルを取り込むことができます。

- ステップ 91ページの1 の使用による構成プログラムからのエクスポート
- このネットワーク・ユーティリティーまたは別のネットワーク・ユーティリティーからの以前の転送

91ページの表12 に示されているように、ファームウェアでは XMODEM と TFTP の両方のファイル転送プロトコルをサポートします。

Xmodem の使用

Xmodem を使用して構成ファイルをネットワーク・ユーティリティーのハード・ディスクに転送するためのファームウェア手順は、次のとおりです。

1. 現行のユーザー・コンソール・セッションをサポートする端末エミュレーションを使用しているワークステーションに、構成ファイルを入れる。
2. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されている手順を使用して、ファームウェア・メインメニューにアクセスする。
3. 次の順序で一連のファームウェア・メニュー選択を行う。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
   b. システム管理ユーティリティー : オプション 12 「Change Management」
   c. 変更管理ソフトウェア制御 : オプション 12 「Xmodem software」
   d. タイプの選択 : 「Config」
   e. バンクの選択 : バンク A または B の選択
   f. Config の選択 : ロック解除位置の選択

   ファームウェアによって、ファイル転送の開始時点が通知されます。
4. 端末エミュレーション・パッケージを表示し、任意の名前を使用して、ワークステーション・サーバーからファイルの転送を開始します。転送が開始すると、ファイル位置の状況が CORRUPT に変更され、完全な構成ファイルが入っていないことを示します。転送が完了すると、ファイル位置の状況が AVAIL に変更されま

す。この確認は、ファームウェアの「Change Management」メニューでオプション 7 の「List Software」を使用して行うことができます。

5. ロードしたばかりの構成を使用するネットワーク・ユーティリティーをブートする。

   オプション 9 の「Set Boot Information」を使用して、現行命令コード・バンクおよび新規構成を選択します。 **Esc** を押し、メインメニューが表示されたら、 **F9** を押して、新規構成のネットワーク・ユーティリティーをブートします。

TFTP の使用

TFTP を使用して構成ファイルをネットワーク・ユーティリティーのハード・ディスクに転送するためのファームウェア手順は、次のとおりです。

1. TFTP サーバー・ソフトウェアがインストールされ、ネットワーク・ユーティリティーへの IP ネットワーク物理接続があるワークステーションに構成ファイルを入れる。
2. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されている手順を使用して、ファームウェア・メインメニューにアクセスする。
3. 使用する IP アドレスを構成する。

   次のメニュー順序に従います。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
   b. システム管理ユーティリティー : オプション 11 「Remote Initial Program Load Setup」
   c. ネットワーク・パラメーター : オプション 1 「IP Parameters」

   次のアドレスを設定します。
   - クライアント IP アドレス : ネットワーク・ユーティリティーの LAN カードの IP アドレス。これは一時アドレスで、そのインターフェースのネットワーク・ユーティリティー操作アドレスに関連付ける必要はありません。
   - サーバー IP アドレス : ワークステーションの LAN アダプターの IP アドレス
   - ゲートウェイ IP アドレス : 中間ルーターがあればその IP アドレス、ない場合は、ワークステーションの IP アドレスを繰り返します。
   - ネットマスク : ネットワーク・ユーティリティーの LAN カードに接続されているサブネット用のマスク
4. 次のメニュー選択によって転送を開始する。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
   b. システム管理ユーティリティー : オプション 12 「Change Management」
   c. 変更管理ソフトウェア制御 : オプション 10 「TFTP software」
   d. タイプの選択 : 「Config」
   e. バンクの選択 : バンク A または B の選択
5. ワークステーション上の構成ファイルのパスおよびファイル名を入力する。
6. プロンプトによる指示が表示された場合は、ファームウェアにファイル転送を行わせたいインターフェースを選択する。

   ファームウェアは構成ファイルを転送し、状況メッセージを出します。完了すると、変更管理メニューが表示されます。

7. ロードしたばかりの構成を使用するネットワーク・ユーティリティーをブートする。

   オプション 9 の「Set Boot Information」を使用して、現行命令コード・バンクおよび新規構成を選択します。 **Esc** を押し、メインメニューが表示されたら、 **F9** を押して、新規構成のネットワーク・ユーティリティーをブートします。

ネットワーク・ユーティリティーからの構成ファイルの転送

次のいずれかの理由がある場合は、ネットワーク・ユーティリティー ***から*** 構成ファイルを転送することができます。

- コマンド行構成を使用していて、ネットワーク・ユーティリティーのハード・ディスク以外に構成のバックアップを取りたい場合
- コマンド行構成を使用していて、別のネットワーク・ユーティリティーに構成をエクスポートしたい場合
- 構成プログラムとコマンド行の両方の構成を使用していて、 talk 6 での変更 (例えば、動的再構成変更) で構成プログラムを更新したい場合

命令コード手順でネットワーク・ユーティリティーに構成を転送する場合は、ネットワーク・ユーティリティーから構成を転送するための逆の手順があります。ステップは実質上同じなので、手順の中で本質的に異なるものだけを以下に挙げてあります。

1. .CFG ファイルを構成プログラムにインポートする。

   .CFG ファイルを構成プログラム・ワークステーションに転送します。**Create router configuration** ではなく、 **Read router configuration** を実行します。
2. SNMP を使用して、構成を構成プログラム内に転送する。**Send configuration** ではなく、 **Retrieve configuration** を実行します。
3. 命令コード TFTP を使用して、ネットワーク・ユーティリティーから構成を送信する。**tftp get config** ではなく、**tftp put config** と入力します。

ネットワーク・ユーティリティーから構成を転送するためのファームウェア・ベースの手順はありません。

第8章 管理の概念と方式

本書で *管理* という用語を使用している場合は、アクティブ・ネットワーク・ユーティリティーで進行していることの監視および制御ができる方法のすべてを意味します。このような方法としては、次のものがあります。

- ローカル・コンソールまたはリモート・コンソールでコマンドを入力して、インターフェースおよびプロトコルの状況の照会および状態の変更を行う。
- 同じコンソールとリモート・ログ記録用のサーバーのどちらかで、イベント・メッセージの実行ログを監視する。
- SNMP MIB ブラウザーを使用して、インターフェースの状況、および対応する SNMP MIB サポートがあるボックスの機能を照会する。
- SNMP ベースの管理プロダクトとそのアプリケーションを使用して、インターフェースの状況、および対応する SNMP MIB サポートがあるボックスの機能の監視および制御を行う。
- SNMP ベースのトポロジー・アプリケーションを使用して、ネットワークおよびその資源のプロトコル固有の (例えば、APPN や DLSw など) ビューを監視する。
- SNMP ベースの管理プロダクトを使用して、ボックスがエラー条件を報告するために送信する SNMP トラップを監視する。
- SNA アラート・フォーカル・ポイント・プロダクト (NetView/390 など) を使用して、ボックスがエラー条件を報告するために送信する SNA アラートを監視する。
- SNA 管理プロダクト (NetView/390 など) を使用して、SNA 資源を制御する。

この章では、このような方式について概説し、ネットワーク・ユーティリティーの管理に使用できるその他の製品の一部について紹介します。

コンソール・コマンド

ボックス状況の照会および変更を行うためのコマンドを入力する場合は、まず最初に、アクティブ・ネットワーク・ユーティリティーへのローカルまたはリモートの接続機構を立ち上げておく必要があります。その方法および * プロンプトにアクセスする方法の詳細については、 15ページの『第2章 ユーザー・コンソールの始動』を参照してください。

コンソールがアクティブになったら、talk 5 を使用して、コンソール・プロセスにアクセスします。[11] そこから、メニュー間をナビゲートし、コマンドを発行して、インターフェースおよびプロトコルの状況を照会し、次のような動的オペレーター変更を行います。

- インターフェースを使用不可および使用可能にする。
- 接続をリサイクルする。
- 構成変更をアクティブにする。

talk 5 コマンド、およびオペレーター・コンソールで表示および変更ができる状況のタイプの概説については、68ページの『操作 (talk 5、コンソール・プロセスの使用)』

11. 接続しているネットワーク・ユーティリティーがそれまでにまったく構成を経ていない場合は、 Config-only モードに入ることになり、talk 5 のコンソール・プロセスに進むことはできません。 25ページの『第3章 初期構成の実行』 の説明に従って、ネットワーク・ユーティリティーの初めての構成を行い、ブートして通常の操作状態に入ります。

を参照してください。最上位の talk 5 コマンドの詳細については、*MAS ソフトウェア使用者の手引き* の「操作/監視プロセス (GWCON - Talk 5) とコマンド」の章に記載してあります。

talk 5 コマンド **net**、**protocol**、および **feature** を使用して、メニュー構造を下方に移動し、インターフェースおよび特定のプロトコルとフィーチャーの監視および制御を行うためのコマンドを使用することができます。インターフェース・レベルの talk 5 コマンドについては、*MAS ソフトウェア使用者の手引き* の中のさまざまなインターフェース・タイプに関する章に記載してあります。プロトコルとフィーチャーの talk 5 コマンドについては、2 巻からなる *MAS プロトコル構成と監視解説書* のさまざまな章、および *MAS フィーチャーの使用と構成* で説明されています。

イベント・メッセージの監視

イベントを監視する理由

Talk 5 コマンドでは、ネットワーク・ユーティリティーの状況のスナップショットは得られますが、ボックスの内部で起こっているイベントのログやトレースを作成することはできません。したがって、ELS (イベント・ログ・システム) を使用することになります。正しい ELS メッセージをアクティブにし、イベント・ログを監視することによって、次のようなイベントをリアルタイムで追跡することができます。

- インターフェースがテスト・フェーズを経て、アップになり、ダウンになる。
- 特定のプロトコルのパケットが送受信される。
- DLC リンクがアップになり、ダウンになる。
- CPU 使用状況がネットワーク活動に応じて変化する。
- 上位プロトコル接続 (例えば、DLSw パートナー接続および回線接続) がアップになり、ダウンになる。

ELS メッセージを監視することによって、次のような一部の基本的な質問への応答を開始することができます。

- 何かが起こっているのか ?
- なぜリンクがアップにならないのか ?
- プロトコルはワークステーションが送信しているトラフィックを確認しているのか ?

イベント・ログ・システムは、基本的な構成の問題をデバッグする強力なツールになります。

ログに記録するイベントの指定

ELS メッセージを使用する場合は、まず最初に、何千何万にも登る事前定義イベントの中で、報告してほしいイベントをシステムに通知しておく必要があります。次のような基準を使用して、アクティブ・メッセージのセットを指定することができます。

サブシステム名

ソフトウェア・コンポーネントの事前定義短縮名 (例えば、IP、TKR、 DLS など) を使用して、そのソフトウェア・コンポーネントから生じる可能性のあるすべてのメッセージを指すことができます。

イベント番号

個々のメッセージをオンまたはオフにしたり、ある範囲のイベント番号を指定することができます。あるサブシステム内のすべてのメッセージをアクティブにした上で、そのサブシステム内で特に頻度の高い一部のメッセージをオフにして、より重大なメッセージが不明確になるのを防ぐことが有用な場合があります。

ログ・レベル

見たいメッセージの重大度レベルを指定することができます。例えば、異常エラー・メッセージだけを見ることも、トレース・メッセージだけを見ることも、単純な通知メッセージを含めることもできます。

グループ名

前にメッセージのグループを定義した時点で選択した名前を指定することができます。

さらに、ある論理インターフェース番号に対してフィルターを設定して、どんなアクティブ・メッセージ・セットの場合でも、特定のインターフェースに関するメッセージだけがログ内に現れるようにすることができます。

イベントのログ記録先の指定

メッセージをアクティブにするときは、次のいずれか 1 つをメッセージのあて先として選択します。

1. モニター・プロセス

   このプロセスに送られたメッセージを表示させて見る場合は、* プロンプトで **talk 2** コマンドを使用します。モニター・プロセスの使用法の説明については、 74ページの『イベント・ログ (talk 2、モニター・プロセスの使用)』を参照してください。

2. リモート・ログ・サーバー

   標準的な *syslog* 機能をサポートして、イベント・メッセージ・パケットのフローを受信し、ファイル内に保管する PC またはワークステーションをセットアップすることができます。ネットワーク・ユーティリティーでは、それぞれのメッセージを UDP/IP パケットに入れて、標準的なネットワーク・インターフェースを通して送り出します。ログ・メッセージ・フローは量が多くなる可能性があるため、ログ・サーバーは通常ネットワーク・ユーティリティーに LAN 接続されます。

3. SNMP 管理ステーションに送信される SNMP トラップ

   ネットワーク・ユーティリティーでは、イベント・メッセージを IBM エンタープライズ特定 SNMP トラップにパッケージし、UDP/IP パケットに入れて、標準的なネットワーク・インターフェースを通して送り出します。

イベント・ログの起動

コマンド行からは、talk 6 と talk 5 のどちらかを使用して、ログに記録したいイベントとログ記録先を選択することができます。どちらのプロセスからでも、**event** サブプロセスに入って、先に進みます。talk 6 のもとでイベントをアクティブにする場合は、変更が有効になるのは、それをディスクに書き込み、ネットワーク・ユーティ

リティーをリブートしてからです。そのようなイベントに関するメッセージは、最初のリブート時から引き続きアクティブです。

talk 5 でイベントをアクティブにする場合は、システムでは、そのようなイベントに関するメッセージをユーザーが指定するあて先 (talk 2、ログ・サーバー、または SNMP 管理ステーション) に即時に配信し始めます。ネットワーク・ユーティリティーをリブートすると、そのようなメッセージはアクティブでなくなります。talk 5 の使用によるイベントの起動は、発生している当面の問題をデバッグする方法として優れています。イベントをオンにし、即時に talk 2 に跳んで、何が起こっているかなどを確認します。後でリブートすれば、イベントは停止し、新たにコマンドを入力する必要はありません。

もう 1 つの有用なデバッグ技法としては、talk 5 イベント・サブプロセスを使用して、どのイベントでも、検出された回数の統計を表示させて見る方法があります。このような統計は、アクティブにされていないイベントに関しても使用可能です。

現行の talk 6 ELS 構成をアクティブにするための talk 5 コマンドはありません。即時起動が必要な場合は、talk 6 で入力した同じコマンドを talk 5 で繰り返す必要があります。

構成プログラムからは、ネットワーク・ユーティリティーがホストにリモート・ログ記録を行うように設定することができるだけです。アクティブな ELS イベントを構成したり、 ELS イベントを特定のあて先に送信したりすることはできません。ただし、構成プログラムでは、次の場合にこの構成情報を保存します。つまり、ユーザーがネットワーク・ユーティリティーから構成をリトリーブし、構成プログラムを使用して構成の他の部分を変更し、構成を元に書き出した場合です。

SNMP 管理ステーションからは、SET を使用して、ほとんどの ELS 構成機能をエンタープライズ特定 ELS MIB を使用して制御することができます。

ELS イベントの起動および制御を行うための主要コマンドの一部についての説明は、113ページの『イベントの監視』を参照してください。ELS の概念と対応する talk 6 および talk 5 のコマンドの詳細な説明については、*MAS ソフトウェア使用者の手引き* の「イベント・ログ・システム (ELS) の構成と監視」の章を参照してください。個々の ELS メッセージすべての説明については、CD-ROM または Web で *イベント・ログ・システム・メッセージの手引き* を参照してください。

シンプル・ネットワーク管理プロトコル (SNMP) サポート

SNMP は、管理ステーションで管理対象ノード内の構成、制御、および状況の情報を照会および設定する場合に使用する業界標準プロトコルです。ネットワーク・ユーティリティーについて言えば、管理ステーションは、通常、SNMP 管理ソフトウェア・プロダクトがインストールされている PC またはワークステーションということになります。管理対象ノードがネットワーク・ユーティリティーということです。

SNMP では、管理ステーションと管理対象ノードの間で、IP ネットワークを通して、UDP パケット内部のフローに要求および応答します。一般的に、管理ステーションが、情報に対する要求およびデータ項目を新しい値に設定する要求を送信して、通信を開始します。管理対象ノードは、これらの要求を実行し、応答するだけです。

ただし、管理対象ノードは、イベントを報告するための、トラップ と呼ばれる非勧誘型メッセージを送信することができます。ネットワーク・ユーティリティーでは、トラップを送信して、ボックスのリブートやインターフェースのダウンなどのようなイベントを報告する場合があります。

*管理情報*ベース *(MIB)* とは、管理ステーションからアクセスすることができる管理対象ノード内で、データ項目を定義する仮想情報ストアのことです。MIB は、人間と管理ステーション・ソフトウェアの両方が読める、厳密に様式設定された記述ファイルの中で定義されます。

管理対象ノードが MIB を サポートする のは、そのソフトウェアが、MIB 内に文書化されているデータ項目に対する要求に応じ、それに対応する内部データ項目を検索または設定できる場合です。MIB 記述ファイルでは、それぞれのデータ項目ごとに、管理ステーションがそれを読み取ることしかできないのか、その値を変更することができるのかを定義します。時には、プロダクトでは、MIB で書き込み可能として文書化されているデータ項目への読み取りアクセスを許可する選択しかしない場合があります。したがって、プロダクトの資料を参照して、特定のプロダクトでインプリメントされているアクセス・レベルを把握しておく必要があります。

ほとんどの業界標準プロトコルおよびインターフェース・タイプには、対応する IETF 標準 MIB があり、RFC 番号が付いています。標準 MIB では、対応するプロトコルまたはインターフェース・タイプのほとんどのインプリメンテーションに共通のデータ項目を定義しています。ベンダーとしては、必ずしも MIB が IETF 内で RFC の状態に達するのを待つことができるとは限らず、標準前の*インターネット・ドラフト・バージョン*の MIB に対するサポートを出荷する場合があります。

プロダクト・ベンダーの多くは、標準 MIB だけでなく、自社の製品に固有のデータ項目を定義するための独自の MIB も開発しています。例えば、ネットワーク・ユーティリティーでは、標準 MIB がないメモリーおよび CPU 使用状況情報にアクセスできる MIB をサポートしています。SNMP 用語では、このようなベンダー MIB は、*エンタープライズ特定* MIB と呼ばれています。

MIB サポート

IBM ネットワーク・ユーティリティー では、資源の監視および管理を行うための標準およびエンタープライズ特定 MIB の包括的なセットをサポートしています。現在、そのような MIB の数は 40 ～ 50 に及んでいます。

ネットワーク・ユーティリティーの MIB サポートが文書に収められている ″README″ ファイルには、ワールド・ワイド・ウェブ (WWW) 上で下記のアドレスの該当するソフトウェア・リリース・ディレクトリーにアクセスして入手することができます。

```
ftp://ftp.networking.raleigh.ibm.com/pub/netmgmt/netu
```

同じディレクトリーには、MIB 記述ファイル自体も入っているので、FTP を使用して検索し、管理ステーションにロードすることができます。可能な場合はいつでも、それらのファイルについて、SNMP バージョン 1 形式でコンパイルし、可能な限り最大限の範囲にわたる管理ステーション・ソフトウェアとの互換性が得られるようにします。

標準 MIB およびインターネット・ドラフト MIB の場合は、コンパイル・プロセスで入門説明テキストやページ形式設定が省かれ、これが MIB を読みやすくする上で役立っています。完全な事前コンパイル・バージョンの RFC MIB またはインターネット・ドラフト MIB を入手する場合は、どの RFC またはインターネット・ドラフトを希望するかに応じて、IETF FTP サイトから検索します。下記の URL から開始して、RFC リポジトリーまたはインターネット・ドラフト・リポジトリーまでリンクをたどります。

```
http://www.ietf.org
```

今回のリリースで新たに次の MIB がサポートされることになりました。

- **レイヤー 2 トンネリング MIB**

  レイヤー 2 トンネリング MIB は、IBM エンタープライズ MIB の 1 つで、これを使用すると、アクティブのレイヤー 2 トンネルについての情報と、それに対応する統計を表示させて見ることができます。トンネルの開始と停止、および認証障害に関するトラップがあります。また、トンネルが確立できるかどうかを、そのトンネルに関する構成情報を基にしてテストするセットを、テスト MIB に対して発行することもできます。トンネルに関する応答時間を決めることができる、テスト MIB があります。

- **ポリシー MIB**

  ポリシー MIB は、IBM エンタープライズ MIB の 1 つで、ほとんどがルーターのポリシー・データベースにロードされたポリシー情報で、構成されています。ポリシーのロード元をローカル構成と LDAP サーバーのどちらか、またはその両方に決めることができます。この MIB では、ポリシーのヒット回数と、IPSec と IKE に関して行われているアクティブ交渉のすべてを常時追跡します。交渉情報は、交渉についての特定の情報に関する IPSec/IKE MIB への逆引き索引として使用できます。また、管理と操作の両 LDAP 構成パラメーターを調べることもできます。この MIB を使用すると、セットが実行できるので、LDAP パラメーターの一部について構成を変更できます。セット時にポリシー・データベースをリフレッシュするオブジェクトがあります。また、ポリシー・テスト MIB もあり、それを使用すると、ポリシー照会のセレクター (発信元とあて先の IP アドレス、プロトコルとポート番号と DS バイト) を設定し、これらのセレクターをもつポリシー照会の結果のポリシーとアクションを判別できます。

- **IPSec/IKE MIB**

  IPSec/IKE MIB は、IBM エンタープライズ MIB の 1 つで、それを使用すると、IKE のフェーズ I とフェーズ II に関するアクティブ交渉情報を表示させて見ることができます。また、エラーだけでなく、暗号化と復号に関する IPSec 統計のテーブルも得られます。トンネルの開始と停止、および認証と復号の障害に関するトラップがあります。この MIB では、保護されているサブネットとアプリケーションについての情報と、セキュリティー・ゲートウェイに関するローカルとリモートの識別情報も表示されます。

始めに

ネットワーク・ユーティリティーで

SNMP 管理ステーションがネットワーク・ユーティリティーと通信できるようにするためには、まずその前に、ネットワーク・ユーティリティー内で該当するアクセス

を使用可能にして、SNMP を構成しておく必要があります。構成プログラムと talk 6 と talk 5 のいずれかを使用して、SNMP を使用可能にし、1 台または複数台の管理ステーションへのアクセスを許可する コミュニティー名 を設定することができます。talk 6 または talk 5 からは、**protocol snmp** を使用して、 SNMP を処理するために Config (構成) およびコンソール・サブプロセスにアクセスします。ステップ 27ページの3 に示されているように、 Quick Config (クィック構成) を使用して、SNMP を使用可能にし、読み取りまたは読み取り/書き込みコミュニティー名を設定することもできます。

詳細な背景情報、ならびに SNMP talk 6 および talk 5 コマンドの説明については、*MAS プロトコル構成と監視解説書 第 1 巻* の「SNMP の使用」および「SNMP の構成と監視」の章を参照してください。

管理ステーションで

管理ステーションで管理対象ノードを有効にサポートできるようにするためには、まずその前に、管理対象ノードでサポートされている MIB が分かっていることが必要です。107ページの『IBM Nways マネージャー・プロダクト』 で説明されている IBM プロダクトのいずれかを使用している場合は、この知識を設定するために特に何かする必要はありません。それぞれにネットワーク・ユーティリティーでサポートされている MIB がすでにコンパイルされているからです。

それ以外の管理プロダクトを使用している場合は、この知識を設定する必要がある可能性があります。管理ステーションには、一般的に、コンパイル済みの MIB モジュールをステーションにロードするための機能が用意されています。ネットワーク・ユーティリティーを管理するための管理ステーションを準備する際は、 103ページの『MIB サポート』 に示されている URL のもとのディレクトリーから、すべての MIB を読み込むように設定します。

ネットワーク・ユーティリティーから管理ステーションにトラップを送信する予定の場合は、管理ステーションがトラップを受信したら、メッセージを発行したり、指定されたアクションを起こすようにセットアップする必要がある可能性もあります。

SNA アラート・サポート

システム・ネットワーク体系 (SNA) では、ネットワーク製品の管理を目的として、豊富なプロトコル・フローのセットが定義されています。その体系の主要部の 1 つに、管理対象ノードが アラート と呼ばれる非勧誘型のエラーおよびイベント報告を、SNA 管理ステーションに送信できる機能があります。アラートには、管理プロダクトが次のようなものをオペレーターに報告できるようにする、一連のサブメッセージが入っています。

- アラートを作成したノードの識別
- アラートのプロンプトを出したエラーまたはイベント
- 考えられる幾つかの問題の原因
- 考えられる訂正処置

アラートの受信用として最も一般的に使用されている SNA 管理プロダクトは、NetView/390 です。 SNA 体系では、このようなプロダクトをアラート・フォーカル・ポイント と呼んでいます。ネットワーク内で、他のプロダクトに代わってアラートの受信および転送ができるプロダクトは、エントリー・ポイント と呼ばれています。

APPN ネットワーク・ノードとして使用されるネットワーク・ユーティリティーには、アラート・フォーカル・ポイントとの LU 6.2 セッションを確立し、ボックス内およびネットワーク内のエラー条件を報告するためのネイティブ SNA アラートを送信することができる機能があります。ネットワーク・ユーティリティーの APPN 機能からアラートを誘発するイベントは、ほぼ 30 前後が事前定義されていますが、そのうちの幾つかを以下に挙げておきます。

- セッションのセットアップ障害
- 無効の XID の受信、XID プロトコル・エラー
- HPR または DLUR の構成またはプロトコル・エラー
- CP-CP セッションの障害
- 資源不足
- サブコンポーネント・プロトコル・エラー

このようなイベントのいずれか 1 つが発生し、ネットワーク・ユーティリティーにアラートを送信するための現行フォーカル・ポイント・セッションがない場合は、アラートは後で送信するために待ち行列に入れられます。この「保留アラート」待ち行列の項目数は、構成することができます。このようなイベントのどれがアラートを誘発するかは、構成することはできません。

アラートが流れる LU6.2 セッションは、フォーカル・ポイントでもネットワーク・ユーティリティーでも確立することができます。APPN ネットワーク・ユーティリティーでアラート・フォーカル・ポイントからのセッションを受け入れ、アラートを送信することができるようにするために、特殊なパラメーターを構成する必要はありません。ネットワーク・ユーティリティーに能動的にセッションを設定し、アラートを転送させたい場合は、1 つまたは複数の *暗黙* フォーカル・ポイントの名前を APPN 構成の一部として構成します。 1 次フォーカル・ポイントに到達できない場合は、ネットワーク・ユーティリティーではその他の構成済みの名前への到達を試みます。

ネットワーク・ユーティリティーは、検出したイベントに関するアラートを送信するだけでなく、 SNA エントリー・ポイントの役割を果たし、セッションの相手側である他の SNA ノードに代わってアラートを転送することもできます。この機能を使用可能にするための構成は必要ありません。

始めに

ネットワーク・ユーティリティーにフォーカル・ポイント・セッションを起動させたい場合は、構成プログラムまたは talk 6 を使用して、フォーカル・ポイント名を構成することができます。 talk 6 からは、**protocol appn** を使用して、 APPN を処理するための Config (構成) サブプロセスにアクセスし、そこで **add focal-point** コマンドを使用します。

詳細な背景情報については、*MAS プロトコル構成と監視解説書 第 2 巻* の APPN に関する「APPN 関連アラートに関するエントリー・ポイント機能」、「構成可能保留

アラート待ち行列」、および「暗黙フォーカル・ポイント」の項を参照してください。 コマンド名については、同じく「ルーター構成プロセス」の項に示されています。

ネットワーク管理プロダクト

SNMP と SNA の両管理フローとも、ネットワーク・ユーティリティーとは別に、ネットワークおよびネットワーク・ユーティリティーの表示を管理したり、ネットワーク・ユーティリティーに状況を照会したり、ネットワーク・ユーティリティーから非勧誘型のイベント報告を受信したりするためのプロダクトを必要とします。ここには、そのようなタスクを実行する場合に使用するプロダクトの一部を挙げてあります。

SNMP MIB ブラウザー

MIB ブラウザー は、PC またはワークステーションで使用され、MIB 定義をロードし、管理対象ノード内のデータ項目を照会または設定し、戻された値および結果を簡単に読める形式に復号することができる、小さいアプリケーションです。SNMP 用語では、管理ステーションの 1 つのことですが、MIB ブラウザーには、次の項で説明するような、本格的な SNMP 管理プラットフォームが備えている能力や精巧性は欠けています。MIB ブラウザーは、そのようなプラットフォームの一部としてパッケージされることが多いのですが、独立型プロダクトとしてもご利用いただけます。

IBM Nways マネージャー・プロダクト

以下の IBM SNMP ネットワーク管理プロダクトは、ネットワーク・ユーティリティーおよびその他のさまざまな IBM 製、および IBM 製以外のネットワーク製品の管理を特に目的としています。そのいずれでも、ネットワーク資源のグラフィック・トポロジー・ビューが、資源の状況および各ネットワークの総合的な状況が色分けされて示されます。それぞれがネットワーク資源の自動ディスカバリー、およびネットワークの変更に応じたネットワーク・マップへの自動更新をサポートします。

IBM Nways Manager for AIX

このプロダクトは、中規模から大規模のネットワーク環境を管理するために設計され、IBM 版 UNIX である AIX が稼働しているワークステーションで稼働します。Nways Manager for AIX は、以前は「NetView for AIX」および「NetView/6000」という名前で呼ばれていた Tivoli TME 10 NetView に加えて稼働します。Tivoli TME 10 NetView には、LAN トポロジーの管理、障害およびイベントの記録、エラー・ログなどの、一般的なネットワーク管理機能が備えられています。Tivoli TME 10 NetView を IBM の SNA Server for AIX と組み合わせれば、 SNMP トラップを SNA アラートにマップすることもできます。ネットワーク・ユーティリティーの場合は、こうすることによって、実質的にすべての定義済みイベントに関して、SNA アラートが流れるようにすることができます。

Nways Manager for AIX には、以下の機能が基本 Tivoli TME 10 NetView の機能に加えて備えられています。

- ネットワーク・ユーティリティー特定管理アプリケーション

ネットワーク・トポロジー・ビューでネットワーク・ユーティリティーを選択すると、ネットワーク・ユーティリティーのフロント・パネルのグラフィックが、インターフェース状況を色分けして表示されます。わきにあるナビゲーション・ウィンドウを使用すれば、ネットワーク・ユーティリティーによって図と表のどちらかの形式で示される SNMP MIB 情報のすべてにアクセスすることができます。このアプリケーションでは、次のことを行うことができます。

- アダプターおよびインターフェースの状況の表示および変更
- コンポーネントまたはインターフェースのレベルでの統計の表示
- リアルタイムで、色分けされた一目瞭然 (りょうぜん) の状況の受信
- パフォーマンスしきい値の定義および監視
- リアルタイム統計および履歴統計の定義および監視
- リアルタイム・イベントの監視

ネットワーク・ユーティリティーアプリケーションから、次のものを立ち上げることができます。

- 2216/ネットワーク・ユーティリティー・グラフィック構成プログラム (ボックスを構成するため)
- ネットワーク・ユーティリティーへの Telnet セッション (コマンド行インターフェースを使用して、ネットワーク・ユーティリティーの構成、監視、および制御ができるようにするため)

ネットワーク・ユーティリティー管理アプリケーションは Java ベースであるため、Nways マネージャーが稼働しているワークステーションでなくても、使用することができます。このアプリケーションは、イントラネットまたはインターネットを通してメイン Nways マネージャー・ワークステーションに接続され、JDK 準拠の Web ブラウザーが稼働している、 PC またはワークステーションから立ち上げることができます。必要とされる Web ブラウザーおよび JDK のバージョンの詳細については、下記にアクセスして、Nways マネージャーのプロダクト前提条件を参照してください。

```
http://www.networking.ibm.com/netmgt
```

Java 管理サポートには、ネットワーク・ユーティリティーのリアルタイム状況の表示、およびパフォーマンス管理を行うことができる機能が含まれています。セキュリティー上の理由により、Java Web ブラウザーから構成プログラムを立ち上げることはできません。

- 分散インテリジェント・エージェント

  大規模ネットワークに関するサポートを提供するために、 Nways マネージャー・ワークステーション以外のボックスを使用して、ネットワーク内の管理対象ノードをポーリングすることができます。ポーリングをマネージャー・ワークステーションからオフロードすると、そのプロセッサーが解放されて他のタスクを行うことができ、ポーリングをポーリングの対象となっている装置に近づけるため、ネットワーク帯域幅が解放されます。マネージャーのこのような「エージェント」は、しきい値を超えた時点で Nways マネージャーに通知するように構成することができます。

  インテリジェント・エージェント・ソフトウェアは Java ベースで、Nways マネージャーからダウンロードされます。これらのエージェントは、ネットワーク内の Java 使用可能 (Java 仮想マシン) ワークステーションのいずれにも置くことができます。Nways マネージャーでは、TME 10 中間レベル・マネージャーが提供する分散ポーリング機能を使用することもできます。

- APPN トポロジー・サポート

  Nways Manager for AIX によって、ネットワークのトポロジーの APPN レベルのビューが得られます。 参加 APPN 資源を検出し、それらを表示させ、それらの状況を色分けされたアイコンとして表示させることができます。 APPN プロトコル・パフォーマンスおよびエラー・イベント (データとグラフ) も得られます。 このアプリケーションでは、ブランチ・エクステンダーや拡張ボーダー・ノードのトポロジーは表示されません。

- DLSw トポロジー・サポート

  Nways Manager for AIX では、ネットワークの DLSw トポロジー・ビューも、DLSw 接続、資源、および色分けされた状況を含めて表示されます。トポロジーは、新しいノードが検出されると最新表示されます。このアプリケーションでは、DLSw IP マルチキャスト・グループのトポロジーは表示されません。

- VLAN、ATM、および RMON サポート

  Nways Manager for AIX には、バーチャル LAN をインプリメントするプロダクト、ATM ネットワーク、および RMON および ECAM プローブからのデータの収集、相関付け、および表示に対する包括的なサポートがあります。

- VPN 管理アプリケーション

  Nways VPN (仮想私設ネットワーク) 管理アプリケーションでは、監視、イベント報告、障害追及、動作制御、アプリケーション・ランチの諸機能からなる豊富な機能セットが得られます。初期バージョンでは、IBM 22xx ルーターに対する VPN 機能の監視と動作制御を提供することに明確に照準を合わせ、現在は標準 MIB オブジェクトが存在していないので、その機能の提供に私用 MIB オブジェクトを使用します。

  Nways VPN 管理アプリケーションは、次の 3 つの VPN 構成要素に集中します。

  – VPN トンネル
  – VPN クライアント
  – ポリシー

  監視機能では、アクティブと直前の VPN トンネルの表示、アクティブと直前の VPN クライアントの表示、定義済みとアクティブの VPN ポリシーの表示が可能です。イベント報告機能では、VPN トンネルの開始時と、 VPN 装置でのセキュリティー・ハッキングの発生時をユーザーに通知します。動作制御機能では、VPN トンネルを使用不可/非アクティブにし、VPN クライアントを使用不可/非アクティブにし、VPN ポリシーをリフレッシュできます。トラブルシューティング機能では、VPN 装置のプロキシー PING と VPN イベント障害ログの表示ができます。アプリケーション・ランチ機能では、さまざまな関連ネットワーク管理アプリケーション (例えば、装置の PSM/JMA など) を立ち上げることができる機能が得られます。

Nways Manager for AIX で ネットワーク・ユーティリティー に対する特定のサポートを初めて備えたバージョンは、バージョン 1.2.2 です。

仕様およびシステム要件を含めて、Nways Manager for AIX に関する詳細が必要な場合は、下記にアクセスしてください。

```
http://www.networking.ibm.com/cma/cmaprod.html
```

上記のサイトにあるページには、別途に有料で提供される Nways Manager for AIX のコンポーネント、およびどのコンポーネントがどの機能を果たすのかが記載されています。

IBM Nways Workgroup Manager for NT

小規模から中規模のネットワーク環境の管理用として設計された Workgroup Manager は、Windows NT バージョン 4.0 で稼働する、32 ビット・ネイティブ Windows NT アプリケーションです。Nways Manager for AIX の場合とは異なり、Workgroup Manager は自己完結型で、下位ネットワーク管理プラットフォームを使用しません。したがって、それ自体に多くのプラットフォーム機能が備えられている必要があります。

Nways Workgroup Manager for NT の主要フィーチャーには、次のようなものがあります。

- IP ネットワークの自動ディスカバリー
- ネットワーク・トポロジーのリアルタイムのグラフィック・ビュー
- MIB をブラウズ、更新、およびコンパイルできる機能
- 色分けされ、集約されたネットワークおよび装置のリアルタイム状況
- トラブル・チケット
- トラップ重大度の指定を含む、トラップ管理
- トラップ・コンパイラー
- ポーリングの構成と通知
- パフォーマンスしきい値の構成と通知
- 在庫管理
- リアルタイム統計および履歴統計の収集と表示
- VPN 管理アプリケーション

Nways Workgroup Manager for NT では、Nways Manager for AIX の場合と正確に同じネットワーク・ユーティリティー特定 Java 管理アプリケーションをサポートします。ネットワーク・ユーティリティー管理アプリケーションは、Java 対応可能 Web ブラウザーから実行することができます。Nways Workgroup Manager for NT では、分散インテリジェント・エージェントもサポートします。

Nways Workgroup Manager for NT では、Nways Manager for AIX でサポートされている APPN および DLSw トポロジー・アプリケーションはサポートしません。Nways Workgroup Manager for NT のトポロジー表示は、管理対象ノード間の IP 接続に基づいています。

Nways Workgroup Manager for NT で ネットワーク・ユーティリティー に対する特定のサポートを初めて備えたバージョンは、バージョン 1.1.2 です。

IBM Nways Manager for HP-UX

このプロダクトは、中規模から大規模のネットワーク環境を管理するために設計され、Hewlett Packard 版 UNIX である HP-UX が稼働しているワークステーションで稼働します。Nways Manager for HP-UX は、以前は「HP OpenView」という名前で呼ばれていた、 HP の *Network Node Manager* 管理プラットフォーム・ソフトウェアに加えて実行されます。

この環境では、ネットワーク・ノード・マネージャーは、トポロジー表示、トラップ管理などを含めて、基本管理プラットフォーム機能を提供します。 Nways Manager for AIX の場合とは異なり、IBM ネットワーク装置を該当する Nways Manager for HP-UX 管理アプリケーションに対応付けることができます。

Nways Manager for HP-UX からは、Nways Manager for AIX からの場合と同じネットワーク・ユーティリティー特定 Java 管理アプリケーションを立ち上げることができます。Nways Manager for HP-UX では、分散インテリジェント・エージェントもサポートします。

Nways Manager for HP-UX では、Nways Manager for AIX でサポートされている APPN および DLSw トポロジー・アプリケーションはサポートしません。

Nways Manager for HP-UX で ネットワーク・ユーティリティー に対する特定のサポートを初めて備えたバージョンは、バージョン 1.2 です。

NetView/390

NetView/390 は、中規模から大規模の SNA ネットワークを管理するためのホスト・ベースの管理プロダクトです。NetView/390 を使用して、ネットワーク・ユーティリティーおよびそれがホストに接続できる SNA プロダクトを管理する方法は、幾つかあります。

- SNA 資源の制御 (リンク、PU および LU の起動および停止)
  - ネットワーク・ユーティリティーが DLSw を実行しているときは、NetView/390 では、DLSw が表しているリンク、およびリモート SNA エンド・ステーションの PU および LU を制御することができます。
  - ネットワーク・ユーティリティーが TN3270 サーバー・サポートを実行しているときは、NetView/390 では、ネットワーク・ユーティリティー内で表されるローカル PU および LU を制御することができます。
  - ネットワーク・ユーティリティーがダウンストリーム・ノードの DLUR を実行しているときは、NetView/390 では、ネットワーク・ユーティリティーがサービスしている PU および LU、およびネットワーク・ユーティリティーとそれらのノードの間のリンクを制御することができます。
  - ネットワーク・ユーティリティーが SNA エンド・ステーション・トラフィックをブリッジしているときは、NetView/390 では、エンド・ステーション PU および LU を制御することができます。
  - ネットワーク・ユーティリティーが APPN、DLSw を実行しているか、SNA トラフィックをブリッジしているときは、NetView/390 では、ホストとネットワーク・ユーティリティーの間の隣接リンクを制御することができます。
  - ネットワーク・ユーティリティーが LSA 直接ゲートウェイ機能を実行しているときは、NetView/390 では、 VTAM にとってローカルに見える LAN リンク、ならびに接続されている SNA エンド・ステーションの PU および LU を制御することができます。
- ネットワーク・エラーおよびトポロジーの監視

- ネットワーク・ユーティリティーが APPN ノードとして使用されている場合は、ネットワーク・ユーティリティーが生成するアラートと他のノードから転送するアラートの両方について、NetView/390 がアラート・フォーカル・ポイントになることができます。
- ネットワーク・ユーティリティーが DLSw、DLUR を実行するか、SNA トラフィックをブリッジしているときは、NetView/390 では、アラート、応答時間情報、またはダウンストリーム PU からのその他の SSCP-PU フローを受信することができます。
- NetView/390 は、Tivoli TME 10 NetView および SNA Server for AIX によってアラートに変換されたネットワーク・ユーティリティー・トラップに関するアラート・フォーカル・ポイントになることができます。
- 関連プロダクトである *SNA トポロジー・マネージャー*、 *APPN 会計*マネージャー、および *APPN トポロジー・インテグレーター* を介して、 NetView/390 は、ネットワーク・ユーティリティーおよびその他の SNMP 対応可能 APPN プロダクトを含めて、 APPN ネットワークのトポロジーを獲得し監視することができます。

第9章 一般的な管理タスク

この章では、重要なネットワーク・ユーティリティー操作の手順とコマンドを示します。これまでの章で紹介した概念の一部を補完する役割を果たす章です。

イベントの監視

この節には、74ページの『イベント・ログ (talk 2、モニター・プロセスの使用)』および 100ページの『イベント・メッセージの監視』に記載されているイベントのログ記録および表示に関する背景情報を補完する情報が記載してあります。ここでは、ログに記録するイベント、およびそのログ記録先を制御するコマンドについて概説します。

イベント・ログ・システムへのアクセス

イベント・ログをアクティブにする場合は、コマンド行インターフェースを使用する必要があります。構成プログラムからでは、一般的なリモート・ログ・パラメーターの構成ができるだけです。

メイン talk 5 と talk 6 のどちらのプロンプトでも、**event** と入力すると、ELS コンソール・サブプロセスと Config (構成) サブプロセスにそれぞれ入ります。talk 5 と talk 6 のどちらで作業する場合でも、本質的には同じコマンドが表示されます。talk 5 ELS コマンドは即時に有効になり、メッセージをオンにして、実行システム内の特定のフローをデバッグする場合は、非常に有用です。 talk 6 では、常にログに記録されるようにして、ネットワーク・ユーティリティーのリブートのつどアクティブにしなくても済むようにしたいイベントを構成します。

イベント・ログを制御するためのコマンド

イベント・ログを起動および停止するための基本的なコマンドは、ログ・メッセージの 3 つのあて先のそれぞれについて 2 つずつで、合計 6 つあります。

- **disp** および **nodisp** では、 talk 2 にローカルでログ記録されるイベントを制御します。
- **trap** および **notrap** では、 SNMP トラップを生成するイベントを制御します。
- **remote** および **noremote** では、 syslogd 対応可能ホストにリモートでログ記録されるイベントを制御します。

これらのコマンドのすべてで同じ方式を使用して、起動または停止の対象となるイベントを指定します。コマンド行上でコマンドの名前の後に続けて、通常は次のいずれか 1 つを入力します (他のオプションもあります)。

- **event** *subsystem.event#* を入力して、単一の事前定義イベントを指定する。

  subsystem は、ELS に認知されている機能コンポーネントの名前であり、例えば、″dls″ で DLSw を示し、 ″esc″ で ESCON を示します。なお、**li sub** と入力すれば、 ELS サブシステム名のリストを表示させることができます。

  event# は、事前定義イベントの名前で、先行ゼロを付けて入力します。なお、**li sub** *subsystem* を入力すれば、特定のサブシステム内のイベントのクィック・リストを表示させることができます。

- **sub** *subsystem logging_level* を入力して、ELS サブシステム内の事前定義イベントのセットを指定する。

  subsystem は、上で説明した ELS サブシステム名です。値「all」では、すべてのサブシステムが選択されます。

  logging_level は任意指定であり、デフォルトでは「standard」で、エラー・メッセージおよび異常通知メッセージがすべて含まれます。値「all」では、サブシステム内のすべてのメッセージが選択されます。

これらのコマンドの例が幾つか下に示してあります。

disp sub all
: すべての ELS サブシステム内のすべてのエラー・メッセージおよび異常通知メッセージの talk 2 へのログ記録を使用可能にします。これは talk 6 での構成に適した汎用設定です。

rem sub dls
: すべての DLS サブシステム内のすべてのエラー・メッセージおよび異常通知メッセージのリモート・ログ記録を使用可能にします。別途に、リモート・ログのためのあて先ホストを構成する必要があります。

disp sub sdlc all
: SDLC サブシステム内のすべてのメッセージの talk 2 へのログ記録を使用可能にします。エラー状態のトレースを試みるときは、すべてのメッセージを使用可能にする場合があります。

nodisp ev sdlc.008
: エラー・ログ内のより重要なメッセージの表示を妨げる場合がある、特に chatty な SDLC メッセージの talk 2 へのログ記録を使用不可にします。

trap ev dls.475
: 特定の DLSw QLLC エラー・イベントの発生時における SNMP トラップの送信を使用可能にします。

これらのコマンド、リモート・ログの構成方法、ログ・レベル、およびその他についての詳細は、*MAS ソフトウェア使用者の手引き* の「イベント・ログ・システム (ELS) の使用」を参照してください。

メモリー使用状況の監視

この節では、ネットワーク・ユーティリティーのメモリーの使用法、およびその状況を監視する方法について説明します。

ネットワーク・ユーティリティーのメモリー使用法

ネットワーク・ユーティリティーには、出荷時に、256 MB と 512 MB のどちらかのメイン・メモリーが備えられています。 システムをブートすると、命令コードがディスクからこのメモリーにロードされ、それぞれのロード・モジュールごとに一定量のメモリー・スペースを占めます。 命令コードがロードされると、システムでは、残りのメモリーを APPN/TN3270 (構成されている場合) とルーティング機能の間で分割します。ルーティング機能には、IP、DLSw、TCP、チャネル・ゲートウェイなど、要するに、APPN および TN3270 サーバーを除くすべての機能が含まれます。

APPN の構成時には、構成プログラムとコマンド行のどちらでその構成を行う場合でも、APPN 用として予約するメモリーの量を指定することができます。ネットワーク・ユーティリティーでは、この値は、最大 TN3270E サーバー構成に必要なメモリーに事前設定されます[12]。 この値は、非 TN3270 APPN アプリケーションの場合でも妥当なはずであり、変更する必要はありません。構成が APPN を使用可能にしない場合は、ネットワーク・ユーティリティーでは、構成された値を無視し、APPN 用としてメモリーを予約しません。 構成が APPN を使用可能にする場合は、ネットワーク・ユーティリティーでは、指定された量のメモリーを APPN に割り振ってから、残りのメモリーすべてをルーティング機能に割り振ります。

実行ネットワーク・ユーティリティー内のメモリー使用状況は、コマンド行コンソールと SNMP 管理ステーションのどちらからでも監視することができます。いずれの場合も、APPN メモリーの状況とルーティング機能メモリーの状況は、別々に表示させて見ることになります。システムにロードされると、これらのメモリー区画は固定され、独立して管理されます。

コマンド行からのメモリーの監視

コマンド行からのルーティング機能メモリーの監視は、次のようにして行います。

1. * プロンプトで **talk 5** と入力し、**Enter** を押して、+ プロンプトを表示させます。
2. **mem** と入力して、現行メモリー状況に関する要約および詳細統計を表示させて見ます。表示出力では、ルーティング機能によって使用されているメモリーを指すのに、*heap (ヒープ)* という用語が使用されています。

コマンド行からの APPN/TN3270 メモリーの監視は、次のようにして行います。

1. * プロンプトで **talk 5** と入力し、**Enter** を押して、+ プロンプトを表示させます。
2. + プロンプトで **p appn** と入力し、**Enter** を押して、 APPN コンソール・サブプロセスにアクセスします。
3. **mem** と入力し、**Enter** を押して、APPN メモリー使用状況に関する要約および詳細統計を表示させて見ます。表示出力では、 APPN メモリーはさまざまな部分に分割され、各部分ごとの状態が示されています。

SNMP の使用によるメモリーの監視

ネットワーク・ユーティリティーでは、ルーティング機能と APPN/TN3270 の両方に関するメモリー使用状況情報にアクセスできる、IBM エンタープライズ特定 MIB をサポートします。

107ページの『IBM Nways マネージャー・プロダクト』で説明されている Nways マネージャー・プロダクトには、 APPN とルーティング機能の両方のメモリー区画に関する全統計サポートが備えられています。いずれの区画についても、使用状況のリアルタイムおよび履歴情報を表示させて見ることができます。いずれの使用状況についても警報しきい値を設定して、メモリー使用率が一定のレベルに達したら、通知を受けられるようにすることができます。

12. 512 MB に対するサポートが導入されたので、構成プログラムは、デフォルトでは、ターゲット・ネットワーク・ユーティリティーのメモリーは 512 MB であるものとみなします。この構成をメモリーが 256 MB のネットワーク・ユーティリティーにロードした場合は、メモリー設定値は、メモリーが 256 MB のボックスの場合のデフォルト値に自動的に下方調整されます。 構成プログラムのデフォルト値を変更する必要はありません。

コマンド行からの構成では、使用可能なルーティング機能メモリーが指定されたしきい値より下に落ちた場合は、ネットワーク・ユーティリティーが SNMP トラップを送信するように、構成することができます。 talk 6 の Config> プロンプトで、コマンド **patch mosheap-lowmark** を入力し、デフォルト値の 10% から変更したい場合は、パーセント値を指定します。

CPU 使用状況の監視

この節では、CPU 監視を制御し、talk 5 から報告を入手したり、定期的なメッセージを talk 2 ログに送信する方法について説明します。

パフォーマンス監視へのアクセス

メイン talk 5 と talk 6 のどちらのプロンプトでも、**perf** と入力すると、パフォーマンス監視コンソール・サブプロセスと Config (構成) サブプロセスにそれぞれ入ります。 talk 6 からでも構成プログラムからでも、CPU 使用状況監視を使用可能または使用不可にし、その操作パラメーターをネットワーク・ユーティリティーの構成の一部として設定することができます。 talk 5 からの場合は、同じ変更を即時に有効にさせることができ、実行ネットワーク・ユーティリティー内の CPU 使用状況に関する報告を入手することができます。

コマンド行からの CPU 使用状況の監視

PERF Console> プロンプトが表示されているときは、次のコマンドが使用できます。

report 現行使用状況、高水準点、および値の分布履歴の要約が示されます。

enable cpu、disable cpu
CPU 使用状況情報の総合的な収集を制御します。デフォルトでは、ネットワーク・ユーティリティーは稼働中、CPU 使用状況が使用可能になっていますが、システム・パフォーマンスに対する影響は無視できる程度です。 TN3270 サーバー機能をネットワーク・ディスパッチャーと一緒に使用している場合は、CPU 使用状況は使用可能のままにしておくことが特に大切です。

enable t2、disable t2
CPU 使用状況を示す、talk 2 での定期的な ELS メッセージの生成が制御されます。このメッセージを使用可能にすれば、 **report** コマンドを繰り返し入力して、CPU 使用状況の変化を監視する必要をなくすることができます。

set、list、clear
統計収集用の時刻ウィンドウを設定します。すべての設定の現行値を表示させます。統計をリセットします。

talk 6 および構成プログラムからでも、 **clear** と **report** を除いて、同じコマンドおよびパラメーターがすべて使用できます。

これらのコマンドおよびその出力の例について詳しくは、 *MAS ソフトウェア使用者の手引き* の「パフォーマンスの構成と監視」を参照してください。

SNMP の使用による CPU 使用状況の監視

ネットワーク・ユーティリティーでは、CPU 使用状況の現行および履歴情報にアクセスできる、 IBM エンタープライズ特定 MIB をサポートします。

107ページの『IBM Nways マネージャー・プロダクト』で説明されている Nways マネージャー・プロダクトには、ネットワーク・ユーティリティーの CPU 使用状況に関する全統計サポートが備えられています。使用状況のリアルタイムと履歴の両方の情報を表示させて見ることができます。使用率のしきい値を設定して、一定のレベルに達したら、通知を受けられるようにすることができます。

第10章 ソフトウェアの保守

この章では、ネットワーク・ユーティリティーのソフトウェア問題用の修正を受け取ってインストールする場合、および新規機能が含まれている新しいソフトウェア・リリースに更新する場合に心得ている必要があることについて説明します。

ここで扱う情報には、以下のものがあります。
- ソフトウェアの名前の付け方とパッケージの仕方
- 新しいソフトウェア・バージョンをワールド・ワイド・ウェブ (WWW) からダウンロードする方法
- ソフトウェアをネットワーク・ユーティリティーにロードする方法
- プロダクト・サービスおよびサポートの依頼の仕方

ソフトウェアのバージョンとパッケージ

バージョン名

ネットワーク・ユーティリティーを作動させるソフトウェアは、マルチプロトコル・アクセス・サービス、または MAS と呼ばれています。IBM 2216-400 を作動させるソフトウェアも MAS とですが、MAS のパッケージは、それぞれの製品に応じて異なり、別になっています。ネットワーク・ユーティリティー用の MAS パッケージには、次のような特徴があります。
- ネットワーク・ユーティリティーを使用予定のアプリケーションに合わせて調整するように、構成デフォルト値が事前設定されている。
- ネットワーク・ユーティリティーの主要な用途向きに機能パッケージが特殊化されている。例えば、2216-400 の汎用マルチプロトコル・ルーティング機能の一部には、IPX、 Appletalk、Banyan Vines、DECNet など、ネットワーク・ユーティリティーのパッケージとしては利用できないものがあります。

特定のレベルの MAS であることを識別するには、以下の番号が使用されます。

バージョン
機能リリースが新しくなると、バージョン番号を新しくする必要がある場合があります。これは、値上げに関連して行われることもありますが、 IBM のソフトウェアの配布方法の変更に関連して行われる場合もあります。バージョン番号が新しくなったからといって、リリース番号だけが新しくなった場合に比べて、そのリリースに新規機能が多くなっていることを意味するわけではありません。

リリース
機能リリースが新しくなるたびに、この番号は変更されます。

修正 この番号では、規模の大きい基本新規機能リリースに対する小規模の変更に過ぎない新規機能リリースであることを示します。「MAS Vv.r Mod m PTF p」の形式で、小数点の後に続くのがこの番号です。

PTF この番号では、下で説明する保守レベルを表します。

ネットワーク・ユーティリティーの初期コード・ベースは MAS V3R1.0 PTF 1 です。IBM では、 2216-400 パッケージの MAS の場合と同じリリース番号を使用しているため、両製品のソフトウェアの機能および保守レベルの相関付けを簡単に行うことができます。

ネットワーク・ユーティリティーで現在稼働しているコードのソフトウェア・レベルを表示させて見る場合は、基本 talk 5 メニューに移動し、**c** (「configuration」を表す) と入力します。このコマンドの出力のソフトウェア・バージョン部分には、「MAS Vv.r Mod m PTF p」の形式が使用されています。

ネットワーク・ユーティリティーのハード・ディスク上のコード・ロードのソフトウェア・レベルを表示させて見る場合は、基本 talk 6 メニューに移動し、**boot** と入力して、ブート Config (構成) サブプロセスに入り、そこで **describe** と入力します。

保守レベル

最新バージョンのネットワーク・ユーティリティー・ソフトウェアが収められているワールド・ワイド・ウェブ (WWW) にアクセスすると、ネットワーク・ユーティリティーのさまざまな保守レベルを表すための次のような用語の一部が表示されます。

GA レベル
IBM のお客さま向けに初めて「出荷可能」になったソフトウェア・レベル。新しいネットワーク・ユーティリティー・ボックスのハード・ディスクに収めて、最初に出荷されたレベルです。 GA レベルのソフトウェアに対しては、そのリリース前に、プロダクト・レベルおよびシステム・レベルの、広範囲にわたるテストが課されます。 一般出荷可能日は、通常、ソフトウェアの新しいバージョンまたはリリースに対応します (PTF でのネットワーク・ユーティリティーの初期リリースは、この通則の例外です)。

PTF 多数の修正が累積し、ほとんどの主要ソフトウェアのレグレッション・テストを経た、主要な保守リリース(「プログラム一時修正」)。 1 つのリリースがしばらく展開されると、IBM では、一般的に、継続的 PTF を新しい製品のハード・ディスクに収めた出荷を始めます。

EPTF 発表される頻度が高く、関連する修正が少なく、修正の影響が生じる特定分野のレグレッション・テストを経た、小規模の保守リリース (「Emergency PTF」)

PTF も EPTF も累積性を有し、それぞれそれ以前の PTF および EPTF すべてに取って代わります。最新の PTF や EPTF をインストールするだけで、それ以前の修正はすべて得られます。

フィーチャー・パッケージ

ネットワーク・ユーティリティーのフィーチャー・パッケージは、ネットワーク・ユーティリティーに 2 種類の異なるモデルがあるので、それぞれのモデルに対応して 2 種類あります。

モデル	説明
TX1	基本コードで、DLSw、APPN、IP、VPN を含む。
TN1	基本コードに TN3720E サーバー機能が加わる。

お買い上げいただいたモデルに応じて、ネットワーク・ユーティリティーには、ハード・ディスクの両方のバンクに、適正なソフトウェア・パッケージがプリロードされています。新しい保守レベルのソフトウェアをロードする場合は、ネットワーク・ユーティリティー上に既存のものと同じパッケージをロードします。

構成プログラムのバージョンは 1 つしかなく、すべてのソフトウェア・パッケージに収められているソフトウェア機能がサポートされることに注意してください。ルーターに搭載されている特定のソフトウェア・パッケージ内でサポートされていない機能を構成しても、ルーター・ソフトウェアでは、構成のその部分を無視します。

コマンド行からでは、実行しているソフトウェア・ロード内に存在していないソフトウェア機能の構成も監視もできません。

ソフトウェアへの Web アクセスの仕方

ネットワーク・ユーティリティー・ソフトウェアを更新する場合は、まず最初に該当する保守レベルをワールド・ワイド・ウェブ (WWW) からダウンロードする必要があります。新しいソフトウェアを探す場合は、まず下記のアドレスのメイン・ネットワーク・ユーティリティー・プロダクト・ページにアクセスします。

```
http://www.networking.ibm.com/networkutility
```

まず **Support** をクリックし、次に **Downloads** をクリックすると、次の情報およびリンクにアクセスできます。

- ソフトウェアへのアクセスに関する一般情報
- ソフトウェアのダウンロードおよびインストールの詳細な手順
- 関連 README ファイルを備えた、最新保守レベルの構成プログラムへのリンク
- 関連 PTF または EPTF 内容ファイルを備えた、最新保守レベルの MAS へのリンク

特定の保守レベルの構成プログラムへのリンクをたどっていくと、サポートされているオペレーティング・システムのそれぞれについて、パック 2 進バージョンの 2216/ネットワーク・ユーティリティーの構成プログラムにアクセスすることができます。これらのファイルは、だれでもダウンロードできます。関連 README ファイルには、新しいバージョンの構成プログラムのアンパックおよびインストールの方法が示されています。

特定の保守レベルの MAS へのリンクをたどっていくと、上記にリストしたネットワーク・ユーティリティー・ソフトウェア・フィーチャーのそれぞれの圧縮パック 2 進バージョンにアクセスすることができます。

IBM ネットワーク顧客 ID およびパスワードが示されないと、これらのファイルはダウンロードできません。この ID およびパスワードは、ユーザー自身が Web 上で登録して作成すれば、即時に使用してファイルをダウンロードすることができます。

この ID およびパスワードは、複数の IBM ネットワーク製品にまたがるものであり、それを使用すると、プロダクト更新に関する E メール通知を予約することができます。登録ページをもっていない場合でも、ネットワーク・ユーティリティー・コード・パッケージの初回ダウンロード時に、Web ページの案内で登録ページにアクセスすることができます。

ファイルのダウンロードとアンパック

特定の MAS 保守リリースをダウンロードするための Web ページには、サポートされるソフトウェア・フィーチャーのそれぞれごとにファイルが収められています。それぞれのファイルには、ネットワーク・ユーティリティー用ソフトウェアの完全なセットが入っています。ある保守レベルのネットワーク・ユーティリティー・ソフトウェアをインストールすると、既存のソフトウェアはすべて新しいレベルで完全に置き換えられます。

特定のファイル内のソフトウェアをダウンロードして、それをルーターに転送する場合は、次のようにします。

1. Web ブラウザーを使用して、完全なファイルを 2 進法でワークステーションにダウンロードします。
2. ルーターへのファイルのロード元になるワークステーションに、ファイルを転送します。このワークステーションは、ルーターへのファイル・サーバーとして使用されるため、サーバー・ワークステーション と呼ばれます。このステップでは、FTP やその他のどんなファイル転送方式を使用しても構いません。
3. サーバー・ワークステーションで、ダウンロードされた単一のファイルを複数のルーター・ソフトウェア・ファイルにアンパックします。このようなファイルは *ロード・モジュール* と呼ばれ、ファイル拡張子「ld」 (システムが大文字小文字の混合をサポートしない場合は、「LD」) が付きます。
4. TFTP または Xmodem を使用して、ロード・モジュールをルーターに転送します。

MAS のリリースによって異なりますが、Web ページには、各ソフトウェア・フィーチャーごとに、それぞれが異なるパック・ユーティリティーで構成された、 2 つのファイルが入っている場合があります。したがって、サーバー・ワークステーションでアンパックできるバージョンを選択します。 通常は、次のような選択になります。

サーバーのオペレーティング・システム	ファイル形式	アンパック・コマンド
DOS、Windows、または OS/2	.zip	pkunzip
UNIX または AIX	.tar	tar -xvf

ルーター・ソフトウェアのアンパックにあたっては、「.ld」ファイルはすべて同じディレクトリーに入れ、適切な読み取りアクセスができるファイル・システム許可を備えるようにしてください。「.ld」ファイルは、いずれも名前を変更することはできません。異なるネットワーク・ユーティリティー・フィーチャー・パッケージ間でも、同一パッケージの異なる保守レベル間でも、ファイルの混合はできません。それぞれのパッケージごとに、サーバー・ワークステーションでパス名を変えて、別々に区別しておきます。

新しい命令コードのロード

命令コード (op-code) は、ネットワーク・ユーティリティーの通常のパケット転送およびシステム・サービスの機能を実行するソフトウェアです。命令コードとしては、基本オペレーティング・システム、プロトコル、フィーチャー、診断プログラム、およびコマンド行インターフェース・コードがあります。 PTF および EPTF の中でソフトウェア変更の大部分を占めるのが、命令コードに加えられる変更です。

新しい命令コードのロードおよび起動には、次のことを行う必要があります。

1. アンパックしたロード・モジュールをサーバー・ワークステーションから、ネットワーク・ユーティリティーのハード・ディスク上にある 2 つの命令コード・バンクのどちらか一方に転送する。
2. 新しい命令コードがロードされているバンクからブートするように、ルーターを設定する。
3. ルーターをリブートするか、後日後刻のリブートにスケジュールする。

表13 には、サーバー・ワークステーションからネットワーク・ユーティリティーのハード・ディスクに命令コードを転送できる、さまざまな方法が要約してあります。どの方式を選択するかは、ワークステーションをルーターに接続できる方法、ワークステーションで使用しているソフトウェア、およびユーザーの好みによって決まります。考慮する必要がある重要事項を以下に幾つか挙げておきます。

- すべての「.ld」ファイルを結合したサイズは、10 MB を超えます。サービス・ポートやモデムでなく、LAN またはネットワーク・インターフェースが使用できる可能性がある場合は、ぜひともそうすることによって、ファイル転送に多大の時間が費やされるのを避けます。
- 命令コードおよびファームウェアから TFTP ベースの方式を使用すれば、単一の操作ですべての「.ld」ファイルが自動的に転送されます。Xmodem の場合は、ソフトウェア・ロードを構成する概略 20 にも登る「.ld」ファイルのそれぞれの名前を手動で指定する必要があります。

表 13. 命令コードのロード

物理的な接続機構	回線 プロトコル	転送 プロトコル	ツール	デフォルトの IP アドレス
サービス・ポート + ヌル・モデム	非同期 端末	Xmodem	ファームウェア	該当しない
サービス・ポート + 外付けモデム PCMCIA モデム	SLIP	TFTP	命令コード	ネットワーク・ユーティリティー = 10.1.1.2 ワークステーション = 10.1.1.3
PCMCIA EtherJet イーサネット LIC (10 Mbps) トークンリング LIC	IP	TFTP	命令コード ファームウェア	ネットワーク・ユーティリティー = 10.1.0.2 ワークステーション = 10.1.0.3
任意の IP ネットワーク・インターフェース	IP	TFTP	命令コード	デフォルト値なし

命令コードの使用

123ページの表13 に示されているように、命令コードから開始することができる転送手順の場合は、いずれも TFTP をファイル転送プロトコルとして使用します。

TFTP の使用

TFTP を使用して命令コードおよびファームウェア・ファイルをネットワーク・ユーティリティーのハード・ディスクに転送するための命令コード手順は、次のとおりです。

1. 使用する IP アドレスを構成する。

   イーサネットまたはトークンリング LIC を含めて、標準ネットワーク・インターフェースを使用している場合は、構成プログラムまたは talk 6 を使用して、通常の方法でインターフェースの IP アドレスを構成します (talk 6 では、 IP サブプロセスで **add address** を使用します)。この構成変更は、先に進む前にアクティブにします。

   PCMCIA EtherJet カードを使用している場合は、 **system set ip** を使用して、次のアドレスを設定します。
   - IP アドレス : EtherJet カードの IP アドレス
   - ネットマスク : EtherJet カードに接続されているサブネット用のマスク
   - ゲートウェイ・アドレス : TFTP サーバー・ワークステーションに到達するための中間ルーターがあれば、その IP アドレスであり、中間ルーターがない場合は、ワークステーション自体の IP アドレス。

   SLIP を使用している場合は、IP アドレスは変更できませんが、 123ページの表13 に示されているものを使用する必要があります。
2. 命令コードおよびファームウェア・ファイルを転送する。

   * プロンプトで、以下のシーケンスに従います。

   ```
   *t 6
   Config>boot
   Boot configuration
   Boot config>tftp get load mod
   ```

   次のようにプロンプトに応答します。
   - サーバー IP アドレス : TFTP サーバー・ワークステーションのアドレスを書き込みます。
   - リモート・ディレクトリー : 「.ld」ファイルがあるサーバー・ワークステーション上のディレクトリーへのパス名を書き込みます。サーバーで予測されている向きのスラッシュを使用します。大文字小文字の区別が意味をもつのは、それがサーバーで意味をもっている場合だけです。
   - あて先バンク : バンク A またはバンク B を選択します。現在アクティブのバンクは選択できません。

   サーバーの IP アドレスおよび構成済みネットワーク・ユーティリティー・インターフェースの IP アドレスに基づいて、ルーターでは、サーバーにアクセスする場合に使用するそのインターフェースを選択します。ルーターでは、適宜、成功または失敗状況メッセージを表示します。
3. 構成ファイルをターゲット・バンクに入れる。

新しいコード・ロードを入れたばかりのバンク内の位置に、必要な構成ファイルを転送します。 新しいコード・ロードが新しい MAS リリースである場合は、このステップに関する重要な背景情報について、85ページの『新しい MAS リリースへの構成の移行』を参照してください。

- 新しいコード・ロードが新しい MAS リリースではないか、またはコマンド行インターフェースだけを使用して、ネットワーク・ユーティリティーを構成する場合は、**copy config** コマンドを使用して、新しいロードでピックアップできる場所に現行構成をコピーします。
- 新しいコード・ロードが新しい MAS リリースであり、もっぱら構成プログラムを使用する場合は、構成プログラムを使用して構成をアップグレードします。その上で、コマンド **tftp get config** (または、 91ページの『新規構成ファイルのロード』で説明されているその他の方式のいずれか) を使用して、アップグレード後の構成をターゲット・バンクに転送します。

4. リブートするか、リブートをスケジュールする。

   新しいロードを即時にアクティブにする場合は、次の手順を **Boot config>** プロンプトから始めて使用します。

   a. **set** コマンドを使用して、ロードしたばかりのバンクを次にブートするために選択し、コピーまたは転送したばかりの構成を選択する。
   b. **Ctrl-p** を押し、**reload** と入力してルーターをリブートする。

   新しいロードを後でアクティブにする場合は、 **Boot config>** プロンプトで **timedload activate** と入力して、バンクおよび構成を選択し、ルーターがリブートする日時を指定します。バンクにロードするかという質問に対しては「NO」と答えることができます。このステップはすでに行ったからです。

上記の手順で使用されているコマンドについて詳しくは、*MAS ソフトウェア使用者の手引き* の「変更管理の構成」の章を参照してください。

ファームウェアの使用

123ページの表13 に示されているように、ファームウェアから Xmodem と TFTP のどちらかを使用して、命令コードをネットワーク・ユーティリティーのハード・ディスクに転送します。Xmodem は推奨できません。命令コード・ファイルがこのように大きい場合は、モデム速度が遅過ぎるし、Xmodem では定期的な対話を必要とするからです。ファームウェアから作業を行っている場合は、LAN インターフェースを介する TFTP が、転送方式として優先されます。ただし、使用する必要が生じた場合に備えて、ここには可能な手順すべてを要約してあります。

Xmodem の使用

Xmodem を使用して命令コードおよびファームウェア・ファイルをネットワーク・ユーティリティーのハード・ディスクに転送するためのファームウェア手順は、次のとおりです。

1. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されている手順を使用して、ファームウェア・メインメニューにアクセスする。
2. 次の順序で一連のファームウェア・メニュー選択を行う。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」

b. システム管理ユーティリティー : オプション 12 「Change Management」
c. 変更管理ソフトウェア制御 : オプション 12 「XMODEM software」
d. タイプの選択 : 「Load Image」
e. バンクの選択 : バンク A またはバンク B の選択

ファームウェアによって、ファイル転送の開始時点が通知されます。

3. 端末エミュレーション・パッケージを表示し、ワークステーション・サーバーからファイル LML.ld の転送を開始します。
4. LML.ld の転送後は、ワークステーション・サーバー上の「.ld」モジュールを、 1 つおきに 1 つずつ転送する必要があります。LML.ld が最初であることが必要ですが、その後は、順序は重要ではありません。Firm.ld を含める必要があります。

   ファイル転送が始まると、バンクの状況が CORRUPT に変更されて、完全な有効コード・ロードが入っていないことを示します。ネットワーク・ユーティリティーが最後のロード・モジュールを受信すると、バンクの状況が AVAIL に変更されます。この確認は、ファームウェアの「Change Management」メニューでオプション 7 の「List Software」を使用して行うことができます。
5. ロードしたばかりの命令コードを使用するルーターをブートします。

   オプション 9 の「Set Boot Information」を使用して、ブートする元の新しい命令コード (および構成) を選択します。 **Esc** を押して、メインメニューが表示されたら、 **F9** を押して、新しい命令コードでネットワーク・ユーティリティーをブートします。

TFTP の使用

TFTP を使用して命令コードおよびファームウェア・ファイルをネットワーク・ユーティリティーのハード・ディスクに転送するためのファームウェア手順は、次のとおりです。

1. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されている手順を使用して、ファームウェア・メインメニューにアクセスする。
2. 使用する IP アドレスを構成する。

   次のメニュー順序に従います。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
   b. システム管理ユーティリティー : オプション 11 「Remote Initial Program Load Setup」
   c. ネットワーク・パラメーター : オプション 1 「IP Parameters」

   次のアドレスを設定します。
   - クライアント IP アドレス : ネットワーク・ユーティリティーの LAN カードの IP アドレス。これは一時アドレスで、そのインターフェースのルーター操作アドレスに関連付ける必要はありません。
   - サーバー IP アドレス : ワークステーションの LAN アダプターの IP アドレス
   - ゲートウェイ IP アドレス : 中間ルーターがあればその IP アドレス、ない場合は、ワークステーションの IP アドレスを繰り返します。
   - ネットマスク : ネットワーク・ユーティリティーの LAN カードに接続されているサブネット用のマスク
3. 次のメニュー選択によって転送を開始する。

a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
b. システム管理ユーティリティー : オプション 12 「Change Management」
c. 変更管理ソフトウェア制御 : オプション 10 「TFTP software」
d. タイプの選択 : 「Load Image」
e. バンクの選択 : バンク A または B の選択
f. ロード・タイプの選択 : 「Modules」

4. すべてのロード・モジュールが入っているディレクトリーへのワークステーション上のパスを入力します。
5. プロンプトによる指示が表示された場合は、ファームウェアにファイル転送を行わせたいインターフェースを選択する。

   今度は、ファームウェアがそれぞれのロード・モジュールを転送し、状況メッセージを示します。完了すると、変更管理メニューが表示されます。
6. ロードしたばかりの命令コードを使用するルーターをブートします。

   オプション 9 の「Set Boot Information」を使用して、ブートする元の新しい命令コード (および構成) を選択します。**Esc** を押して、メインメニューが表示されたら、 **F9** を押して、新しい命令コードでネットワーク・ユーティリティーをブートします。

ファームウェアのアップグレード

概要

ファームウェアは、ネットワーク・ユーティリティーの電源オンおよびブート論理を駆動する下位レベルのソフトウェアです。ハード・ディスクにではなく、非揮発性フラッシュ・メモリーに常駐しているので、ディスク上のオペレーショナル・ソフトウェア・ロードの破壊などの障害が発生した場合は、新しいソフトウェアまたは構成ファイルを検索して、バックアップおよび実行ができます。ファームウェアの *アップグレード* とは、新しいバージョンのファームウェアをフラッシュに書き込んで、以前のバージョンを置き換えることを意味します。

ファームウェアをアップグレードする必要があるのは、次の 2 つの条件がある場合です。

1. IBM が問題の修正に必要な PTF または EPTF を出荷し、その PTF または EPTF がファームウェア・アップグレードを必要とする場合。ファームウェアのアップグレードが必要かどうかについては、それぞれの PTF または EPTF に関連する資料に記載されています。
2. 新しい MAS 機能リリースをインストールしたい場合。新しいリリースに移行する場合は、ほとんど常にファームウェア・アップグレードが必要です。

ネットワーク・ユーティリティーのコード・ダウンロード Web ページには、新しいバージョンのファームウェアを収めた別のファイルがあるわけではありません。そうではなく、ファームウェアは、命令コード・ロード・モジュールと共に、.zip および .tar ファイル内にパックされたロード・モジュールの 1 つです。ファームウェア・ロード・モジュールには、「Firm.ld」というファイル名が付いています。すべての

PTF および EPTF には、それぞれ新しい Firm.ld ファイルが入っています。これは、たとえそのファイルの内容がそれ以前の保守レベルの場合と同じ場合でもそうです。

122ページの『ファイルのダウンロードとアンパック』および 123ページの『新しい命令コードのロード』に記載されている手順に従うと、Web から新しいバージョンのファームウェアがダウンロードされ、ハード・ディスクのバンク A またはバンク B に転送されます。Firm.ld をディスク・バンクに入れ、そのバンクからリブートしても、フラッシュ・メモリーから実行されているアクティブ・ファームウェアにはまったく影響がありません。新しいファームウェアにアップグレードするするためには、新しいファームウェアをフラッシュ・メモリーに書き込む必要があります。

手順の概説

Web から新しいファームウェアをダウンロードし、ネットワーク・ユーティリティーのフラッシュ・メモリーに入れるための一般的な方式は、2 通りあります。次のようにして、新しい命令コードのインストールと共に、ファームウェアのアップグレードを行う方式を推奨します。

1. 122ページの『ファイルのダウンロードとアンパック』の説明に従って、新しい保守レベルの命令コードとファームウェアを両方とも Web からローカル・サーバーにダウンロードします。
2. 123ページの『新しい命令コードのロード』で説明されている TFTP または Xmodem 手順のどちらか一方を使用して、新しい命令コードおよびファームウェア「.ld」ファイルをネットワーク・ユーティリティーのハード・ディスク内のバンクの 1 つに転送します。
3. 129ページの『ローカル・ディスク手順』で説明されている手順の 1 つを使用して、現在すでにディスク上にある Firm.ld のコピーをフラッシュ・メモリーに書き込みます。

推奨方式に加えて、ファームウェアだけを独立してネットワーク・ユーティリティー内に転送し、命令コードの転送および起動を伴うことなく、フラッシュに書き込むこともできます。これは、次のようにして行います。

1. 122ページの『ファイルのダウンロードとアンパック』の説明に従って、新しい保守レベルの命令コードとファームウェアを両方とも Web からローカル・サーバーにダウンロードします。ファームウェアだけを Web からダウンロードすることはできません。命令コードと一緒にパッケージされているからです。
2. ネットワーク・ユーティリティーのハード・ディスク上のバンク以外の場所に、Firm.ld だけを転送し、同じ手順でフラッシュに書き込みます。 130ページの『ファイル転送手順』で説明されているように、ファイル転送には Xmodem と TFTP のどちらを使用しても構いません。

ファームウェアだけを独立して転送する方式は、アップグレード方式としては推奨できません。その理由は単に、ハード・ディスクのバンク A または B への新しい命令コードのインストール時にすでに行っている、Firm.ld ファイル転送と重複することになるからです。ローカル・ディスク手順の方が迅速で簡単です。

ローカル・ディスク手順

新しい一組の命令コードとファームウェアをハード・ディスクのバンク A または B に転送してしまったら、下記のどちらかの手順に従って、そのディスク・バンク内のファームウェアをアクティブにします。

命令コードの使用

注： この手順が使用できるのは、MAS V3.2 以降の命令コードを実行している場合です。そのようなレベルを初めてインストールする場合は、リブートして新しい命令コードを有効にしてからでないと、この手順を使用して、ファームウェアを同じレベルにアップグレードすることはできません。

1. **talk 6** と入力した上で、 **boot** と入力して、ブート Config (構成) サブプロセスにアクセスします。
2. **update** と入力して、ファームウェア・アップグレードを開始します。
3. プロンプトが表示されたら、新しいレベルの命令コードとファームウェアを転送したバンク (A または B) を選択します。

   また、″P″ オプションも選択できるので、それを使用して、前にディスクに (ただし、バンク A でも B でもない) 保管した有効なファームウェア・レベルによるフラッシュの再書き込みを行うことができます。フラッシュが破壊された状態になり (フラッシュ書き込み中にシステムで電力損失が生じたためと考えられる)、直前のファームウェア・レベルに戻りたい場合は、これが使用できます。
4. システムでは、ユーザーが指定した場所に入っている新しいファームウェア・レベルを用いてフラッシュ・メモリーに書き込み、新しい「回復イメージ」 (″P″ で選択したもの) を適宜自動的に作成します。フラッシュ・メモリーでのファームウェアの更新中は、ネットワーク・ユーティリティーの電源をオフにしないようにします。

update コマンドによって新しいファームウェア・レベルがフラッシュ・メモリーに書き込まれますが、更新後のファームウェアが稼働し始めるのは、次回のリブート後になります。したがって、 `Boot config>` プロンプトからのファームウェア・アップグレードが必要な、新しい保守レベルをインストールする最も簡単な方法は、次のようにすることです。

1. **tftp get load m** を使用して、新しい命令コードとファームウェアをディスクにロードする。
2. **update** を使用して、新しいファームウェアをフラッシュに書き込む。
3. **copy** を使用して、構成ファイルを新しいコード・バンクにコピーする。
4. **set** を使用して、次回ブートする場合の新しいコード・バンクを選択する。
5. **Ctrl-p** を押し、**reload** と入力して、ネットワーク・ユーティリティーをリブートし、新しいファームウェアと新しい命令コードを同時に使用する。

ファームウェアの使用

新しいレベルの命令コードとファームウェアをディスク・バンク A または B に転送したら、新しい命令コードを使用するためにリブートしますが、以前のファームウェア内で停止して、次のようにしてフラッシュ・メモリーに新しいファームウェアを書き込みます。

1. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されている手順を使用して、ファームウェア・メインメニューにアクセスする。
2. 次の順序で一連のファームウェア・メニュー選択を行う。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
   b. システム管理ユーティリティー : オプション 7 「Update System Firmware」
   c. F/W 更新オプション : オプション 3 「Use a Local Image File」

   ファームウェアがローカル・ファイル名を尋ねてきます。次のどちらか一方を入力します。
   c:\sys0\firm.ld (バンク A の場合)
   c:\sys1\firm.ld (バンク B の場合)
3. 「Do you want to continue?」という質問に「Yes」と応答する。ファームウェアがフラッシュ・メモリーへの新しいファームウェアの書き込みを開始します。
4. 更新の進行中は待機し、システムをオフにしないようにする。
5. 完了したら、**Enter** を押してシステムを再始動する。この手順のステップ 1 で自動ブートを使用可能にした場合は、新しいファームウェアがブートアップして、新しい命令コードに入ります。

ファイル転送手順

ローカル Xmodem または TFTP サーバーからネットワーク・ユーティリティーにファームウェアだけを転送し、そのファームウェアをアクティブにする場合は、次の手順のどちらかに従います。表16 に示されているように、両方の手順で以前のファームウェア・ユーザー・インターフェースを使用して、多数ある接続タイプのいずれかを介してファイル転送を開始します。128ページの『手順の概説』で説明されているように、ローカル・ディスク手順の方がこれらの手順を使用するより速い場合があります。

表 14. ファームウェアのロード

物理的な接続機構	回線 プロトコル	転送 プロトコル	ツール	デフォルトの IP アドレス
サービス・ポート + ヌル・モデム サービス・ポート + 外付けモデム PCMCIA モデム	非同期 端末	Xmodem	ファームウェア	該当しない
PCMCIA EtherJet イーサネット LIC (10 Mbps) トークンリング LIC	IP	TFTP	ファームウェア	ネットワーク・ユーティリティー = 10.1.0.2 ワークステーション = 10.1.0.3

Xmodem の使用

Xmodem を使用して命令コードおよびファームウェア・ファイルをネットワーク・ユーティリティーのハード・ディスクに転送するためのファームウェア手順は、次のとおりです。

1. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されている手順を使用して、ファームウェア・メインメニューにアクセスする。

2. 次の順序で一連のファームウェア・メニュー選択を行う。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
   b. システム管理ユーティリティー : オプション 12 「Change Management」
   c. 変更管理ソフトウェア制御 : オプション 12 「XMODEM software」
   d. タイプの選択 : 「Load Image」
   e. バンクの選択 : バンク A またはバンク B の選択

   ファームウェアによって、ファイル転送の開始時点が通知されます。
3. 端末エミュレーション・パッケージを表示し、ワークステーション・サーバーからファイル LML.ld の転送を開始します。
4. LML.ld の転送後は、ワークステーション・サーバー上の「.ld」モジュールを、 1 つおきに 1 つずつ転送する必要があります。LML.ld が最初であることが必要ですが、その後は、順序は重要ではありません。Firm.ld を含める必要があります。

   ファイル転送が始まると、バンクの状況が CORRUPT に変更されて、完全な有効コード・ロードが入っていないことを示します。ネットワーク・ユーティリティーが最後のロード・モジュールを受信すると、バンクの状況が AVAIL に変更されます。この確認は、ファームウェアの「Change Management」メニューでオプション 7 の「List Software」を使用して行うことができます。
5. ロードしたばかりの命令コードを使用するルーターをブートします。

   オプション 9 の「Set Boot Information」を使用して、ブートする元の新しい命令コード (および構成) を選択します。 **Esc** を押して、メインメニューが表示されたら、 **F9** を押して、新しい命令コードでネットワーク・ユーティリティーをブートします。

TFTP の使用

TFTP の使用によるファームウェア・ファイル転送および更新の手順は、次のとおりです。

1. 51ページの『ブート・オプション : 高速ブートとファームウェアへのアクセス』に記載されている手順を使用して、ファームウェア・メインメニューにアクセスする。
2. 使用する IP アドレスを構成する。

   次のメニュー順序に従います。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
   b. システム管理ユーティリティー : オプション 11 「Remote Initial Program Load Setup」
   c. ネットワーク・パラメーター : オプション 1 「IP Parameters」

   次のアドレスを設定します。
   - クライアント IP アドレス : ネットワーク・ユーティリティーの LAN カードの IP アドレス。これは一時アドレスで、そのインターフェースのルーター操作アドレスに関連付ける必要はありません。
   - サーバー IP アドレス : ワークステーションの LAN アダプターの IP アドレス
   - ゲートウェイ IP アドレス : 中間ルーターがあればその IP アドレス、ない場合は、ワークステーションの IP アドレスを繰り返します。
   - ネットマスク : ネットワーク・ユーティリティーの LAN カードに接続されているサブネット用のマスク

3. 次の順序で一連のメニュー選択を行って転送を開始する。
   a. システム管理サービス (メインメニュー) : オプション 4 「Utilities」
   b. システム管理ユーティリティー : オプション 7 「Update System Firmware」
   c. F/W 更新オプション : オプション 1 「TFTP a Remote Image File」

   次のファイル名を入力します。

   - ローカル・ファイル名 : ネットワーク・ユーティリティーのハード・ディスクのルート・ディレクトリーに保管される一時ファイルの名前を選択します。パス名を指定しないようにします。 3 文字以内のファイル名拡張子を使用します。
   - リモート・ファイル名 : ワークステーション上のファームウェア・ロード・モジュールのパスおよびファイル名 (「Firm.ld」であることが必要)。Web からダウンロードした .zip または .tar ファイルをアンパックしたディレクトリーであることが必要です。

   ファームウェアが使用するアダプターおよびポートを選択すると、ルーターが TFTP 取得操作を開始します。
4. TFTP の完了後、ファームウェア・コンソールで、「Do you want to continue?」という質問に「Yes」と応答する。ファームウェアがフラッシュ・メモリーへの新しいファームウェアの書き込みを開始します。
5. 更新の進行中は待機し、システムをオフにしないようにする。
6. 完了したら、**Enter** を押してシステムを再始動する。新しいファームウェアがブートアップすると、現行命令コードに入ります。

サービスおよびサポートの依頼の仕方

ネットワーク・ユーティリティーを IBM の業務提携先や販売店から購入した場合は、サービスおよびサポートを受ける方法について、購入元にお問い合わせください。

ネットワーク・ユーティリティーを IBM から購入した場合は、以下の形式の援助がご利用いただけます。

- ハードウェアまたはコードの問題に関するサービスおよびサポート

  電話によるサポートの場合 :
  – 米国内 - 電話連絡先は 1 800 IBM-SERV (1 800 426-7378) です。
  – 米国以外 - 電話番号については、現地の IBM サービス技術員にお問い合わせください。

  電話を掛ける前に、ネットワーク・ユーティリティーのバック・プレートでマシンのタイプ、モデル、および製造番号を調べておいていただきます。ソフトウェアの問題である場合は、ネットワーク・ユーティリティーからメモリー・ダンプを転送して、IBM サポート担当員に送信するために使用できるように、TFTP サーバーおよびインターネット接続を用意しておいていただく必要がある可能性があります。

  ワールド・ワイド・ウェブ (WWW) によって下記のアドレスの IBM Service and Support にアクセスしていただくこともできます。

  `http://www.networking.ibm.com/support/networkutility`

ネットワーク・ユーティリティー製品を選択して、製品技術ヒント、FAQ、およびコード更新を入手します。 さらに、将来のコード更新の通知を受け取ることができるように予約しておくこともできます。

- 初期インストールに関する構成ヘルプおよびハウツー質問の場合
  - 米国内 - 電話連絡先は 1 800 IBM-SERV (1 800 426-7378) です。これは無料サービスです。
  - 米国以外 - 現地の IBM サービス技術員にご連絡ください。 米国以外では、有料サービスになる可能性があります。
- ネットワーク設計、計画、または問題判別に関するサービスおよびサポート契約
  - 米国内 - 電話連絡先は 1-800-IBM-SERV (1 800 426-7378) です。
  - 米国以外 - 現地の IBM サービス技術員にご連絡ください。

第3部 構成および管理の詳細

第11章 概説

この章には、本書の135ページの『第3部 構成および管理の詳細』と題する部分の概要を示してあります。ネットワーク・ユーティリティーで使用できるアプリケーションについて概説し、それらのアプリケーションの一部が他の章でどのように記述されているかについて説明します。

主要なネットワーク・ユーティリティー機能

IBM のマルチプロトコル・アクセス・サービス・ソフトウェア・テクノロジーの使用によって、ネットワーク・ユーティリティーではさまざまなネットワーク機能をサポートします。ネットワーク・ユーティリティーは、少数の物理インターフェースが必要なネットワーク位置で、CPU およびメモリーに集中されている機能が果たせるように、特に設計されています。

ネットワーク・ユーティリティーのモデル別主要アプリケーションには、次のようなものがあります。

モデル TN1 - ネットワーク・ユーティリティー TN3270E サーバー

TN3270E サーバー

TN3270E サーバー機能によって、IP デスクトップ・ユーザーは、SNA ホスト・アプリケーションへのアクセスが得られます。

IP ネットワーク全般にわたって分散している TN3270 クライアントの数が中規模から大規模の場合は、地区事務所またはホスト・データ・センターに 1 台または複数台のネットワーク・ユーティリティーを配置すれば、アクセスできるようにすることができます。

また、ネットワーク・ユーティリティー・モデル TN1 では、モデル TX1 の機能もすべてサポートされます。

モデル TX1 - ネットワーク・ユーティリティー・トランスポート

データ・リンク交換 (DLSw)

DLSw によって、IP バックボーン・ネットワークをまたがって、ネイティブ SNA エンド・ステーション (ワークステーション、コントローラー、 FEP、またはホスト) 接続性が得られます。 FRAD および X.25 PAD プロダクトで行われるような DLC タイプの変換も実行されます。

地区事務所またはホスト・データ・センターに 1 台または複数台のネットワーク・ユーティリティーを配置すれば、多数の事業所に置かれている小型 DLSw ルーターからの TCP 接続を終端することができます。

拡張ピアツーピア・ネットワーキング機能 (APPN)

APPN によって、SNA バックボーン・ネットワークをまたがって、ネイティブ SNA エンド・ステーション (ワークステーション、コントローラー、FEP、またはホスト) 接続性が得られます。エンタープライズ・エクステンダー・フィーチャーによれば、これと同じ接続性が IP バックボーン・ネットワークをまたがって使用できます。

ネットワーク・ユーティリティーは、大容量 APPN ネットワーク・ノードが必要とされる場所であれば、どこにでも配置することができます。IP ネットワークの端に置けば、他のエンタープライズ・エクステンダー製品からのトラフィックを受信することができます。また、2 つの異なる APPN ネットワークの接続時には、ネットワーク・ユーティリティーを使用すれば、拡張ボーダー・ノード機能が得られます。

チャネル・ゲートウェイ

ネットワーク・ユーティリティーでは、ESCON (光ファイバー・ケーブル) アダプターとパラレル・チャネル (バスおよびタグ・ケーブル) アダプターを両方ともサポートします。これらのアダプターの一方を使用すると、ネットワーク・ユーティリティーは、S/390 ホストからローカル LAN、 ATM ネットワーク、または高速シリアル・ラインまで SNA トラフィックと IP トラフィックを両方ともルーティングする、ゲートウェイとして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

この機能を使用すると、多くの IP ベースのアプリケーション・サーバー (例えば、 TN3270 サーバー、HTTP Web サーバー、または FTP サーバー) は、イントラネット上またはインターネット上のクライアント・ワークステーションに対して、単一の IP アドレス外観を示すことができます。ネットワーク・ディスパッチャー機能では、このようなクライアントからの TCP 接続要求に応じ、使用可能なサーバーまでルーティングします。サーバー間の負荷平衡、および障害物理サーバーのバイパスによる「論理サーバー」高可用性の両方が得られます。

ネットワーク・ユーティリティーは、ホスト・データ・センターで、このようなサーバー機能を提供するホストの前、または TN3270E サーバー機能を提供するネットワーク・ユーティリティー、モデル TN1 の前に置くことができます。

高速媒体変換

ネットワーク・ユーティリティーは、それ自体がサポートするアダプター上のインターフェース間で、ブリッジとして使用することができます。

VPN (仮想私設ネットワーク)

VPN 機能は、L2TP、L2F、PPTP、IPSEC、IKE、PKI、Diffserv、LDAP といった一群のトンネリング・プロトコルとセキュリティー・プロトコルで構成されています。これらのプロトコルを一括して使用することによって、ネットワーク・ユーティリティーが、私設の WAN や LAN ではなく、公衆インターネットをエンタープライズ独自の私設ネットワークの拡張部として使用できるように構成できます。ネットワーク・ユーティリティーがこのように構成されると、遠方にあるエンタープライズの事務所や業者や顧客へのネットワーク・トラフィックのトンネル終端点として使用できます。ルーター上にセキュリティー・ポリシーを構成し、これで、ネットワーク・トラフィックは認証や暗号化、またはその両方が必要であるか、平文によるフローが可能であるかを動的に判別します。セキュリティー・ポリシーによって、エンタープライズ・データの公衆ネットワークによる移送が、専用回線を使用する場合に匹敵する安全性と高信頼性と柔軟性をもって、大幅な費用節減のもとに確保されます。

ネットワーク・ユーティリティーは、インターネットとエンタープライズのイントラネットの間の境界点に配して、多数のレイヤー 2 トンネルや IPSEC トンネルを終端させることができます。これらのトンネルがエンタープライズ・ネットワークの延長となって、公衆インターネットの経済性と遍在性を支えます。

本書では、説明を拡張し、構成例を示す場合に備えて、上記の機能の中から重要なものを選択してサブセットにまとめてあります。以降の章では、次のものを扱っています。

- TN3270E サーバー、複数のサーバーの前にオプションでネットワーク・ディスパッチャー付き
- チャネル・ゲートウェイ、SNA トラフィックと IP トラフィックの両用
- データ・リンク交換、TCP 終端とローカル DLC 変換の両方付き
- VPN (仮想私設ネットワーク)

それ以外のネットワーク・ユーティリティー機能の理解および構成に役立つヘルプについては、次のようなソフトウェアに関する中心的な資料を参照してください。

- *MAS プロトコル構成と監視解説書 第 1 巻*
- *MAS プロトコル構成と監視解説書 第 2 巻*
- *MAS フィーチャーの使用と構成*
- *MAS ソフトウェア使用者の手引き*

構成ヘルプは、IBM レッドブックでも得られます。これらは、 IBM 2216 モデル 400 専用の資料には違いありませんが、構成事例の中には該当するものもあります。

- *IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume 1* (SG24-4957)
- *IBM 2210 Nways Multiprotocol Router and IBM 2216 Nways Multiaccess Connector Description and Configuration Scenarios Volume 2* (SG24-4956)

章のレイアウトと規則

本書の第 12 章 ～ 第 20 章は、次のように編成されています。

章のレイアウト

4 つの主要機能 (TN3270E サーバー、チャネル・ゲートウェイ、データ・リンク交換、 VPN) のそれぞれに、次のように 2 章ずつを当てています。

- 概要を説明する章の内容
  - サポートされる機能の要約
  - ネットワーク構成例の説明
  - 機能を管理する方法の概要
- 「構成例の詳細」の章の内容
  - 主要な構成例のラベル付き図
  - 構成プログラムを使用する場合とコマンド行を使用する場合の構成パラメーター付き突き合わせ表

4 つの「構成例」の章に図示し説明してある構成は、実際の作業構成です。これらの構成に一致する 2 進構成ファイルは、ワールド・ワイド・ウェブ (WWW) から

ダウンロード可能です。 これらのファイルにアクセスする場合は、下記のアドレスから Support および Downloads リンクをたどってください。

http://www.networking.ibm.com/networkutility

さらに、295ページの『第18章 サンプル・ホスト定義』には、ネットワーク・ユーティリティー構成との突き合わせを行うために、IBM ホスト・ソフトウェア・プロダクトを構成するための詳細な例が挙げてあります。

構成例表の規則

4 つの「構成例」の章で使用されている構成パラメーター表は、すべて同じ形式を踏襲しています。表の欄および規則は、次のとおりです。

構成プログラム・ナビゲーション
パラメーター値を入力するパネルが表示されるまでにたどる順序での一連のフォルダー名およびパネル名

構成プログラム値
パラメーター名とその値

構成プログラム・パネルに表示されているパラメーターが、表にリストされていない場合は、デフォルト値を使用しました。 ***ユーザーの構成では、2216-400 ではなく、ネットワーク・ユーティリティーが正しいデフォルト値をもつようにする必要があります。***

コマンド行コマンド
コマンド行インターフェースを使用して同じパラメーターを構成する場合に入力するコマンドは、次のようになります。

- コマンド・シーケンスは、talk 6 の Config> プロンプトから始まります。必要な場合は、初期コマンドで、メニュー・システム内の正しい場所にアクセスする方法、およびその結果表示されるコマンド・プロンプトが示してあります。
- パラメーターが指定されていないコマンドは、入力値を尋ねるか、パラメーターがないかどちらかです。システムからのパラメーター・プロンプトは、この書体 で示してあります。
- 値プロンプトおよび入力する値がそれ自体で説明になっている場合は、詳細は示されていません。
- 「他のデフォルトを受け入れる」では、(**Enter** を押して) デフォルト値を受け入れる必要がある他のパラメーター・プロンプトがあることを意味します。

注 それぞれの表の下部の注釈を参照する番号

第12章 TN3270E サーバー

概説

ここでは、TN3270 について概説し、ネットワーク・ユーティリティーに実装されている TN3270E サーバー機能について要約します。

TN3270 とは

今日では、多くの企業が単一の IP 専用バックボーンへの WAN トラフィックの統合を検討しています。それと同時に、ワークステーション構成を単純化し、デスクトップでの TCP/IP プロトコル・スタックのみの実行を試みている企業もあります。ただし、こうした企業でもほとんどが、SNA アプリケーション・ホストへのアクセスを必要としていることに変わりはありません。

TN3270 を使用すると、デスクトップからネットワークを通して IP を実行し、TN3270 サーバーを介して SNA ホストに接続できるので、こうした要件が満たされます。クライアントは、TCP 接続を使用して、サーバーに接続します。サーバーでは、サーバーが SNA ホストとの間で維持している SNA 従属 LU-LU セッションにクライアント・セッションをマップすることによって、ダウンストリーム TN3270 クライアントに対してゲートウェイ機能を提供します。TN3270 サーバーは、TN3270 データ・ストリームと SNA 3270 データ・ストリームの間の変換を処理します。

TN3270 ソリューションを展開するためには、デスクトップ・ワークステーションに TN3270 クライアント・ソフトウェアをインストールし[13]、 以下で説明する場所のどこか 1 個所に TN3270 サーバー・ソフトウェアをインストールします。クライアント・ソフトウェアは IBM およびその他の多くのベンダーから入手することができ、ワークステーション内の TCP/IP スタック上で稼働します。 特定のクライアント・プロダクトには、次の 2 つのレベルの標準サポートのいずれか一方が用意されています。

- 基本 TN3270 クライアント

  これらのクライアントは RFC 1576 (TN3270 Current Practices)、または RFC 1646 (TN3270 Extensions for LU name and Printer Selection)、あるいはその両方に準拠しています。

- TN3270E クライアント

  これらのクライアントは RFC 1647 (TN3270 Enhancements)、および RFC 2355 (TN3270 Enhancements) に準拠しています。

TN3270E クライアントをサポートできるサーバー・インプリメンテーションが、TN3270E サーバーと呼ばれています。

13. プリンターを表す小規模の専用 TN3270 クライアント・プロダクトも入手できます。

TN3270 サーバー機能の配置

TN3270 サーバー機能が配置できるのは、ネットワーク内のさまざまな製品および位置で、それには次のようなものがあります。

- SNA ホスト自体

  IBM およびその他のベンダーでは、ホスト TCP/IP スタック上に収まり、ホスト内で VTAM に接続する TN3270 サーバー・ソフトウェアを提供しています。

- ネットワーク内のルーターまたはネットワーク・ユーティリティー

  IBM およびその他のベンダーでは、TN3270 サーバー機能をネットワーク・ハードウェア製品に組み込んで提供しています。これらの製品は、SNA ホストに直接隣接して置くこともできるし、ネットワーク内でホストへの SNA 接続が得られる位置であればどこにでも置くことができます。IBM 製のルーター (2210 または 2216) またはネットワーク・ユーティリティーを使用していて、ホストで APPN が稼働している場合は、エンタープライズ・エクステンダー・テクノロジーを使用して、ホストへの IP 接続が得られる位置であればどこにでもサーバーを置くことができます。

- ネットワーク内のソフトウェア・プロダクト

  IBM およびその他のベンダーでは、AIX、OS/2、Windows/NT などのオペレーティング・システムを使用している中性能サーバーにインストールする、 TN3270 サーバー・ソフトウェア・プロダクトを提供しています。これらのプロダクトは、ネットワーク内でアプリケーション・ ホストへの SNA 接続が得られる位置であればどこにでも置くことができます。

TN3270 サーバー・プロダクトおよびネットワーク内位置の選択は、次のような要因がからむ複雑な選択になります。

- ホストの容量およびサイクルの影響
- パフォーマンスおよび容量の値段
- 可用性
- サーバー障害の影響
- 拡張容易性

ネットワーク・ユーティリティーは、高性能 TN3270E サーバー・インプリメンテーションで、大規模ネットワークへの拡張容易性を備えています。これをネットワーク・ディスパッチャー・フィーチャーと組み合わせれば、大規模 TN3270 導入システムでのサーバー冗長度と負荷共用を実現することができます。また、データ・センターから離れた SNA または IP ネットワーク内にネットワーク・ユーティリティーを配して、拡張容易性、増分追加、およびサーバー障害による影響の削減という同様の利点を得ることもできます。

ネットワーク・ユーティリティーの TN3270E サーバー機能

標準準拠

ネットワーク・ユーティリティーに実装されている TN3270E サーバー機能では、下記の RFC がサポートされています。

RFC 1576 - TN3270 Current Practices
RFC 1646 - TN3270 Extensions for LU names and Printers
RFC 1647 - TN3270 Enhancements

RFC 2355 - TN3270 Enhancements (これによって RFC 1647 は廃止される)

基本 TN3270 クライアントと TN3270E クライアントの両方を同時に処理できます。

ホスト接続

すでに説明したように、TN3270 クライアントから SNA ホストへのパスには、次の 2 つの部分があります。

- クライアントからサーバーへの IP を介する TCP 接続
- サーバーかホストへの SNA LU-LU セッション

サーバーからホストへの SNA 接続の形式は、サーバーが PU および従属 LU を表す方法によって異なります。ネットワーク・ユーティリティーを TN3270 サーバーとして使用している場合は、 2 つの異なる方法のどちらかを構成して、リンクを確立し、VTAM に対して PU および LU を表すことができます。

- SNA サブエリア・リンクの使用

  ネットワーク・ユーティリティーのセットアップをこの方法で行うのは、ホストで APPN が稼働していない場合です。すべての PU のそれぞれについて、別々の DLC レイヤー・リンクを構成します (最大 LU 数 253)。複数の PU には、複数のパラレル・ホスト・リンクが必要です。これらのリンクの 1 つでネットワーク・ユーティリティーに到着する SNA フレームは、対応する内部 PU に直接流れ込みます。

  サブエリア・ホスト・リンクは、SNA サブエリア境界機能を提供するプロダクトへの単一 DLC レイヤー・ホップである必要があります。一般的に、このプロダクトは、FEP 内で稼働する NCP とホスト内の VTAM 自体のどちらかです。ネットワーク・ユーティリティーからのサブエリア・リンクは、ブリッジやその他の DLC レイヤー転送機構 (例えば、プロトコル変換装置や外部 DLSw ルーターなど) を横断できます。ネットワーク・ユーティリティーでは、サブエリア・ホスト処理装置接続機構として次のリンク・タイプをサポートします。
  - トークンリング : 物理、ATM LAN エミュレーション、またはチャネル LSA
  - イーサネット : 物理、ATM LAN エミュレーション、またはチャネル LSA
  - FDDI : 物理のみ
  - フレーム・リレー PVC : ブリッジまたはルート RFC 1490/2427 フォーマット
  - DLSw
- APPN 従属 LU リクエスター (DLUR) リンクの使用

  ネットワーク・ユーティリティーのセットアップをこの方法で行うのは、ホストで APPN がその従属 LU サーバー (DLUS) 機能と共に稼働している場合です。たとえ複数のローカル PU を定義している場合でも、1 つの DLC レイヤー・リンクを構成して、DLUR-DLUS「パイプ」を伝達します。このリンクでネットワーク・ユーティリティーに到着する SNA フレームは、DLUR 機能に流れ、そこから正しい内部 PU に転送されます。

  DLUR を使用する場合は、ISR と HPR のどちらかのルーティングを使用して、APPN ネットワークを通るルートを選択して、ホストに到達することができます。ネットワーク・ユーティリティーでは、ホストへの「ファースト・ホップ」APPN リンクとして、次のリンク・タイプをサポートします。
  - トークンリング : 物理、ATM LAN エミュレーション、またはチャネル LSA
  - イーサネット : 物理、ATM LAN エミュレーション、またはチャネル LSA
  - FDDI : 物理のみ

– フレーム・リレー PVC : ブリッジまたはルート RFC 1490/2427 フォーマット
– ATM (ネイティブであり、LAN エミュレーションではない) : HPR のみ
– チャネル MPC+: HPR のみ
– PPP
– SDLC: ISR のみ
– X.25: ISR のみ
– DLSw: ISR のみ
– IP (エンタープライズ・エクステンダー) : HPR のみ

DLUR および HPR ルーティングを使用する場合は、ネットワーク・ユーティリティー TN3270E サーバーは、 SNA アプリケーション・ホストから IP ネットワークをまたがって配置することができるという点に、特に注意してください。エンタープライズ・エクステンダーによって、セッション・レベルのサービス・クラスおよび IP ネットワークをまたがる伝送優先順位が維持されます。

一般的な TN3270E サーバー構成

この節には、ネットワーク・ユーティリティー TN3270 サーバー・サポートの構成に関する一般的な情報が記載されています。具体的な構成例については、 151 ページを参照してください。

APPN プロトコルのもとでの TN3270 サブエリアの構成

ネットワーク・ユーティリティーに実装されている TN3270 サーバーでは、すべての SNA 機能が、 APPN プロトコル内に一括して組み込まれています。つまり、たとえ *SNA サブエリア接続機構を構成し、SNA ホストで APPN が稼働していない場合*でも、APPN プロトコルの構成サービスおよびコンソール・サービスを使用する必要があることを意味します。特に、次のことを行う必要があります。

- ポート、リンク、および TN3270 サーバー機能を構成する場合は、コマンド行および構成プログラムで APPN プロトコルを完了する。
- TN3270 監視コマンドを使用する場合は、コマンド行で APPN プロトコルを完了する。
- それでもノード・レベルで APPN を構成する。

SNA サブエリア・サポートを構成する場合も、実際上、ネットワーク・ユーティリティーが APPN ネットワーク・ノードとして機能することに変わりはありませんが、他の APPN ノードへのリンク上だけに限られます。構成する *唯一の* ポートおよびリンクが SNA ホスト接続機構用である場合は、APPN 機能は何の目的にもかないません。

APPN 環境での構成

APPN および TN3270 サーバーは、構成プログラムとコマンド行の両方で完全に構成可能です。構成プログラムからは、TN3270 構成パラメーターは常時使用可能です。TN3270 構成を作成して、ネットワーク・ユーティリティー・モデル TX1 にダウンロードした場合は、TN3270 サーバー機能をサポートしないモデルなので、ネットワーク・ユーティリティーでは、構成のうちで TN3270 部分を無視します。モデル TX1 に対してコマンド行から作業している場合は、 TN3270 を構成および監視するためのコマンドは、単に APPN メニューに表示されないだけのことです。

構成プログラムから APPN/TN3270 構成を変更する場合は、変更を行ったら、構成をネットワーク・ユーティリティーに転送し、リブートして変更を有効にします。

コマンド行から APPN/TN3270 構成を変更する場合は、talk 6 に移動し、そこで **p appn** と入力した上で、変更を行うためのコマンドを発行します。変更をアクティブにするには、次の 2 つのオプションが選択できます。

- 構成をディスクに書き込み、ネットワーク・ユーティリティーをリブートしてアクティブにする。
- talk 6 APPN **activate** コマンドを発行して、変更後の APPN/TN3270 構成を動的にアクティブにする。

  変更した構成項目に応じて、APPN によって変更が即時にアクティブになる場合と、 APPN (ネットワーク・ユーティリティー全体ではない) を再始動して、変更をアクティブにする場合とがあります。後の場合は、talk 5 に移動して、**p appn** と入力すると、APPN の再始動中、`APPN is not currently active` というメッセージが表示されます。talk 5 コマンドを用いてポーリングすれば、再始動の完了時を表示させて確認することができます。

暗黙および明示 LU 名とマッピング

ネットワーク・ユーティリティーの TN3270 サーバー機能を構成するときは、ネットワーク・ユーティリティーでサポートすることになり、競合する可能性があるクライアント・セッションの 1 つ 1 つに、ローカル LU 名を作成します。ネットワーク・ユーティリティー内で定義する LU 名が、VTAM 内での LU 名と何らかの関連をもつ必要はありません。

TN3270 クライアントが TCP を介してサーバーに接続すると、特定の LU 名を要求することもできるが、特定のタイプの任意の LU に対する総称要求を出すこともできます。 クライアントが特定の名前を要求するように構成している場合は、VTAM LU 名ではなく、サーバー (ネットワーク・ユーティリティー) で定義されているローカル名の 1 つを指定します。

単一のネットワーク・ユーティリティーで特性が類似した何千何万もの LU をサポートすることができるため、それぞれの LU を個別に構成する必要はありません。それよりもむしろ、*暗黙* LU の大きなプールを作成して、特定の LU 名を要求することがないクライアントに対処することができます。その上で、少数の *明示* LU を追加して、特定の名前を要求するクライアントに対処します[14]。

後で構成例を見れば分かるように、各ローカル PU を定義するごとに、それぞれ暗黙 LU をグループで定義します。 LU 名マスク、LU の数、LU が属するプールを指定します。明示 LU を構成する場合は、LU 名と NAU アドレス (2 〜 254) を指定します。 ネットワーク・ユーティリティーが構成をアクティブにするとき、明示 LU 用として NAU アドレスを予約した上で、グループ名マスクと使用可能な NAU アドレスの 1 つを使用して、暗黙 LU の名前を生成します。

14. 暗黙/明示の区別は、ネットワーク・ユーティリティー内だけのことです クライアントは暗黙 LU 名を要求することができ、その LU が使用可能であれば、ネットワーク・ユーティリティーはその要求に対処します。 重要な点は、クライアントが特に明示 LU 名を要求しない限り、サーバーがクライアントに明示 LU を割り当てることは決してないということです。

MAS V3.2 PTF01 では、次のように、LU 定義とクライアント・マッピングの分野で重要な機能強化を導入しています。

- LU の名前付きプールを定義できる。

  LU プーリングは、TN3270E サーバー機能の機能強化の 1 つで、一部の TN3270E ネットワークの構成を簡易化します。この機能を使用すると、SNA LU を名前付き『プール』のグループに分けることができます。そうすると、TN3270E クライアントでは、プールの名前を LU 名として使用して、接続を要求できます。そこで、TN3270E サーバーでは、指定されたプールから LU を選択して、クライアントの要求に対処します。

- クライアント IP アドレスと LU 名や LU プール名の間のマッピングを構成できる。

  TN3270E サーバーのクライアント IP アドレスと LU 名のマッピング機能によって、管理者が TN3270E サーバーの LU へのクライアント・アクセスを制御するためのメカニズムが得られます。

  マッピングによって、管理者は、クライアント構成を変更しなくても、クライアント IP アドレスやサブネットがマップされ、使用する SNA 資源 (LU またはプール) を構成できるので、中央管理が強化されます。

- サーバーがそれぞれの PU ごとに、従属 LU アドレスのリストを VTAM に送信して、VTAM でその独自の LU 定義を動的に作成できるようにすることができる。

  従属 LU の動的定義 (DDDLU) は、VTAM 機能の 1 つで、 VTAM による論理装置の認識が、関連 PU の大ノード起動時ではなく、 VTAM への論理装置の接続時に行われるようにすることができます。

  VTAM によってプロンプトが出されると、TN3270E サーバー機能が DDDLU を使用して、そのローカル LU を VTAM 内に作成します。サーバーは、ACTPU の受信時に LU 定義要求のすべてを送信するのではなく、LU が実際に定義を必要とするまで待ちます。LU 定義が行われるのは、TN3270 クライアントが接続され、VTAM に対して定義されていなかった LU を必要とするときです。

- TN3270 サーバー機能用として複数のローカル TCP ポートを構成できる。

  この機能強化によって、TN3270E サーバーが『listen』するための複数の TCP ポートを定義できます。このサポートを使用すると、クライアントでは、ポート番号を使用して必要な SNA 資源を指定できます。

- TN3270E 交渉を使用不可にできる。

  この機能強化では、基本 TN3270E サポートだけに従う場合とは異なり、追加されたポートが TN3270E サーバーになるために交渉するかどうか指定できます。この機能強化を必要とするのは、初期 TN3270 拡張交渉の受信の処理が適正に行われない一部の基本 TN3270 クライアントです。

上記の諸機能の構成について詳しくは、 MAS V3.2 以降の *MAS プロトコル構成と監視解説書 第 2 巻* を参照してください。

MAS V3.3 では、ホスト開始 DDLU を導入しています。

- ホスト開始 DDLU によって、VTAM に対してすでに定義されている LU の場合は、 TN3270E サーバーに対して冗長定義を行う必要はなくなります。TN3270E サーバーは、 LU のそれぞれを VTAM 上での起動時に動的に定義することになります。

構成例

ネットワーク・ユーティリティーは、TN3270E サーバーとしては、幾つかの構成で展開することができます。例えば、リモートにある支所に配置することも、データ・センターに配置することもできます。従来の SNA サブエリア接続を経由してホストに接続することもできるし、 APPN を使用することもできます。データ・センターでは、チャネル接続構成内に配置することもできるし、既存の IBM 3745/46 通信制御装置、2216-400、 3172 相互接続制御装置、OSA アダプター、または OEM ゲートウェイによって提供されるチャネル接続型接続を使用して、キャンパス LAN (または、 ATM クラウド）に常駐する独立型サーバーとして使用することもできます。

TN3270 インプリメンテーションの最も重要な要素の 1 つは、拡張容易性です。ネットワーク・ユーティリティー・ソリューションでは、高可用性および冗長度が得られるだけでなく、非常に大きい構成に規模を拡張することもできます。

以下の事例には、ネットワーク・ユーティリティーを TN3270E サーバーとして効果的に使用する方法が示されています。

NCP へのサブエリア接続を経由する TN3270

この事例 (152ページの図6 に図示されている) は、すべてのホスト・アクセスが IBM 3745/46 通信制御装置を通して、 IBM ネットワーク構成プログラム (NCP) によって行われる、従来の SNA サブエリア・ネットワークを示すものです。ネットワーク・ユーティリティーが設置されているのは、ローカル・キャンパスとリモート・サイトの両方にあるダウンストリーム・ワークステーションで、TN3270 サーバー・サポートが得られるようにするためです ネットワーク・ユーティリティーは、通常のサブエリア接続を経由して、FEP を通してホストに接続しています

最大 20 000 の TN3270 セッションが、 152ページの図6 に図示されているように設置された単一のネットワーク・ユーティリティーで処理できます。ネットワークの拡張に応じて、ネットワーク・ユーティリティーの追加による TN3270E サーバー容量の追加を行うだけで、ソリューションは容易に拡張することができます。また、別の IBM ルーターまたはネットワーク・ユーティリティーを設置して、ネットワーク・ディスパッチャーとして使用することによって、TN3270E 間に自動負荷平衡を設定することもできます (ネットワークの規模拡張方法の例については、156ページの『高度に拡張が容易な耐障害 TN3270E』を参照してください)。

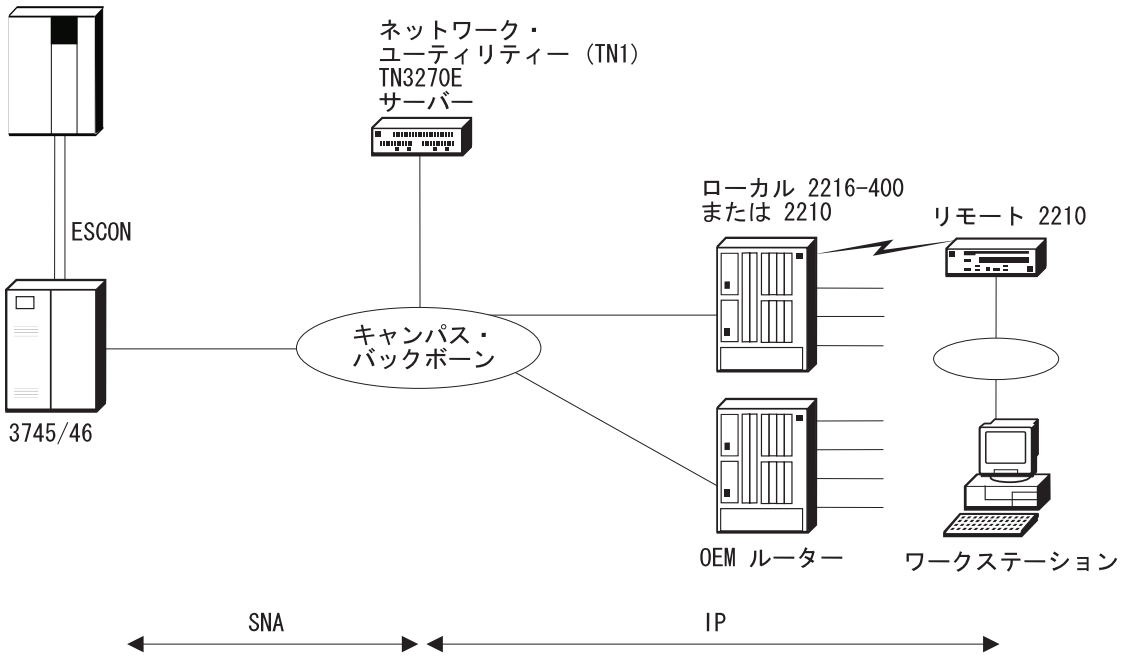


図 6. 37xx を介するサブエリア接続を経由する TN3270

構成のかぎ

TN3270E サーバー機能の構成は、この事例では非常に簡明です。ただし、以下の点には注意する必要があります。

- APPN と TN3270E サーバーのサブエリア・インプリメンテーションの両方があります。両方とも APPN サポートがネットワーク・ユーティリティーにインストールされることを必要とし、両方とも APPN 構成プロセス内で構成されます。このことは、たとえ純然たるサブエリア構成で APPN 機能を使用しない場合でも、該当します。これがインプリメンテーション・ステートメントであるのは、TN3270E サーバー機能で、 APPN SNA スタックがホストへのサブエリア接続と APPN 接続の両方に使用されるからです。

  また、APPN と TN3270E サーバー構成に関連する以下の追加事項についても注意してください。

  – APPN サポートは使用可能にされている必要がある。
  – ポートおよび 1 つまたは複数のリンク・ステーションを定義して、VTAM への接続を定義する必要がある。
  – サブエリア構成の場合は、リンク・ステーションを定義し、SSCP セッションの勧誘を指定すると、PU がネットワーク・ユーティリティー上に暗黙に定義される この PU で最大 253 のダウンストリーム LU をサポートします。253 を超える LU が必要な場合は、複数のリンク・ステーションを定義する必要があります。各リンク・ステーションでは、それぞれ異なるサービス・アクセス・ポイント (SAP) と異なるローカル・ノード ID (IDNUM) を使用する必要があります。
- TN3270E サーバーのパラメーターの構成にあたっては、サーバーの IP アドレスは、内部ボックス IP アドレスとインターフェース IP アドレスの 1 つのどちらに

設定しても構いません。TN3270 用として選択したアドレスは、通常の IP Telnet の使用によるボックスの管理には使用不能になる場合があることを、忘れないようにしてください。[15]

- ダウンストリーム LU は、明示と暗示のどちらとして定義することもできます。
  - 装置による同じ LU 名の常時使用を確保する必要がある場合は、明示定義を使用する (例えば、プリンターは通常明示定義を使用します)。
  - 装置のグループが大きく、使用可能 LU の共通プールを使用することができ、毎度同じ LU 名を使用する必要がない場合は、暗黙定義を使用する。

この事例で必要な構成パラメーターを詳しく検討したい場合は、 174ページの表17 をごらんください。

チャネル・ゲートウェイを介するサブエリア接続を経由する TN3270

この事例は、154ページの図7 に図示してあるように、前掲の事例と似ていますが、ここでは、ネットワーク・ユーティリティーが IBM 3172、IBM 2216、IBM 3746、マルチアクセス・エレクロージャー (MAE) 付き、または OEM 装置などの LAN チャネル・ゲートウェイを介して、ホストに接続する点が異なっています。これらのゲートウェイでは、外部通信アダプター (XCA) パススルーが使用され、通常は NCP で提供される SNA 境界機能は得られません。ゲートウェイでは、この機能は VTAM によって提供されます。

既存のゲートウェイに TN3270 サーバーが構成されている場合は、ネットワーク・ユーティリティーを使用して、既存の TN3270 作業負荷をオフロードし、ネットワーク要件の拡大に応じて追加の TN3270 容量を備えることができます。

既存の 2216 または 3746 があれば、TN3270E サーバー要件に応じて、ネットワーク・ユーティリティーの設置台数を増分的に増やしながら、ホストへの複数のチャネル接続を使用することができます。ネットワーク・ディスパッチャーの動的負荷平衡フィーチャーを使用して、効率を最適化することができます。

15. この同じアドレスで Telnet を使用する必要がある場合は、TN3270E サーバーが別のポート (例えば、24) を使用するように構成して、Telnet がポート番号 23 を使用できるようにすることができます。このためには、TN3270 クライアント・ワークステーションがこの同じポートを使用するように構成されることが必要です。

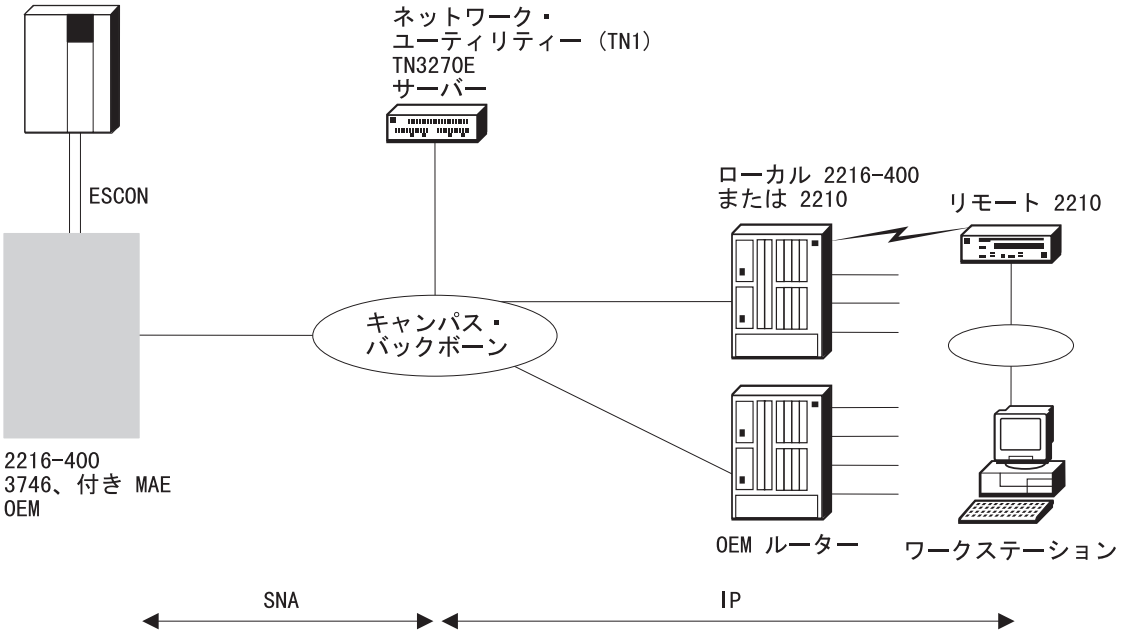


図 7. LAN ゲートウェイを介するサブエリア接続を経由する TN3270

構成のかぎ

ネットワーク・ユーティリティーの観点から展望すれば、この事例の構成は、前掲の事例の場合と同じです ホスト定義も同じです。両方の事例のいずれの場合も、TN3270E サーバー内の PU 用として交換回線大ノードを定義すればよいだけです。

OSA アダプターを介する TN3270

この事例は、155ページの図8 に図示してあります。ここでは、ネットワーク・ユーティリティーは、 S/390 開放型システム・アダプター (OSA) を介してホストに接続します。直前のゲートウェイ事例の場合と同様、SNA 境界機能はホスト内にあります。

TN3270 サーバー機能はホスト自体に常駐できますが、この機能を外部にある別のプラットフォームにオフロードしたいと考えるユーザーが多いようです。ネットワーク・ユーティリティーの場合は、ホスト接続の方式を変更しなくても、拡張容易性を備えた、費用効果性の高い TN3270E サーバー機能を提供できるので、この要件に適合します。したがって、既存の投資のてこ入れが可能です。

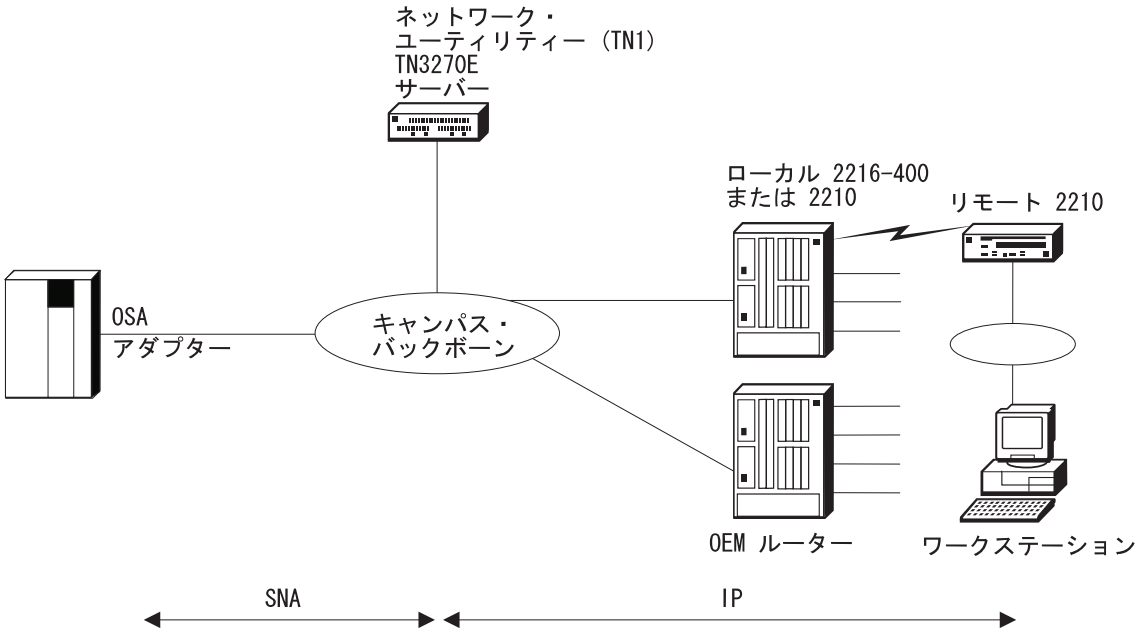


図 8. OSA アダプターを介する TN3270

構成のかぎ

ネットワーク・ユーティリティーの観点から展望すれば、この事例の構成は、前掲の 2 つの事例の場合と同じです

DLSw を介する TN3270 サブエリア SNA

DLSw 接続を介する TN3270E サブエリア SNA を使用すると、リモート・ノードやリモートの事業所で 2 台目のルーターが不要になります。この機能を使用しない場合は、156ページの図9 に示されているように、事業所内にルーターが 2 台ないと、IP を介して TN3270E サーバーを稼働させることはできません。 DLSw サブエリア上で TN3270E サーバー・サポートを使用すれば、 DLSw と TN3270E のサポートが単一のネットワーク・ユーティリティー内で組み合わされるので、ネットワーク・ユーティリティー・ボックスが 2 台ある必要はありません。

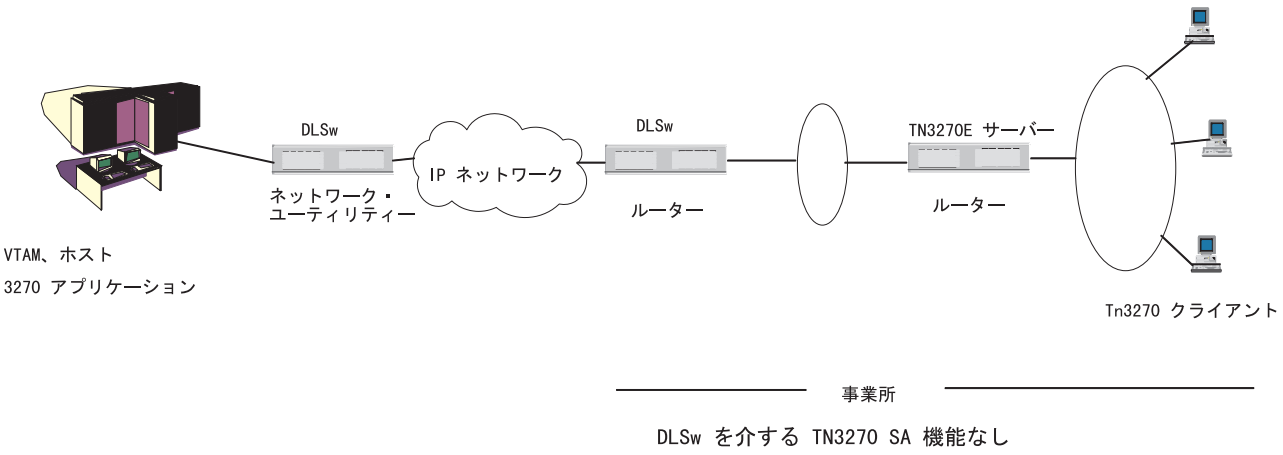


*図 9. ネットワーク・ユーティリティー上で DLSw を介する TN3270E サブエリア・サポートを **使用しない** 場合の一般的な事業所構成*

図10 に示されているように、TN3270E サーバーと DLSw が、複数 PU サブエリア機能を備えた単一のネットワーク・ユーティリティー内でサポートされます。この機能では、ネットワーク・ユーティリティー内に APPN/DLSw インターフェースがあります。このインターフェースを通して、リンク・ステーションが 58 台稼働できます。つまり、SNA PU タイプ 2 を 58 台稼働させることができます。新規の複数 PU サブエリア機能は、ローカル DLSw かリモート DLSw を介して稼働できます。ローカル DLSw では、LSA ESCON 接続、 X.25 QLLC、SDLC のリンクをサポートします。

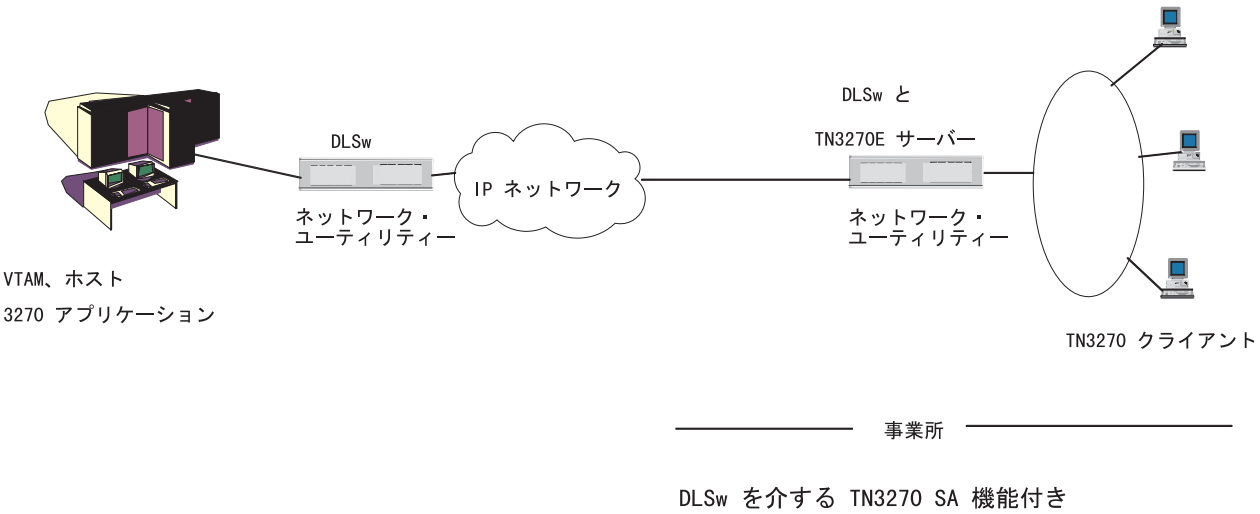


*図 10. ネットワーク・ユーティリティー上で DLSw を介する TN3270E サブエリア・サポートを **使用する** 場合の一般的な事業所構成*

高度に拡張が容易な耐障害 TN3270E

この事例は、157ページの図11 に図示してありますが、 151ページの『NCP へのサブエリア接続を経由する TN3270』で説明した事例の拡張の 1 つです。ここでは、複数のネットワーク・ユーティリティー装置によってソリューションの規模を拡大し

て、大規模な 3270 環境用の TN3270E サーバー・サポートを提供しています。また、別のネットワーク・ユーティリティーがネットワーク・ディスパッチャーとして構成され、負荷平衡に備えて展開されています[16]。新しいネットワーク・ディスパッチャー・アドバイザー TN3270 用を使用すれば、ネットワーク・ディスパッチャーでは、それぞれのネットワーク・ユーティリティー TN3270E サーバーから負荷統計をリアルタイムで収集することができるので、TN3270 間における負荷配分を可能な限り最適化することができます。

このソリューションには、TN3270E サーバーの 1 つに障害が生じた場合を考慮して、高可用性が備えられています。クライアント・セッションのディスパッチ先となるサーバーは、ユーザーからは透過的です。障害が起こった場合は、そのサーバーを通るセッションは失われますが、ユーザーは、TN3270E サーバーの同じ着信 IP アドレスを使用して、別のネットワーク・ユーティリティーを介してホストにログオンするだけです

ネットワーク・ディスパッチャー機能では、2 番目のネットワーク・ユーティリティーがネットワーク・ディスパッチャーとして構成され、1 次のバックアップとして使用される、冗長ハードウェアを使用することもできます

この構成では、追加の TN3270E サーバー容量を追加するだけで、TN3270E サポートの規模を任意のサイズまで拡張することができます。これは、ネットワーク要件の拡大に応じて、非介入的ではなく、増分的に行うことができます。

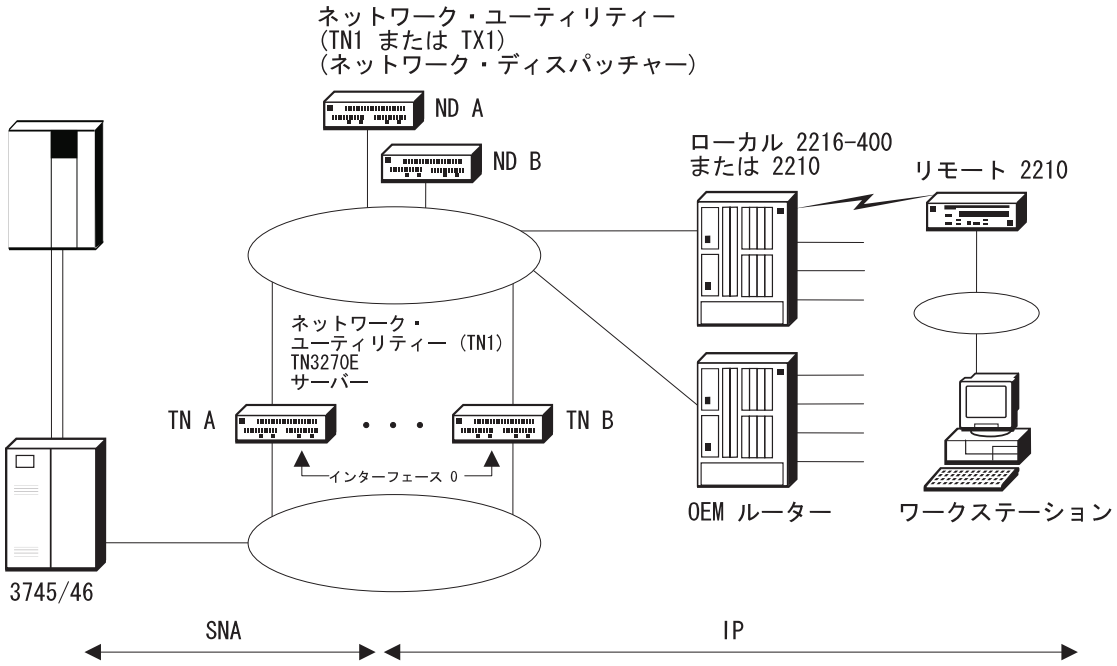


図 11. 高度に拡張が容易な耐障害 TN3270E

16. MAS V3.2 の時点では、ネットワーク・ディスパッチャー機能によって、同じネットワーク・ユーティリティー内で稼働する TN3270 サーバー機能へのクライアント・セッションをディスパッチすることもできます。

構成のかぎ

TN3270E サーバーに関する限り、ネットワーク・ディスパッチャーがあってもなくても、構成は同じです。事実、クライアントからのトラフィックが別のマシンを介してディスパッチされているかどうかは、TN3270E サーバーには分かりません。TN3270E サーバーに関する基本的な構成点については、 151ページの『NCP へのサブエリア接続を経由する TN3270』を参照してください。この事例の TN3270E サーバーに関する構成パラメーターの完全なセットについては、181ページの表18 を参照してください。

ただし、この構成では、高可用性を確保するために、IP アドレスの割り当てに特別の注意が必要です。151ページの『NCP へのサブエリア接続を経由する TN3270』では、TN3270E サーバーは、ルーター ID と同じアドレス (LAN インターフェースとも同じアドレス) で構成されています。ネットワーク・ディスパッチャー環境では、IP アドレスの割り当てはやや異なっています。

1 つのネットワーク・ディスパッチャーと 1 つまたは複数の TN3270E サーバーが、クラスターと呼ばれるものを形成します。IP アドレスは、このクラスターを対象として定義され、ワークステーションは、この IP アドレスに TN3270 パケットを送信します。ネットワーク・ディスパッチャーがこのようなパケットを受信し、処理のためにクラスター内のサーバーに転送します。

ネットワーク・ディスパッチャーがこのようなパケットのあて先 IP アドレスを変更することはないため、各 TN3270E サーバーも、それぞれこの同じ IP アドレスを用いて構成する必要があります。TN3270E サーバーが OSPF または RIP を経由して、このアドレスをネットワークに同報通信することがないようにする必要があります。これらのサーバーがクラスター・アドレスに応答しないようにしたいからです。クラスター・アドレスに応答するのは、ネットワーク・ディスパッチャーだけであることが必要です[17]。

ルーターには TN3270E サーバーの IP アドレスが分かっている必要があります。パケットをサーバー機能に転送するためです。このアドレスをルーターに分からせる方法の 1 は、これを 2 次アドレスとしてインターフェースに指定することです。図 12 には、157ページの図11 に図示されている可用性が高い耐障害 TN3270 構成に関する、このような IP アドレスの割り当て体系の例が示してあります。

17. クラスター・アドレスは、PING することはできません ネットワーク・ディスパッチャーは、クラスター・アドレスへの PING には応答しません。TCP および UDP パケットを処理するだけです。

```
TN3270E Server #1 (TNA):
    Internal address  172.128.252.3
    Interface 0       172.128.2.3      (2nd address: 172.128.1.100)
    Interface 1       172.128.1.3
    OSPF Router ID    172.128.1.3
    TN3270E Server    172.128.1.100    (same as cluster address)

TN3270E Server #2 (TNB):
    Internal address  172.128.252.4
    Interface 0       172.128.2.4      (2nd address: 172.128.1.100)
    Interface 1       172.128.1.4
    OSPF Router ID    172.128.1.4
    TN3270E Server    172.128.1.100    (same as cluster address)

Network Dispatcher #1 (NDA):
    Internal address  172.128.252.1
    Interface 0 addrs 172.128.1.1
    OSPF Router ID    172.128.1.1
    Cluster address   172.128.1.100
       Port 23
         Server 1     172.128.1.3
         Server 2     172.128.1.4

Network Dispatcher #2 (NDB):
    Internal address  172.128.252.2
    Interface 0 addrs 172.128.1.2
    OSPF Router ID    172.128.1.2
    Cluster address   172.128.1.100
       Port 23
         Server 1     172.128.1.3
         Server 2     172.128.1.4
```

図 12. 高度に拡張が容易な耐障害 TN3270 事例の IP アドレスの割り当て

クラスター・アドレスは、ネットワーク・ユーティリティー・マシンのインターフェース 0 に対して、2 番目のアドレスとして割り当てられていることに注意してください。この事例では、インターフェース 0 が接続している LAN セグメントでは、IP トラフィックはまったく伝達されることがなく、TN3270E サーバーからホストへの SNA サブエリア・トラフィックが伝達されるだけです。

ネットワーク・ディスパッチャーの構成は標準的です。この事例で必要な構成パラメーターの完全なセットについては、1 次ネットワーク・ディスパッチャーに関する186ページの表19 を参照してください。バックアップ・ネットワーク・ディスパッチャーの場合のこの構成との相違点については、190ページの表20 を参照してください。

APPN を介する DLUR 経由の TN3270

この事例は、160ページの図13 に図示してありますが、APPN を使用してホストとの通信を行います。ネットワーク・ユーティリティーが APPN 高性能ルーティング (HPR) を使用し、ホストとの高速トランスポート・プロトコル (RTP) セッションを確立します HPR は、TN3270E サーバーから VTAM まで全行程で使用されます。したがって、障害が発生した場合は、パラレル・ゲートウェイがあれば、代替パスへの非介入切り替えが確保されます。これが特に重要なのは、パラレル・シスプレックス環境の場合です。

さらに、HPR は、ネットワーク・ユーティリティーのエンタープライズ・エクステンダー・フィーチャーによって、IP 全般にわたってサポートされます。このことが重要

なのは、 TN3270E サーバーをリモート・ロケーションに配置し、IP を使用して、APPN トラフィックをデータ・センターにトランスポートして戻したい場合です。

チャネル・ゲートウェイは、ネットワーク・ユーティリティーとホストの間の RTP セッションのために、 APPN 自動ネットワーク・ルーティング (ANR) を実行する APPN ネットワーク・ノードです。

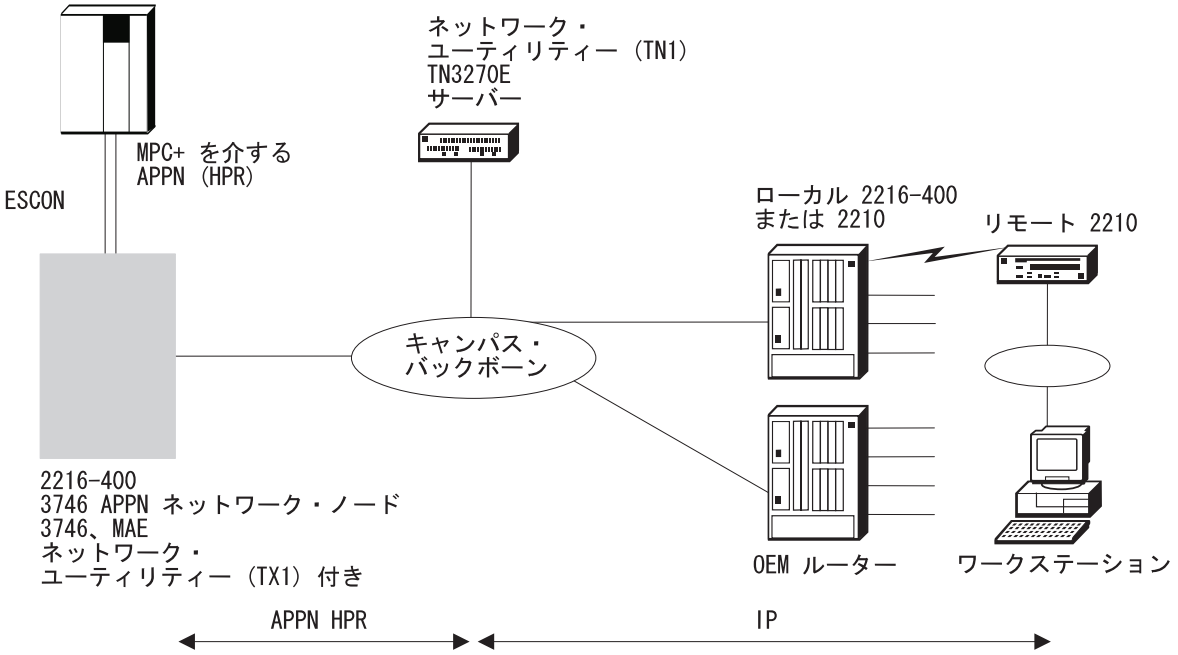


図 13. APPN を介する DLUR 経由の TN3270

APPN を介して TN3270E サーバーをホストに接続するときは、ネットワーク・ユーティリティー上に DLUR サポートを構成する必要があります。DLUR フィーチャーによって、従属 LU が含まれている T2.0 または T2.1 装置のサポートが APPN ノードに拡張されます。 APPN ネットワーク・ノード上の DLUR 機能は、 DLUS と共に動作します。 DLUS 機能は、混合 APPN/サブエリア・ネットワークのどの部分にも常駐できますが、通常は VTAM によって提供されます。

従属 LU フロー (SSCP-PU および SSCP-LU) は、DLUR APPN ノードと DLUS SSCP の間に確立された LU 6.2 パイプ (CP-SVR) 内でカプセル化されます。CP-SVR パイプは、DLUR と DLUS の間で新しい CPSVRMGR モードを使用する LU 6.2 セッションのペアで形成されます。このパイプによって SSCP 機能 (DLUS 内の) が DLUR APPN ノードにもたらされ、そこで従属 LU が入っている T2.0/T2.1 を接続する場合に、使用可能にすることができます。

構成のかぎ

ダウンストリーム・ワークステーションの観点から展望すれば、TN3270E サーバーは、アップリンク上のホストと通信する場合に、SNA サブエリアを使用しても、APPN を使用しても、同じに見えます。ネットワーク・ユーティリティーでは、TN3270 サーバー・パラメーターを構成する方法は、SNA サブエリア事例の場合と同じですが、

ローカル LU を構成する方法は異なっています。各 PU をそれぞれサブエリア・リンクに対応付けるのではなく、ローカル PU の構成は、リンク・アソシエーションを伴わずに行います。これらのローカル PU との間での DLUS-DLUR パイプ上のトラフィックのルーティングは、DLUR 機能が担当します。

APPN では、DLUR サポートがネットワーク・ユーティリティー内に構成されることを必要とします。DLUR は、非常に簡単に構成でき、必須パラメーターは DLUS の CP 名だけで、これは VTAM です。

APPN および DLUR サポートに関して、追加のホスト定義を幾つか行う必要があります。これらのコマンドの例については、295ページの『第18章 サンプル・ホスト定義』を参照してください。

この事例で必要な構成パラメーターを詳しく検討したい場合は、 193ページの表21 をごらんください。

分散 TN3270E サーバー

以上の構成では、データ・センター内でネットワーク・ユーティリティーをどのように展開すれば、ネットワーク内の TN3270E サーバー機能を集中することができるかを示してきました。この構成は、162ページの図14 に図示してありますが、ネットワーク・ユーティリティーをどのようにリモート・ロケーションにも配置すれば、分散 TN3270E サーバー機能が得られるかを示す、ほんの一例です。

この構成では、ネットワーク・ユーティリティーは、リモート・ロケーションのワークステーションに TN3270E サーバー・サービスを提供しています。TN3270 構成の場合は常にそうですが、ワークステーションは IP を使用して、TN3270E サーバーと通信します。 TN3270E サーバーは、データ・センター内のホストに戻る APPN 接続を介する DLUR を使用しています。

この例では、組織内 WAN は、IP トラフィックしか伝達しない公衆フレーム・リレー・ネットワークです。したがって、ネットワーク・ユーティリティーは、IP 専用 WAN による APPN HPR トラフィックの伝達ができるようにする、エンタープライズ・エクステンダー・フィーチャーを使用するように構成されています。

エンタープライズ・エクステンダー・トラフィックは、ホスト・ゲートウェイで終端し、ここで HPR トラフィックのカプセルを外した上で、ネットワーク・ノードを通して、APPN トラフィックをホストへの MPC+ パス上に送り出します。これは非常に高速で、低オーバーヘッドのパケット転送機能なので、単一のゲートウェイで大量のトラフィックを処理することができます。

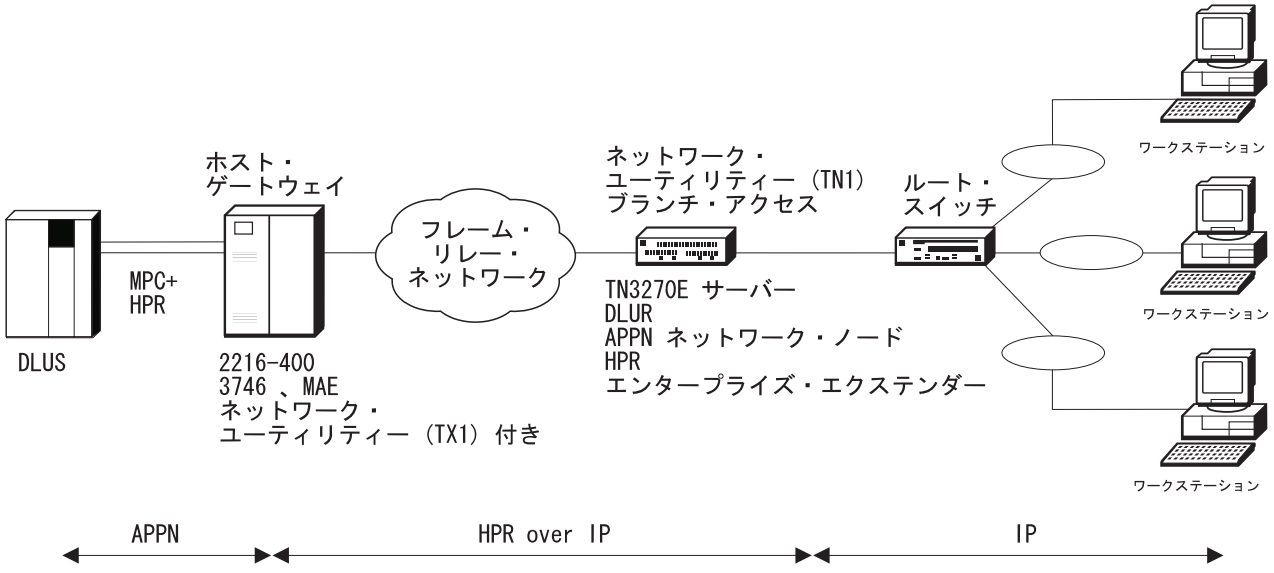


図 14. 分散 TN3270E サーバー

構成のかぎ

ダウンストリーム・ワークステーションの観点から展望すれば、ホストへのアップストリーム接続で SNA サブエリアと APPN のどちらを使用するかに関係なく、TN3270E サーバーは、リモートの事業所にあっても、データ・センターにあっても同じに見えます。したがって、ネットワーク・ユーティリティー内の TN3270E サーバー機能は、これまでに示した事例の場合とまったく同じ構成になっています。

APPN および DLUR は、フレーム・リレー IP リンクを介する APPN のポート定義の一点を除いて、構成が 159ページの『APPN を介する DLUR 経由の TN3270』の場合と同じです。 APPN が「HPR over IP」 (エンタープライズ・エクステンダー・フィーチャー) を使用するように構成するときは、ポート・タイプ IP を指定します。次に、このポート用のリンク・ステーションを追加するときは、 159ページの『APPN を介する DLUR 経由の TN3270』で行ったように隣接 FEP の MAC アドレスを指定するのではなく、「HPR over IP」ネットワークの他端 (この例では、ホスト・ゲートウェイ) の IP アドレスを指定します[18]。 IP ネットワークは、ホスト・ゲートウェイへのトラフィックを使用可能な最適のパスを通して送達します。 TN3270E サーバーとホストの間の接続に RTP セッションが使用されるため、信頼性の高いトランスポートが確保されます。

TN3270E サーバーの管理

ここでは、TN3270E サーバー機能の監視および管理ができる方法の一部を紹介します。

18. ホスト・ゲートウェイも、ここで説明されている方法とほぼ同じようにして、「HPR over IP」ポートを備える構成にする必要があります。

注: ここで説明する監視機能の場合は、 MAS V3.2 以降の命令コードの使用が前提になります。MAS V3.2 で、新しい TN3270 監視コマンドが幾つか、 TN3270E サブメニューとして導入されました。

コマンド行監視

コマンド行から現在稼働中の TN3270 サーバー状況を表示させて見る場合は、まず最初に talk 5 に移動して、**p appn** と入力します。`Protocol APPN is available but not configured` というメッセージが表示された場合は、基本 APPN 構成を完了し、ネットワーク・ユーティリティーをリブートして APPN を起動する必要があります。148ページの『APPN プロトコルのもとでの TN3270 サブエリアの構成』で説明されているように、たとえ TN3270 サブエリア接続しか使用していない場合でも、APPN はアクティブにする必要があります。

APPN 監視プロンプト `APPN >` が表示されたら、**tn** (「TN3270E」の短縮形) と入力すると、TN3270E サーバー状況を監視するためのサブメニューが表示されます。

これで以下のコマンドを監視プロンプト `TN3270E >` で使用することができます。

list status

システムの応答が *TN3270E is not configured or not active* であれば、現在アクティブの APPN 構成で TN3270 サーバー機能を十分に使用可能にしなかったことになります。このエラーが検出され、機能を構成しなかった場合は、選択した TN3270 サーバーの IP アドレスがインターフェース・アドレスとしても、内部 IP アドレスとしてもアクティブになっていないと思われます。それ以外に考えられる理由がないかどうか、『第13章 TN3270E サーバー構成例の詳細』の TN3270 構成の例を検討した上で、APPN/TN3270 構成を変更し、148ページの『APPN 環境での構成』の説明に従って、その構成をアクティブにします。

サーバー機能がアクティブである場合は、このコマンドによって次の情報が得られます。

- 現在使用中の構成情報

  TN3270E IP Address

  クライアントが接続するサーバーの IP アドレスですが、ネットワーク・ディスパッチャーを使用している場合は、クラスター・アドレスでもあります。

  NetDisp Advisor Port Number

  ネットワーク・ディスパッチャーが、負荷情報を検索する場合に接続できる TCP ポート

  Keepalive type

  クライアントがまだアクティブであるかどうか確認するために、サーバーがクライアントをポーリングするかどうか、およびする場合はその方法。表示される可能性のある値は、次のとおりです。

  None サーバーがクライアントをポーリングすることはなく、データの送信試行時になって、初めてクライアント不在を検出することになります。

NOP サーバーは TCP レベルでクライアントをポーリングし、クライアント・ソフトウェアには、応答できる機能の必要はありません。

Timing mark
サーバーは TN3270 レベルでクライアントをポーリングし、クライアント・ソフトウェアは特定の時間ウィンドウ内に応答する必要があります。

Automatic Logoff
アクティブでない (どちらの方向にもデータ・フローがない) 期間後に、サーバーがクライアントを切断するかどうか。

- 要約統計

Number of connections
TN3270 クライアントからのアクティブ TCP 接続の現行数

Number of available Logical Unit Application (LUA) LUs
VTAM から起動された LU か、動的 LU で、PU が VTAM から起動された LU の数

Number of defined LUs
TN3270E サーバーに対して定義されている LU の数

Number of LUA LUs pending termination
3270 から終了されたが、VTAM から完全には終結処理されていない LU の数

Number of connections in SSCP-LU state
対応する LU がこの状態 (ACTLU は受信したが、BIND はまだ受信されていない) にある、現在アクティブのクライアント TCP 接続の数

Number of connections in LU-LU state
対応する LU がこの状態 (BIND を受信し、完全にアクティブ) にある、現在アクティブのクライアント TCP 接続の数

list connections
このコマンドは、次のように修飾子を付けても付けなくても入力できます。

- **list connections**

  現在アクティブのクライアント接続 (TCP 接続がアクティブのクライアント接続) がすべて表示されます。

- **list connections** *client ip address*

  指定した IP アドレスが発信元で、現在アクティブの接続がすべて表示されます。

- **list connections** *resource name*

  指定した LU 名やプール名に対応付けられる、現在アクティブの接続がすべて表示されます。

list connection コマンドのそれぞれで、以下の情報がそれぞれのセッションごとに表示されます。

Local LU
ネットワーク・ユーティリティーで構成され、サーバー機能がこのクライアント TCP 接続をマップした LU 名

Class LU のタイプで、次のものがあります。

IW 暗黙ワークステーション

EW 明示ワークステーション
IP 暗黙プリンター
EP 明示プリンター

Assoc LU
ワークステーション LU の場合に、対応するプリンター LU があればその名前

Client Addr
クライアントの IP アドレス

Status
接続が SSCP-LU 状態と LU-LU 状態のどちらであるか。

Prim LU
VTAM に通知されている 1 次 LU 名

Sec LU
VTAM に通知されている 2 次 LU 名

Idle Min
この接続がユーザー・データを伝達してからの分数

list port
追加の TN3270 ポートと定義済みパラメーターが表示されます。

list mapping
すべての LU 名マップ項目が一覧表示されます。

list pools
すべての TN3270E 暗黙プールが一覧表示されます。

以上のリスト・コマンド以外にも、TN3270 サーバー・ユーザーは、機能が依存する他の APPN または SNA 資源の状況を照会することができる必要があります。次のような APPN 監視コマンドが、一般的に使用されます。

aping - リモート LU への接続性のテスト
li port - インターフェース状況の表示
li link - 論理リンクの状況の表示

ホスト接続に DLUR を使用している場合は、以下のコマンドが特に役立ちます。

li appc - DLUS-DLUR パイプの状況の検査
li local - TN3270 サーバー機能で使用される内部 PU の状況の表示
li dlur - DLUR PU の状況の表示

APPN 構成を検討する場合は、talk 6 にアクセスして、**list all** と入力します。

イベント・ログ・サポート

一般的に、APPN/TN3270 ELS メッセージには、IBM サポート要員のために、デバッグおよびトレース情報を取り込んでおく目的があります。これらの機能には、広範囲のログおよびトレース・サポートがありますが、ELS メッセージ自体には、下位レベル情報がしっかりパックされています。

通常は、IBM サポート要員の指示のもとで、APPN/TN3270 トレースおよびログを起動します。一般的な手順では、可能性のあるトレースの大きなリストの一部を、APPN 構成の一環として使用可能にします。構成プログラムからは、APPN ノード・サービス・フォルダーを表示させて見ます。talk 6 からは、**set trace** コマンドを使

用します。この構成変更をアクティブにすると、これらのトレースの出力が、APPN メモリーのトレース・テーブルに流れ込み、APPN ELS メッセージがアクティブになっていれば、ELS にも流れ込みます。トレースを起動する必要がある問題が検出された場合は、IBM サポートでは、デバッグ情報を取り込む指針となる詳細な手順を提供します。

SNA 管理サポート

APPN では、さまざまなエラー条件に対して SNA アラートを生成し、他の SNA 装置からのアラートを転送することができます。このサポートについては、 105ページの『SNA アラート・サポート』で説明しています。TN3270 サーバー機能に固有のアラートはありませんが、ネットワーク・ユーティリティー自体が生成するアラートが、TN3270 にかかわる SNA 資源に関連する場合があります。

VTAM または NetView/390 オペレーター・コンソールから、111ページの『NetView/390』で説明しているように、TN3270 にかかわるリンク、PU、および LU を制御することができます。

SNMP MIB およびトラップ・サポート

ネットワーク・ユーティリティーでは、やがて発表される TN3270 サーバー機能に関する下記の両標準 MIB のインターネット・ドラフト・バージョンをサポートします。

TN3270 Base MIB
TN3270 Response Time MIB

これらの MIB に対するネットワーク・ユーティリティー・サポートには、次のことができる機能が含まれます。

- サーバーの構成、状況、および統計の表示
- 応答時間収集のためのクライアント・グループのセットアップ
- VTAM 名からローカル名への LU 名とクライアント IP アドレスとのマッピングの表示
- クライアント IP アドレスと VTAM LU 名とのマッピングの表示
- 現行クライアント・グループに関する応答時間データの収集

さらに、ネットワーク・ユーティリティーでは、APPN および SNA 機能に関連する下記の IETF MIB をサポートします。

RFC 2155、APPN
RFC 2051、APPC
RFC 2232、DLUR
RFC 2238、HPR
RFC 1666、SNA NAU
インターネット・ドラフト、拡張ボーダー・ノード

ネットワーク・ユーティリティーでは、APPN に関連する下記の IBM エンタープライズ特定 MIB をサポートします。

APPN メモリー
APPN 料金計算
APPN HPR NCL
APPN HPR ルート・テスト

APPN 周辺アクセス・ノード (ブランチ・エクステンダー)

これらの MIB によって、ネットワーク・ユーティリティー内の APPN および SNA 資源 (TN3270 用として使用されるものも含む) の包括的なビューが得られます。

ネットワーク管理アプリケーション・サポート

107ページの『IBM Nways マネージャー・プロダクト』で説明されている Nways マネージャー・プロダクトには、 TN3270 応答時間監視に対する特殊化された統計サポート、ならびに TN3270 サーバー資源を表示できる機能が用意されています。応答時間監視を開始する場合は、IP アドレスおよびマスクを使用して、1 つまたは複数のクライアントからなるグループを選択します。定義したそれぞれのグループごとに、マネージャーが応答時間統計を事前定義時間バケット (1 秒未満、1 ～ 2 秒、その他) に収集します。収集された情報を使用して、グループ別に合計履歴応答期間を表示させて見たり、データを別のグラフィック形式で示すカスタム・レポートを作成したりすることができます。

TN3270 資源およびその状況を表示させて見る場合は、基本 TN3270 MIB 内のさまざまなテーブルからの情報を組み合わせた、特定のパネルを使用します。APPN および SNA 資源全般を表示させて見る場合は、APPN MIB からの情報にアクセスする、特定のパネルを使用します。また、内蔵ブラウザー・サポートを使用すれば、これらの MIB のいずれに入っている情報でも表示させて見ることができます。

Nways Manager for AIX では、ネットワークのトポロジーの APPN レベルのビューが得られます。参加 APPN 資源を検出し、それらを表示させ、それらの状況を色分けされたアイコンとして表示させることができます。APPN プロトコル・パフォーマンスおよびエラー・イベント (データとグラフ) も得られます。このアプリケーションでは、ブランチ・エクステンダーや拡張ボーダー・ノードのトポロジーは表示されません。

TN3270 サーバーの機能強化

従属 LU の動的定義

従属 LU の動的定義 (DDDLU) を使用すれば、VTAM と TN3270E の両方での LU の重複定義を避けることができます。DDDLU によって、LU の定義は 1 個所だけで、つまり、ネットワーク・ユーティリティーだけで行われるようにすることができます。 VTAM では、必要な LU の数に応じて、1 つまたは複数の PU を定義するだけで済みます。DDDLU を実装すれば、将来の LU 定義要件に備えた、VTAM 内での定義や保守の必要もなくなります。

TN3270E クライアントがルーター内に定義されている LU の 1 つを使用する接続を要求すると、ルーターは VTAM に Reply/PSID NMVT コマンドを送信します。このコマンドでは、LU のローカル・アドレスと装置タイプ情報 (3270) が、 SSCP-PU セッションを使用して VTAM に送信されます。そうすると、VTAM では、 PU 定義から、問題の LU に定義がないことを確認します。この時点で、VTAM は、パラメーター値に関する LUGROUP モデル・ステートメントと、LU に関する動的名前生成のための LUSEED 値を使用して、LU 定義を作成します。

特定の LU 名と特定のポート上に 3270 プリンターを必要とする LU も、同じ交換回線大ノードのもとで定義できます。次のサンプルを参照してください。

表 15. DDDPU のサンプル

```
DDDPU          VBUILD TYPE=SWNET
DDPU           PU  ADDR=02,      x
               IDBLK=077,          x
               IDNUM=22160,        x
                 PUTYPE=2,           x
                USSTAB=US327X,       x
                LUGROUP=GROUP1,      x
               LUSEED=DDLU###,         x
               DLOGMOD=D4C32XX3        x
SALE01       LU  LOCADDR=98,           x     1
                 DLOGMOD=D4C32XX3,       x
               LOGAPPL=CICSA
SALEPRT      LU   LOCADDR=99,           x      2
               LOGMODE=SAL3287,
               LOGAPPL=CICSA
```

1. このサンプル定義では、特定の要件のため、LU 'SALE01' が LOCADDR=98 にあることが要求されました。したがって、この特定の LU は、この要件を満たすために、この 'DDDPU' のもとで定義されます。
2. この定義では、プリンターも特定のポート上にある必要があります。一部のアプリケーション (例えば、CICS アプリケーション) の場合は、特にこうなります。販売部門用のアプリケーションは、LOGMODE=SAL3287 で、ポート 99 上にプリンターが必要であり、起動時にアプリケーション CICSA に接続される必要があります。

TN3270E サーバー内で LU (ローカル LU) に指定されている名前は、同じ LU に対して VTAM で生成された名前に一致する必要はありません。クライアントが、プールから任意の LU を単に選択するのではなく、特定の LU を必要とする場合は、TN3270E 内で指定されている LU 名を使用する必要があります。ただし、ホスト・アプリケーションでは、VTAM が動的に生成する LU 名を使用します。これらの 2 つの名前は、LU のローカル・アドレスを介して相互に結び付けられています。

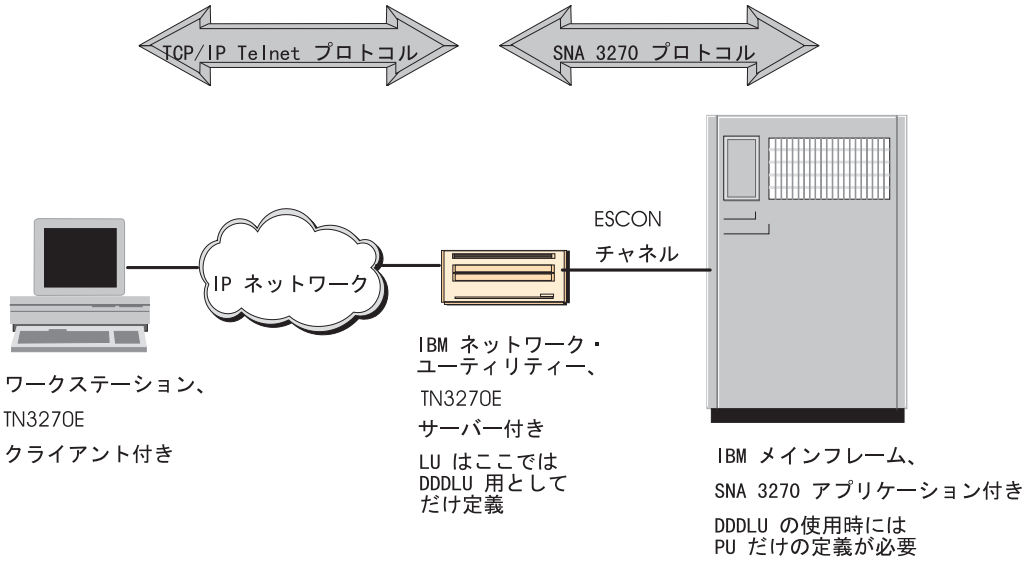


図 15. DDDLU を使用して、ESCON 接続ネットワーク・ユーティリティー上で稼働する TN3270E サーバー

LU の動的定義は、VTAM 出口ルーチン「従属 LU の定義の選択 (SDDLU)」で行われます。IBM 提供の SDDLU 出口プログラムを使用する場合は、 LUGROUP モデルの大ノードだけでなく、PU 定義内で名前構造用の LUSEED パラメーターを指定する必要があります。ユーザー独自の出口プログラムを使用する場合は、その慣用に従う必要があります。

この概念については、*VTAM Network Implementation Guide* (SC31-8372) の『Defining Dependent LUs Dynamically』と題する項に詳述されています。

LU は明示 (TN3270E にローカルで定義) で構いませんが、この場合は、クライアントは、ワークステーションで正確な LU 名を指定する必要があります。ユーザー (TN3270 クライアント) によって要求される LU は、暗黙の場合もあり、この場合は、LU のプールに属しています。

IP アドレスと LU 名のマッピングも、DDDLU の場合はサポートされます。さらに、IP アドレスと LU 名のマッピングに使用される別の PU のもとで、異なる方法で定義された明示 LU が、他にあっても構いません。

TN3270 ホスト開始動的 LU 定義

重複 LU 定義を避ける方法としては、DDDLU 以外にも、ホスト開始動的 LU (HIDLU) があります。HIDLU を使用すると、LU が VTAM だけで定義されるようにすることができます。ネットワーク・ユーティリティー (または、 2216) では、1 つまたは必要な数の PU を定義するだけで、これらの PU に関して LU は一切定義しません。

クライアントがそのような LU の使用を要求すると、TN3270E では、PU とその LU の起動要求を VTAM に送信します。VTAM 定義の LU が起動されると、制御ベクトル 0E 内の ACTLU コマンドで、LU 名がネットワーク・ユーティリティーに伝えられます。

この方法で定義された LU の場合は、VTAM とネットワーク・ユーティリティーの両方で同じ名前になります。

HIDLU を使用する場合は、VTAM での PU 定義内でパラメーター **INCLUD0E=YES** を使用する必要があります。この機能には、VTAM V4R4、APAR OW25501 と OW31805 付きが必要です。HIDLU では、表示端末が定義できるだけです。プリンターはサポートされません。HIDLU 定義は、他のローカル (ネットワーク・ユーティリティー内) 定義の LU (暗黙でも明示でも、DDDLU 定義の LU でも構いません) と同時に使用できます。

TN3270 ホスト・オンデマンド・クライアント・キャッシュ機能

ホスト・オンデマンド (HOD) を使用すると、Web ブラウザー・クライアントは、SNA 3270 と 5250 のホスト・アプリケーションに接続できます。端末エミュレーション (TN3270 や TN5250) は、クライアントのブラウザー内で、 Java アプレットとして稼働します。ホスト・アプリケーションへの接続は、 TN3270 (または、TN5250) サーバーを経由して行われます。

Java アプレットは、通常、Web サーバーとして稼働する HOD サーバーから検索されます。

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と、TN3270 サーバーとして稼働している IBM 2216 や 2212、またはネットワーク・ユーティリティーは、HOD アプレットをキャッシュに入れ、要求に応じてクライアントに提供できます。

HOD クライアント・キャッシュでは、HOD サーバーをオフロードでき、戦略的に配されれば、HOD ページとアプレットを一段と迅速にクライアント・ワークステーションにロードできます。HOD クライアント・キャッシュ機能を使用すると、それ以外にも、ネットワーク内の特定の回線/帯域幅に負荷を配分して、輻輳 (ふくそう) を取り除くことができるという利点が得られます。この機能は、 talk 6 と構成プログラムのどちらかを使用して、ネットワーク・ディスパッチャー機能を使用し、その機能のもとで定義されます。まず最初に、クラスター・アドレスがネットワーク・ディスパッチャーに対して定義され、次に、ポート番号 (複数の場合もある) と HOD サーバー・アドレスがそのクラスター・アドレスのもとで定義されます。

HOD クライアント・キャッシュの基本動作原理は、次のとおりです。クライアントは、HOD サーバーの実アドレスではなく、ND クラスター・アドレスをブラウザー内で使用します。HOD サーバーに対する要求がクラスター・アドレスであるポート 80 (HTTP ポート番号) に達すると、セッションの確立を必要とされる Java アプレットが HOD キャッシュから転送されます。アプレットやそれ以外の必要なページがネットワーク・ユーティリティーのキャッシュ内にない場合は、ルーターが HOD サーバーに接続し、それらの項目をダウンロードし、キャッシュ内に保管して、クライアントに提供します。これでページとアプレットがキャッシュ内に入ったので、次のユーザーからはヒットして、キャッシュから直接入手することになります。したがって、ネットワーク・ユーティリティーでこの HOD クライアント・キャッシュ機能を使用すると、ネットワーク・ユーティリティーに Java アプレットを分散することで、クライアントがこれらのアプレットを HOD サーバーからロードする必要がなくなり、ネットワークの使用率の改善に役立ちます。この機能を使用した場合は、Java アプレットに対する要求を送達するのは、ネットワーク・ユーティリティーであるため、HOD サーバーに対して余分な負荷が生じることもありません。

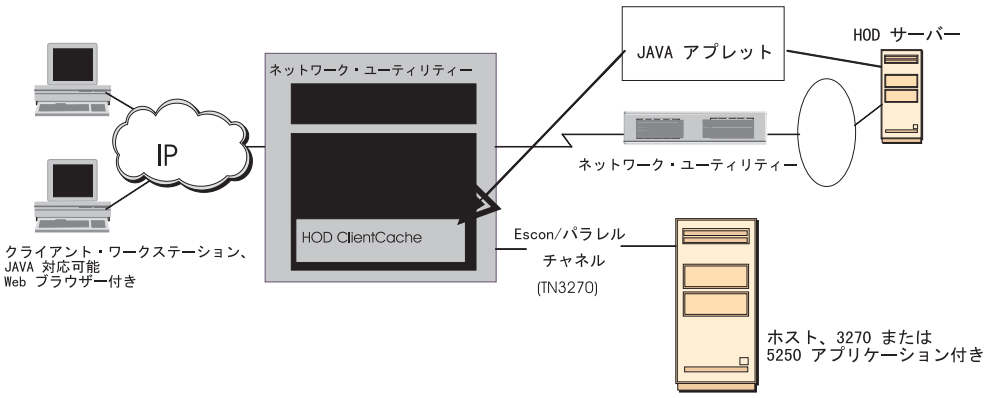


図 16. TN3270E サーバーと HOD キャッシュを使用する事例

HOD クライアント・キャッシュ機能が使用できるのは、TN3270E サーバー機能が使用されている場合だけです。

第13章 TN3270E サーバー構成例の詳細

この章には、145ページの『第12章 TN3270E サーバー』の TN3270E サーバー・ネットワーク構成の例の幾つかに関する図と構成パラメーター表が挙げてあります。パラメーター値は、実際の作業テスト構成での値が示してあります。

構成パラメーター表の欄および規則の説明については、 144ページの『構成例表の規則』を参照してください。

ネットワーク・ユーティリティー ワールド・ワイド・ウェブ (WWW) ページには、ここに挙げてある構成パラメーター表に一致する 2 進構成ファイルが収められています。これらのファイルにアクセスする場合は、下記のアドレスから Download リンクをたどってください。

```
http://www.networking.ibm.com/networkutility
```

この章に記載されている構成は、次のとおりです。

表 16. 構成例情報の相互参照

構成記述	パラメーター表
151ページの『NCP へのサブエリア接続を経由する TN3270』	174ページの表17
156ページの『高度に拡張が容易な耐障害 TN3270E』、TN3270 サーバー TN A の場合	181ページの表18
156ページの『高度に拡張が容易な耐障害 TN3270E』、ネットワーク・ディスパッチャー ND A の場合	186ページの表19
159ページの『APPN を介する DLUR 経由の TN3270』	193ページの表21
167ページの『従属 LU の動的定義』	197ページの『従属 LU の動的定義』
169ページの『TN3270 ホスト開始動的 LU 定義』	204ページの『ホスト開始動的 LU 定義』
170ページの『TN3270 ホスト・オンデマンド・クライアント・キャッシュ機能』	211ページの『TN3270E ホスト・オンデマンド (HOD) クライアント・キャッシュ』
155ページの『DLSw を介する TN3270 サブエリア SNA』	217ページの『DLSw を介する TN3270E サブエリア SNA』

LAN サブエリア経由、DLUR 経由、ネットワーク・ディスパッチャー使用の TN3270

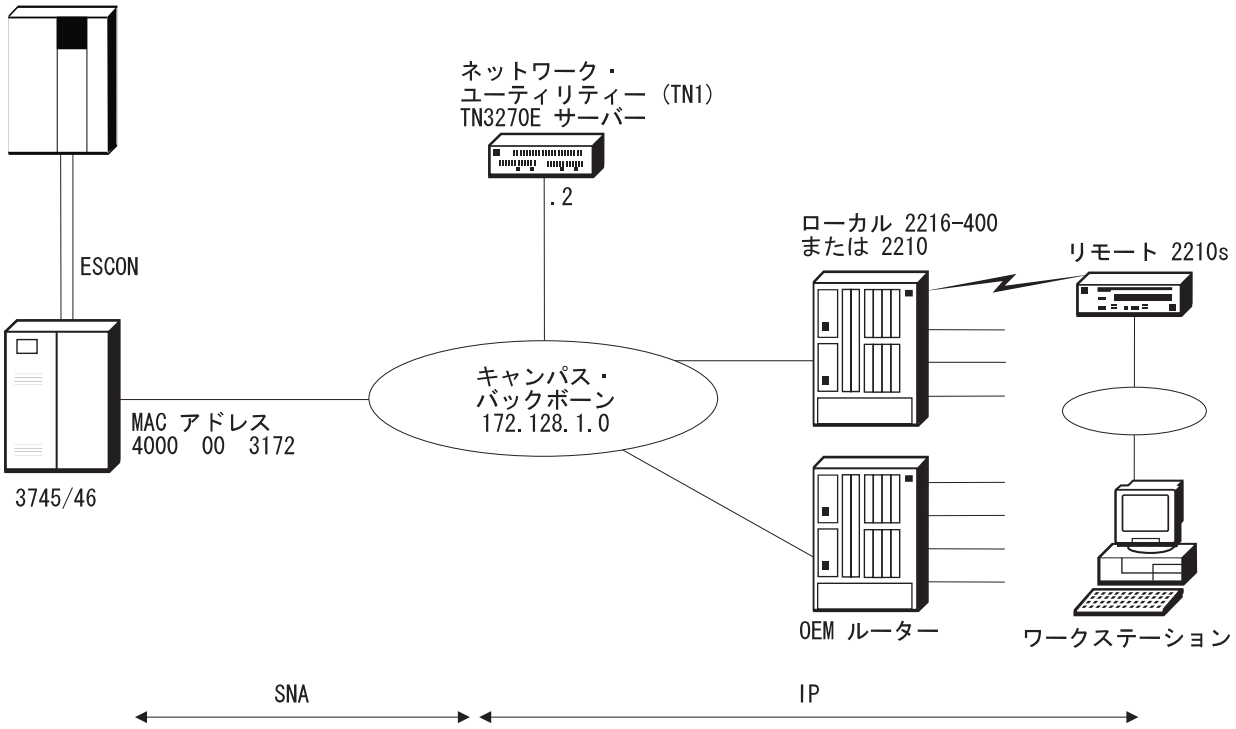


図 17. TN3270E サブエリア

表 17. TN3270E サブエリア. この構成の説明については 151 ページを、図については 174 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR	次の行の "add dev" を参照	1
装置 アダプター ポート	スロット 1/ポート 1: インターフェース 0: TR	Config>**add dev tok**	2
装置 インターフェース	インターフェース 0 MAC アドレス 400022AA0001	Config>**net 0** TKR Config>**set phy 40:00:22:AA:00:01**	

表 17. TN3270E サブエリア (続き). この構成の説明については 151 ページを、図については 174 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
システム 一般	システム名 : NU_A ロケーション : XYZ 連絡先 : 管理者	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	3
プロトコル IP 一般	内部アドレス : 172.128.252.2 ルーター ID: 172.128.1.2	Config>**p ip** IP Config>**set internal 172.128.252.2** IP Config>**set router-id 172.128.1.2**	
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.2 サブネット・マスク : 255.255.255.0	IP Config>**add address**	
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf** (他のデフォルトを受け入れる)	
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック)	OSPF Config> **set interface** Interface IP address: **172.128.1.2** Attaches to area: **0.0.0.0** (他のデフォルトを受け入れる)	

表 17. TN3270E サブエリア (続き). この構成の説明については 151 ページを、図については 174 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル APPN 一般	APPN ネットワーク・ノード (チェックして使用可能) ネットワーク ID: NUBNODE コントロール・ポイント名 : CPNU	Config>**p appn** APPN config> **set node** Enable APPN Network ID: **NUBNODE** Control point name: **CPNU** (他のデフォルトを受け入れる)	4
プロトコル APPN インターフェース	(インターフェース 0 トークンリングを強調表示) (構成タブをクリック) APPN ポートを定義 (チェックして使用可能) ポート名 : TR3270 高性能ルーティング (HPR) のサポート (チェックを消して使用不可) 複数 PU をサポート (チェックして使用可能)	APPN config>**add port** APPN Port Link Type: **TOKEN RING** Port name: **TR3270** Enable APPN Support multiple PUs High performance routing: **No** (他のデフォルトを受け入れる)	5

表 17. TN3270E サブエリア (続き). この構成の説明については 151 ページを、図については 174 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル APPN インターフェース	(インターフェース 0 トークンリングを強調表示) (リンク・ステーション・タブをクリック) STAT001 (新規定義) 一般 - 1 タブ : リンク・ステーション名 : STAT001 SSCP セッション要求 (チェック) リンク・サポート APPN 機能 (チェックを消す) 一般 - 2 タブ : 隣接ノードの MAC アドレス : 400000003172 ノード ID: 12244 ローカル SAP アドレス : 04 (**Add** をクリックして、リンク・ステーションを作成) STAT002 (新規定義) 一般 - 1 タブ : リンク・ステーション名 : STAT002 SSCP セッション要求 (チェック) リンク・サポート APPN 機能 (チェックを消す) 一般 - 2 タブ : 隣接ノードの MAC アドレス : 400000003172 ノード ID: 12245 ローカル SAP アドレス : 08 (**Add** をクリックして、リンク・ステーションを作成)	APPN config>**add link** Port name for the link station: **TR3270** Station name: **STAT001** MAC address of adjacent node:**400000003172** Solicit SSCP Session: **Yes** Local Node ID: **12244** Local SAP address: **4** Does link support APPN function?: **No** (他のデフォルトを受け入れる) APPN config>**add link** Port name for the link station: **TR3270** Station name: **STAT002** MAC address of adjacent node:**400000003172** Solicit SSCP Session: **Yes** Local Node ID: **12245** Local SAP address: **8** Does link support APPN function?: **No** (他のデフォルトを受け入れる)	6
プロトコル APPN TN3270E サーバー 一般	TN3270E (チェックして使用可能) IP アドレス : 172.128.1.2 自動ログオフ (チェックして使用可能)	APPN config>**tn** TN3270E config>**set** Enable TN3270E Server TN3270E Server IP Address: **172.128.1.2** Automatic logoff: **Yes** (他のデフォルトを受け入れる)	7

表 17. TN3270E サブエリア (続き). この構成の説明については 151 ページを、図については 174 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル APPN TN3270E サーバー LU	ローカル PU 名 : STAT001 (**Implicit Pool** をクリック) LU 名マスク : @LU1A 暗黙ワークステーション 定義の数 : 10 ローカル PU 名 : STAT002 (**Implicit Pool** をクリック) LU 名マスク : @LU2A 暗黙ワークステーション 定義の数 : 10 (**LUs** をクリックして、明示 LU を定義) LU 名 : PC03A NAU アドレス : 5 (**Add** をクリック)	TN3270E config>**add imp** Station Name: **STAT001** LU name mask: **@LU1A** Number of Implicit LUs in Pool: **10** TN3270E config>**add imp** Station Name: **STAT002** LU name mask: **@LU2A** Number of Implicit LUs in Pool: **10** TN3270E config>**add lu** Station Name: **STAT002** LU name: **PC03A** NAU address: **5**	8

表 17. TN3270E サブエリア (続き). この構成の説明については 151 ページを、図については 174 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注

注:

1. **add dev** で定義するのは、単一のポートであり、アダプターではありません。
2. 構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。 コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。
3. 書き込み対応可能 SNMP コミュニティーが必要なのは、構成ファイルを構成プログラムからルーターに直接ダウンロードしたい場合だけです。ルーターへの構成ファイルの TFTP を実行する場合は、SNMP は必要ありません。
4. 純然たる SNA サブエリア・ネットワークで、APPN が使用されていない場合は、ネットワーク ID はどんな値でも構いません。ネットワーク内で APPN が使用されている場合は、ネットワーク ID は APPN ネットワーク命名規則に適合する必要があります。
5. この例では、SNA サブエリアを使用して、ホストへの TN3270E サーバー接続が行われていますが、それでも APPN は使用可能にする必要があります。理由は、TN3270E サーバー・コードでは、ホストへの APPN 通信とサブエリア通信の両方に、 APPN SNA スタックを使用するからです。
6. リンク・ステーションを作成すると、PU も暗黙的に作成することになります。ここでは、このような PU に「ローカル・ノード ID」が割り当てられています。これは、VTAM の SW 大ノード定義内の「IDNUM」に一致する必要があります。ID ブロックは、ネットワーク・ユーティリティーでは常に 077 です。複数のリンク・ステーション (PU) を定義する必要がある場合は、各リンク・ステーションごとに、それぞれ異なるローカル SAP アドレスが必要です。

   `Solicit SSCP session` を `yes` に設定すると、リンクがサブエリア接続として定義されます。
7. MAS V3.2 以降、TN3270E サーバーには独自のコマンド行サブメニューがあります。
8. 暗黙 LU の場合は、プールを定義するだけで済みます。`@LU1A` は、プール内に実 LU 名を作成する場合に使用されるテンプレートです。この例では、プール内に LU が 10 あるので、生成される LU 名は、`@LU1A2`、 `@LU1A3`、`@LU1A4`、...、`@LU1A11` で、これは VTAM 内で定義されている PU の LOCADDR 2 〜 11 に対応します。同様に、`@LU2A` では、`@LU2A2`、`@LU2A3`、`@LU2A4` が生成されます。LU 名 `@LU2A5` が使用されないのは、NAU アドレス 5 は明示定義用として予約されているためです。したがって、プール内の残りの LU は、 `@LU2A6` 〜 `@LU2A12` になります。

   明示 LU の場合は、ここに示されている LU 名は、ワークステーションの 3270 エミュレーション構成で定義されている名前に一致する必要があります。 NAU アドレスでは、VTAM の交換回線大ノード内の該当する PU 定義内の LOCADDR を指します。

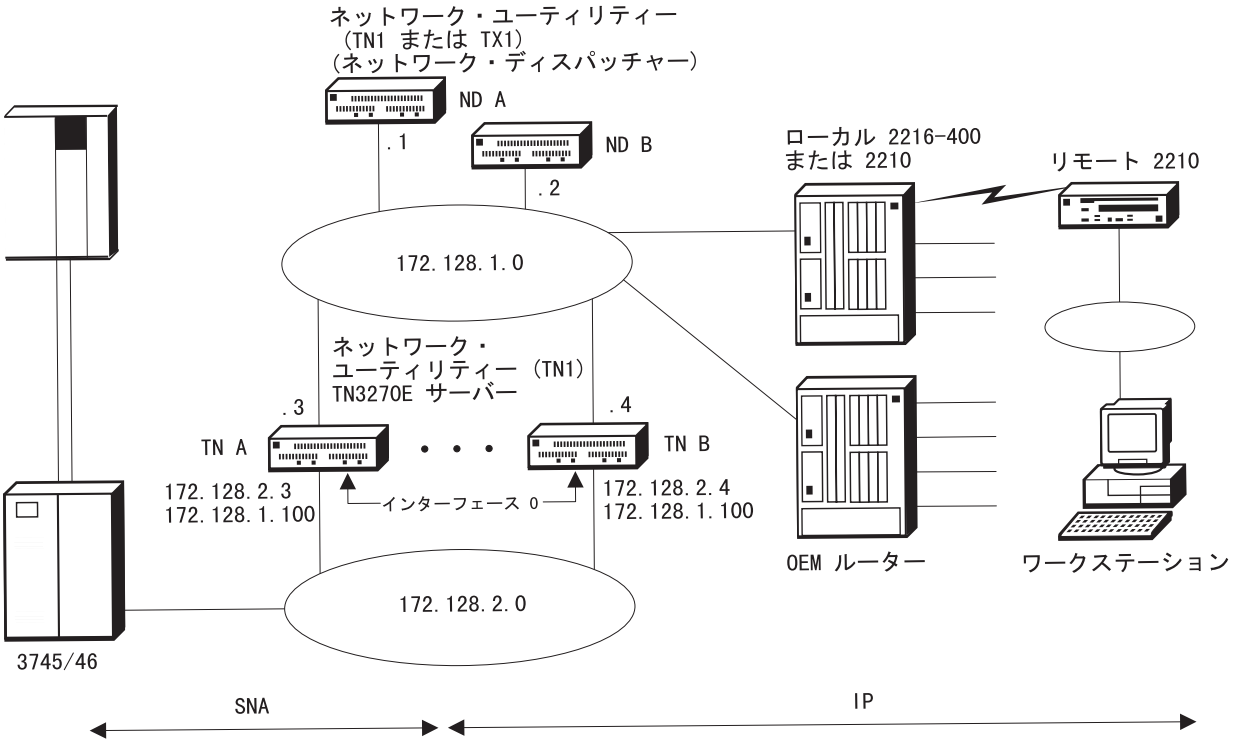


図 18. TN3270E サーバー構成 - 高度に拡張が容易な耐障害 TN3270

表 18. TN3270E サーバー構成 - 高度に拡張が容易な耐障害 TN3270. この構成の説明については 156 ページを、図については 180 ページを参照してください。
この表には、TN A サーバーの構成が示されています。*この例でのネットワーク・ディスパッチャーの構成については、 186ページの表19 および 190ページの表20 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR	次の行の "add dev" を参照	1
装置 アダプター ポート	スロット 1/ポート 1: インターフェース 0: TR スロット 1/ポート 2: インターフェース 1: TR	Config>**add dev tok** (それぞれのインターフェースごとに 1 回)	2
装置 インターフェース	インターフェース 0 MAC アドレス 400022AA0053 インターフェース 1 MAC アドレス 400022AA0003	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:53** TKR config>**exit** Config>**net 1** TKR config>**set phy 40:00:22:AA:00:03**	
システム 一般	システム名 : NU_A ロケーション : XYZ 連絡先 : 管理者	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	3
プロトコル IP 一般	内部アドレス : 172.128.252.3 ルーター ID: 172.128.1.3 同一サブネット (チェック)	Config>**p ip** IP config>**set internal 172.128.252.3** IP config>**set router-id 172.128.1.3** IP config>**enable same-subnet**	4
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.2.3 サブネット・マスク : 255.255.255.0 IP アドレス : 172.128.1.100 サブネット・マスク : 255.255.255.0 インターフェース 1 (TR スロット 1 ポート 2) IP アドレス : 172.128.1.3 サブネット・マスク : 255.255.255.0	IP config>**add address 0 172.128.2.3 255.255.255.0** IP config>**add address 0 172.128.1.100 255.255.255.0** IP config>**add address 1 172.128.1.3 255.255.255.0**	5、6

表 18. TN3270E サーバー構成 - 高度に拡張が容易な耐障害 TN3270 (続き). この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、TN A サーバーの構成が示されています。** *この例でのネットワーク・ディスパッチャーの構成については、 186ページの表19 および 190ページの表20 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf**	
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF インターフェース	インターフェース 1 OSPF (チェック)	OSPF Config> **set interface** Interface IP address: **172.128.1.3** Attaches to area: **0.0.0.0** (他のデフォルトを受け入れる)	7
プロトコル APPN 一般	APPN ネットワーク・ノード (チェックして使用可能) ネットワーク ID: NUBNODE コントロール・ポイント名 : CPNU	Config>**p appn** APPN config> **set node** Enable APPN Network ID: **NUBNODE** Control point name: **CPNU** (他のデフォルトを受け入れる)	8
プロトコル APPN インターフェース	(インターフェース 0 トークンリングを強調表示) (**構成**タブをクリック) APPN ポートを定義 (チェックして使用可能) ポート名 : TR3270 高性能ルーティング (HPR) のサポート (チェックを消して使用不可) 複数 PU をサポート (チェックして使用可能)	APPN config>**add port** APPN Port Link Type: **TOKEN RING** Port name: **TR3270** Enable APPN Support multiple PUs High performance routing: **No** (他のデフォルトを受け入れる)	9

表 18. TN3270E サーバー構成 - 高度に拡張が容易な耐障害 TN3270 (続き). この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、TN A サーバーの構成が示されています。** *この例でのネットワーク・ディスパッチャーの構成については、 186ページの表19 および 190ページの表20 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル APPN インターフェース	(インターフェース 0 トークンリングを強調表示) (**リンク・ステーション**タブをクリック) STAT001 (新規定義) 一般 - 1 タブ : リンク・ステーション名 : STAT001 SSCP セッション要求 (チェック) リンク・サポート APPN 機能 (チェックを消す) 一般 - 2 タブ : 隣接ノードの MAC アドレス : 400000003172 ノード ID: 12244 ローカル SAP アドレス : 04 (**Add** をクリックして、リンク・ステーションを作成) STAT002 (新規定義) 一般 - 1 タブ : リンク・ステーション名 : STAT002 SSCP セッション要求 (チェック) リンク・サポート APPN 機能 (チェックを消す) 一般 - 2 タブ : 隣接ノードの MAC アドレス : 400000003172 ノード ID: 12245 ローカル SAP アドレス : 08 (**Add** をクリックして、リンク・ステーションを作成)	APPN config>**add link** Port name for the link station: **TR3270** Station name: **STAT001** MAC address of adjacent node:**400000003172** Solicit SSCP Session: **Yes** Local Node ID: **12244** Local SAP address: **4** Does link support APPN function?: **No** (他のデフォルトを受け入れる) APPN config>**add link** Port name for the link station: **TR3270** Station name: **STAT002** MAC address of adjacent node:**400000003172** Solicit SSCP Session: **Yes** Local Node ID: **12245** Local SAP address: **8** Does link support APPN function?: **No** (他のデフォルトを受け入れる)	10
プロトコル APPN TN3270E サーバー 一般	TN3270E (チェックして使用可能) IP アドレス : 172.128.1.100 自動ログオフ (チェックして使用可能)	APPN config>**tn** TN3270E config>**set** Enable TN3270E Server TN3270E Server IP Address: **172.128.1.100** Automatic logoff: **Yes** (他のデフォルトを受け入れる)	11

表 18. TN3270E サーバー構成 - 高度に拡張が容易な耐障害 TN3270 (続き). この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、TN A サーバーの構成が示されています。** *この例でのネットワーク・ディスパッチャーの構成については、 186ページの表19 および 190ページの表20 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル APPN TN3270E サーバー LU	ローカル PU 名 : STAT001 (**Implicit Pool** をクリック) LU 名マスク : @LU1A 暗黙ワークステーション 定義の数 : 10 ローカル PU 名 : STAT002 (**Implicit Pool** をクリック) LU 名マスク : @LU2A 暗黙ワークステーション 定義の数 : 10	TN3270E config>**add imp** Station Name: **STAT001** LU name mask: **@LU1A** Number of Implicit LUs in Pool: **10** TN3270E config>**add imp** Station Name: **STAT002** LU name mask: **@LU2A** Number of Implicit LUs in Pool: **10**	12

表 18. TN3270E サーバー構成 - 高度に拡張が容易な耐障害 TN3270 (続き). この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、TN A サーバーの構成が示されています。** *この例でのネットワーク・ディスパッチャーの構成については、 186ページの表19 および 190ページの表20 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注

注:

1. **add dev** で定義するのは、単一のポートであり、アダプターではありません。
2. 構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。 コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。
3. 書き込み対応可能 SNMP コミュニティーが必要なのは、構成ファイルを構成プログラムからルーターに直接ダウンロードしたい場合だけです。ルーターへの構成ファイルの TFTP を実行する場合は、SNMP は必要ありません。
4. 「same-subnet function (同一サブネット機能)」を使用可能にする必要があるのは、同一サブネット内の IP アドレスをもつ 2 つのインターフェースを使用しているからです (172.128.1.3 が TR 1 に割り当てられ、172.128.1.100 (クラスター・アドレス) が 2 番目のアドレスとして TR 0 に割り当てられます)。
5. インターフェース 0 には、2 つの IP アドレスが割り当てられ、そのうちの 1 つは、ネットワーク・ディスパッチャーで使用されているクラスター・アドレスです。TN3270E サーバーが後続のステップで同一アドレスをもつ構成になります。TN3270 トラフィックはすべて、ネットワーク・ディスパッチャーを介してこのアドレスに送信されます。このトラフィックがネットワーク・ユーティリティーの内部 IP 待ち行列に到達するためには、このアドレスはインターフェース・アドレスと内部アドレスのどちらかに割り当てられる必要があります。この例では、インターフェースの 2 番目のアドレスとして、インターフェースに割り当てられています。
6. インターフェース 0 は、SNA ゲートウェイに接続されている、LAN セグメント上にあることに注意してください。このセグメントが LLC トラフィックを、 TN3270 サーバーからゲートウェイまで伝達します。ネットワーク・ユーティリティーの構成の残りによっては、このセグメントには IP トラフィックがない場合もあります。ただし、 TN3270E サーバーはすべて、このセグメント上のインターフェースに同じ IP アドレスが割り当てられることになるので、サブネット・アドレス (172.128.2) が割り当てられ、TN3270E サーバーはすべて、IP アドレスの競合を避けるため、このサブネット上にもアドレス (この場合は、172.128.2.3) があります。
7. 非常に重要なのは、ネットワーク・ディスパッチャーのクラスター・アドレス上で OSPF を使用可能に ***しない*** ことです。これを使用可能にすると、クラスター・アドレスが、TN3270E サーバー上にある (ネットワーク・ディスパッチャー・マシンに加えて) として、ネットワークに同報通信されることになります。
8. 純然たる SNA サブエリア・ネットワークで、APPN が使用されていない場合は、ネットワーク ID はどんな値でも構いません。ネットワーク内で APPN が使用されている場合は、ネットワーク ID は APPN ネットワーク命名規則に適合する必要があります。
9. この例では、SNA サブエリアを使用して、ホストへの TN3270E サーバー接続が行われていますが、それでも APPN は使用可能にする必要があります。理由は、 TN3270E サーバー・コードでは、ホストへの APPN 通信とサブエリア通信の両方に、 APPN SNA スタックを使用するからです。
10. リンク・ステーションを作成すると、PU も暗黙的に作成することになります。ここでは、このような PU に「ローカル・ノード ID」が割り当てられています。これは、VTAM の SW 大ノード定義内の「IDNUM」に一致する必要があります。ID ブロックは、ネットワーク・ユーティリティーでは常に 077 です。複数のリンク・ステーション (PU) を定義する必要がある場合は、各リンク・ステーションごとに、それぞれ異なるローカル SAP アドレスが必要です。
11. MAS V3.2 以降、TN3270E サーバーには独自のコマンド行サブメニューがあります。
12. 暗黙 LU の場合は、プールを定義するだけで済みます。`@LU1A` は、プール内に実 LU 名を作成する場合に使用されるテンプレートです。この例では、プール内に LU が 10 あるので、生成される LU 名は、`@LU1A2`、 `@LU1A3`、...、`@LU1A11` で、これは VTAM 内で定義されている PU の LOCADDR 2 ～ 11 に対応します。同様に、`@LU2A` では、`@LU2A2`、`@LU2A3`、...、`@LU2A11` が生成されます。

表 19. ネットワーク・ディスパッチャー構成 - 高度に拡張が容易な耐障害 TN3270. この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、1 次ネットワーク・ディスパッチャー ND A の構成が示されています。** *バックアップ・ネットワーク・ディスパッチャーの構成については、190ページの表20 を参照してください。 この例での TN3270E サーバーの構成については、174ページの表17 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR	See ″add device″ on next row	1
装置 アダプター ポート	スロット 1/ポート 1: インターフェース 0: TR	Config>**add dev tok**	2
装置 インターフェース	インターフェース 0 MAC アドレス : 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
システム 一般	システム名 : NU_A ロケーション : XYZ 連絡先 : 管理者	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	3
プロトコル IP 一般	内部アドレス : 172.128.252.1 ルーター ID: 172.128.1.1	Config>**p ip** IP config>**set internal 172.128.252.1** IP config>**set router-id 172.128.1.1**	4
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.1 サブネット・マスク : 255.255.255.0	IP config>**add address**	
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf**	

表 19. ネットワーク・ディスパッチャー構成 - 高度に拡張が容易な耐障害 TN3270 (続き). この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、1 次ネットワーク・ディスパッチャー ND A の構成が示されています。** *バックアップ・ネットワーク・ディスパッチャーの構成については、190ページの表20 を参照してください。 この例での TN3270E サーバーの構成については、174ページの表17 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック)	OSPF Config> **set interface** Interface IP address **172.128.1.1** Attaches to area **0.0.0.0** (他のデフォルトを受け入れる)	
フィーチャー ネットワーク・ディスパッチャー ルーター 実行プログラム	実行プログラム (チェック)	Config>**feat ndr** NDR Config>**enable executor**	
フィーチャー ネットワーク・ディスパッチャー ルーター クラスター 詳細	クラスター・アドレス : 172.128.1.100	NDR Config>**add cluster** Cluster Address: **172.128.1.100** (他のデフォルトを受け入れる)	
フィーチャー ネットワーク・ディスパッチャー ルーター クラスター ポート	ポート番号 23	NDR Config>**add port** Cluster Address **172.128.1.100** Port number **23** (他のデフォルトを受け入れる)	
フィーチャー ネットワーク・ディスパッチャー ルーター クラスター サーバー	サーバー・アドレス : 172.128.1.3 172.128.1.4	NDR Config>**add server** Cluster Address: **172.128.1.100** Port number: **23** Server Address: **172.128.1.3** (他のデフォルトを受け入れる) (172.128.1.4 について繰り返す)	

表 19. ネットワーク・ディスパッチャー構成 - 高度に拡張が容易な耐障害 TN3270 (続き). この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、1 次ネットワーク・ディスパッチャー ND A の構成が示されています。** *バックアップ・ネットワーク・ディスパッチャーの構成については、190ページの表20 を参照してください。 この例での TN3270E サーバーの構成については、174ページの表17 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
フィーチャー ネットワーク・ディスパッチャー ルーター マネージャー	マネージャー (チェック) 比率 アクティブ : 10 新規 : 10 アドバイザー : 80 システム : 0	NDR Config>**enable manager** NDR Config>**set manager propor** Active: **10** New: **10** Advisor: **80** System: **0** (他のデフォルトを受け入れる)	5
フィーチャー ネットワーク・ディスパッチャー ルーター アドバイザー	アドバイザー (チェック) アドバイザー名 : TN3270 アドバイザー・ポート : 23 タイムアウト : 10	NDR Config>**add advisor** Advisor name: **3** (for TN3270) Timeout: **10** (他のデフォルトを受け入れる) NDR Config>**enable advisor** Advisor name: **3** (for TN3270) Port number: **23**	6
フィーチャー ネットワーク・ディスパッチャー ルーター バックアップ	バックアップ (チェックして使用可能) バックアップの役割 : PRIMARY スイッチバック戦略 : MANUAL	NDR Config>**add backup** Role: **0**=PRIMARY Switch back strategy: **1**=MANUAL	7
フィーチャー ネットワーク・ディスパッチャー ルーター 到達	到達アドレス : (それぞれのアドレスを入力し、**Add** をクリック) 172.128.1.3 172.128.1.4	NDR Config>**add reach** Address to reach: **172.128.1.3** (172.128.1.4 について繰り返す)	8
フィーチャー ネットワーク・ディスパッチャー ルーター ハートビート	発信元アドレス : 172.128.1.1 着信先アドレス : 172.128.1.2 (アドレスを入力し、**Add** をクリック)	NDR Config>**add heartbeat** Source Heartbeat address: **172.128.1.1** Target Heartbeat Address: **172.128.1.2**	8

表 19. ネットワーク・ディスパッチャー構成 - 高度に拡張が容易な耐障害 TN3270 (続き). この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、1 次ネットワーク・ディスパッチャー ND A の構成が示されています。** *バックアップ・ネットワーク・ディスパッチャーの構成については、190ページの表20 を参照してください。 この例での TN3270E サーバーの構成については、174ページの表17 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注

注:

1. **add dev** で定義するのは、単一のポートであり、アダプターではありません。
2. 構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。 コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。
3. 書き込み対応可能 SNMP コミュニティーが必要なのは、構成ファイルを構成プログラムからルーターに直接ダウンロードしたい場合だけです。ルーターへの構成ファイルの TFTP を実行する場合は、SNMP は必要ありません。
4. アドバイザーおよびマネージャー機能がネットワーク・ディスパッチャーの実行プログラムと通信するためには、内部アドレスを設定する必要があります。
5. アクティブ、新規、アドバイザー、およびシステムの値は、加算して 100 になる必要があります。アドバイザーの比率は、デフォルトで 0 です。これを変更して、アドバイザー入力を使用して TN3270 トラフィックの負荷平衡を図ることができるようにする必要があります。この場合は、80 に設定して、アクティブおよび新規の接続の場合よりもはるかに大きい重みを与えてあります。
6. 通信ポート番号 (デフォルトで 10008) は、サーバーの「ネットワーク・ディスパッチャー・アドバイザー・ポート」に一致する必要があります。
7. スイッチバック戦略は、1 次とバックアップの両ネットワーク・ディスパッチャーで同一であることが必要です。IBM では、SNA セッションを中断させる確率が最も低くなる時点に、スイッチバックをスケジュールできるように、手動設定を推奨します。
8. 到達アドレスとは、ネットワーク・ディスパッチャーが、正しく機能していることを判別するために、到達できる必要があるアドレスです。 1 次では、この情報を規則的な間隔でバックアップに送信します。バックアップが、 1 次よりも到達可能性に優れていると判断した場合は、切り替えを実行して、 1 次の役割を引き継ぎます。ネットワーク・ディスパッチャーが使用するそれぞれのサブネットごとに、ホストを少なくとも 1 つ選択します。また、クラスター内のそれぞれのサーバーごとに、アドレスを追加します。この例では、ネットワーク・ディスパッチャーが使用するインターフェースは 1 つだけであり、サーバーは両方ともこのインターフェースと同じサブネット上にあります。
9. ここでは、1 次ネットワーク・ディスパッチャーが、バックアップ・ネットワーク・ディスパッチャーにハートビートを送信する場合に使用する、接続を構成します。1 次とバックアップの間に複数の接続がある場合は、パスを幾つか定義することができます。ハートビートは、最初に使用可能なパスを通って送信されます。最も堅固なソリューションは、それぞれのネットワーク・ユーティリティー内で使用可能な 2 番目のスロットを使用して、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・ディスパッチャーの間に、2 番目のパスを構成することです。

表 20. ネットワーク・ディスパッチャー構成 - 高度に拡張が容易な耐障害 TN3270. この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、1 次ネットワーク・ディスパッチャーの構成を示す 186ページの表19 を基にして、バックアップ・ネットワーク・ディスパッチャーの場合の構成の相違点が示してあります。** *この表に示されている相違点を除けば、バックアップ・ネットワーク・ディスパッチャーに関する定義は、1 次ネットワーク・ディスパッチャーの場合と同じです。 相違点は、インターフェース・アドレスおよびネットワーク・ディスパッチャーのバックアップ機能に対応しています。 ネットワーク・ディスパッチャーに関連するパラメーターで、ここに示されていないものについては、1 次の場合に構成した値と同じであることが必要です。 また、ハードウェア構成についても、1 次とバックアップの両ネットワーク・ディスパッチャーで同一にすることをお勧めします。 この例での TN3270E サーバーの構成については、181ページの表18 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 インターフェース	インターフェース 0 MAC アドレス 400022AA0002	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:02**	
システム 一般	システム名 : NU_ND2	Config>**set host**	
プロトコル IP 一般	内部アドレス : 172.128.252.2 ルーター ID: 172.128.1.2	Config>**p ip** IP config> **set internal 172.128.252.2** **set router-id 172.128.1.2**	1
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.2 サブネット・マスク : 255.255.255.0	Config>**p ip** IP config>**add address**	
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック)	Config>**p ospf** OSPF Config> **set interface** Interface IP address: **172.128.1.2** Attaches to area: **0.0.0.0** (他のデフォルトを受け入れる)	
フィーチャー ネットワーク・ディスパッチャー ルーター バックアップ	バックアップ (チェックして使用可能) バックアップの役割 : BACKUP スイッチバック戦略 : MANUAL	Config>**feat NDR** NDR Config>**add backup** Role: **1**=BACKUP Switch back strategy: **1**=MANUAL	
フィーチャー ネットワーク・ディスパッチャー ルーター ハートビート	発信元アドレス : 172.128.1.2 着信先アドレス : 172.128.1.1 (アドレスを入力し、**Add** をクリック)	NDR Config>**add heartbeat** Source Heartbeat address: **172.128.1.2** Target Heartbeat Address: **172.128.1.1**	2

表 20. ネットワーク・ディスパッチャー構成 - 高度に拡張が容易な耐障害 TN3270 (続き). この構成の説明については 156 ページを、図については 180 ページを参照してください。 **この表には、1 次ネットワーク・ディスパッチャーの構成を示す 186ページの表19 を基にして、バックアップ・ネットワーク・ディスパッチャーの場合の構成の相違点が示してあります。** *この表に示されている相違点を除けば、バックアップ・ネットワーク・ディスパッチャーに関する定義は、1 次ネットワーク・ディスパッチャーの場合と同じです。 相違点は、インターフェース・アドレスおよびネットワーク・ディスパッチャーのバックアップ機能に対応しています。 ネットワーク・ディスパッチャーに関連するパラメーターで、ここに示されていないものについては、1 次の場合に構成した値と同じであることが必要です。 また、ハードウェア構成についても、1 次とバックアップの両ネットワーク・ディスパッチャーで同一にすることをお勧めします。 この例での TN3270E サーバーの構成については、181ページの表18 を参照してください。*

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注

注:

1. アドバイザーおよびマネージャー機能がネットワーク・ディスパッチャーの実行プログラムと通信するためには、内部アドレスを設定する必要があります。
2. バックアップは、1 次ネットワーク・ディスパッチャーの場合とすべて同じ情報を用いて構成して、1 次が障害を起こした場合には、バックアップが 1 次の役割をすべて (1 次がオンラインに戻った時点での 1 次へのハートビートおよび到達可能性情報の送信も含めて) 引き継ぐことができるようにする必要があります。

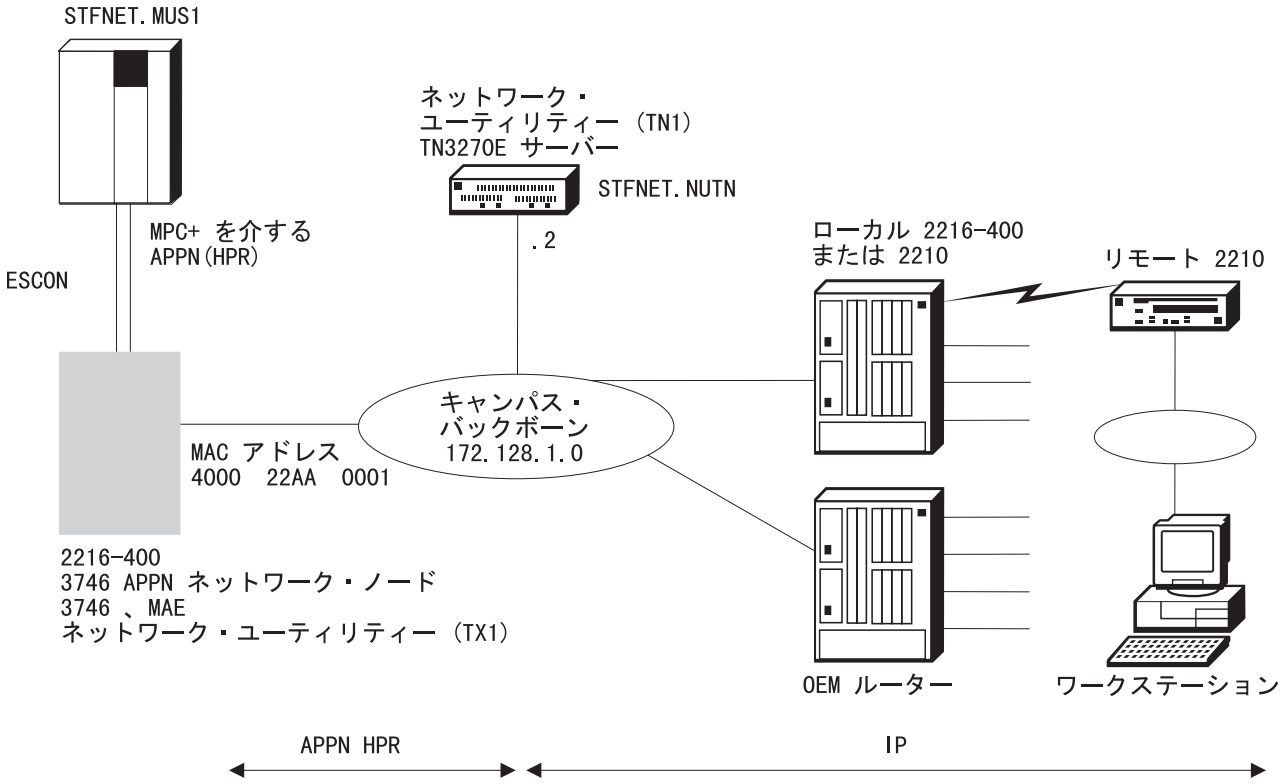


図 19. APPN を介する DLUR 経由の TN3270

表 21. APPN を介する DLUR 経由の TN3270. この構成の説明については 159 ページを、図については 192 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR	次の行の ″add dev″ を参照	1
装置 アダプター ポート	スロット 1/ポート 1: インターフェース 0: TR	Config>**add dev tok**	2
装置 インターフェース	インターフェース 0 MAC アドレス 400022AA0011	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:11**	
システム 一般	システム名 : NU_A ロケーション : XYZ 連絡先 : 管理者	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	3
プロトコル IP 一般	内部アドレス : 172.128.252.2 ルーター ID: 172.128.1.2	Config>**p ip** IP config>**set internal 172.128.252.2** IP config>**set router-id 172.128.1.2**	
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.2 サブネット・マスク : 255.255.255.0	IP config>**add address**	
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf**	

表 21. APPN を介する DLUR 経由の TN3270 (続き). この構成の説明については 159 ページを、図については 192 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック)	OSPF Config> **set interface** Interface IP address: **172.128.1.2** Attaches to area: **0.0.0.0** (他のデフォルトを受け入れる)	
プロトコル APPN 一般	APPN ネットワーク・ノード (チェックして使用可能) ネットワーク ID: STFNET コントロール・ポイント名 : NUTN	Config>**p appn** APPN config> **set node** Enable APPN Network ID: **STFNET** Control point name: **NUTN** (他のデフォルトを受け入れる)	
プロトコル APPN インターフェース	(インターフェース 0 トークンリングを強調表示) (構成タブをクリック) APPN ポートを定義 (チェックして使用可能) ポート名 : TR001	APPN config>**add port** APPN Port Link Type: **TOKEN RING** Port name: **TR001** Enable APPN (他のデフォルトを受け入れる)	4
プロトコル APPN インターフェース	(インターフェース 0 トークンリングを強調表示) (リンク・ステーション・タブをクリック) TRTG001 (新規定義) 一般 - 1 タブ : リンク・ステーション名 : TRTG001 一般 - 2 タブ : 隣接ノードの MAC アドレス : 400022AA0001 隣接ノード・タイプ : APPN ネットワーク・ノード (**Add** をクリックして、リンク・ステーションを作成)	APPN config>**add link** Port name for the link station: **TR001** Station name: **TRTG001** MAC address of adjacent node: **400022AA0001** (他のデフォルトを受け入れる)	5

表 21. APPN を介する DLUR 経由の TN3270 (続き). この構成の説明については 159 ページを、図については 192 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル APPN DLUR	DLUR (チェックして使用可能) 1 次 DLUS の 完全修飾 CP 名 : STFNET.MVS1	APPN config>**set dlur** Enable DLUR Fully-qualified CP name of primary DLUS: **STFNET.MVS1** (他のデフォルトを受け入れる)	6
プロトコル APPN TN3270E サーバー 一般	TN3270E (チェックして使用可能) IP アドレス : 172.128.1.2 自動ログオフ (チェックして使用可能)	APPN config>**tn** TN3270E config>**set** Enable TN3270E Server TN3270E Server IP Address: **172.128.1.2** Automatic logoff: **Yes** (他のデフォルトを受け入れる)	7
プロトコル APPN TN3270E サーバー ローカル PU	リンク・ステーション名 : PUPS08T ノード ID: 12244 リンク・ステーション名 : PUPS18T ノード ID: 12245	TN3270E config>**exit** APPN config>**add loc** Station Name: **PUPS08T** Local Node ID: **12244** (他のデフォルトを受け入れる) APPN config>**add loc** Station Name: **PUPS18T** Local Node ID: **12245** (他のデフォルトを受け入れる)	8
プロトコル APPN TN3270E サーバー LU	ローカル PU 名 : PUPS08T (**Implicit Pool** をクリック) LU 名マスク : @LU1A 暗黙ワークステーション 定義の数 : 5 ローカル PU 名 : PUPS18T (**Implicit Pool** をクリック) LU 名マスク : @LU2A 暗黙ワークステーション 定義の数 : 5	APPN config>**tn** TN3270E config>**add imp** Station Name: **PUPS08T** LU name mask: **@LU1A** Number of Implicit LUs in Pool: **5** TN3270E config>**add imp** Station Name: **PUPS18T** LU name mask: **@LU2A** Number of Implicit LUs in Pool: **5**	9

表 21. APPN を介する DLUR 経由の TN3270 (続き). この構成の説明については 159 ページを、図については 192 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注

注:

1.

add dev で定義するのは、単一のポートであり、アダプターではありません。

構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。 コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。

書き込み対応可能 SNMP コミュニティーが必要なのは、構成ファイルを構成プログラムからルーターに直接ダウンロードしたい場合だけです。 ルーターへの構成ファイルの TFTP を実行する場合は、SNMP は必要ありません。

APPN を使用するときは、高性能ルーティング (HPR) と中間セッション・ルーティング (ISR) のどちらでも使用できます。 デフォルトでは HPR で、この事例でもこれを使用しています。

指定されている MAC アドレスは、APPN ホスト・ゲートウェイの MAC アドレスです。

DLUS の CP 名はホスト VTAM です。

これらの PU 用として入力されたローカル・ノード ID は、ホスト VTAM の PU 定義内の IDNUM フィールドに一致する必要があります。

MAS V3.2 以降、TN3270E サーバーには独自のコマンド行サブメニューがあります。

暗黙 LU の場合は、プールを定義するだけで済みます。`@LU1A` は、プール内に実 LU 名を作成する場合に使用されるテンプレートです。 この例では、プール内に LU が 5 あるので、生成される LU 名は、`@LU1A2`、 `@LU1A3`、`@LU1A4`、`@LU1A5`、および `@LU1A6` で、これは VTAM 内で定義されている PU の LOCADDR 2 ～ 6 に対応します。 同様に、@LU2A では、`@LU2A2` ～ `@LU2A6` が生成されます。

従属 LU の動的定義

この事例では、VTAM V4R4 が稼働する MVS と、ホストに ESCON 接続された IBM 2216 が使用されました。ネットワーク・ユーティリティーは、2 ポートのトークンリング・アダプターがスロット 1 に、ESCON アダプターがスロット 2 に取り付けられていました。LSA ループバック・プロトコルが、ESCON チャネルを介する通信に使用されました。ネットワーク・ユーティリティーは、ネットワーク・ノードとして定義され、VTAM との通信に APPN/ISR を使用していました。TN3270E の PU と LU は、DLUR/DLUS を使用して VTAM に接続されていました。

DDDLU 機能のテストには、次の VTAM 定義が使用されました。

- X5303 -- LSA を使用する ESCON 接続に必要な XCA 大ノード
- SW5303N -- ネットワーク・ユーティリティー内の NN PU 用の VTAM 交換回線大ノード
- DDDPU -- LUGROUP を参照し、LUSEED パラメーターが指定された、 PU ステートメントだけが入っている動的定義 LU 用の VTAM 交換回線大ノード
- DDGROUP -- 3270 LU に関するモデル定義をもつ VTAM LUGROUP 大ノード

この事例での 2216 構成ファイルは DDD でした。

198ページの図20 に、この事例での VTAM と 2216 の両方で異なるパラメーターの関係が示してあります。

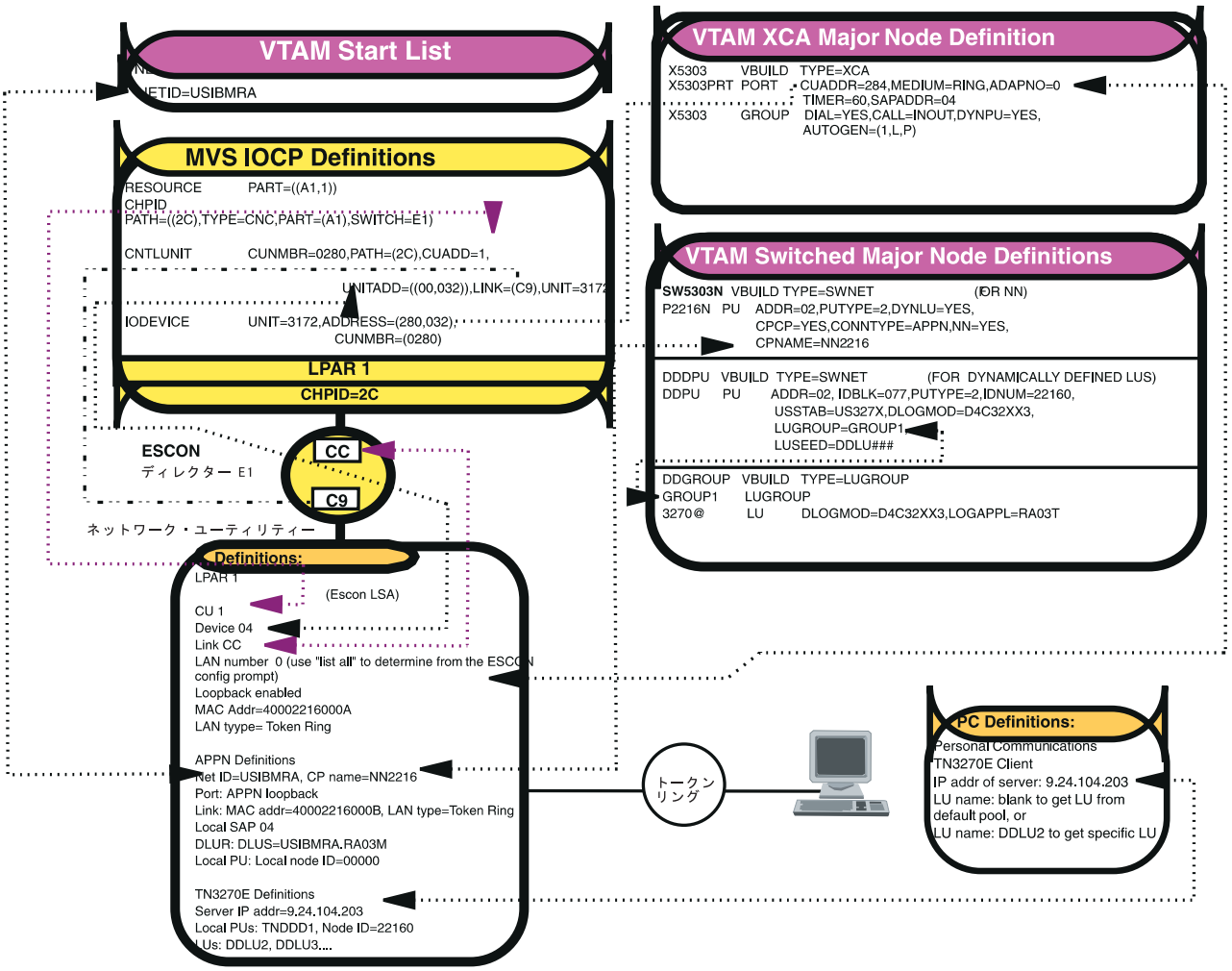


図 20. パラメーターの関係、ネットワーク・ユーティリティー/2216 TN3270E が稼働、DDDLU 使用と APPN/DLUR LSA ループバックを ESCON チャネルを介して使用

表22 に示してあるのは、使用された実際の VTAM XCA 大ノードのリストです。

表 22. ESCON チャネル接続用の XCA 大ノード X5303

```
*************************Top of Data ***********************
X5303    VBUILD TYPE=XCA
X5303    VBUILD TYPE=XCA
X5303PRT PORT  ADAPNO=0,
X5303PRT PORT  ADAPNO=0,                                     *
               CUADDR=284,                                   *
               SAPADDR=4,                                    *
               MEDIUM=RING
X5303GRP GROUP DIAL=YES,CALL=INOUT,DYNPU=YES,                *
               AUTOGEN=(1,L,P)
*********************** Bottom of Data ********************
```

199ページの表23 には、2216 内のネットワーク・ノード用の実際の VTAM SW5303N 交換回線大ノードが記載してあります。

表 23. 2216 ネットワーク・ノード用の交換回線大ノード SW5303N

```
***************************** Top of Data ******************************
SW5303N  VBUILD TYPE=SWNET
P2216N   PU    ADDR=02,          X
               PUTYPE=2,                                            X
               CPCP=YES,         X
               CONNTYPE=APPN,    X
               USSTAB=US327X,                                       X
               NN=YES,           X
               DYNLU=YES,        X
               CPNAME=NN2216
***************************** Bottom of Data ***************************
```

APPN コントロール・ポイント PU (例えば、表23 に示されているネットワーク・ノードなど) の場合は、ID Block 番号も ID NUm 番号も必要ありません。ネットワーク・ノードは、完全修飾ネットワーク名によって相互に認識できます。

表 24. LUGROUP 大ノード DDGROUP、LU 定義のモデル

```
***************************** Top of Data ******************************
DDGROUP  VBUILD TYPE=LUGROUP
GROUP1   LUGROUP
3270@    LU    DLOGMOD=D4C32XX3,LOGAPPL=RA03T       1
***************************** Bottom of Data ***************************
```

1. 3270@ という名前で装置タイプ 3270 を指定します。最後の文字として @ を使用することによって、製品 3270 のどの型式番号にも該当することを指定します。LU ステートメント・パラメーターは、 DLOGMOD と LOAGAPPL だけしか示されていません。ただし、追加の LU パラメーターが必要であれば指定して構いません。

表 25. 動的定義 LU 用の交換回線大ノード DDDPU

```
***************************** Top of Data ******************************
DDDPU    VBUILD TYPE=SWNET
DDPU     PU    ADDR=02,                                             X
               IDBLK=077,      1                                    X
               IDNUM=22160,                                         X
               PUTYPE=2,                                            X
               USSTAB=US327X,                                       X
               LUGROUP=GROUP1,    2                                 X
               LUSEED=DDLU###,    3                                 X
               DLOGMOD=D4C32XX3
***************************** Bottom of Data ***************************
```

1. IBM ネットワーク・ユーティリティーでは、IDBLK 値として 077 を使用します。
2. このパラメーターでは、LUGROUP 大ノード内の名前が GROUP1 の LUGROUP ステートメントを指します。 表24 を参照してください。
3. この LUSEED 値によって、動的に作成された LU は、DDLU で始まり、その後に 3 桁の 10 進数の形式で表される LU ローカル・アドレスが続く名前になります。

表 26. MAS 3.3 構成プログラムを使用して行われた DDD 構成 (2 の 1)

構成プログラム・ナビゲーション	構成プログラム値
装置 スロット	スロット 1: 2 ポート TR スロット 2: ESCON

表 26. MAS 3.3 構成プログラムを使用して行われた DDD 構成 (2 の 1) (続き)

構成プログラム・ナビゲーション	構成プログラム値
装置 チャネル・アダプター ESCON インターフェース ESCON インターフェース	プロトコル・タイプ : LSA LAN タイプ : トークンリング MAC アドレス (LSA バーチャル LAN の場合は、VTAM 側) : 例えば、40002216000A **Loopback** をクリック **Add** をクリック
装置 チャネル・アダプター ESCON インターフェース ESCON サブチャネル	装置アドレス : 4 サブチャネル・タイプ : 読み取り/書き込み LPAR: 1 リンク・アドレス : CC CU: 1 **Add** をクリック
装置 チャネル・アダプター APPN ループバック・ネット	LAN タイプ : トークンリング MAC アドレス : 40002216000B **Add** をクリック
システム 一般	システム名 : DDD ロケーション : 機械室 連絡先 : ユーザーの名前
システム ユーザー	名前 : ユーザー ID 許可 : 管理者 パスワード : パスワード 繰り返しパスワード : パスワード **Add** をクリック
システム SNMP Config (構成) コミュニティー 一般	名前 : 公衆 アクセス・タイプ : 読み取り/書き込みトラップ **Add** をクリック
プロトコル IP 詳細	内部アドレス : 9.24.104.203
プロトコル IP インターフェース	インターフェース 1 (TR スロット 1 ポート 2) IP アドレス : 9.24.106.9 サブネット・マスク : 255.255.255.0 **Add** をクリック IP アドレス : 9.24.104.203 サブネット・マスク : 255.255.255.0 **Add** をクリック
プロトコル APPN 一般	**APPN network node** をクリック ネットワーク ID : USIBMRA コントロール・ポイント名 : NN2216
プロトコル APPN DLUR	**DLUR** をクリック 1 次 DLUS の完全修飾名 : USIBMRA.RA03M

表 27. MAS 3.3 構成プログラムを使用して行われた DDD 構成 (2 の 2)

構成プログラム・ナビゲーション	構成プログラム値
プロトコル APPN インターフェース	回線項目 **APPN Net--Token Ring** を クリック 見出し **Configure** をクリック (タブ General を選択) **Define APPN Port** をクリック **Service Any Node** をクリック ***off* High Performance Routing (HPR)** をクリック サポート **Support Multiple PUs** をクリック タブ **Port Definition** を選択 ローカル SAP アドレス指定 : 04
プロトコル TN3270E サーバー 一般	**TN3270E** を クリック IP アドレス : 9.24.104.203
プロトコル TN3270E サーバー ローカル PU	リンク・ステーション名 : TNDDD1 ノード ID : 22160 1 次 DLUS: USIBMRA.RA03M **Add** をクリック
プロトコル TN3270E サーバー LU	**TNDDD1** を選択 見出し **LUs** をクリック LU 名 : DDLU2 クラス : 暗黙 NAU アドレス : 2 **Add** をクリック LU 名、クラス、NAU アドレスを繰り返す 各 LU ごとにシーケンスを追加

構成の監視

ネットワーク・ユーティリティーでは、一般的に **talk 5/appn/tn3270e** のもとで、使用中の接続、プール、マッピング、その他の状況を監視できます。

LU、PU、プールなど、すべてのローカル定義資源を表示させる場合は、**talk 6/appn/tn3270e** が使用できます。TN3270E の構成については、 202ページの表28 をごらんください。

表 28. talk 6/p app/tn3270e のもとでの TN3270E の構成の表示

```
DDD TN3270E config>LIST ALL
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 9.24.104.203
TN3270E Port Number: 23
Default Pool Name: PUBLIC
NetDisp Advisor Port Number: 10008
Client IP Address Mapping: N
Keepalive type: NONE
Automatic Logoff: N    Timeout: 30
        Enable IP Precedence: N

DLUS Link Station: TNDDD1
        Fully-qualified CP name of primary DLUS: USIBMRA.RA03M
        Fully-qualified CP name of backup DLUS:
        Local Node ID: 22160
        Auto activate : YES
        Host Initiated Dynamic LU Definition: NO
        LU Name   NAU addr     Class             Assoc LU Name   Assoc NAU
addr
        ------------------------------------------------------------------------
        DDLU2        2     Implicit Workstation
        DDLU3        3     Implicit Workstation
        DDLU4        4     Implicit Workstation
--More--
        DDLU5        5     Implicit Workstation
        DDLU6        6     Explicit Workstation
        DDLU7        7     Explicit Workstation


Client IP Address mapping
-------------------------
Client IP Address              Address Mask      Resource Name
-----------------------------------------------------


Multiple Port
-----------------------------
Port Number    Enable TN3270E    Resource Name
-----------------------------------------------
DDD TN3270E config>
```

203ページの表29 に示されているコマンドでは、まず最初に **talk 5/appn/tn3270e** が表示されます。

次に、list status によって、TN3270E 資源の最新状況が表示されます。この時点では、エンド・ユーザー・セッションでアクティブのものはありませんが、 LU が 6 つある PU が SSCP-LU セッションでアクティブです。

表 29. talk 5/appn/tn3270 へのアクセスによる TN3270E の状況の表示

```
DDD *TALK 5

DDD +PROTOCOL APPN
APPN GWCON
DDD APPN >TN3270E
TN3270E GWCON
DDD TN3270E >LIST STATUS
TN3270E Server Status Summary

TN3270E IP Address: 9.24.104.203
NetDisp Advisor Port Number: 10008
  Keepalive type: None
  Automatic Logoff: N
  Client IP Address mapping : N
  Number of connections                   : 1
  Number of available LUA LU's            : 5
  Number of LUA LU's pending termination  : 0
  Number of defined LU's                  : 6
  Number of connections in SSCP-LU state  : 0
  Number of connections in LU-LU state    : 1     1
 DDD TN3270E >
```

この番号は、ネットワーク・ユーティリティーと VTAM アプリケーションのもとで定義された LU 間に確立される LU-LU セッション数に伴って増えます。

最初のユーザーがセッションを確立し、クライアントの LU 名フィールドをブランクのままにしておくと、**talk 5/appn/tn3270e** のもとでの LIST CONNECTIONS では、表30 のようになります。

表 30. 最初のセッション確立、LU はデフォルトのプールから選択

```
DDD TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
DDLU5      IW              9.24.106.217      LU-LU  RA03T07   DDLU005   0
DDD TN3270E >
```

2 番目のユーザーがセッションを得て、やはり特定の LU 名もプール名も指定しなかった場合は、表31 に示すような接続のリストが表示されます。

表 31. デフォルトのプールを使用する 2 つのセッション

```
DDD TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
DDLU2      IW              9.24.106.127      LU-LU  RA03T08   DDLU002   0
DDLU5      IW              9.24.106.217      LU-LU  RA03T07   DDLU005   4
DDD TN3270E >
```

204ページの表32 には、3 番目のユーザーが、明示 LU DDLU7 を要求して、接続された場合に表示される接続のリストの例を示してあります。

表 32. 暗黙 LU ユーザーが 2、明示 LU ユーザーが 1 の場合の接続のリスト

```
DDD TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
DDLU7      EW              9.24.106.146      LU-LU  RA03T09   DDLU007   0
DDLU2      IW              9.24.106.127      LU-LU  RA03T08   DDLU002   6
DDLU5      IW              9.24.106.217      LU-LU  RA03T07   DDLU005   6
DDD TN3270E >
```

ホスト開始動的 LU 定義

この事例では、VTAM V4R4 が稼働する MVS と、ホストに ESCON 接続された IBM ネットワーク・ユーティリティーが使用されました。ネットワーク・ユーティリティーは、2 ポートのトークンリング・アダプターがスロット 1 に、 ESCON アダプターがスロット 3 に取り付けられていました。LSA ループバック・プロトコルが、ESCON チャネルを介する通信に使用されました。ネットワーク・ユーティリティーは、ネットワーク・ノードとして定義され、 VTAM との通信に APPN/ISR を使用していました。TN3270E の PU と LU は、 DLUR/DLUS を使用して VTAM に接続されていました。

ホスト開始動的 LU (HIDLU) 定義機能のテストには、次の VTAM 定義が使用されました。

- X5303 -- LSA ループバック ESCON 接続ネットワーク・ユーティリティー用の XCA 大ノード。DDDLU について前に示した事例の場合とまったく同じです。
- SW5303N -- ネットワーク・ユーティリティー APPN ネットワーク・ノード用の交換回線大ノード。 DDDLU について前に示した事例の場合とまったく同じです。
- SWHID -- ネットワーク・ユーティリティー内で明示 LU 定義を作成する LU 定義が入っている交換回線大ノード
- SWIMP -- ネットワーク・ユーティリティー内で暗黙 LU 定義を作成する LU 定義が入っている交換回線大ノード。暗黙 LU では、プール (複数の場合もある) に進みます。

  注: VTAM に対しては、LU はすべて -- 暗黙でも明示でも -- 同じ定義になります。したがって、LU は、ネットワーク・ユーティリティーでのプール定義に応じて、明示になったり暗黙になったりします。

VTAM とネットワーク・ユーティリティー構成の間のパラメーターの関係が、 205ページの図21 に示してあります。

ネットワーク・ユーティリティー、APPN/DLUR の LSA ループバック、ホスト開始動的 LU のパラメーター関係

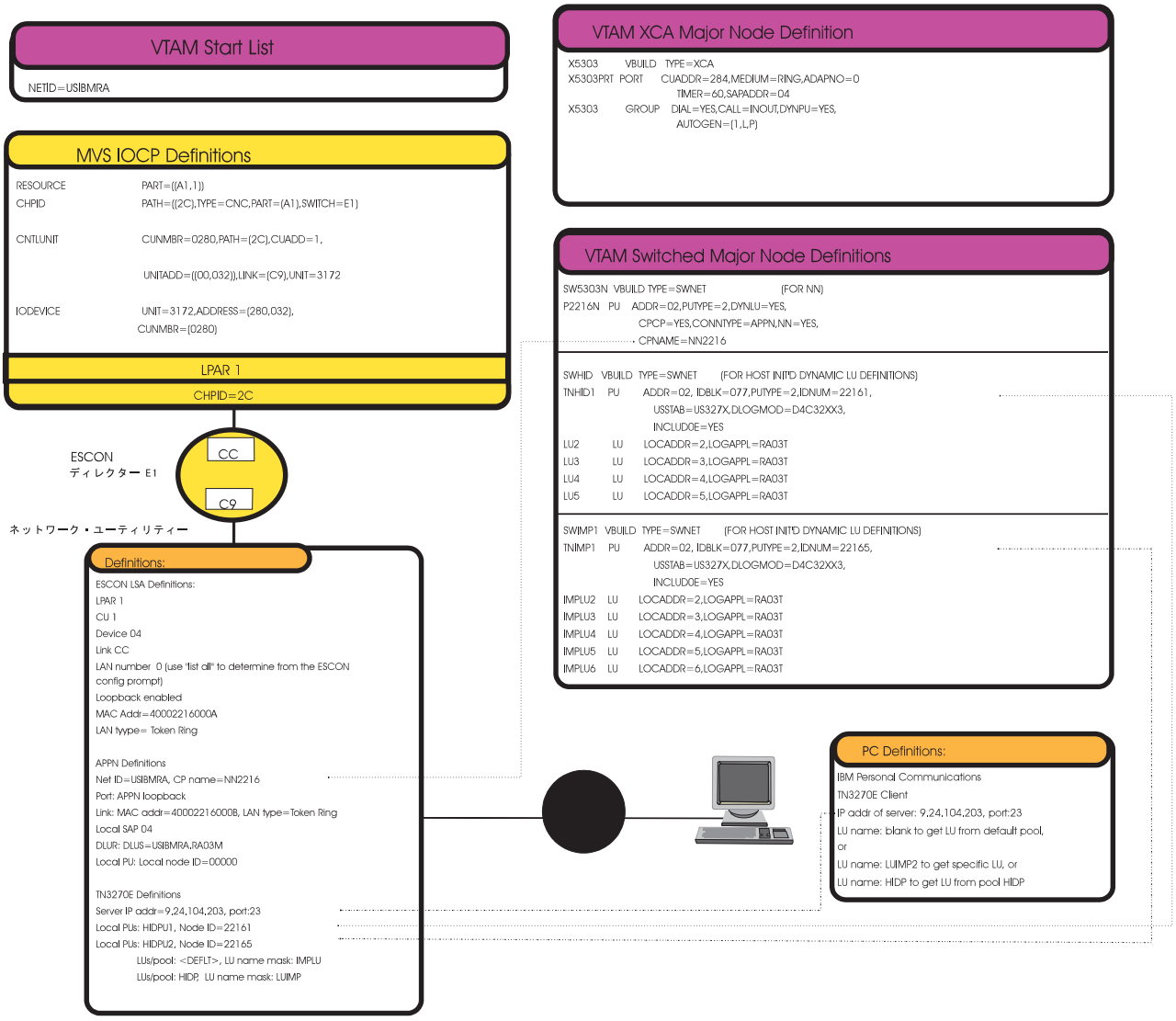


図 21. HIDLU 定義構成用パラメーターの関係

実際の SWHID 交換回線大ノードが 206ページの表33 に示してあります。

表 33. VTAM での交換回線大ノード SWHID1 の定義

```
****************************** Top of Data ********************************
SWHID1   VBUILD TYPE=SWNET
TNHID1   PU    ADDR=02,                                                  X
               IDBLK=077,      1                                         X
               IDNUM=22161,                                              X
               PUTYPE=2,                                                 X
               USSTAB=US327X,                                            X
               INCLUD0E=YES,   2                                         X
               DLOGMOD=D4C32XX3
LU2      LU    LOCADDR=02,LOGAPPL=RA03T
LU3      LU    LOCADDR=03,LOGAPPL=RA03T
LU4      LU    LOCADDR=04,LOGAPPL=RA03T
LU5      LU    LOCADDR=05,LOGAPPL=RA03T
****************************** Bottom of Data *****************************
```

1. ネットワーク・ユーティリティーでは、IDBLK 値 077 を使用します。
2. このパラメーターは新規で、HIDLU 定義に必要です。

表33 に示されているのは、プールで定義されたネットワーク・ユーティリティー LU に関する交換回線大ノード定義です。

これらの LU は、ここに示されている名前 (LU2 ～ LU5) を使用して、ネットワーク・ユーティリティーで定義されることになります。これらの VTAM ネットワーク NAU を表す LU が TN3270E サーバーに対してすでに定義されていたわけではないので、 LU は明示 LU になります。

TN3270 クライアントがこれらの LU の 1 つにアクセスする場合は、クライアントの LU 名フィールドに LU 名を定義する必要があります。

また、ホスト開始動的 LU を定義して、ネットワーク・ユーティリティー内のプールにアクセスすることもできます。この場合は、構成プログラム (または、 talk 6) で、ネットワーク・ユーティリティー内の 1 つまたは複数のプールを定義し、LU か LU 範囲の数だけでなく、プールに入る LU に関する LU 名マスクも指定して行います。PU TNIMP1 のもとでの次の LU は、このようにして定義されました。

表 34. VTAM での交換回線大ノード SWIMP1 の定義

```
****************************** Top of Data ********************************
SWIMP1   VBUILD TYPE=SWNET
TNIMP1   PU    ADDR=02,                                                  X
               IDBLK=077,      1                                         X
               IDNUM=22165,                                              X
               PUTYPE=2,                                                 X
               USSTAB=US327X,                                            X
               INCLUD0E=YES,   2                                         X
               DLOGMOD=D4C32XX3
IMPLU2   LU    LOCADDR=02,LOGAPPL=RA03T
IMPLU3   LU    LOCADDR=03,LOGAPPL=RA03T
IMPLU4   LU    LOCADDR=04,LOGAPPL=RA03T
IMPLU5   LU    LOCADDR=05,LOGAPPL=RA03T
IMPLU6   LU    LOCADDR=06,LOGAPPL=RA03T
****************************** Bottom of Data *****************************
```

1. ネットワーク・ユーティリティーでは、IDBLK 値 077 を使用します。
2. このパラメーターは新規で、HIDLU 定義に必要です。

交換回線大ノード SWIMP で定義された LU は、208ページの表36 に示されているように、MAS 構成での定義のため、ネットワーク・ユーティリティーでは、明示 LU と暗黙 LU の両方になります。

最初の 3 つの LU、つまり、IMPLU2、IMPLU3、IMPLU4 は、プール HIDP に入ります。TN3270E ユーザーは、TN3270E クライアントの LU 名フィールドを空のままにしておけば、これらの LU のどれか 1 つにアクセスできます。

次の LU、つまり、IMPLU5 は、MAS 構成プログラム内で定義され、デフォルトのプール <DEFLT> に入ります。ユーザーは、TN3270E クライアントで LU 名フィールドを空のままにしておけば、この LU にアクセスできます。

最後の LU、つまり、IMPLU6 の場合は、ネットワーク・ユーティリティーにプールがまったく定義されていません。したがって、IMPLU6 という名前の明示 LU になります。

注: TN3270E サーバー内でプールを定義するときは、LU 名マスクも指定する必要があります。このマスクが実際に VTAM の LU 名をオーバーライドし、1 つのプールに属する暗黙 LU は、LU 名マスクに基づく名前をもつことになります。VTAM から直接 LU 名を入手するのは、明示 LU (プールに入らない) を定義するときだけです。

表 35. MAS 3.3 構成プログラムを使用して行われた HIDLU 構成 (2 の 1)

構成プログラム・ナビゲーション	構成プログラム値
装置 スロット	スロット 1: 2 ポート TR スロット 2: ESCON
装置 チャネル・アダプター ESCON インターフェース ESCON インターフェース	プロトコル・タイプ : LSA LAN タイプ : トークンリング MAC アドレス (LSA バーチャル LAN の場合は、VTAM 側) : 例えば、40002216000A **Loopback** をクリック **Add** をクリック
装置 チャネル・アダプター ESCON インターフェース ESCON サブチャネル	装置アドレス : 4 サブチャネル・タイプ : 読み取り/書き込み LPAR: 1 リンク・アドレス : CC CU: 1 **Add** をクリック
装置 チャネル・アダプター APPN ループバック・ネット	LAN タイプ : トークンリング MAC アドレス : 40002216000B **Add** をクリック
システム 一般	システム名 : HID ロケーション : 機械室 連絡先 : ユーザーの名前
システム ユーザー	名前 : ユーザー ID 許可 : 管理者 パスワード : パスワード 繰り返しパスワード : パスワード **Add** をクリック
システム SNMP Config (構成) コミュニティー 一般	名前 : 公衆 アクセス・タイプ : 読み取り/書き込みトラップ **Add** をクリック

表 35. MAS 3.3 構成プログラムを使用して行われた HIDLU 構成 (2 の 1) (続き)

構成プログラム・ナビゲーション	構成プログラム値
プロトコル IP 詳細	内部アドレス : 9.24.104.203
プロトコル IP インターフェース	インターフェース 1 (TR スロット 1 ポート 2) IP アドレス : 9.24.106.9 サブネット・マスク : 255.255.255.0 **Add** をクリック IP アドレス : 9.24.104.203 サブネット・マスク : 255.255.255.0 **Add** をクリック
プロトコル APPN 一般	**APPN network node** をクリック ネットワーク ID : USIBMRA コントロール・ポイント名 : NN2216
プロトコル APPN DLUR	**DLUR** をクリック 1 次 DLUS の完全修飾名 : USIBMRA.RA03M

表 36. MAS 3.3 構成プログラムを使用して行われた HIDLU 構成 (2 の 2)

構成プログラム・ナビゲーション	構成プログラム値
プロトコル APPN インターフェース	回線項目 **APPN Net--token ring** を クリック **Configure** をクリック (タブ General を選択) **Define APPN Port** をクリック **Service Any Node** をクリック ***off* High Performance Routing (HPR)** をクリック **サポート** **Support Multiple PUs** をクリック タブ **Port Definition** を選択 ローカル SAP アドレス指定 : 04
プロトコル TN3270E サーバー 一般	**TN3270E** を クリック IP アドレス : 9.24.104.203
プロトコル TN3270E サーバー プール	プール名 : HIDP **Add** をクリック
プロトコル TN3270E サーバー ローカル PU	リンク・ステーション名 : HIDPU1 ノード ID : 22161 **Host-Initiated Dynamic LUs allowed** **for PU** をクリック 1 次 DLUS: USIMBRA.RA03M **Add** をクリック リンク・ステーション名 : HIDPU2 **Host-Initiated Dynamic LUs allowed** **for PU** をクリック ノード ID : 22165 1 次 DLUS: USIBMRA.RA03M **Add** をクリック

表 36. MAS 3.3 構成プログラムを使用して行われた HIDLU 構成 (2 の 2) (続き)

構成プログラム・ナビゲーション	構成プログラム値
プロトコル TN3270E サーバー LU	回線 HIDPU2 を選択 見出し Implicit pool をクリック プール名選択 : <DEFLT> LU 名マスク : IMPLU **Specify Address Ranges** をクリック アドレス範囲数 : 5 **Add** をクリック プール名選択 : HIDP LU 名マスク : LUIMP **Specify Address Ranges** をクリック アドレス範囲数 : 2 〜 4 **Add** をクリック

構成の監視

HIDLU の構成は、**protocol appn** と **tn3270e** のもとで、talk 5 で監視できます。

talk 5 のもとでは、表37 に示されているように、すべてのインターフェースを監視できます。

表 37. Talk 5 のもとでのインターフェース・コマンドの表示

```
HID +INTERFACE
                                                Self-Test  Self-Test Maintenance
Net   Net'   Interface   Slot-Port               Passed     Failed      Failed
0     0      TKR/0       Slot: 1   Port: 1          1          0         0
1     1      TKR/1       Slot: 1   Port: 2          1          0         0
2     2      ESCON/0     Slot: 3   Port: 1          1          0         0
3     2      LSA/0       Slot: 0   Port: 0          1          3         0
4     4      TKR/2       Slot: 0   Port: 0          1          0         0
```

表 38. Talk 5 のもとでの統計

```
HID +STATISTICS
Net   Interface      Unicast  Multicast      Bytes    Packets      Bytes
                   Pkts Rcv   Pkts Rcv   Received      Trans      Trans
0     TKR/0           22521      25742    1399673      22522     472997
1     TKR/1           24301    1476136   97150812      23588     582533
2     ESCON/0         11453          0    2976076       9930    1481020
3     LSA/0           11452          0    2976060       9929    1480999
4     TKR/2               0          0          0          0          0
```

talk 5 レベルでコマンド **p app** (protocol appn) を発行すると、表39 に示すように、CP-CP 接続の検査など、 APPN 関連機能を監視できます。

表 39. VTAM への NN-NN 接続の検査

```
HID +PROTOCOL APPN
HID APPN >LIST CP-CP_SESSIONS
          CP Name Type     Status    ConWinner ConLoser ConWinner ConLoser
                                        ID        ID    Sense     Sense
============================================================================
    USIBMRA.RA03M  NN     Active     3710C590  3710C592 00000000  00000000
```

TN3270E 機能は、APPN のもとにあり、コマンド **TN3270E** を発行して、表41 に示すようにアクセスできます。TN3270E レベルでは、**LIST** コマンドが、表40 に示されている完成候補を伴って発行できるだけです。

表 40. TN3270E のもとでの LIST オプション

```
HID TN3270E >LIST ?

Possible completions:
        CONNECTIONS
        MAPPING
        POOLS
        PORTS
        STATUS
(you may cycle through these commands by pressing the TAB key)
HID TN3270E >LIST
```

表 41. TN3270E セッションの監視

```
HID APPN >TN3270E
TN3270E GWCON
HID TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
IMPLU5     IW              9.24.106.127      LU-LU  RA03T01   IMPLU5    38
```

表41 には、最初のセッションが確立された後の TN3270E 接続が示されています。TN3270E クライアントでは LU 名を定義しなかったので、デフォルトのプールから LU 名が選択されました。

次に、別のユーザーが、HIDP プール名をクライアント内の LU 名に指定して、TN3270E 接続を行います。表42 に例示されているようなリストが表示されます。

表 42. 2 番目のユーザーのセッション後の LIST CONNECTIONS

```
HID TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
------------------------------------------------------------------------------
LUIMP4     IW              9.24.106.217      LU-LU  RA03T07   IMPLU4    1
IMPLU5     IW              9.24.106.127      LU-LU  RA03T01   IMPLU5    45
```

3 番目のユーザーが、クライアント内で IMPLU6 を定義して、セッションを確立すると、211ページの表43 に示すような接続のリストが表示されます。

表 43. 3 番目のユーザーの接続後の LIST CONNECTIONS

```
HID TN3270E >LIST CONNECTIONS
Connection information for all the LUs

Local LU  Class  Assoc LU   Client Addr     Status   Prim LU  Sec LU  Idle
Min
-------------------------------------------------------------------------------
IMPLU6     EW              9.24.106.146      LU-LU  RA03T09   IMPLU6    0
LUIMP4     IW              9.24.106.217      LU-LU  RA03T07   IMPLU4    4
IMPLU5     IW              9.24.106.127      LU-LU  RA03T01   IMPLU5    48
```

TN3270E ホスト・オンデマンド (HOD) クライアント・キャッシュ

HOD クライアント・キャッシュ機能に関しては、ネットワーク・ディスパッチャーのもとで、TN3270E サーバーと HOD 機能の両方を構成する必要があります。この構成の場合は、199ページの表26 で DDDLU に関して行い、 207ページの表35 で HIDLU に関して行った構成とまったく同じ構成を保持できます。この事例では、HIDLU 定義は TN3270E サーバー用として定義されました。

環境の HOD クライアント・キャッシュ部分に関しては、HIDLU や DDDLU の場合 (この章の既出の節) にすでに行った他の定義に加えて、ネットワーク・ディスパッチャー 'Executor' と HOD クライアント・キャッシュの両方を定義する必要があります。

この事例での HOD サーバーの設置では、NT サーバー、NT サービス・パック 3、Web サーバー、HOD サーバーがインストールされました。

HOD サーバー・ボックス上のループバック・アドレスは、ネットワーク・ディスパッチャーのクラスター IP アドレスを指すように定義する必要があります。ネットワーク・ディスパッチャーのクラスター IP アドレスは、 PING できません。

次に示す事例では、ループバック・アダプターは、次のようにして MS NT サーバー上で定義されました。

1. 「**Start**」をクリックしてから、「**Settings**」をクリックする。
2. 「**Control Panel**」をクリックし、「**Network**」をダブルクリックする。
3. MS ループバック・アダプター・ドライバーを追加する。
4. 「Network」ウィンドウで、「**Adapters**」をクリックする。
5. 「MS Loopback Adapter」を選択して、「**OK**」をクリックする。
6. プロンプトが出たら、インストール CD かインストール・ディスケットを挿入する。
7. 「Network」ウィンドウで、「**Protocols**」をクリックする。
8. 「TCP/IP」プロトコルを選択してから、「**Properties**」をクリックする。
9. 「Loopback Adapter」を選択して、「**OK**」をクリックする。
10. ループバック・アダプター・アドレスをネットワーク・ディスパッチャーのクラスター・アドレスに設定して、サブネット・マスク (255.0.0.0) を受け入れる。ゲートウェイ・アドレスは入力しません。

HOD サーバーの定義にあたっては、次のアクションも忘れないで実行します。Windows NT サーバーに関する事例では、クラスター IP アドレス (9.24.104.207) は、コマンド **netstat -r** の発行後に、 Gateway 欄に表示されます。この欄で、複数の項目にクラスター IP アドレスが表示されている場合は、無関係のルートを削除する必要があります。クラスター IP アドレスと同じネットワーク・アドレスで始まり、残りはゼロばかりのものを削除します。この場合は、削除の対象になる項目は、 IP アドレス 9.0.0.0 の行です。

ネットワーク・ユティリティー、ホスト開始動的 LU がある HOD クライアント・キャッシュのパラメーターの関係

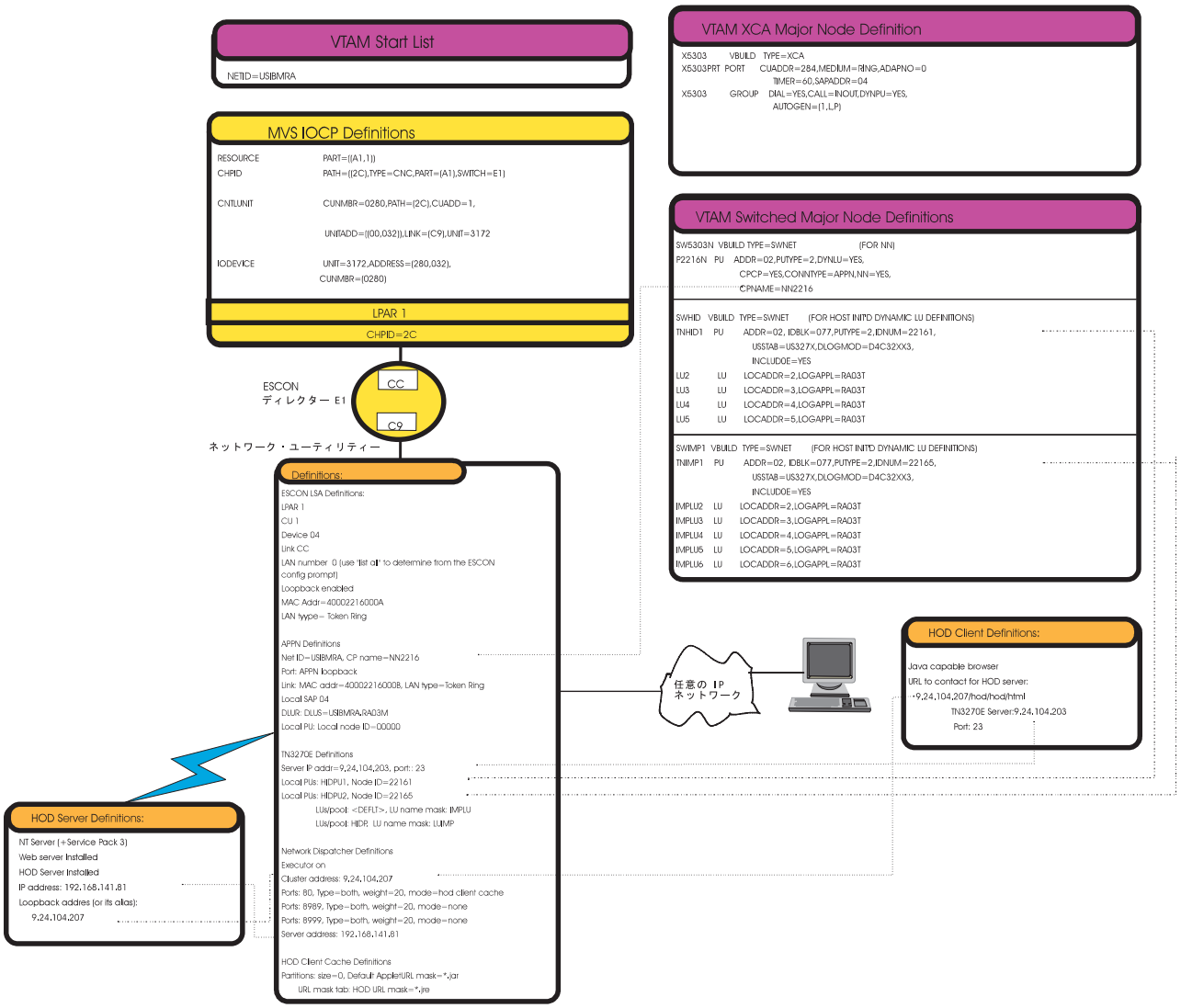


図 22. HOD クライアント・キャッシュ・パラメーターの関係

ホスト・オンデマンド・クライアント・キャッシュ構成の場合は、 199ページの表26 や 207ページの表35 で前に行われた DDDLU 構成や HIDLU 構成の上に、HOD が追加されるだけです。 これらの構成には、 TN3270E 構成がすでに含まれているからです。

表 44. HOD クライアント・キャッシュ構成

構成プログラム・ナビゲーション	構成プログラム値			
装置 インターフェース	インターフェース 0: スロット/ポート =1/1 **Interface** をクリック			
プロトコル IP インターフェース アドレス	**Interface 0** をクリック IP アドレス : 192.168.141.82 マスク 255.255.255.240 (この事例の場合) **ADD** をクリック			
プロトコル IP OSPF インターフェース	**address 192.168.141.82** をクリック OSPF ボックスにチェック・マーク			
フィーチャー ネットワーク・ディスパッチャー Executor	**Executor** をクリック (executor 'オン')			
フィーチャー ネットワーク・ディスパッチャー クラスター 詳細	クラスター・アドレス : 9.24.104.207 残りはデフォルト値 **ADD** をクリック			
フィーチャー ネットワーク・ディスパッチャー	*番号* 80	*タイプ* 両方	*モード* HOD クライアント	*重み* 20
クラスター ポート	8989 8999	両方 両方	なし なし	20 20
フィーチャー ネットワーク・ディスパッチャー クラスター サーバー	3 つのポートすべて : アドレス : 192.168.141.81 (NT サーバー) 重み : 20 サーバーの状態 : アップ **ADD** をクリック			
フィーチャー ネットワーク・ディスパッチャー クラスター HOD クライアント・キャッシュ プロキシー	デフォルト値を除く			
フィーチャー ネットワーク・ディスパッチャー クラスター HOD クライアント・キャッシュ パーティション	パーティション : デフォルト・アプレット : *.jar その他のパラメーターはデフォルトのまま URL マスク : URL マスク : *jre URL マスク・タイプ : Include **ADD** をクリック			

この例では、Netscape ブラウザーは、**http://9.24.104.207/hod/hod.html** に向けられ、214ページの図23 の画面が表示されました。3270 のアイコンを右マウス・ボタンでクリックすると、214ページの図24 の画面が表示されます。 214ページの図24 では、TN3270E サーバー・パラメーターは、ネットワーク・ユーティリティーでの定義と同じです。

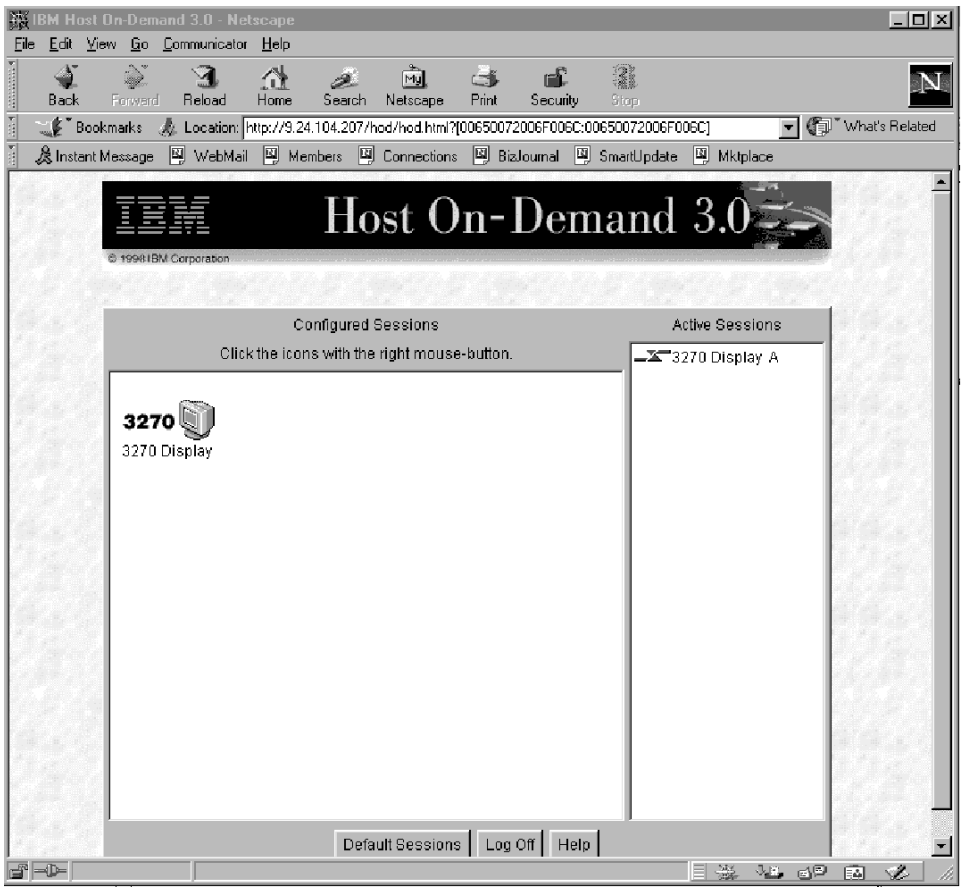


図 23. インターネット・ブラウザー (Netscape) 上での HOD クライアント画面

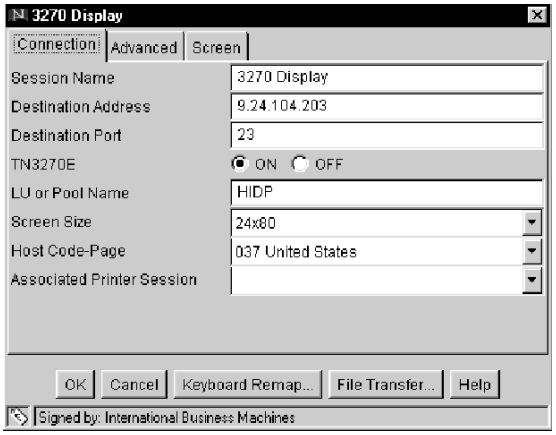


図 24. HOD クライアントでの TN3270E サーバー定義

この定義の後は、3270 のアイコンをダブルクリックする (左マウス・ボタンで) と、次の画面 (215ページの図25) が表示されます。

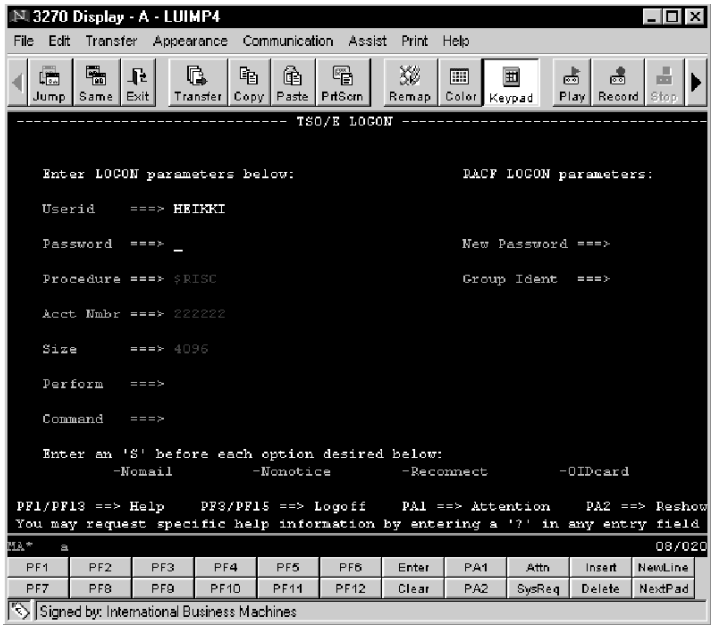


図 25. 接続の確立後の HOD クライアント画面

構成の監視

HOD の構成を監視する場合は、次のようにコマンドを発行します。

表 45. T5/ELS でのキャッシュ監視の開始

```
HODCAC0 *TALK 5
HODCAC0 +EVENT
HODCAC0 ELS>NODISPLAY SUBSYSTEM ALL ALL
Complete
HODCAC0 ELS>DISPLAY SUBSYSTEM WEBH ALL
HODCAC0 ELS>    ..(Ctrl-P)
HODCAC0 *TALK 2
:
00:00:01  DOLOG: Server 192.168.141.81 has been set up.
:
00:20:01 WEBH.017: Client connection 31AE11C accepted as Socket 31BF564
00:20:01 WEBH.015: Conn (31AE11C) HTTP Proxy(cluster 9.24.104.207 port 80)
partition (0) opened
00:20:01 WEBH.009: HTTP Proxy(cluster 9.24.104.207 port 80) conn (31AE11C)
new req being parsed
00:20:01 WEBH.012: HTTP Proxy(cluster 9.24.104.207 port 80) partition (0)
conn (31AE11C) not using cache because object not found in cache     1
 :
 :
 :
```

1. 初めて、クライアントがクラスター・アドレスから Java アプレットの要求を発行しました。したがって、このメッセージでは、ネットワーク・ユーティリティーのキャッシュ内に見つからないことが説明されています。

表 46. HOD クライアント・キャッシュ定義の監視

```
HODAC0 +FEATURE
Feature name or number [WAN Restoral System] ? hod
Host On-Demand Client Cache Console
HODCAC0 HOD Client Cache>LIst All
HOD Client Cache Partition 0    Status: Enabled
     Cluster address: 9.24.104.207  Port 80
1 partition(s) active.
External Cache Manager: Disabled
```

表 47. HOD クライアント・キャッシュの表示

```
HODCAC0 HOD Client Cache>LIst PArtition
HOD Client Cache Partition 0      Status: Enabled
        Cluster address: 9.24.104.207   Port 80
Partition size: Current - 1030296 bytes Highest - 1030296 bytes Maximum - Unlimited
Number of objects: Current - 37  Highest - 37  Maximum - Unlimited
Maximum object size: Unlimited
HOD Client Cache purge interval : 600 minute(s)
Hit ratio: 61%
Total number of hits:  59      1
Total number of misses:  37
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
Objects explicitly Included: 0
Total number of purged objects: 0
Purged objects (Cache full):     0
               (Object stale):   0
               (Purged by user): 0
               (Invalidation):   0
```

1. ネットワーク・ユーティリティー内のキャッシュ・ヒットの数。HOD クライアントがキャッシュをヒットすると、ネットワーク・ユーティリティーから Java アプレットが送達/ダウンロードされ、HOD サーバー上のロードやトラフィックが NT サーバー上にインストールされることはありません。

表 48. 別の HOD クライアントからの Java アプレットの要求時の画面の表示

```
HODCAC0 HOD Client Cache>LIst PArtition
HOD Client Cache Partition 0      Status: Enabled
         Cluster address: 9.24.104.207   Port 80
Partition size: Current - 1030296 bytes Highest - 1030296 bytes Maximum - Unlimited
Number of objects: Current - 37  Highest - 37  Maximum - Unlimited
Maximum object size: Unlimited
HOD Client Cache purge interval : 600 minute(s)
Hit ratio: 61%               1
Total number of hits:  59    2
Total number of misses:  37
Object Excluded (Object too large):          0
                (Object expired)             0  .....
:
:
```

1. キャッシュ・ヒット率は、HOD クライアントの要求の増加に伴って高くなります。

2. キャッシュへのヒットの合計数も、他の HOD クライアント要求に伴って増えます。これによって、Java アプレットがネットワーク・ユーティリティーの HOD クライアント・キャッシュから送達されることが立証されます。

これで、この章の既出の節での DDDLU や HIDLU の場合と同様にして、 TN3270E の接続が監視できます。

DLSw を介する TN3270E サブエリア SNA

DLSw を介する TN3270E サブエリア SNA 機能の事例については、 221ページの図 26 をごらんください。ネットワーク・ユーティリティー A は、ESCON チャネル接続で、PPP リンクを介してネットワーク・ユーティリティー B にも接続されています。以下に示す構成画面で分かるように、 VTAM ホストへの接続はサブエリアなので、ネットワーク・ユーティリティー A 上には APPN 機能はありません。ホスト上では、ネットワーク・ユーティリティー内のローカル ノード ID (サンプル事例では '221B1') を指している VTAM 交換回線大ノード (IDNUM パラメーターを指定して) を定義する必要があります。これは純然たるサブエリア SNA 接続ですが、定義はネットワーク・ユーティリティー B 上で APPN のもとで行われます。

表 49. ネットワーク・ユーティリティー A 上での DLSw 構成

```
dlsa-ok DLSw config>ENABLE DLSW
Data Link Switching is now enabled
dlsa-ok DLSw config>ADD TCP
Enter the DLSw neighbor IP Address [0.0.0.0]? 172.16.220.253
Connectivity Setup Type (a/p) [a]? p
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]?
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neighbor has been changed
dlsa-ok DLSw config>OPEN-SAP
Enter Interface number [0]? 1
Enter the SAP in hex (range 0-FE), 'SNA', 'NB', or 'LNM'  [4]? sna
```

これは、上記の 表49 や 221ページの図26 に示されているように、ネットワーク・ユーティリティー A の場合に必要な定義です。

ネットワーク・ユーティリティー B が構成される場合は、APPN プロンプトのもとで、DLSw と TN3270E サーバーを構成する必要があります。

表 50. ネットワーク・ユーティリティー B 上での DLSw 構成

```
dlsb-ok DLSw config>ENABLE DLSW
Data Link Switching is now enabled
dlsb-ok DLSw config>ADD TCP
Enter the DLSw neighbor IP Address [0.0.0.0]? 9.24.104.203
Record already exists, can be changed
Connectivity Setup Type (a/p) [a]? a
Transmit Buffer Size (Decimal) [5120]?
Receive Buffer Size (Decimal) [5120]?
Maximum Segment Size (Decimal) [1024]?
TCP Keepalive (E/D) [D]?
NetBIOS SessionAlive Spoofing (E/D) [D]?
Neighbor Priority (H/M/L) [M]?
TCP Neighbor has been changed
dlsb-ok DLSW config>OPEN-SAP
Enter Interface number [0]? 1
Enter SAP in hex (range 0-FE), 'SNA', 'NB', or 'LNM'  [4]? sna
dlsb-ok DLSw config>EXIT
```

表 51. APPN パッケージと TN3270E パッケージのロード (まだロードされていない場合)

```
2216 Config>load add package appn
appn package configured successfully

This change requires a reload.
2216 Config>load add package tn3270e
tn3270e package configured successfully
This change requires a reload.
```

APPN パッケージと TN3270E パッケージのどちらか、または両方がロードされていない場合は、命令コードからメモリーにロードして、使用できるようにする必要があります。 APPN パッケージと TN3270E パッケージのロードについては、上記の 表 51 をごらんください。

表 52. APPN のもとでのリンク・ステーションの追加

```
dlsb-ok Config>PROTOCOL APPN
dlsb-ok APPN config>ADD/UPDATE LINK-STATION
APPN Station
Port name for the link station [ ]? dls65
Station name (Max 8 characters) [ ]? tnpub1
WARNING!! You are changing an existing record.
        Activate link automatically (Y)es (N)o  [Y]
        MAC address of adjacent node [40002216000A]?
        SAP address of adjacent node (04-EC) [4]?
        Solicit SSCP Session: (Y)es (N)o  [Y]?
                Local Node ID (5 hex digits)  [221B1]?
                Enable Host Initiated Dynamic LU Definition : (Y)es (N)o [N]?
        Local SAP address (04-EC)  [4]?
        Does link support APPN function: (Y)es (N)o  [N]?  N
Edit TG Characteristics: (Y)es (N)o  [N}?
Write this record? [Y]? y
The record has been written.
```

表 53. APPN のもとでのポートの追加

```
dlsb-ok APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P, [ ]? d
Port Name (Max 8 characters) [D65534]? dls65

WARNING!! You are changing an existing record.
Enable APPN on this port (Y)es (N)o? y
Port Definition
     Support multiple PU (Y)es (N)o [Y] y
All active port names will be of the form <port name sap>
     Service any node: (Y)es (N)o [N] n
     Maximum BTU size (768-4096) [2048]?
     Maximum number of link stations (1-65535) [65535]?
     Percent of link stations reserved for incoming calls (0-100) [0]?
     Percent of link stations reserved for outgoing calls (0-100) [0]?
     Local SAP address (04-EC) [4]?
     Locally administered MAC address (hex) [40002216B00B]?
Edit TG characteristics (Y)es (N)o [N]?
Write this record? [Y]? y
The record has been written.
```

表 54. APPN のもとでの TN3270E サーバーの定義

```
dlsb-ok APPN config>TN3270E
lsadirect TN3270E config>SET
TN3270E Server Parameters
        Enable TN3270E Server (Y/N) [Y]?
        TN3270E Server IP Address [9.24.104.203]? 172.16.220.2
        Port Number [23]?
        Enable Client Address Mapping (Y/N) [N]?
        Default Pool name (Max 8 characters) [PUBLIC]?
        NetDisp Advisor Port Number [10008]?
        Keepalive type:
         0 = none,
         1 = Timing Mark,
         2 = NOP [0]?
        Automatic Logoff (Y/N) [N]?
        Enable IP Precedence (Y/N) [N]?
Write this record? [Y]?
dlsb-ok TN3270E config>ADD/UPDATE IMPLICIT-POOL
TN3270E Server Implicit Definitions
        Pool Name (Max 8 characters)  [<DEFLT>]?
        Station Name (Max 8 characters)  []? tnpub1
WARNING!! You are changing an existing record.
        LU Name Mask (Max 5 characters)  [@01LU]?
        LU Type  ( 1 - 3270 mod 2 display
                   2 - 3270 mod 3 display
                   3 - 3270 mod 4 display
                   4 - 3270 mod 5 display) [1]? 1
        Specify LU Address Ranges (s) (y/n)  [N]?
        Number of Implicit LUs in Pool(1-253)  [5]?
Write this record? [Y]? y
The record has been written.
```

以上の画面で、ネットワーク・ユーティリティー B での TN3270E サーバーの定義は完了です。

VTAM での対応する定義は、下記の 表55 のようにして行います。

表 55. VTAM 交換回線大ノード定義

```
SWB1              VBUILD     TYPE=SWNET
TNPUB1            PU     ADDR=02,                          X
                         IDBLK=077,                       X
                         IDNUM=221B1,                       X
                         PUTYPE=2,                          X
                         USSTAB=US327X,                     X
                         DLOGMOD=D4C32XX3
LUB2              LU     LOCADDR=02,LOGAPPL=RA03T
LUB3              LU     LOCADDR=03,LOGAPPL=RA03T
LUB4              LU     LOCADDR=04,LOGAPPL=RA03T
LUB5              LU     LOCADDR=05,LOGAPPL=RA03T
LUB6              LU     LOCADDR=06,LOGAPPL=RA03T
```

以上の定義が正しく行われると、機能はすでにネットワーク・ユーティリティー・ボックス上で作動可能な状態になっています。

構成の全般像については、221ページの図26 をごらんください。

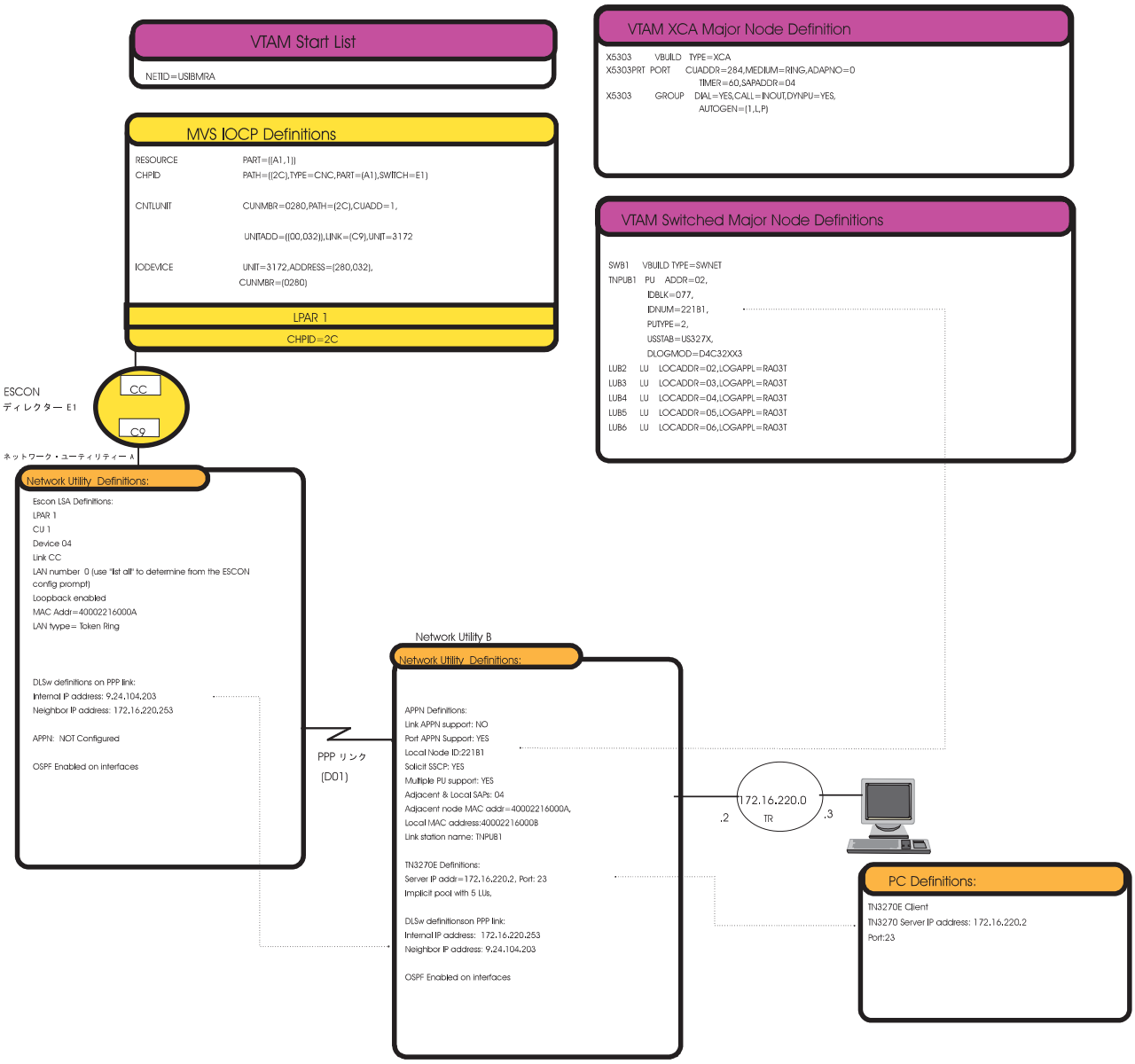


図 26. DLSw を介する TN3270E サブエリア接続のパラメーターの関係

DLSw を介する TN3270E SNA サブエリア構成の監視

以上の定義を完了したら、構成とその状況について、ネットワーク・ユーティリティー側と VTAM 側の両方で監視する必要があります。

表 56. ネットワーク・ユーティリティー B で定義した LU の VTAM 画面の表示

```
D NET,ID=SWB1,E
IST097I DISPLAY ACCEPTED
IST075I NAME=SWB1, TYPE=SW SNA MAJ NODE 774
IST486I STATUS=ACTIV, DESIRED STATE-ACTIV
IST1656I VTAMTOPO=REPORT, NODE REPORTED - YES
IST084I NETWORK RESOURCES:
IST089I TNPUB1     TYPE=PU_T2.1        , ACTIV
IST089I LUB2       TYPE=LOGICAL UNIT   , ACTIV
IST089I LUB3       TYPE=LOGICAL UNIT   , ACTIV
IST089I LUB4       TYPE=LOGICAL UNIT   , ACTIV
IST089I LUB5       TYPE=LOGICAL UNIT   , ACTIV
IST089I LUB6       TYPE=LOGICAL UNIT   , ACTIV
IST314I END
```

ネットワーク・ユーティリティー B の構成は、下に示すようにして監視できます。

表 57. 'T 6' のもとでの TN3270E サーバーの表示

```
dlsb-ok *TALK 6
Gateway user configuration
dlsb-ok Config>PROTOCOL APPN
dlsb-ok APPN config>TN3270E
dlsb-ok TN3270E config>LIST ALL
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 172.16.220.2
TN3270E Port Number: 23
Default Pool Name: PUBLIC
NetDisp Advisor Port Number: 10008
Client IP Address Mapping: N
Keepalive type: NONE
Automatic Logoff: N    Timeout: 30
        Enable IP Precedence: N
Link Station: TNPUB1
        Local Node ID: 221B1
        Auto Activate: YES
        Host Initiated Dynamic LU Definition: NO
        Implicit Pool Information
        Pool Name: <DEFLT>
               Number of LUs: 5
               LU Mask: @01LU
        LU Name    NAU Addr     Class     Assoc LU Name  Assoc NAU addr
------------------------------------------------------------------------
        LUB2          2       Explicit Workstation
Client IP Address Mapping
-------------------------
Client IP Address              Address Mask      Resource Name
-------------------------------------------------------------
Multiple Port
-------------------------------------------------------------
PORT NUMBER   ENABLE TN3270E     RESOURCE NAME  DISABLE FILTERING
----------   --------------     -------------  -----------------
dlsb-ok TNE3270E config>
```

表 58. DLSw の接続とセッションの監視

```
(ctrl-p)
dlsb-ok *TALK 5
CGW Operator Console
dlsb-ok +PROTOCOL DLSW
Data Link Switching Console
dlsb-ok DLSw>LIST TCP SESSIONS
Group/Mcast@     IP Address  Conn State  CST Version ACTSes SesCreates
-------------------------------------------------------------------------------
     1          9.24.104.203  ESTABLISHED  A  AIW V2RO    1        1
dlsb-ok DLSw>LIST DLSW SESSIONS ALL
Source     Destination   State   Flags   Dest IP Addr    Id
-----------------------------------------------------------
 1 APPN  04 40002216000a04 Connected     9.24.104.203     0
```

表 59. APPN リンクの監視

```
dlsb-ok APPN >LIST LINK_INFORMATION
   Name    Port Name  Intf   Adj CP Name   Type    HPR  State
============================================================
TNPUB1     DLS65     65534 USIBMRA.RA03M   NN   INACTIVE ACT_LS 1
```

1. APPN がアクティブで、セッション中であることを意味します。

表 60. TN3270E のもとでの LU-LU 接続の表示

```
dlsb-ok APPN >TN3270E
TN3270E GWCON
dlsb-ok TN3270E >LIST CONNECTIONS
Connection information for all the LUs
Local LU  Class  Assoc LU  Client Addr  Status  Prim LU  SEC LU  Idle Min
-------------------------------------------------------------------------
@01LU6     IW              9.24.106.44  LU-LU   RA03T03  LUB6       1
```

表 61. TN3270E サーバーの状況

```
dlsb-ok TN3270E >LIST STATUS
TN3270E Server Status Summary
TN3270E IP Address: 172.16.220.2
NetDisp Advisor Port Number: 10008
   Keepalive type: None
   Automatic Logoff: N
   Client IP Address mapping: N
   Number of Connections                   :1
   Number of Available LUA LU's            :5
   Number of LUA LU's pending termination  :0
   Number of defined LU's                  :6
   Number of connections in SSCP-LU state  :0
   Number of connections in LU-LU state    :1
```

TN3270E LSA SNA サブエリア接続

SNA をトランスポートするときは、同じ 2216 内の SNA サブエリア・リンクを使用して、TN3270E サーバーを構成できます。この構成では、ホスト内に次の定義が必要です。

- XCA 大ノード定義

表 62. VTAM XCA 交換回線大ノード定義

```
X5303    VBUILD TYPE=XCA
X5303PRT PORT  ADAPNO=0,                                    *
               CUADDR=284,                                  *
               SAPADDR=4,                                   *
               MEDIUM=RING
X5303GRP GROUP DIAL=YES,CALL=INOUT,DYNPU=YES,               *
               AUTOGEN=(1,L,P)
```

- 交換回線大ノード定義

表 63. VTAM 交換回線大ノード : SWB1

```
SWB1     VBUILD TYPE=SWNET
TNPUB1   PU    ADDR=02,              X
               IDBLK=077,            X
               IDNUM=221B1,          X
               PUTYPE=2,             X
               USSTAB=US327X,        X
               DLOGMOD=D4C32XX3
LUB2     LU    LOCADDR=02,LOGAPPL=RA03T
LUB3     LU    LOCADDR=03,LOGAPPL=RA03T
LUB4     LU    LOCADDR=04,LOGAPPL=RA03T
LUB5     LU    LOCADDR=05,LOGAPPL=RA03T
LUB6     LU    LOCADDR=06,LOGAPPL=RA03T
```

ネットワーク・ユーティリティー、TR/PPP 接続をサポートする LSA SNA サブエリア TN3270E サーバーのパラメーターの関係

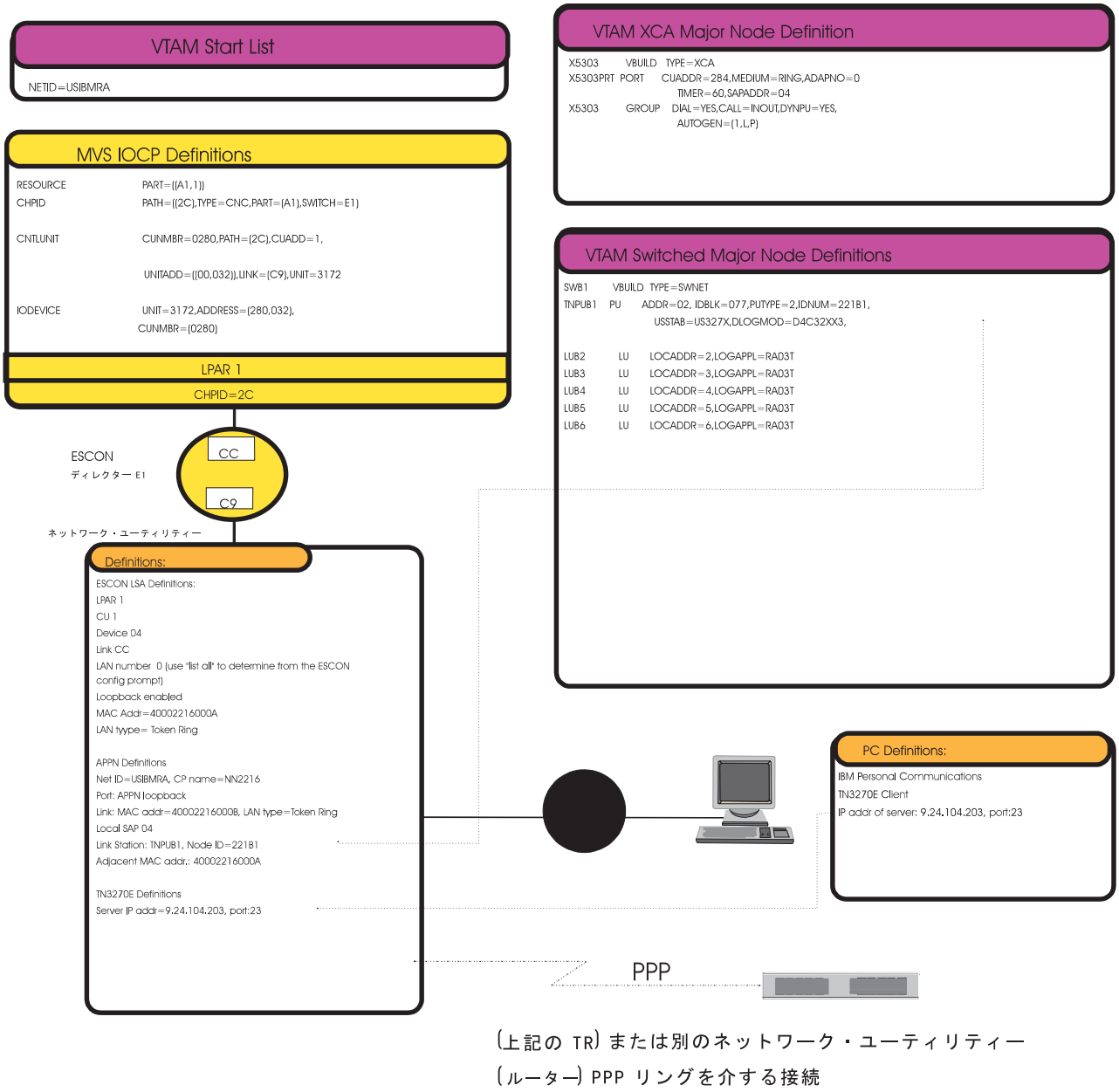


図 27. TR/PPP 接続をサポートする TN3270E の LSA SNA サブエリア

TN3270E サーバー PU に関する交換回線大ノード定義は、次に示すようにして定義されました。

表 64. ESCON 構成のリスト

```
lsadirect ESCON Config>LIst
Net:  4   Protocol: APPN Loopback   LAN type: Token-Ring/802.5   1
          APPN loopback MAC address: 40002216000B
Net:  3   Protocol: LSA    LAN type: Token Ring      LAN number:  0
          Maxdata: 2052
          Loopback is enabled.
          MAC address: 40002216000A
          Block Timer:   10 ms    ACK length:   10 bytes
```

1. APPN ループバック・ネットワーク番号 (4) です。この番号は、227ページの表66 に示されているように、後で定義 **APPN config>add port** で使用されます。

これで、以下の画面に示されているように、APPN ポート、APPN リンク、 TN3270E サーバーの定義を追加できます。APPN パッケージと TN3270E パッケージのどちらか、または両方がロードされていない場合は、 218ページの表51 をごらんください。

表 65. 基本 APPN CP 名定義

```
2216 Config>protocol appn
2216 APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [  ]? usibmra
Control point name (Max 8 characters) [  ]? NN2216
Enable branch extender or border node
        (0=Neither, 1=Branch Extender, 2=Border Node) [0]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y]?
The record has been written.
2216 APPN config>ex
2216 Config>write
Config Save: Using bank A and config number 1
2216 Config>
2216 *reload y
```

表 66. APPN ポートとリンク・ステーションの追加

```
lsadirect APPN config>ADD/UPDATE PORT
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(M)PC, (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P  [ ]? t
Interface number(Default 0): [0]? 4          1
Port name (Max 8 characters) [T00004]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
        Support multiple PU (Y)es (N)o [N]?
        Service any node: (Y)es (N)o [Y]?
        High performance routing: (Y)es (N)o [N]?
        Maximum BTU size (768-17745) [2048]?
        Maximum number of link stations (1-65535) [65535]?
        Percent of link stations reserved for incoming calls (0-100) [0]?
        Percent of link stations reserved for outgoing calls (0-100) [0]?
        Local SAP address (04-EC) [4]?
        Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
lsadirect APPN config>
lsadirect APPN config>
lsadirect APPN config>
lsadirect APPN config>
lsadirect APPN config>ADD/UPDATE LINK-STATION
APPN Station
Port name for the link station [ ]? T00004
Station name (Max 8 characters) [ ]? tnpub1
        Activate link automatically (Y)es (N)o [Y]?
        MAC address of adjacent node [000000000000]? 40002216000A
        Solicit SSCP Session: (Y)es (N)o [N]? y
                Local Node ID (5 hex digits) [00000]? 221B1
                Enable Host Initiated Dynamic LU Definition : (Y)es (N)o [N]?
        Does link support APPN function: (Y)es (N)o [Y]? n
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
```

1. 225ページの表64 に示されているように、LSA ループバック・インターフェース番号です。

表 67. TN3270E の定義

```
lsadirect APPN config>TN3270E
lsadirect TN3270E config>SET
TN3270E Server Parameters
        Enable TN3270E Server (Y/N) [Y]?
        TN3270E Server IP Address [9.24.104.203]?
        Port Number [23]?
        Enable Client Address Mapping (Y/N) [N]?
        Default Pool name (Max 8 characters) [PUBLIC]?
        NetDisp Advisor Port Number [10008]?
        Keepalive type:
         0 = none,
         1 = Timing Mark,
         2 = NOP [0]?
        Automatic Logoff (Y/N) [N]?
        Enable IP Precedence (Y/N) [N]?
Write this record? [Y]?
The record has been written.
lsadirect TN3270E config>ADD/UPDATE IMPLICIT-POOL
TN3270E Server Implicit Definitions
        Pool name (Max 8 characters) []?
        Station name (Max 8 characters) []?
Invalid name please re-enter
        Station name (Max 8 characters) []? tnpub1
        LU Name Mask (Max 5 characters) [@01LU]?
        LU Type  ( 1 - 3270 mod 2 display
                   2 - 3270 mod 3 display
                   3 - 3270 mod 4 display
                   4 - 3270 mod 5 display) [1]?
        Specify LU Address Ranges(s) (y/n) [N]?
        Number of Implicit LUs in Pool(1-253) [1]? 5
Write this record? [Y]?
```

構成の監視

この構成は、221ページの『DLSw を介する TN3270E SNA サブエリア構成の監視』に示されている場合に似たコマンドを使用して監視できます。表示されている結果も似ています。

第14章 チャネル・ゲートウェイ

概説

ネットワーク・ユーティリティーには、ESCON チャネルまたはパラレル・チャネルによるホスト接続性が備えられています。したがって、ネットワーク・ユーティリティーは、ホストから他のネットワークへのゲートウェイとして機能することができます。

サポートされる構成

ホスト・ソフトウェアからネットワーク・ユーティリティーへのインターフェースは、3 つあります。

最初のインターフェースは、8232 互換サポートで、LAN チャネル・ステーション (LCS) と呼ばれています。このインターフェースでは、直接 LAN 接続およびブロック化/非ブロック化構造用の多数のコマンドを定義します。LAN レディー・フレームは、ホストからバーチャル LAN アダプターに送信され、その逆にも送信されます。このインターフェースは、TCP/IP (VM および MVS 版、AIX/370 版) によって使用されます。

2 番目のインターフェースは、リンク・サービス体系 (LSA) サポートで、これにはホスト内で VTAM を介してアクセスします。

LSA サポートは、VTAM が SNA スタックのデータ・リンク制御 (DLC) レイヤーの論理リンク制御 (LLC) 部分を使用できるようにするための、制御インターフェースです。LLC タイプ 1 (コネクションレス型) および LLC タイプ 2 (コネクション型) データ・トランスポートへのアクセスが組み込まれています。このインターフェースは、VTAM によって、SNA サブエリアと APPN ISR および HPR の両データ・トランスポート用として使用されます。

3 番目のインターフェースは、マルチパス・チャネル (MPC+) サポートで、これにはホスト内で VTAM を介してアクセスします。MPC+ サポートは、複数の読み取りおよび書き込みサブチャネルが、ホストとチャネル接続装置の間の単一の伝送グループとして扱えるようにするプロトコル・レイヤーです。このインターフェースは、OS/390 によって、APPN HPR、TCP/IP、および HPDT UDP データ・トランスポート用として使用されます。このチャネルでは、複数の物理チャネル・インターフェースにわたって共用される MPC+ サブチャネルは、サポートしないことに注意してください。

ネットワーク・ユーティリティーでは、64 の ESCON サブチャネルをサポートでき、LCS サブチャネル・ペア、LSA サブチャネル、MPC+ グループは、どのような組み合わせでも構いません。したがって、最大 32 の LCS バーチャル LAN アダプター、32 の LSA バーチャル LAN アダプター、または 32 の MPC+ グループ (1 つの MPC+ グループには、少なくとも 1 つの読み取りサブチャネルと 1 つの書き込みサブチャネルが組み込まれている必要があります) が可能です。

LSA および LCS バーチャル LAN アダプターでは、ホストとの通信用として、トークンリング・インターフェース、FDDI インターフェース、またはイーサネット・インターフェースをエミュレートします。だからといって、リモート・ネットワーク・インターフェースのフォーマットが制限されるわけではありません。ただ、 3172 相互接続制御プログラムの既存のホスト・インターフェースを維持して、ホスト・サポート変更を不要にすることだけが意図されているに過ぎません。

各バーチャル LAN アダプターまたは MPC+ グループでは、それぞれ 1 つのホスト接続タイプ (LCS/LSA/MPC+) しかサポートできません。LSA および LCS サブチャネルでは、複数のバーチャル LAN アダプター (例えば、1 つのトークンリング・インターフェースと 1 つのイーサネット・インターフェース) がサポートできます。単一のサブチャネルまたはペア上における同一タイプの複数のバーチャル LAN アダプターのサポートに、認知されている値はありませんが、構成がそれをあらかじめ排除することはありません。

ホスト LAN ゲートウェイ機能

ホスト LAN ゲートウェイ機能によって、ホスト・アプリケーションで LAN ベースのワークステーションと通信することができます。ホスト LAN ゲートウェイ機能によってサポートされるホスト・アプリケーションには、2 つの主要なものとして、TCP/IP と VTAM があります。これらのアプリケーションでは、チャネルを通してトランスポートするために、LAN フレームをカプセル化して、チャネル制御ワード (CCW) にします。これは、「ブロック化」とも呼ばれています。CCW は、単一の論理単位として送信される LAN フレームのブロックで構成されるからです。CCW は、後で、受信側で「非ブロック化」されて個々のフレームになります。

ネットワーク・ユーティリティーの LAN ゲートウェイ機能の多くの基になっているのは、 3172 相互接続制御プログラム (ICP) です。3172 ICP ゲートウェイ機能とネットワーク・ユーティリティー・チャネル機能には、確かに違いがありますが、ホストとネットワーク・ユーティリティー・チャネルの間のハードウェア・インターフェースおよびソフトウェア・インターフェースは、ホストと 3172 ICP の間のインターフェースと同じです (ただし、ネットワーク・ユーティリティー内で提供される IP ルーティング・サポートを除く)。ソフトウェア・インターフェースを保持するためには、ネットワーク・ユーティリティーが LAN アダプターの外観を作成して、ホスト・アプリケーションに実 LAN と通信しているものと思い込ませておく必要があります。

ESCON チャネルの概念

サブチャネル

ESCON チャネル・インターフェースは、256 の論理アドレスに分割されています (「サブチャネル」という呼び方は、正確ではありませんが、従来からの行きがかり上、そう呼びならわされています)。各ホスト・アプリケーション・インターフェースでは、それぞれ 1 つまたは複数のサブチャネルを使用して、ホスト・アプリケーションをネットワーク・ユーティリティーに接続します。構成時には、各サブチャネルには、それぞれ固有の相対索引が割り当てられます。これはその論理アドレスに一致してもしなくても構いません。ESCON チャネルは、複数のホスト上の複数のアプリケーションによって共用される場合もありますが、各ホスト・アプリケーショ

ンでは、それぞれそのサブチャネルを専用します (このことは、後で説明するように、MPC+ には厳密には該当しませんが、 MPC+ レベルについては該当します。MPC+ サブチャネルは、非 MPC+ アプリケーションとは共用できません)。ネットワーク・ユーティリティーでは、同時に最大 64 のサブチャネルをサポートします。

チャネル・プロトコル

ネットワーク・ユーティリティーでは、上述の 3 つのホスト・ソフトウェア・インターフェースに対応する、 3 つのチャネル・プロトコルをサポートします。各プロトコルでは、それぞれそのサブチャネルの使用のしかたが異なり、1 つのサブチャネルでは一度に 1 つしかプロトコルをサポートできません。サポートされるチャネル・プロトコルは、 LAN チャネル・ステーション (LCS)、リンク・サービス体系 (LSA)、およびマルチパス・チャネル (MPC+) です。

LAN チャネル・ステーション (LCS): LCS は、ホスト内の TCP/IP アプリケーションでサポートされるチャネル・プロトコルです。各アプリケーションが、それぞれ連続するサブチャネル・ペア (1 つはチャネルから読み取るための TCP/IP 用、1 つはチャネルに書き込むための TCP/IP 用) を定義します。LCS インターフェースによって、チャネルを通して LAN MAC フレームをトランスポートすることが可能になり、 LAN インターフェースの起動、停止、および照会を行うためのコマンド・インターフェースが得られます。各 MAC フレームには、それぞれそのフレームのバーチャル LAN アダプターあて先を識別するヘッダーがあります。

リンク・サービス体系 (LSA): LSA は、チャネルを通る SNA トラフィックをサポートするためのインターフェースです。各 LSA パスは、それぞれがホスト・アプリケーションとネットワーク・ユーティリティーの間の両方向サブチャネルです。ホスト・ソフトウェア (VTAM) では、それぞれの書き込みコマンドの直後に、チャネルからデータを検索するための読み取りコマンドを発行します。ネットワーク・ユーティリティーでは、ホスト・アプリケーションが読み取るものがある場合は、Attention コマンドも発行します。LSA にはコマンド・インターフェースがあり、これによって、VTAM では、サービス・アクセス・ポイント (SAP) をオープンして、IEEE 802.2 論理リンク制御 (LLC) インターフェースを使用して、ダウンストリーム・ワークステーションと通信することができます。LSA サブチャネルのチャネル・ブロック化/非ブロック化機構は、LCS サブチャネル・ペアの場合と同じです。

マルチパス・チャネル (MPC+): MPC+ は、チャネル用のデータ・リンク制御 (DLC) インターフェースです。各 MPC+ パスは、それぞれ 1 つまたは複数の読み取りサブチャネルと、1 つまたは複数の書き込みサブチャネルの結合によって形成された 1 つの伝送グループで構成されます。複数の物理 ESCON チャネルにまたがる MPC+ 伝送グループについては、今回のリリースではサポートしていません。VTAM とネットワーク・ユーティリティーは、初期化時にサブチャネルの数および方向を識別するために、 XID を交換するので、各フレームには、それぞれ送信および受信アプリケーションを識別するためのヘッダーが付きます。

ブロック: ホスト・チャネル・インターフェースでは、制御フレームおよびデータ・フレームを、最大 32 KB (MPC+ の場合は、36 KB) のブロックにパッケージします。データ・ブロックのフォーマットは、MPC+ と非 MPC+ のホスト・アプリケーションでは異なっています。LSA および LCS ブロックは、1 つまたは複数の連続するフレームで構成され、それぞれのフレームには、その LAN タイプおよび LAN 番号であて先装置を識別するヘッダーが付いています。MPC+ ブロックには、1 つまたは複

数の「連続しない」フレームが含まれ、ブロックの最初の 4 KB には MPC+ PDU ヘッダー、およびブロックの最後の 32 KB に保管されているアプリケーション・データのオフセットが入っています。MPC+ グループは、インプリメンテーションの整合性を確保するためにも、「LAN タイプ」および「LAN 番号」で識別されます。

データのブロックが送信されるのは、データでいっぱいになったときか、ブロックの遅延タイマー (ブロックがデータでいっぱいになるのを送信前にアダプターが待つ時間が、これによって決まります) が満了したときかどちらかです。データのブロックを受信し、個々のフレームをデバイス・ドライバーに転送するプロセスが、「非ブロック化」と呼ばれています。

バーチャル LAN アダプター: まず、これまでの歩みを振り返って見ると、3172 相互接続制御プログラム (ネットワーク・ユーティリティーは部分的にこれを基にしています) では、フレームをホスト・チャネルから 1 つまたは複数の LAN に転送していました。この構成では、各サブチャネルは、それぞれ 1 つまたは複数のデバイス・ドライバーに接続されていました。ホストからのデータは、非ブロック化プログラムが受信し、これがフレーム・ヘッダーに入っている LAN タイプおよび LAN 番号に応じて、 LAN アダプターのいずれか 1 つにフレームを配布していました。ホスト・アプリケーションが複数の LAN アダプターにアクセスする必要がある場合は、構成ファイルに、それぞれの LAN アダプターごとに 1 つずつ項目を入れました。

ネットワーク・ユーティリティーでは、各サブチャネルをそれぞれ 1 つまたは複数の LAN アダプターに接続するのではなく、サブチャネルをすべて基本ネット・ハンドラーに接続し、これを 1 つまたは複数のバーチャル・ネット・ハンドラーに接続します。それぞれのバーチャル・ネット・ハンドラーでは、3 つのチャネル・プロトコルのいずれか 1 つ (LSA/LCS/MPC+) をサポートし、プロトコル・アプリケーションのいずれか 1 つ (LLC/IP/APPN) でフレームを送受信し、これがネットワーク接続を表す別のネット・ハンドラーにデータを送信します。実 LAN アダプターは、ネットワーク・ユーティリティーに接続されていてもいなくても構いません。

既存のホスト・インターフェースを保持するために、ネットワーク・ユーティリティーは、LSA および LCS 接続用の複数の LAN アダプターの外観を呈します。構成パラメーターに応じて、バーチャル・ネット・ハンドラーは、該当するプロトコルにトークンリング・アダプター、イーサネット・アダプター、 FDDI アダプターのいずれかとして登録します。基本ネット・ハンドラーによって、ホストでは、3172 の実 LAN アダプターを制御する場合と同様にして、「バーチャル LAN アダプター」の起動および停止を行うことができます。それぞれのバーチャル LAN アダプターには独自の MAC アドレスがあるので、ネットワーク・ユーティリティーがホストには、実際のローカル・エリア・ネットワーク上の 1 つまたは複数の LAN アダプターに見えます。

単一のサブチャネル (またはペア) が、1 つまたは複数のバーチャル LAN アダプターに接続できます。このことは、単一のホスト・アプリケーションが、同じサブチャネルでタイプの異なる LAN (トークンリング、イーサネット、FDDI) と通信できるようにする場合に必要です。 LAN 向けのフレームは、フレーム・ヘッダー内の LAN タイプおよび LAN 番号によって、正しいあて先に送信されます。

ただし、この逆が言えるのは LSA 接続の場合だけです。単一の LCS バーチャル LAN アダプターは、 1 つのサブチャネルにしか接続できません。この制限があるため、ホスト向けのフレームは、バーチャル・ネット・ハンドラーによって、それぞ

れのホスト向けのフレームごとに、MAC アドレスまたは IP アドレスを強制的に調べなくても、正しいサブチャネルに送信できるようにすることによって、データ・スループットが向上することになりました。複数の VTAM では、それぞれが固有の番号の SAP をオープンする場合は、単一の LSA ネット・ハンドラーを共用することができます。LCS ネット・ハンドラーの場合は、これはできません。すべての TCP/IP トラフィックでマルチプロトコル SAP 番号 'AA'x が使用されるからです。図28 を参照してください。

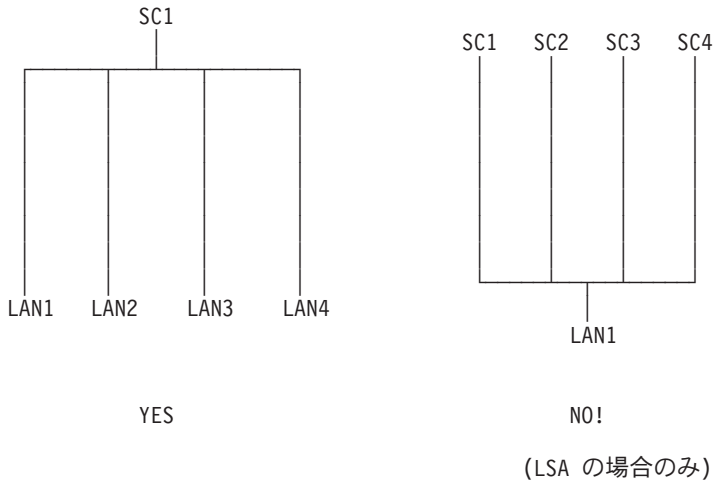


図 28. LAN - サブチャネル間構成

MPC+ グループ: MPC+ では、LSA インターフェースと LCS インターフェースの両方に共通のバーチャル LAN アダプターの概念を使用しません。MPC+ では、ネットワーク・ユーティリティーの LAN ゲートウェイ外観をサポートしないからです。MPC+ の場合の等価インターフェースは、MPC+ グループです。 MPC+ グループは、ホストとネットワーク・ユーティリティーの間で、単一のデータ・パイプの役割を務めるように構成された、一組の ESCON サブチャネルです。 MPC+ グループは、少なくとも 1 つの「読み取り」サブチャネルと、少なくとも 1 つの「書き込み」サブチャネルで構成されます。読み取りまたは書き込みとして指定できるサブチャネルの数は任意であり、複数の MPC+ グループを定義することもできますが、1 台のネットワーク・ユーティリティーにつき合計サブチャネル数が最大 64 という条件が付きます。

データは、MPC+ グループ内のアクティブ・サブチャネルのいずれかまたはすべてを通して送信することができます。グループ上でのデータ順序の維持は、 MPC+ エンドポイントが行います。サブチャネルの数は、MPC+ グループの定義時に固定されます。

MPC+ グループは、バーチャル LAN アダプターの場合と同じ「LAN タイプ」および「LAN 番号」を使用して、マイクロコード内で識別されます。フレームがマイクロコードによって非ブロック化されると、それぞれのフレームには、MPC+ の「LAN タイプ」、およびその受信が行われたサブチャネルに関連する MPC+ グループに対応する「LAN 番号」が与えられます。したがって、マイクロコードおよびネット・ハンドラーでは、LSA フレームおよび LCS フレームの場合と整合性のある方法で、MPC+ フレームを処理することができます。

LLC ループバック: LLC ループバックとは、ネットワーク・ユーティリティー内の APPN 機能および DLSw 機能との VTAM 接続を可能にするための、バーチャル LAN アダプター概念の拡張です。 SNA 接続を確立するために、LSA インターフェースでは、IEEE 802.2 フレームを使用して、それ自体とリモート装置の間に、LANを隔ててLLC 接続を作成します。 図29 を参照してください。

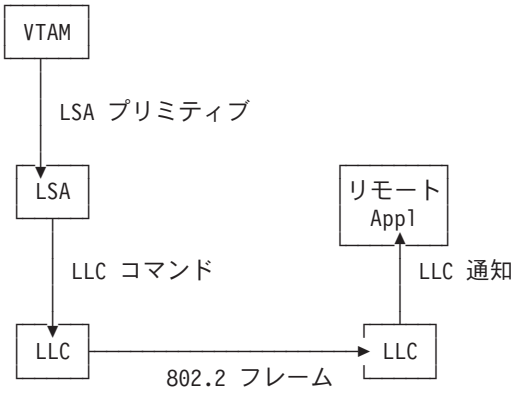


図 29. 通常の LLC 接続

LLC ループバックによって、ネットワーク・ユーティリティーは、ネットワーク・ユーティリティー内の他の LLC ユーザー (APPN および DLSw) と直接通信することができます。LSA からの LLC コマンドは、 802.2 フレームに変えるのではなく、LLC 通知に変換され、該当する LLC ユーザーに送信されます。図30 を参照してください。

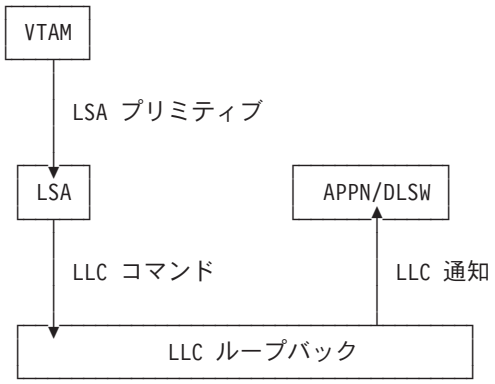


図 30. LLC ループバック接続

LLC ループバックによって、ネットワーク・ユーティリティー内の APPN ネットワーク・ノードは、VTAM への隣接ノードとしての役割を務めることができます。また、VTAM は、データ・リンク交換を使用してリモートの装置およびアプリケーションに接続することができ、VTAM の LSA サポートを変更する必要はありません。ループバック接続は、VTAM には通常の LLC 接続と同じものに見えるからです。

構成例

ここでは、ネットワーク・ユーティリティーをメインフレーム・システムへのチャネル・ゲートウェイとして使用する、4 つのサンプル構成について説明します このうち 3 つのサンプルでは、 ESCON チャネル構成を示し、1 つのサンプルでは、パラレル・チャネル構成を示しています。 これらの構成は、次のとおりです。

- ESCON チャネル・ゲートウェイ (SNA および IP)
- パラレル・チャネル・ゲートウェイ (SNA および IP)
- ESCON チャネル・ゲートウェイ (APPN および IP)
- ESCON チャネル・ゲートウェイ - 高可用性

これらの構成はすべて、ネットワーク・ユーティリティー・モデル TN1 と TX1 のどちらを使用しても作成することができます。同じマシン内に TN3270E サーバー機能を構成する計画でない限り、モデル TN1 で提供される余分な機能は必要ありません。

ESCON チャネル・ゲートウェイ

この事例は、図31 に図示してあります。ネットワーク・ユーティリティーは、リモート・サイトからとメイン・サイトの LAN セグメントからのホストへの SNA トラフィックと IP トラフィックの両方をサポートするように構成されています ESCON チャネル・アダプターは、SNA トラフィックをトランスポートするための LSA 直接インターフェースと、IP 転送を実行するための LCS インターフェースを備えるように構成されています。

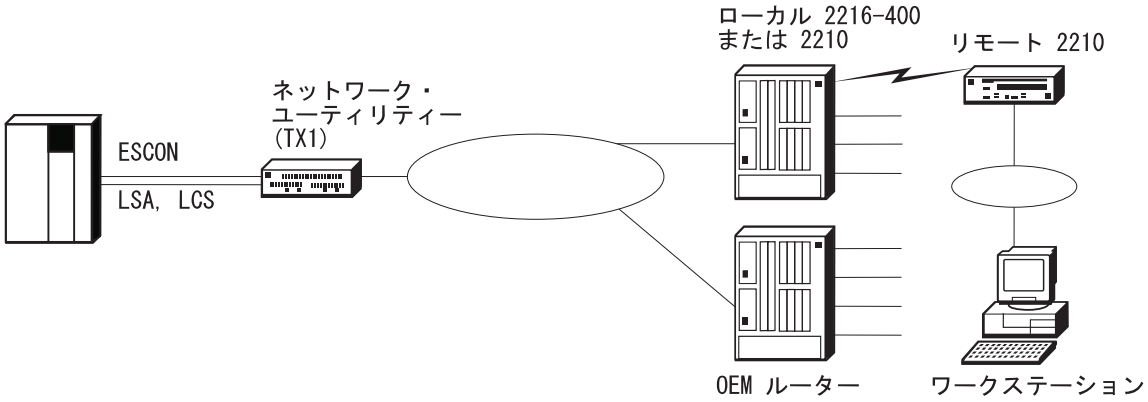


図 31. ESCON チャネル・ゲートウェイ

構成のかぎ

LCS インターフェースと LSA インターフェースの両方に関するサブチャネル定義は、ホスト内でホスト・チャネル・サブシステムに対してネットワーク・ユーティリティーを定義する場合に使用されるパラメーターに一致する必要がありますネットワーク・ユーティリティーで構成する主要なサブチャネル・パラメーターは、236 ページの表68 に示してあります。

表 68. ネットワーク・ユーティリティー・サブチャネル構成パラメーター

コマンド	説明
device	ネットワーク・ユーティリティーを選択するためにチャネル・パス上を送信される装置アドレス S/370 入出力体系内のサブチャネル番号とも呼ばれます。 2 桁の 16 進値で、範囲は 00 ～ FF です。この値は、実装置に関する CNTLUNIT マクロ命令の UNITADD ステートメントによって、入出力構成プログラム (IOCP) 内で定義されます。 **有効な値 :** X'00' ～ X'FF' **デフォルト値 :** なし
cu	ホスト内でネットワーク・ユーティリティーに関して定義される制御装置アドレス。 この値は、CNTLUNIT マクロ命令の CUADD ステートメントによって、ホスト IOCP 内で定義されます。 **有効な値 :** X'0' ～ X'F' **デフォルト値 :** X'0'
link	このパラメーターが有効なのは、IBM 9032 ESCON ディレクター (ESCD) がネットワーク・ユーティリティーとホストの間に使用されている場合です ESCD が使用されている場合は、リンク・アドレスは、ホスト が接続される ESCON ディレクター (ESCD) のポート番号です。 パス内に ESCD が 2 つある場合は、動的接続によって定義されている ESCD のホスト側ポート番号です。ESCD が通信パス内にない場合は、この値は X'01' に設定される必要があります。 **有効な値 :** X'01' ～ X'FE' **デフォルト値 :** X'01'
lpar	論理区画番号。これによって、複数の論理ホスト区画が 1 つの ESCON ファイバーを共用できます。 この値は、RESOURCE マクロ命令によってホスト IOCP 内で定義されます。 ホストが ESCON 複数イメージ機能 (EMIF) を使用していない場合は、デフォルト値の 0 が LPAR 番号として使用されます。 **有効な値 :** X'0' ～ X'F' **デフォルト値 :** X'0'

LPAR および CU パラメーター: ネットワーク・ユーティリティー上で LSA、LCS、または MPC+ インターフェースを定義するときは、 CU および LPAR パラメーターに正しい値を指定する必要があります

CU パラメーターに関する注:

CU の値を設定する必要があるのは、複数の LPAR、またはネットワーク・ユーティリティーにアクセスする必要がある複数の MVS や OS/390 イメージがある場合です。その場合は、それぞれの LPAR ごとにインターフェース定義 (LSA、 LCS、または MPC+) を作成する必要があり、それぞれが CU パラメーターとして異なる値を使用することになります。

さらに、CU パラメーターの値は、 IOCP 定義の CNTLUNIT マクロ内の CUADD パラメーターに一致する必要があります。

以前は、新しい LPAR (区画) が構成されたら、それと共に必ず固有の番号が構成される必要がありました。しかし、PTF01 以降、CU 番号と LPAR は、ESCON では相互に独立しています。したがって、LPAR 番号ごとに固有の CU 番号が必要ということはなくなりました。これによって、ユーザーの構成の柔軟性が増し、大規模ホスト・システムでの操作が単純化されました。

LPAR パラメーターに関する注:

まず重要なのは、ホストが複数の論理区画 (LPAR) に分割されているかどうかということです。分割されていないければ、LPAR パラメーターはゼロです。

分割されている場合は、それぞれの区画を名前で指定し、それぞれに数値を割り当てる、ホストの入出力構成プログラム (IOCP) 定義内に RESOURCE マクロが必要です。この数値は、ネットワーク・ユーティリティーの構成時に LPAR パラメーターに使用されます

2 番目に問題になるのは、チャネル・パス識別子 (CHPID) が 1 つまたは複数の LPAR 間で共用されるかどうかということです[19]。

共用チャネルを使用しない (または、EMIF がない) 場合は、 LPAR パラメーターの値は 0 になります。

ESCON アダプターごとの LPAR の最大数は、32 から 64 に増えました。これをサポートするために、アダプター 1 つにつき、サブチャネルの最大数を 32 から 64 に増やし、アダプター 1 つにつき、バーチャル・ネットワークの最大数を 16 から

19. LPAR 間でチャネルを共用する場合は、EMIF が必要です。

32 に増やしました。したがって、LSA ユーザーが 32 を超える LPAR を構成する必要がある場合は、これが利点になります。

図32 には、ホストは区画に分割されているが、チャネル・パスは LPAR 間で共用されていない例が示してあります。

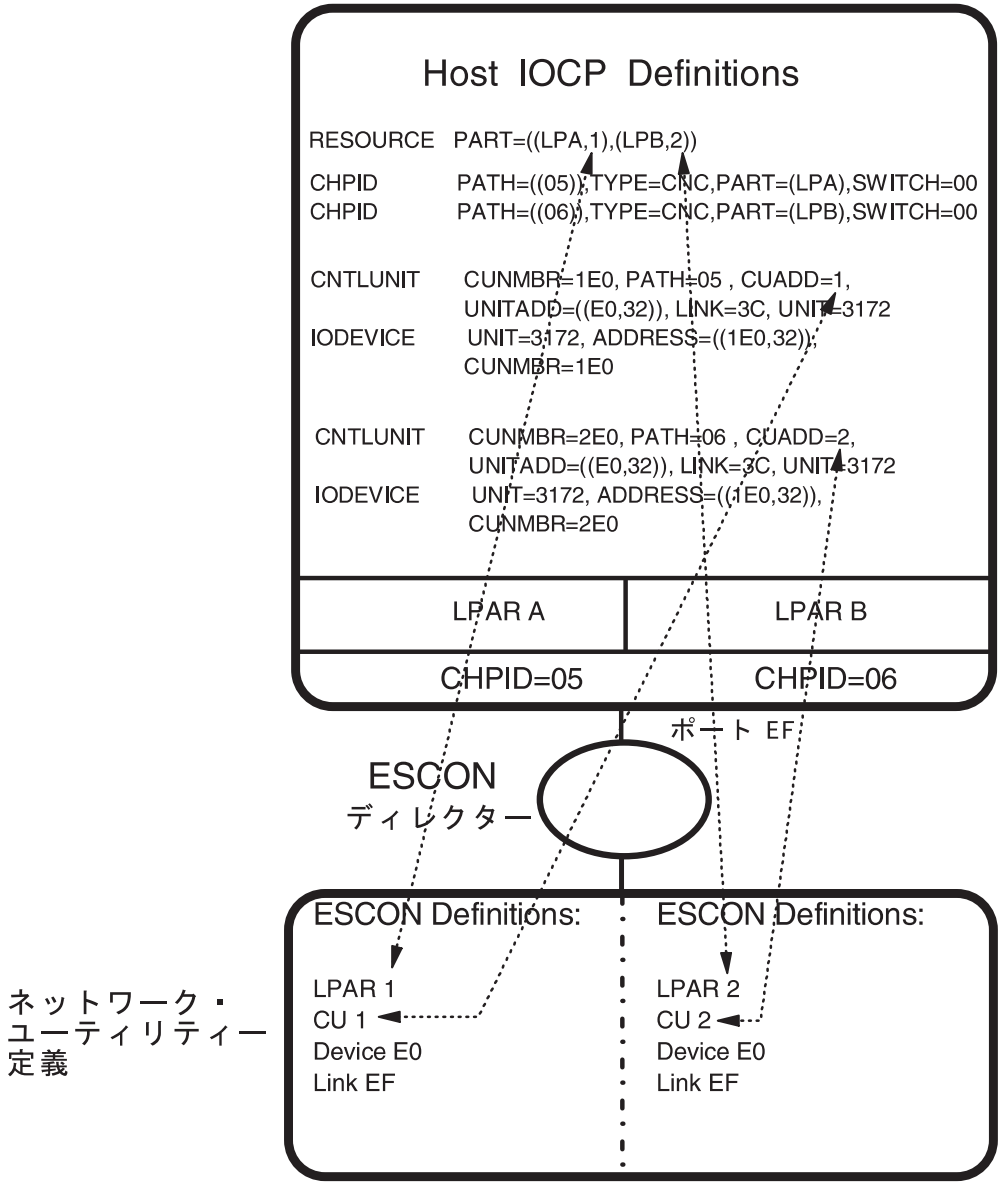


図 32. ホスト/ネットワーク・ユーティリティー間のパラメーターの関係 (非共用 CHPID)

ホスト上で EMIF を使用している場合は、複数の LPAR でネットワーク・ユーティリティーへの同一 CHPID を共用することができます。この場合は、やはりネットワーク・ユーティリティー上に 2 つのインターフェースが定義されている必要があり、それぞれに CU パラメーターとして異なる値が指定されることになります。その他のパラメーターは同じ値を使用できます。239ページの図33 には、ホストが区画に分割

され、両方の区画で同じ CHPID を使用できるように、 EMIF が使用されている例が示してあります。

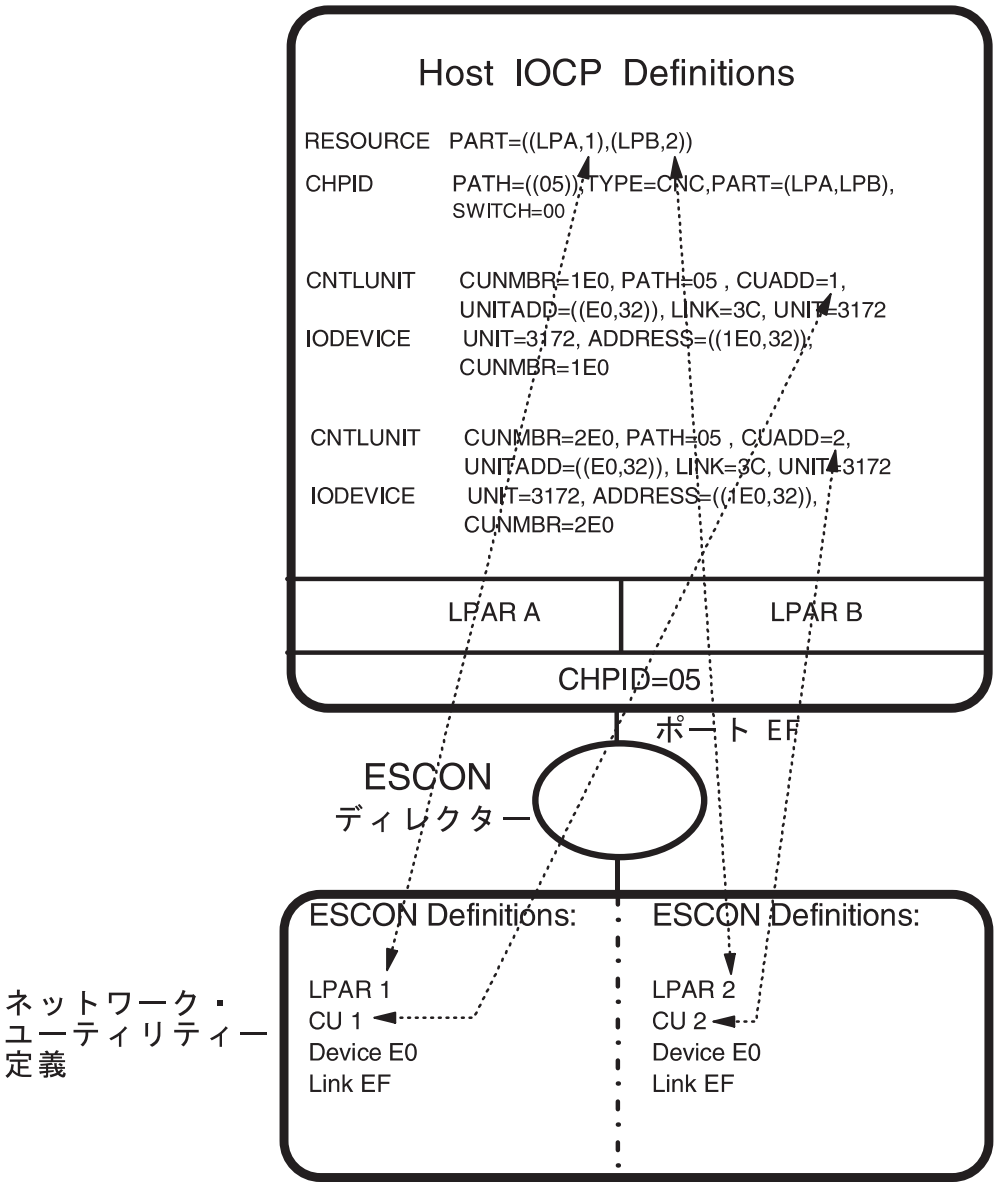


図 33. ホスト/ネットワーク・ユーティリティー間のパラメーターの関係 (共用 チャネル)

LSA 直接インターフェース: 240ページの図34 には、ネットワーク・ユーティリティーに関する構成パラメーターが、 LSA インターフェース定義に関するホスト・パラメーターとどのように相関するかが示してあります

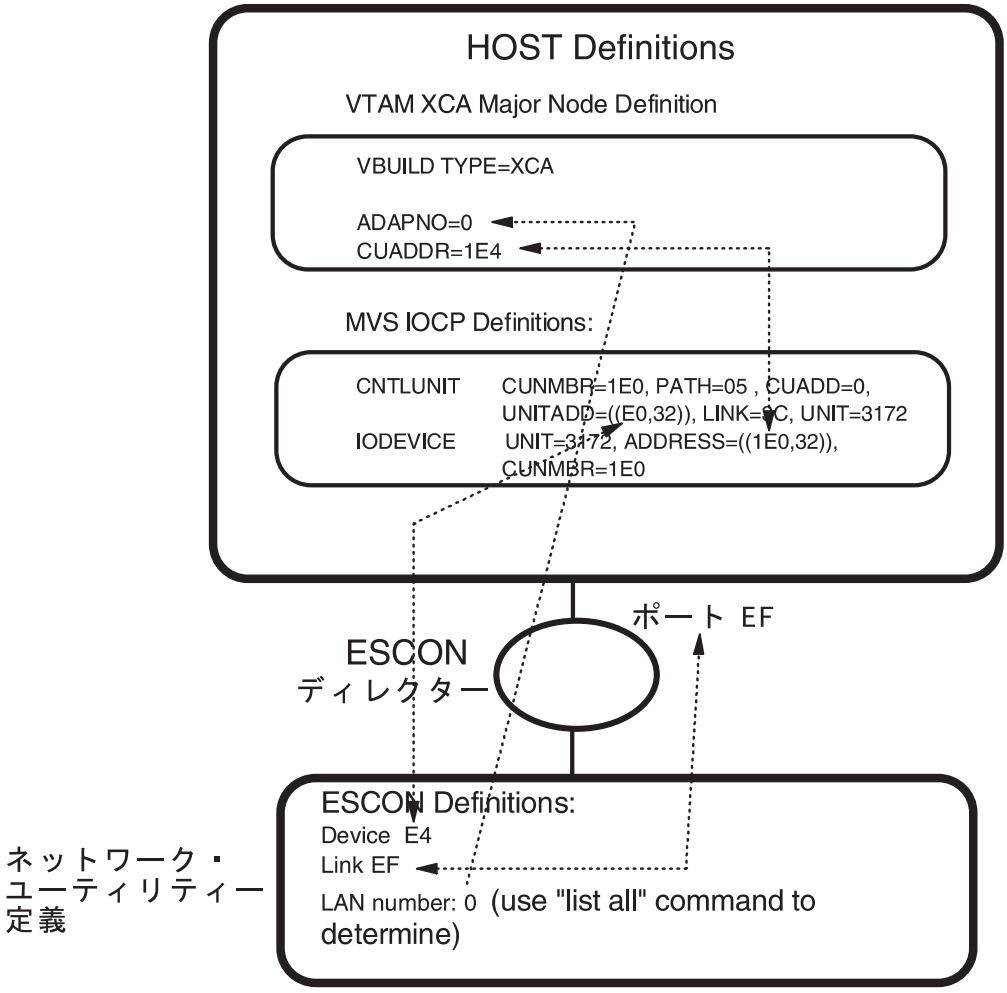


図 34. ホスト/ネットワーク・ユーティリティー間のパラメーターの関係 - LSA

注:

1. LSA では、ホストとネットワーク・ユーティリティーの間で単一の両方向サブチャネルを使用します。VTAM では、それぞれの書き込みコマンドの直後に、チャネルからデータを検索するための読み取りコマンドを発行します。
2. ネットワーク・ユーティリティーの LSA インターフェース定義内で指定される装置アドレスは、 IOCP の CNTLUNIT マクロ内の UNITADD パラメーターで指定されている範囲内であることが必要です。例えば、図34 の UNITADD パラメーターには、E0 (16 進数) から始まる 32 (10 進数) の装置アドレスがネットワーク・ユーティリティー定義用として予約されていることが示されています。装置アドレス E4 がネットワーク・ユーティリティーの LSA インターフェースに指定されています。E4 は 16 進数の E0 ～ FF の範囲内にあるので、他の装置 (または、このネットワーク・ユーティリティー上のインターフェース) がそのサブチャネルの使用を試みない限り、これは OK です
3. VTAM XCA 大ノード定義内の CUADDR パラメーター内で指定される値は、IOCP の IODEVICE マクロ内の ADDRESS パラメーターで指定されている範囲内にあることが必要です。例えば、図34 の XCA 大ノード定義内の CUADDR パラメーターは、16 進数 1E4 であり、IODEVICE ステートメント内の ADDRESS パラメーターが指定している 1E0 ～ 1FF の範囲内です。

4. IODEVICE マクロ内の ADDRESS パラメーター、および CNTLUNIT マクロ内の UNITADD パラメーターに指定されている値は、***規則のみによって*** 関連付けられています。この例では、ADDRESS パラメーターの値は、***論理チャネル識別子*** (この場合は 1) を、 UNITADD 値の前に付加することによって、UNITADD パラメーターの値から決められています。これに該当する場合はしばしばあります。ただし、ネットワーク・ユーティリティーの LSA 定義上で装置アドレスを定義する場合は、ADDRESS パラメーターではなく、UNITADD パラメーターを使用して、値の有効範囲を決めます
5. ネットワーク・ユーティリティー上に LSA 直接インターフェースを定義する場合は、そのインターフェースをネットワーク・ユーティリティー上の LAN インターフェースの 1 つに対応付けます。実際、こうして LSA 直接インターフェースがこの同じ LAN セグメント上に置かれます。あて先アドレスがこの LAN セグメント上のネットワーク・ユーティリティー・アダプターの MAC アドレスであるフレームは、すべてホストへのチャネルを通って自動的に転送されます。

このインターフェース・タイプに関するホスト定義の詳細な説明およびサンプルについては、295ページの『第18章 サンプル・ホスト定義』を参照してください。

この事例で必要な構成パラメーターを詳しく検討したい場合は、 174ページの表17 をごらんください。

LCS インターフェース: LCS インターフェースを定義すると、ネットワーク・ユーティリティー内にバーチャル LAN が作成されます。この LAN 上には、2 つの IP ステーション、つまり、ネットワーク・ユーティリティーとホストがあります。この LAN は、ネットワーク内で固有の IP サブネットであることが必要です。LCS インターフェースに MAC アドレスも必要です。LCS インターフェースを作成したら、このインターフェースに IP アドレスを割り当てることを忘れないようにします。

ネットワーク・ユーティリティーには、LCS インターフェースを操作する方法が、次のように 3 つ用意されています。

1. LCS ルーティング

   上記で説明し、構成例に記載されている LCS サポートは、MAS V1R1.1 でリリースされた初期 2216 LCS サポートです。このタイプの LCS サポートでは、ホスト IP トラフィックをネットワーク・ユーティリティー内の IP ルーティング機能に渡します。このタイプの LCS サポートを用いて構成したネットワーク・ユーティリティーで 3172 を置き換える場合は、ネットワーク・ユーティリティーの内部にバーチャル LAN セグメント用の追加の IP サブネットを構成する必要があります。
2. LCS ブリッジング

   MAS V3.2 では、ネットワークの IP トポロジーに変更を加えなくても、3172 の置き換えができるようにするため、「LCS ブリッジング」 (公式には「TCP/IP パススルー」と呼ぶ) を導入しています。このモードでは、ネットワーク・ユーティリティーは単に、LCS ブリッジ・ポートと他の構成済みブリッジ・ポートの間で、IP トラフィックをブリッジするだけです。フレームはポートからポートへと転送されるので、IP ルーティングは実行されません。このモードを使用可能にする場合は、LCS インターフェースに対して IP アドレスを指定するのではなく、MAC

アドレスを定義して、その上でのブリッジングを使用可能にします。この機能の構成について詳しくは、MAS V3.2 *ソフトウェア使用者の手引き* を参照してください。

3. LCS 3172 エミュレーション

   MAS V3.2 PTF01 によって、「3172 エミュレーション」と呼ぶことができる、3番目のタイプの LCS サポートが使用可能になりました。この LCS モードには、LCS バーチャル・インターフェースを単一の LAN インターフェースにマップすることによって、 3172 の振る舞いが正確に反映されています。複数のパスがさまざまなブリッジ使用可能インターフェース間に存在している LCS ブリッジングの場合とは異なり、 LCS パススルーでは、特定のサブチャネルと特定の LAN アダプターの間に、独立した固定パスがセットアップされます。1 つのパス上のトラフィックは、他のどこでも見ることはできません。このモードを使用可能にする場合は、3172 エミュレーションをこのモード用として使用可能にし、IP アドレスは指定しないで、LCS の定義時に ″NET″ パラメーターを使用することによって、LCS MAC アドレスを定義するのではなく、特定の LAN アダプターを参照します。こうすることによって、接続する LAN の LAN タイプと MAC アドレスをピックアップします。

このチャネル・ゲートウェイ機能によって、ネットワーク・ユーティリティーは、TCP/IP ネットワーク内でドロップイン 3172 置換として機能できます。TCP/IP ホストから受信されたフレームは、ダウンストリーム LAN アダプターに直接渡され、ネットワーク・ユーティリティーの IP ルーター機能とブリッジング機能はバイパスされます。LCS パススルー機能に対応する LAN アダプターによって受信された IP フレームと ARP フレームは、 TCP/IP ホストへの送達のために LCS に直接渡されます。ネットワーク・ユーティリティーによる 3172 LCS 機能の置換は、以前の LCS 方式の場合とは異なり、IP ネットワーク・トポロジーの変更や追加のブリッジ・ホップの追加を必要としません。

V3.2 PTF01 以降、現在は構成されていない LPAR を使用して、新規 ESCON バーチャル・インターフェース (LSA、MPC +、または LCS) を動的に追加できます。以前は、動的追加ネットワークは、すでに構成済みの LPAR 上のサブチャネルを使用してしか構成できませんでした。新規 LPAR 論理パスをもつインターフェースの追加には、物理チャネル・インターフェース全体を使用不可にする必要がありました。この新規サポートを使用する場合は、スペア・インターフェースを構成し、『talk 6』を使用して新規バーチャル・インターフェースを追加し、『talk 5』を使用して新規ネットワークを起動します。

パラレル・チャネル・ゲートウェイ

この事例は、243ページの図35 に図示してあります。これは、ホストへの接続が、ESCON チャネル経由ではなく、S/370 バスおよびタグ (パラレル・チャネル) を経由している点を除けば、ESCON チャネル・ゲートウェイと同じです。 ESCON ゲートウェイの場合と同様、この構成でも、 LSA 直接接続を SNA トラフィック用として使用し、 LCS インターフェースを IP トラフィック用として使用します。

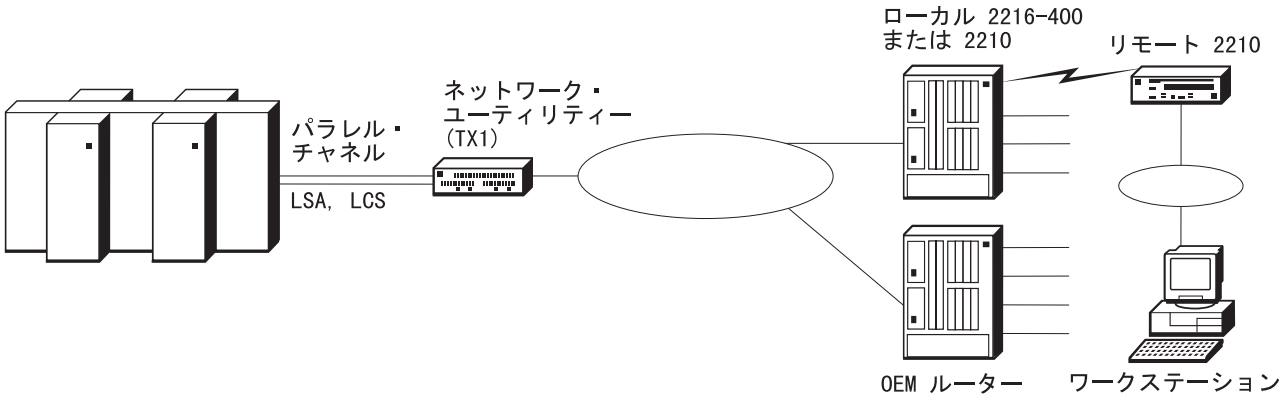


図 35. パラレル・チャネル・ゲートウェイ

構成のかぎ

この事例での構成は、ESCON ゲートウェイ (235ページの『ESCON チャネル・ゲートウェイ』を参照) の場合の構成と非常によく似ています。LSA および LCS インターフェースの構成の方が必要なパラメーターが少ないのは、LPAR、リンク・アドレス、制御装置の値が、バスおよびタグ接続ではいずれも必要ないからです。ただし、装置アドレスは、チャネル上でネットワーク・ユーティリティーを識別するためにやはり必要です

この事例で必要な構成パラメーターを詳しく検討したい場合は、 155ページの図8 をごらんください。また、295ページの『第18章 サンプル・ホスト定義』にも、パラレル・チャネル・アダプターを装着したネットワーク・ユーティリティーに関するホスト IOCP 定義のサンプルが記載されています。

チャネル・ゲートウェイ (MPC+ を介する APPN および IP)

この事例は、244ページの図36 に図示してあります。ここでは、マルチパス・チャネル (MPC+) グループを使用して、ネットワーク・ユーティリティーとホストの間で IP トラフィックと APPN トラフィックの両方をトランスポートします。 MPC+ では、ESCON サブチャネルのグループを使用して、データ転送パフォーマンスの最大化を図ります。

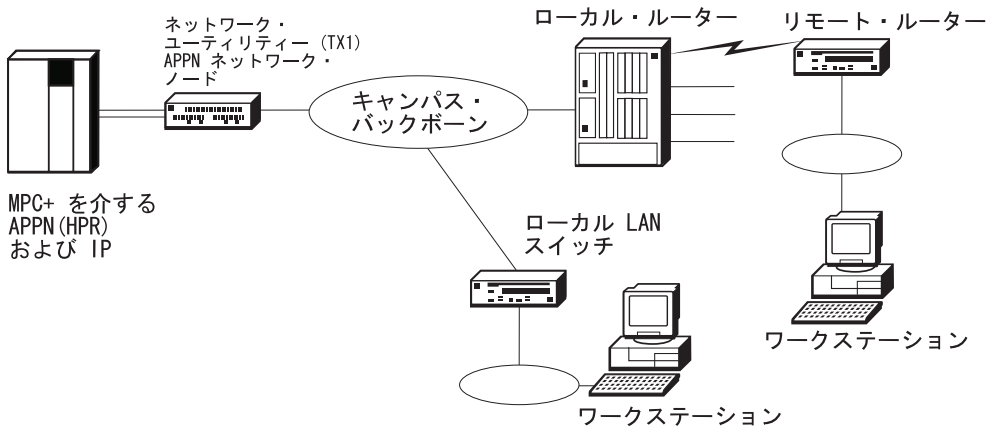


図 36. チャネル・ゲートウェイ (APPN および IP)

ネットワーク・ユーティリティーを通って着信する APPN トラフィックには、リモートの事業所のルーターからの幾つかの異なるタイプがあります

- ホストへの APPN 接続を用いて構成されている事業所の TN3270E サーバーからの TN3270 トラフィック (このタイプの構成の例については、161ページの『分散 TN3270E サーバー』を参照してください)
- PU 2.0 (従属) 装置に対するサポートを提供している事業所のルーターからの DLUR トラフィック
- 中央側のメインフレームと通信している分散プロセッサー (例えば、 AS/400 プロセッサーなど) からの APPN ホスト間トラフィック

上記のそれぞれの場合に、ネットワーク・ユーティリティーでは、APPN の ANR 転送のみを提供しています。[20] ただし、ANR 機能の提供に加えて、この事例のネットワーク・ユーティリティーは、TN3270E サーバー・サポートおよび DLUR サポートが確保できるように構成することもできます。DLUR サポートがあれば、ローカル・キャンパスの PU 2.0 装置でホストにアクセスすることができ、TN3270E サーバーによって、ローカル・キャンパスのワークステーションおよびプリンター、または分散 TN3270E サーバーがない事業所で TN3270 サポートが得られます。

構成のかぎ

この事例でのネットワーク・ユーティリティーの構成にあたっては、以下の点に注意してください

- APPN トラフィック用と TCP/IP トラフィック用に別々の MPC+ グループを定義することもできれば、APPN と TCP/IP の間で共用される単一のグループを定義することもできます。
- MPC+ グループには、最大で 64 のサブチャネルを収めることができます。なお、少なくとも 1 つの読み取りサブチャネルと、1 つの書き込みサブチャネルが定義されている必要があります。 talk 6 コマンド行で (`ESCON Add Virtual` プロンプトで)、**sub addr** コマンドを使用すると、読み取りサブチャネルが追加され、**sub addw** コマンドを使用すると、書き込みサブチャネルが追加されます。

20. RTP セッションは、会話の各端の APPN ノード間です。

- TCP/IP は、他のインターフェースの場合と同様にして、MPC+ インターフェース上に構成されます。特に、MPC+ バーチャル・ネット・ハンドラーの IP アドレスを構成すると、MPC+ インターフェースを介する TCP/IP が使用可能になります。
- APPN は、他のインターフェースの場合と同様にして、MPC+ 接続を介して構成されます。**add port** コマンドを使用するときは、 MPC+ を表すポート・タイプ **M** を指定します。
- MPC+ チャネルを介する APPN / HPR トラフィックを実行する場合は、 2 つの VTAM 定義を作成する必要があります。
  - 回線制御、サブチャネル、バッファーの数、および使用されるチャネル・プログラムを定義するトランスポート資源リスト (TRL) エレメント
  - ローカル PU 定義があるローカル SNA 大ノード
- LSA および LCS 定義の場合と同様、サブチャネル・パラメーターは、ホスト・チャネル・サブシステムに対してネットワーク・ユーティリティーを定義するときに、ホスト定義で使用されるパラメーターに一致する必要があります サブチャネル・パラメーターの説明については、236ページの表68 を、それらのパラメーターが MPC+ 定義に関するホスト・パラメーターとどのように相関するかについては、246ページの図37 を、それぞれ参照してください。

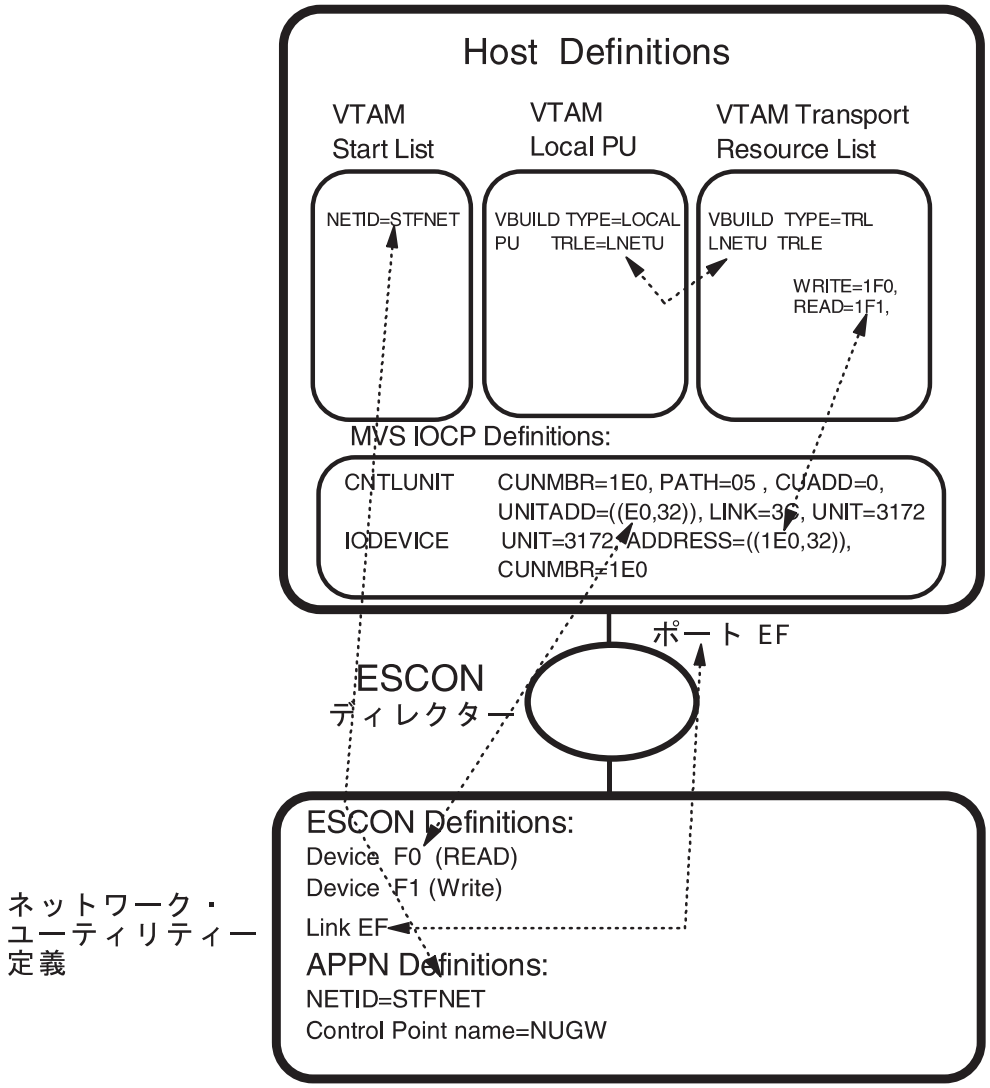


図 37. ホスト/ネットワーク・ユーティリティー間のパラメーターの関係 - MPC+

注:

1. ネットワーク・ユーティリティーの MPC+ インターフェース定義内で指定される装置アドレスは、 IOCP の CNTLUNIT マクロ内の UNITADD パラメーターで指定されている範囲内であることが必要です。例えば、図37 の UNITADD パラメーターには、E0 (16 進数) から始まる 32 (10 進数) の装置アドレスがネットワーク・ユーティリティー定義用として予約されていることが示されています。装置アドレス F0 および F1 は、ネットワーク・ユーティリティーの MPC+ インターフェースに指定されています。F0 および F1 は 16 進数の E0 ～ FF の範囲内にあるので、他の装置 (または、このネットワーク・ユーティリティー上のインターフェース) がこれらの同じサブチャネルの使用を試みない限り、これは OK です。
2. VTAM TRL 大ノード定義内で指定される値は、 IOCP の IODEVICE マクロ内の ADDRESS パラメーターで指定されている範囲内にあることが必要です。例えば、図37 のTRL 大ノード定義では 1F0 と 1F1 を指定しており、これは IODEVICE ステートメント内の ADDRESS パラメーターで指定している、1E0 ～ 1FF の範囲内です。

3. IODEVICE マクロ内の ADDRESS パラメーター、および CNTLUNIT マクロ内の UNITADD パラメーターに指定されている値は、***規則のみによって*** 関連付けられています。この例では、ADDRESS パラメーターの値は、***論理チャネル識別子*** (この場合は 1) を、 UNITADD 値の前に付加することによって、UNITADD パラメーターの値から決められています。これに該当する場合はしばしばあります。ただし、ネットワーク・ユーティリティーの MPC+ 定義上で装置アドレスを定義する場合は、ADDRESS パラメーターではなく、UNITADD パラメーターを使用して、値の有効範囲を決めます

これらのホスト定義の例については、295ページの『第18章 サンプル・ホスト定義』を参照してください。

ESCON インターフェース上の動的ルーティング・プロトコル

単一ホスト環境では、ESCON サブネット上でルーティング・プロトコル (例えば、RIP) を実行する必要はありません。この場合は、ネットワーク・ユーティリティーをデフォルト・ゲートウェイとして、ホストの TCP/IP プロファイル内に追加するだけで十分です。

ただし、複数のホストや複数のネットワーク・ユーティリティー・ゲートウェイがある場合は、 ESCON インターフェース上での RIP の実行を考慮する必要があります。この環境で動的ルーティング・プロトコルを実行すると、代替パスがある場合は、ネットワーク障害をう回することができます。

ネットワーク・ユーティリティーでは、RIP の V1 と V2 の両方をサポートします。RIP V2 では、可変長サブネット、および RIP V1 では得られないその他の拡張フィーチャーが提供されるので、こちらの選択がお勧めです。

OSPF への ESCON サブネットのインポート

ネットワーク上で OSPF を実行している場合は、ESCON サブネットを OSPF にインポートする必要があります (ただし、ホストの TCP/IP が OSPF をサポートしていない場合)。これが行われていない場合は、ESCON インターフェース上のホスト TCP/IP にアクセスできるのは、ネットワーク・ユーティリティー上のインターフェースに直接接続されているワークステーションだけになります。

この事例で必要な構成パラメーターを詳しく検討したい場合は、 160ページの図13 をごらんください。

ESCON チャネル・ゲートウェイ - 高可用性

この事例は、248ページの図38 に図示してあります。それぞれにホストへの ESCON チャネル接続がある、冗長ネットワーク・ユーティリティーが使用されます。また、キャンパス・バックボーンも重複し、各ネットワーク・ユーティリティーがそれぞれ異なるバックボーンに接続します。

この構成内では、たとえキャンパス・バックボーンの 1 つまたはネットワーク・ユーティリティーに障害が生じた場合でも、相変わらずホストにアクセスすることができます。2216 から着信するトラフィックには、1 つのキャンパス・バックボーンまた

はネットワーク・ユーティリティーを通って、ホストに至る有効なパスが相変わらずあります。これは、IP トラフィックと SNA トラフィックの両方について言えます。

ESCON ディレクター (ESCD) が、この構成では、特にパラレル・シスプレックス環境で重要です。これによって、シスプレックス内のゲートウェイと LPAR の間の接続のメッシュができるからです。こうして、ホスト・アクセスに関して最高水準の耐障害性が得られます。

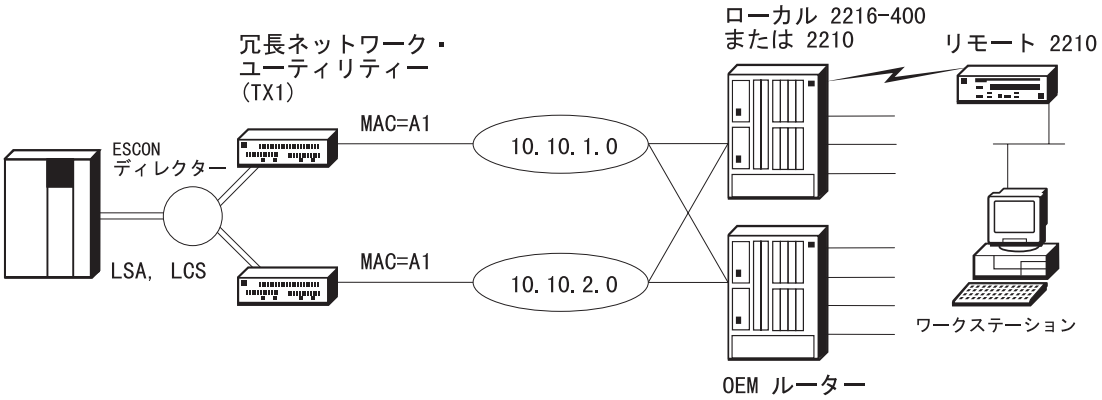


図 38. ESCON チャネル・ゲートウェイ - 高可用性

構成のかぎ

この事例での構成は、235ページの『ESCON チャネル・ゲートウェイ』での構成と非常によく似ています。それぞれのネットワーク・ユーティリティーが、別々の LSA および LCS インターフェースが定義された、LAN チャネル・ゲートウェイとして構成されています。ネットワーク・ユーティリティーを LAN チャネル・ゲートウェイとして構成する場合に必要なパラメーターについては、174ページの表17 を参照してください。

各ネットワーク・ユーティリティーがそれぞれ別のトークンリング上にあるので、それぞれの中のトークンリング・インターフェースに、同じ MAC アドレスを使用することができます。ただし、各インターフェースに使用される IP アドレスについては、各インターフェースがそれぞれ別のサブネット上にあるので、異なる必要があります。

注: この例では、ESCON チャネル上での LSA 接続および LCS 接続の使用が示されていますが、高可用性環境では、MPC+ の使用も同等に有効です。

ゲートウェイ機能の管理

この章および 275ページの『DLSw LAN チャネル・ゲートウェイ』に挙げてある構成例には、チャネル DLC の異なる使用が幾つか示されています。

- 直接 LSA インターフェースは、フレーム転送への DLSw または APPN 関与を伴わない LAN インターフェースにマップします。

- LCS ルーティングまたは MPC+ バーチャル・インターフェースは、 IP ルーティング・コードには別のインターフェースに見えるので、IP はその通常のルーティング機能を実行して、他のインターフェースにフレームを転送します。

  LCS ブリッジングは、ブリッジ・コードには別の LAN ブリッジ・ポートに見えるので、ブリッジングはその通常の機能を実行して、他のポートにフレームを転送します。
- ループバック LSA バーチャル・インターフェースは、DLSw と APPN のいずれにもリンクに見えます。
- MPC+ バーチャル・インターフェースは、APPN にはリンクに見える可能性があります。

ネットワーク・ユーティリティーのゲートウェイ機能の完全な範囲を管理する場合は、IP、ブリッジング、DLSw、および APPN を適宜管理する必要があります。ここでは、上位レイヤー機能を説明の対象とするのではなく、チャネルの物理インターフェースおよびバーチャル・インターフェースの監視および管理ができる方法に焦点を絞って説明します。

コマンド行監視

チャネル資源の状況を階層的に表示する talk 5 コマンドに、以下のようにしてアクセスします。

1. * プロンプトで **talk 5** と入力し、**Enter** を押して、+ プロンプトを表示させます。
2. + プロンプトで、**int** と入力して、**Enter** を押し、管理および監視の対象となる物理 ESCON または PCA インターフェースの論理インターフェース番号を書き留めます。

   物理インターフェースは、一般的に *基本ネット* と呼ばれ、その上に多くの LSA、LCS、または MPC+ バーチャル・インターフェースが定義されている場合があります。基本ネットおよびすべてのバーチャル・インターフェースには、それぞれ異なるインターフェース番号があります。
3. + プロンプトで、**net** *base n number* を入力し、**Enter** を押して、ESCON または PCA コンソール・サブプロセスにアクセスします。コマンド・プロンプトは、適宜 `ESCON>` または `PCA>` に変わります。

   これらのプロンプトでは、**li nets** コマンドを使用して、この基本ネットを使用しているすべての (LSA、LCS、MPC+) バーチャル・インターフェースの現在の状態を表示させて見ることができます。また、 **li sub** と入力して、この基本ネットに関して現在稼働中のサブチャネル構成を表示させて見ることもできます。
4. 基本ネット `ESCON>` または `PCA>` プロンプトで、 **net** *virtual net number* を入力し、**Enter** を押して、この基本ネットを使用する特定のバーチャル・インターフェースに関する詳細を表示させて見ることができます。選択したバーチャル・インターフェースに応じて、コマンド・プロンプトは `LSA>`、`LCS>`、または `MPC+>` に変わります。

   これらのプロンプトのそれぞれが、該当のバーチャル・インターフェース・タイプに関連する構成および現在の状況を表示させるための、 **list** コマンドをサポートします。
5. これらのネスト・レベルのいずれからバックアウトする場合も、 **exit** と入力し、**Ctrl-p** を押して、* プロンプトに戻ります。

これらのコマンドの出力の例および詳細な説明については、*MAS ソフトウェア使用者の手引き* の「ESCON およびパラレル・チャネル・アダプターの構成と監視」の章を参照してください。

イベント・ログ・サポート

チャネル機能内で発生するイベントは、下記の ELS サブシステムの対象になります。

ESC 下位レイヤー ESCON イベント
PCA 下位レイヤー・パラレル・チャネル・イベント
LSA LSA バーチャル・インターフェースに関連するイベント
LCS LCS バーチャル・インターフェースに関連するイベント
MPC+ MPC+ バーチャル・インターフェースに関連するイベント

イベント・ログを使用可能にする場合は、talk 5 または talk 6 で、 **event** と入力して、ELS コンソールまたは Config (構成) サブプロセスにアクセスします。ログ出力が talk 2 に表示されるようにしたい場合は、 **disp sub** *subsystem name* を入力し、**Enter** を押して、通常のエラー報告を使用可能にするか、**disp sub** *subsystem name* **all** を入力して、すべてのメッセージを使用可能にします。ある問題を視覚的に最もよく把握するためには、ESCON または PCA サブシステムの 1 つとバーチャル・インターフェース・サブシステムの 1 つの両方を使用可能にすることができます。これらのコマンドを talk 5 で使用すると、即時に talk 2 に移動して、イベントを発生時に監視することができます。

li sub *subsystem name* コマンドを、talk 5 と talk 6 ELS サブプロセスのどちらかで使用して、これらのサブシステムのそれぞれによって報告されるイベントの感触をつかむことができます。

SNA 管理サポート

VTAM または NetView/390 オペレーター・コンソールから、111ページの『NetView/390』で説明されているように、LSA 直接ゲートウェイ機能、DLSw、または APPN に関連した SNA 資源を制御することができます。

チャネル機能自体が SNA アラートを送信することはありません。アラートに変換できるトラップを送信することもありませんが、チャネル ELS メッセージに関するトラップを使用可能にし、107ページの『IBM Nways Manager for AIX』で言及されているプロダクトを使用して、そのようなトラップをアラートに変換することができます。

SNMP MIB およびトラップ・サポート

ネットワーク・ユーティリティーでは、ESCON に関する IBM エンタープライズ特定 MIB をサポートします。この MIBによって、次の情報へのアクセスが得られます。

- 物理インターフェースのリストおよびそれぞれのファイバー信号状況
- チャネル・リンクのリストおよびそれぞれのホスト接続状況
- チャネル・ステーションにそれぞれの構成と正常/エラー・トラフィックの両統計を添えたリスト

ESCON MIB でトラップを定義することはありません。パラレル・チャネル機能には、 MIB サポートはありません。

ESCON チャネル・インターフェースとパラレル・チャネル・インターフェースが両方とも、インターフェース MIB (RFC 1573) 内で表されているので、管理ステーションでそれらの状況および基本的なインターフェース別トラフィック統計にアクセスすることができます。ネットワーク・ユーティリティーでは、管理ステーションにインターフェース状態を制御させることができ、トラップを送信して、インターフェースがいつアップまたはダウンになるか報告することができます。

ネットワーク管理アプリケーション・サポート

107ページの『IBM Nways マネージャー・プロダクト』で説明されているネットワーク・ユーティリティーの Java ベースのアプリケーションには、ESCON MIB およびインターフェース MIB に対する統合サポートが備えられています。これらの MIB からの重要な情報を表示する特定のパネルだけでなく、色分けされたインターフェース状況も表示させて見ることができます。また、内蔵ブラウザー・サポートを使用すれば、これらの MIB のいずれに入っている情報も表示させて見ることができます。

Nways マネージャー・プロダクトからのインターフェース・アップ/ダウン・トラップの発行を、使用不可または使用可能にすることができます。

第15章 チャネル・ゲートウェイの構成例の詳細

この章には、229ページの『第14章 チャネル・ゲートウェイ』のチャネル・ゲートウェイ・ネットワーク構成の例の幾つかに関する図と構成パラメーター表が挙げてあります。パラメーター値は、実際の作業テスト構成での値が示してあります。

構成パラメーター表の欄および規則の説明については、 144ページの『構成例表の規則』を参照してください。

ネットワーク・ユーティリティー ワールド・ワイド・ウェブ (WWW) ページには、ここに挙げてある構成パラメーター表に一致する 2 進構成ファイルが収められています。これらのファイルにアクセスする場合は、下記のアドレスから Download リンクをたどってください。

```
http://www.networking.ibm.com/networkutility
```

この章に記載されている構成は、次のとおりです。

表 69. 構成例情報の相互参照

構成記述	パラメーター表
235ページの『ESCON チャネル・ゲートウェイ』	254ページの表70
242ページの『パラレル・チャネル・ゲートウェイ』	259ページの表71
243ページの『チャネル・ゲートウェイ (MPC+ を介する APPN および IP)』	266ページの表72

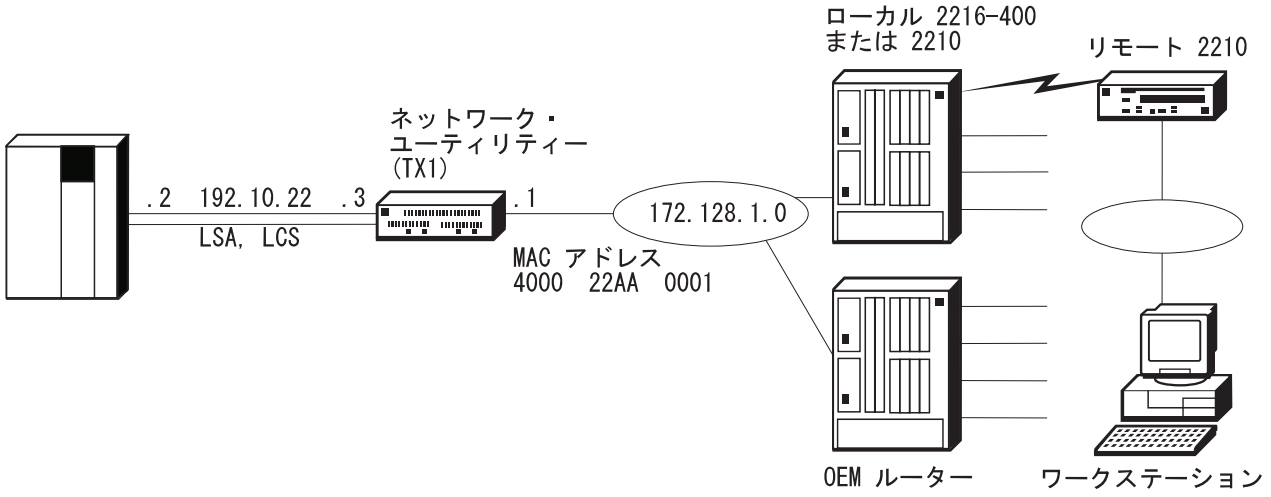


図 39. ESCON チャネル・ゲートウェイ

表 70. ESCON チャネル・ゲートウェイ. この構成の説明については 235 ページを、図については 253 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR スロット 2: ESCON	次の行の "add device" を参照	1
装置 アダプター ポート	スロット 1 ポート 1: インターフェース 0: TR スロット 2 ポート 1: インターフェース 1: ESCON	Config>**add dev tok** Config>**add dev esc**	2
装置 インターフェース	インターフェース 0 MAC アドレス : 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
装置 チャネル・アダプター ESCON インターフェース ESCON インターフェース	インターフェース 2 (新規定義) 基本ネットワーク番号 : 1 プロトコル・タイプ : LSA 最大データ・フレーム : 2052 LAN ネットワーク番号 : 0 (**Add** をクリックして、 インターフェース 2 を作成)	Config>**net 1** ESCON Config>**add lsa** (インターフェース 2 として追加) ESCON Add Virtual>**maxdata 2052** ESCON Add Virtual>**net 0** (次の行との同一セッション内で継続)	3、4、5
装置 チャネル・アダプター ESCON インターフェース ESCON サブチャネル	インターフェース 2 (LSA インターフェースを強調表示) 装置アドレス : E4 リンク・アドレス : EF (**Add** をクリック)	ESCON Add Virtual>**subchannel add** ESCON Add LSA Subchannel>**device E4** ESCON Add LSA Subchannel>**link EF** (**exit** を 2 回入力した上で、 **list all** と入力)	6
装置 チャネル・アダプター ESCON インターフェース ESCON インターフェース	インターフェース 3 (新規定義) 基本ネットワーク番号 : 1 プロトコル・タイプ : LCS LAN タイプ : トークンリング 最大データ・フレーム : 2052 MAC アドレス : 400022AA0009 (**Add** をクリックして、 インターフェース 3 を作成)	Config>**net 1** ESCON Config>**add lcs** (インターフェース 3 として追加) ESCON Add Virtual>**lantype token** ESCON Add Virtual>**Maxdata 2052** ESCON Add Virtual>**mac 40:00:22:AA:00:09** (次の行との同一セッション内で継続)	

表 70. ESCON チャネル・ゲートウェイ (続き). この構成の説明については 235 ページを、図については 253 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 チャネル・アダプター ESCON インターフェース ESCON サブチャネル	インターフェース 3 (LCS インターフェースを強調表示) 装置アドレス : E0 リンク・アドレス : EF (**Add** をクリック)	ESCON Add Virtual>**subchannel add** ESCON Config LCS Subchannel>**device E0** ESCON Config LCS Subchannel>**link EF** (**exit** を 2 回入力した上で、 **list all** と入力)	7
システム 一般	システム名 : NU_A ロケーション : XYZ 連絡先 : 管理者	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	
プロトコル IP 一般	内部アドレス : 172.128.252.1 ルーター ID: 172.128.1.1	Config>**p ip** IP config>**set internal 172.128.252.1** IP config>**set router-id 172.128.1.1**	
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.1 サブネット・マスク : 255.255.255.0 インターフェース 3 (LCS インターフェース) IP アドレス : 192.10.22.3 サブネット・マスク : 255.255.255.0	IP config>**add address** (インターフェース 1 つにつき 1 回)	8
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf**	8

表 70. ESCON チャネル・ゲートウェイ (続き). この構成の説明については 235 ページを、図については 253 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF AS 境界ルーティング	AS 境界ルーティング (チェックして使用可能) 直接ルートのインポート (チェックして使用可能)	OSPF config>**enable as** Import direct routes (他のデフォルトを受け入れる)	9
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック)	OSPF Config> **set interface** Interface IP address: **172.128.1.1** Attaches to area: **0.0.0.0** (他のデフォルトを受け入れる)	

注 :

1. **add dev** で定義するのは、単一のポートであり、アダプターではありません。
2. 構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。
3. タイプ LSA のインターフェースを選択すると、『LAN type』のフィールドが使用不可 (ぼかし表示) になり、『LAN net number』と『loopback』のチェック・ボックスが表示されます。
4. 『LAN number』のフィールドが使用不可になるのは、値がルーターによって自動的に割り当てられるからです。この値は、『ADAPTNO』に関するホスト定義内で構成される必要があります。
5. インターフェースを『Add』すると、新しいインターフェースが生成され、使用可能な次のインターフェース番号が割り当てられます。
6. サブチャネルの構成時に入力する値は、ホストで構成された値に一致する必要があります。これらの値を一致させる方法については、 295ページの『第18章 サンプル・ホスト定義』 を参照してください。
7. LCS バーチャル・インターフェース用としてサブチャネルを追加するときは、たとえ LCS がサブチャネルを 2 つ必要とする場合でも、定義する必要があるのは 1 つだけです。LCS では、ここで定義されたサブチャネルに加えて、次のサブチャネルを自動的に使用します。LCS では、偶数の装置アドレス (この場合は E0) を書き込みサブチャネルとして使用し、奇数の装置アドレス (E1) を読み取りサブチャネルとして使用します。
8. OSPF の代わりに RIP を使用することもできます。
9. ESCON インターフェースから OSPF 内に直接ルートをインポートする必要があるのは、ESCON インターフェース上では OSPF が使用可能にされないからです。代わりに、ESCON インターフェース上のサブネットがネットワーク・ユーティリティー内の OSPF 内にインポートされた上で、ネットワークに伝送されます。これが必要なのは、ネットワーク・ユーティリティーが LCS 接続を通して OSPF 更新を送信する場合に、ホストでエラー・メッセージが生じるのを防ぐためです。ホストの TCP/IP では、 OSPF ルーターからのリンク状態公示を (まだ) サポートしていません。

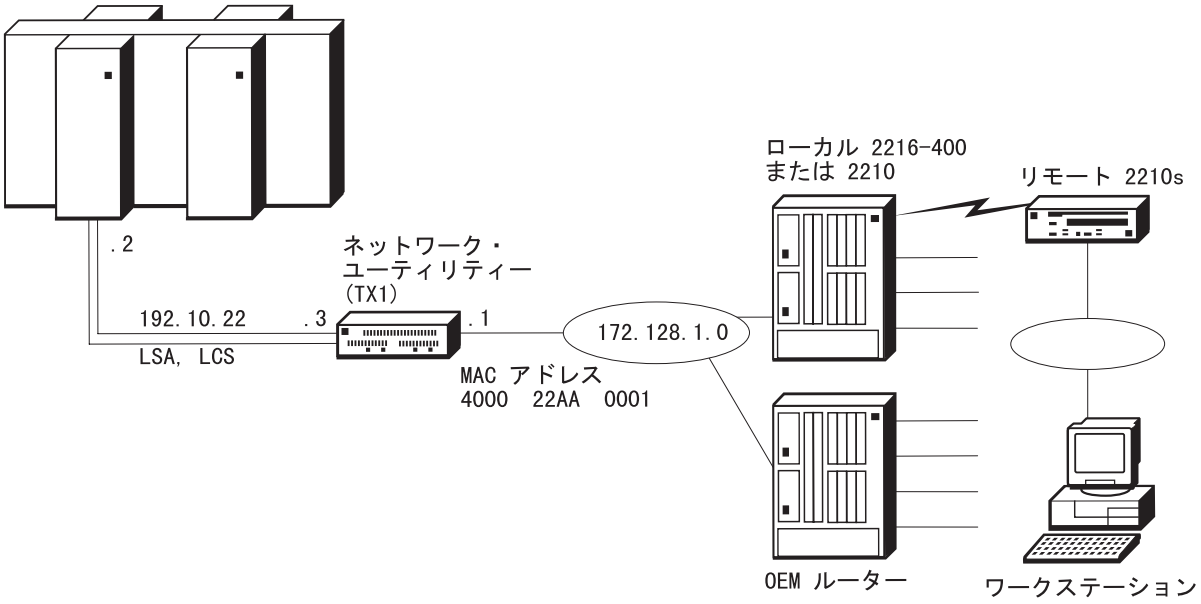


図 40. パラレル・チャネル・ゲートウェイ

表 71. パラレル・チャネル・ゲートウェイ. この構成の説明については 242 ページを、図については 258 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR スロット 2: パラレル・チャネル・ アダプター (PCA)	次の行の "add device" を参照	1
装置 アダプター ポート	スロット 1/ポート 1: インターフェース 0: TR スロット 2/ポート 1: インターフェース 1: PCA	Config>**add dev tok** Config>**add dev PCA**	2
装置 インターフェース	インターフェース 0 MAC アドレス : 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
装置 チャネル・アダプター PCA インターフェース PCA インターフェース	インターフェース 2 (新規定義) 基本ネットワーク番号 : 1 プロトコル・タイプ : LSA LAN ネットワーク番号 : 0 (**Add** をクリックして、 インターフェース 2 を作成)	Config>**net 1** PCA Config>**add lsa** (インターフェース 2 として追加) PCA Add Virtual>**net 0** (次の行との同一セッション内で継続)	3、4、5
装置 チャネル・アダプター PCA インターフェース PCA サブチャネル	インターフェース 2 (LSA インターフェースを強調表示) 装置アドレス : 00 サブチャネル・タイプ : 読み取り/書き込み (**Add** をクリック)	PCA Add Virtual>**subchannel add** PCA Add LSA Subchannel>**device 00** (**exit** を 2 回入力した上で、 **list all** と入力)	6
装置 チャネル・アダプター PCA インターフェース PCA インターフェース	インターフェース 3 (新規定義) 基本ネットワーク番号 : 1 プロトコル・タイプ : LCS MAC アドレス : 400022AA0009 (**Add** をクリックして、 インターフェース 3 を作成)	Config>**net 1** PCA Config>**add lcs** (インターフェース 3 として追加) PCA Add Virtual>**mac 40:00:22:AA:00:09** (次の行との同一セッション内で継続)	
装置 チャネル・アダプター PCA インターフェース PCA サブチャネル	インターフェース 3 (LCS インターフェースを強調表示) 装置アドレス : 02 サブチャネル・タイプ : 書き込み (**Add** をクリック)	PCA Add Virtual>**subchannel add** PCA Add LCS Subchannel>**device 02** (**exit** を 2 回入力した上で、 **list all** と入力)	7

表 71. パラレル・チャネル・ゲートウェイ (続き). この構成の説明については 242 ページを、図については 258 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
システム 一般	システム名 : NU_A ロケーション : XYZ 連絡先 : 管理者	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	
プロトコル IP 一般	内部アドレス : 172.128.252.1 ルーター ID: 172.128.1.1	Config>**p ip** IP config>**set internal 172.128.252.1** IP config>**set router-id 172.128.1.1**	
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.1 サブネット・マスク : 255.255.255.0 インターフェース 3 (LCS インターフェース) IP アドレス : 192.10.22.3 サブネット・マスク : 255.255.255.0	IP config>**add address** (インターフェース 1 つにつき 1 回)	8
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf**	8
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF AS 境界ルーティング	AS 境界ルーティング (チェックして使用可能) 直接ルートのインポート (チェックして使用可能)	OSPF Config>**enable as** Import direct routes (他のデフォルトを受け入れる)	9

表 71. パラレル・チャネル・ゲートウェイ (続き). この構成の説明については 242 ページを、図については 258 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック)	OSPF Config>**set interface** Interface IP address: **172.128.1.1** Attaches to area: **0.0.0.0** (他のデフォルトを受け入れる)	

注 :

1. **add dev** で定義するのは、単一のポートであり、アダプターではありません。
2. 構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。
3. タイプ LSA のインターフェースを選択すると、『LAN type』のフィールドが使用不可 (ぼかし表示) になり、『LAN net number』と『loopback』のチェック・ボックスが表示されます。
4. 『LAN number』のフィールドが使用不可になるのは、値がルーターによって自動的に割り当てられるからです。この値は、『ADAPTNO』に関するホスト定義内で構成される必要があります。
5. インターフェースを『Add』すると、新しいインターフェースが生成され、使用可能な次のインターフェース番号が割り当てられます。
6. サブチャネルの構成時に入力する値は、ホストで構成された値に一致する必要があります。これらの値を一致させる方法については、 295ページの『第18章 サンプル・ホスト定義』 を参照してください。
7. LCS バーチャル・インターフェース用としてサブチャネルを追加するときは、たとえ LCS がサブチャネルを 2 つ必要とする場合でも、定義する必要があるのは 1 つだけです。LCS では、ここで定義されたサブチャネルに加えて、次のサブチャネルを自動的に使用します。LCS では、偶数の装置アドレス (この場合は 02) を書き込みサブチャネルとして使用し、奇数の装置アドレス (03) を読み取りサブチャネルとして使用します。
8. OSPF の代わりに RIP を使用することもできます。
9. PCA インターフェースから OSPF 内に直接ルートをインポートする必要があるのは、PCA インターフェース上では OSPF が使用可能にされないからです。代わりに、PCA インターフェース上のサブネットがネットワーク・ユーティリティー内の OSPF 内にインポートされた上で、ネットワークに伝送されます。これが必要なのは、ネットワーク・ユーティリティーが LCS 接続を通して OSPF 更新を送信する場合に、ホストでエラー・メッセージが生じるのを防ぐためです。ホストの TCP/IP では、 OSPF ルーターからのリンク状態公示を (まだ) サポートしていません。

ネットワーク・ユーティリティーには、LCS インターフェースを操作する方法が、次のように 3 つ用意されています。

次の例には、LCS パススルー構成が示してあります。

```
*t 6
Gateway user configuration
config>add dev esc
Device Slot #(1-8) [1] ?3
Adding ESCON Channel device in slot 3 port 1 as interface #4
Use "net 4" to configure ESCON Channel parameters
Config>net 4
ESCON Config>add lcs
ESCON Add Virtual>?
LANtype
MAC address
MAXdata
BLKtimer
ACKlen
SUBchannels
ENable 3172 Emulation
Exit
ESCON Add Virtual>enable
Enabling LCS 3172 Emulation for network 5.
Please set the Network link using the "Net" command.
ESCON Add Virtual>?
BLKtimer
ACKlen
SUBchannels
DISable 3172 Emulation
NET link
Exit
ESCON Add Virtual>net 0
ESCON Add Virtual>sub add
Please add or configure one subchannel for an LCS virtual interface.
Although LCS requires two subchannels, it is only necessary to specify
one subchannel.  An adjacent subchannel will be chosen such that the
two subchannels will form a sequential pair with the write subchannel
(device address is even) before the read subchannel (device address
is odd).
ESCON Config LCS subchannel>?
LINk address (ESCD Port)
LPAR number
CU logical address
Device address
Exit
ESCON
ESCON Config LCS Subchannel>link f7
ESCON Config LCS Subchannel>lpar 0
ESCON Config LCS Subchannel>cu 0
ESCON Config LCS Subchannel>dev 20
ESCON Config LCS Subchannel>ex
ESCON Add Virtual>ex
>

ESCON Config>list
Net   5   Protocol: LCS    LAN type: Token Ring         LAN number: 0
          3172 Emulation is enabled
          MAC address: Obtained from net 0
          Block timer:    5 ms   ACK length:    10 bytes
ESCON config>list all
Net   5   Protocol: LCS    LAN type: Token Ring         LAN number: 0
          3172 Emulation is enabled
          MAC address: Obtained from net 0
          Block timer:    5 ms   ACK length:    10 bytes
          Read Subchannels:
```

```
          Sub  0   Dev addr: 21  LPAR: 0  Link addr: F7    CU addr: 0
          Write Subchannels:
          Sub  1   Dev addr: 20  LPAR: 0  Link addr: F7    CU addr:  0
ESCON Config
```

次の例には t 5 プロンプトが示され、3172 エミュレーションが使用可能にされています。

```
LCS> list all
LCS Virtual Adapter
LCS Information for Net 5
--- ----------- --- --- --
LAN Type: Token-Ring           LAN Number: 0
Local Read Subchannel number:  1
Local Write Subchannel number: 0
MAC Address: 08005AFE0144
LCS 3172 Emulation to net 0
Status: Down
```

図41 には、ホストとネットワーク・ユーティリティーの間で、LCS インターフェース定義に関して、パラメーターがどのように相関するかが示してあります

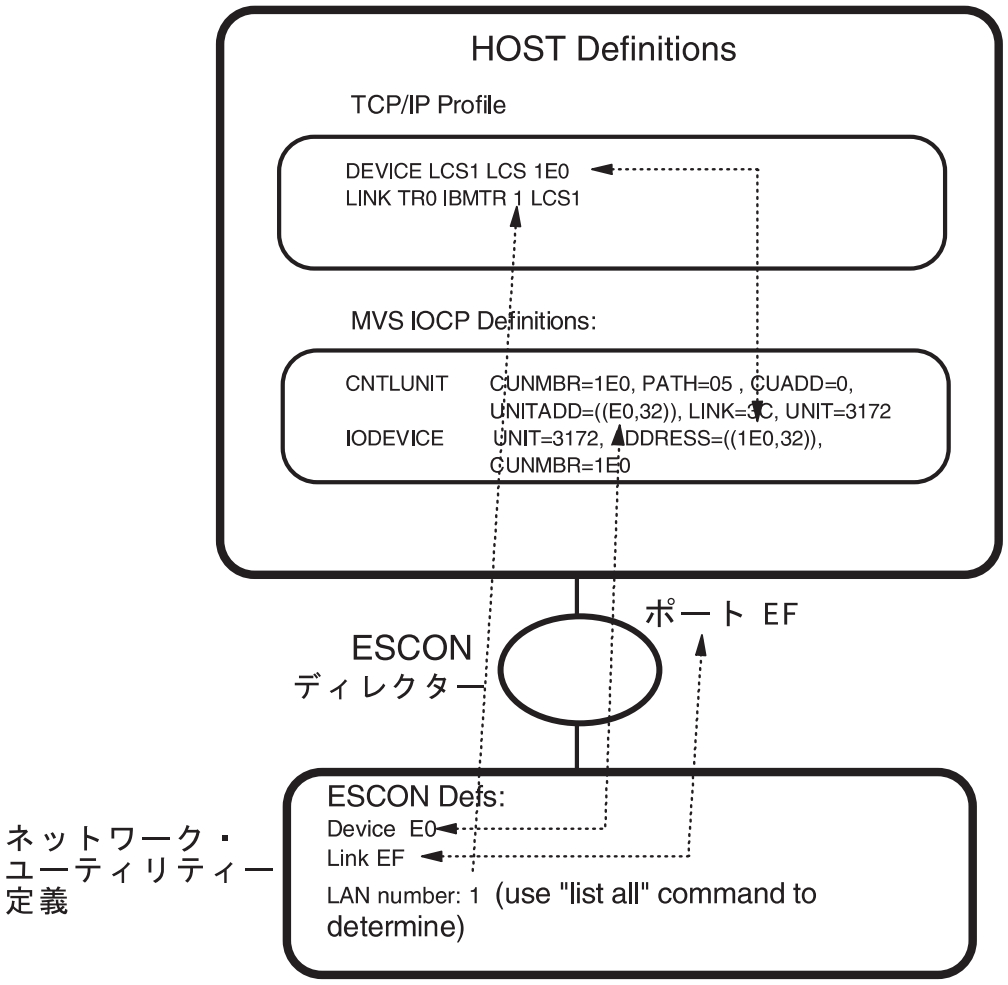


図41. ホスト/ネットワーク・ユーティリティー間のパラメーターの関係 - LCS

注:

1. LCS では、サブチャネルのペアを、1 つは読み取り用として、もう 1 つは書き込み用として使用します。 LCS インターフェースで使用されるサブチャネルを構成するときは、実際には、 1 つのサブチャネル・アドレスだけを指定すれば済みます。 LCS が 2 つの隣接サブチャネルを LCS 接続用として、1 つは読み取りに (装置アドレスが奇数)、 1 つは書き込みに (装置アドレスが偶数)、自動的に割り当てます。
2. ネットワーク・ユーティリティーの LCS インターフェース定義内で指定される装置アドレスは、 IOCP の CNTLUNIT マクロ内の UNITADD パラメーターで指定されている範囲内であることが必要です。例えば、263ページの図41 の UNITADD パラメーターには、E0 (16 進数) から始まる 32 (10 進数) の装置アドレスがネットワーク・ユーティリティー定義用として予約されていることが示されています。装置アドレス E0 がネットワーク・ユーティリティーの LCS インターフェースに指定されています。ネットワーク・ユーティリティーが自動的に E1 も割り振ります。E0 および E1 は 16 進数の E0 ～ FF の範囲内にあるので、他の装置 (または、このネットワーク・ユーティリティー上のインターフェース) がこれらの同じサブチャネルの使用を試みない限り、これは OK です
3. ホストの TCP/IP プロファイル内の DEVICE ステートメント内で指定される値は、IOCP の IODEVICE マクロ内の ADDRESS パラメーターで指定されている範囲内にあることが必要です。例えば、263ページの図41 のホストの TCP/IP プロファイル内の DEVICE ステートメントは、16 進数の 1E0 であり、これは IODEVICE ステートメント内の ADDRESS パラメーターで指定している、 1E0 ～ 1FF の範囲内です。
4. IODEVICE マクロ内の ADDRESS パラメーター、および CNTLUNIT マクロ内の UNITADD パラメーターに指定されている値は、***規則のみによって*** 関連付けられています。この例では、ADDRESS パラメーターの値は、***論理チャネル識別子*** (この場合は 1) を、 UNITADD 値の前に付加することによって、UNITADD パラメーターの値から決められています。これに該当する場合はしばしばあります。ただし、ネットワーク・ユーティリティーの LCS 定義上で装置アドレスを定義する場合は、ADDRESS パラメーターではなく、UNITADD パラメーターを使用して、値の有効範囲を決めます

このインターフェース・タイプに関するホスト定義の詳細な説明およびサンプルについては、295ページの『第18章 サンプル・ホスト定義』を参照してください。

この事例で必要な構成パラメーターを詳しく検討したい場合は、 174ページの表17 をごらんください。

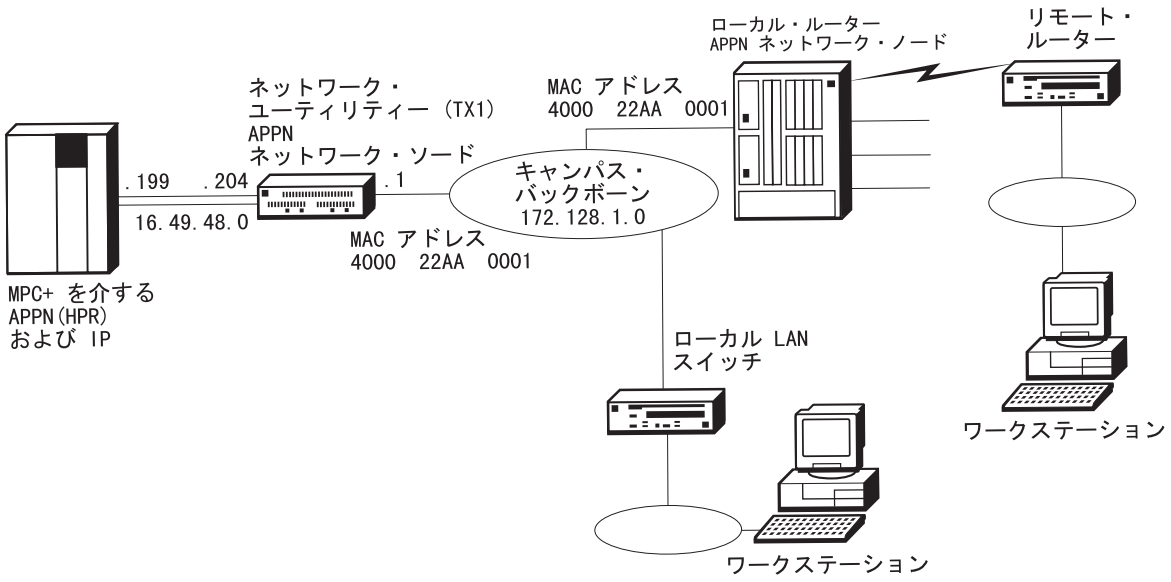


図 42. チャネル・ゲートウェイ (MPC+ を介する APPN および IP)

表 72. チャネル・ゲートウェイ (MPC+ を介する APPN および IP). この構造の説明については 243 ページを、図については 265 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR スロット 2: ESCON	次の行の "add device" を参照	1
装置 アダプター ポート	スロット 1/ポート 1: インターフェース 0: TR スロット 2/ポート 1: インターフェース 1: ESCON	Config>**add dev tok** Config>**add dev esc**	2
装置 インターフェース	インターフェース 0 MAC アドレス : 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
装置 チャネル・アダプター ESCON インターフェース ESCON インターフェース	インターフェース 2 (新規定義) 基本ネットワーク番号 : 1 プロトコル・タイプ : MPC+ (**Add** をクリックして、 インターフェース 2 を作成)	Config>**net 1** ESCON Config>**add mpc** (インターフェース 2 として追加) ESCON Add Virtual> (次の行との同一セッション内で継続)	3
装置 チャネル・アダプター ESCON インターフェース ESCON サブチャネル	(インターフェース 2 を強調表示) 装置アドレス : F0 リンク・アドレス : EF サブチャネル・タイプ : 読み取り (**Add** をクリックして、サブチャネルを定義) 装置アドレス : F1 リンク・アドレス : EF サブチャネル・タイプ : 書き込み (**Add** をクリックして、サブチャネルを定義)	ESCON Add Virtual>**sub addr** ESCON Add MPC+ Read Subchannel>**dev f0** ESCON Add MPC+ Read Subchannel>**link ef** ESCON Add MPC+ Read Subchannel>**exit** ESCON Add Virtual>**sub addw** ESCON Add MPC+ Write Subchannel>**dev f1** ESCON Add MPC+ Write Subchannel>**link ef** (type **exit** twice and then **list all**)	4
システム 一般	システム名 : NU_A ロケーション : XYZ 連絡先 : 管理者	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	5

表 72. チャネル・ゲートウェイ (MPC+ を介する APPN および IP) (続き). この構造の説明については 243 ページを、図については 265 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル IP 一般	内部アドレス : 172.128.252.1 ルーター ID: 172.128.1.1	Config>**p ip** IP config>**set internal 172.128.252.1** IP config>**set router-id 172.128.1.1**	
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.1 サブネット・マスク : 255.255.255.0 インターフェース 2 (MPC+ インターフェース) IP アドレス : 16.49.48.204 サブネット・マスク : 255.255.255.0	IP config>**add address** (インターフェース 1 つにつき 1 回)	
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf**	6
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF AS 境界ルーティング	AS 境界ルーティング (チェックして使用可能) 直接ルートのインポート (チェックして使用可能)	OSPF Config>**enable as** Import direct routes (他のデフォルトを受け入れる)	7
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック)	OSPF Config>**set interface** Interface IP address: **172.128.1.1** Attaches to area: **0.0.0.0** (他のデフォルトを受け入れる)	
プロトコル APPN 一般	APPN ネットワーク・ノード (チェックして使用可能) ネットワーク ID: STFNET コントロール・ポイント : NUGW	Config>**p appn** APPN config> **set node** Enable APPN Network ID: **STFNET** Control point name: **NUGW** (他のデフォルトを受け入れる)	

表 72. チャネル・ゲートウェイ (MPC+ を介する APPN および IP) (続き). この構造の説明については 243 ページを、図については 265 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル APPN インターフェース	(インターフェース 0 トークンリングを強調表示) (構成タブをクリック) APPN ポートを定義 (チェックして使用可能) ポート名 : TR001	APPN config>**add port** APPN Port Link Type: **TOKEN RING** Port name: **TR001** Enable APPN (他のデフォルトを受け入れる)	
プロトコル APPN インターフェース	(インターフェース 0 トークンリングを強調表示) (リンク・ステーション・タブをクリック) TRTG001 (新規定義) 一般 - 1 タブ : リンク・ステーション名 : TRTG001 一般 - 2 タブ : 隣接ノードの MAC アドレス : 400022AA0011 隣接ノード・タイプ : APPN ネットワーク・ノード (**Add** をクリックして、リンク・ステーションを作成)	APPN config>**add link** Port name for the link station: **TR001** Station name: **TRTG001** MAC address of adjacent node: **400022AA0011** (他のデフォルトを受け入れる)	8
プロトコル APPN インターフェース	(インターフェース 2 ESCON-MPC+ を強調表示) (構成タブをクリック) APPN ポートを定義 (チェックして使用可能) ポート名 : MPC001	APPN config>**add port** APPN Port Link Type: **MPC** Interface Number: **2** Port name: **MPC001** Enable APPN (他のデフォルトを受け入れる)	
プロトコル APPN インターフェース	(インターフェース 2 ESCON-MPC+ を強調表示) (リンク・ステーション・タブをクリック) MPCTG001 (新規定義) 一般 - 1 タブ : リンク・ステーション名 : MPCTG001 一般 - 2 タブ : 隣接ノード・タイプ : APPN ネットワーク・ノード (**Add** をクリックして、リンク・ステーションを作成)	APPN config>**add link** Port name for the link station: **MPC001** Station name: **MPCTG001** Adjacent Node Type: **0** = APPN Network Node (他のデフォルトを受け入れる)	

注 :

1. **add dev** で定義するのは、単一のポートであり、アダプターではありません。
2. 構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。
3. インターフェースを『Add』すると、新しいインターフェースが生成され、使用可能な次のインターフェース番号が割り当てられます。
4. サブチャネルの構成時に入力する値は、ホストで構成された値に一致する必要があります。これらの値を一致させる方法については、 295ページの『第18章 サンプル・ホスト定義』 を参照してください。
5. 書き込み対応可能 SNMP コミュニティーが必要なのは、構成ファイルを構成プログラムからルーターに直接ダウンロードしたい場合だけです。ルーターへの構成ファイルの TFTP を実行する場合は、SNMP は必要ありません。
6. OSPF の代わりに RIP を使用することもできます。
7. ESCON インターフェースから OSPF 内に直接ルートをインポートする必要があるのは、ESCON インターフェース上では OSPF が使用可能にされないからです。代わりに、ESCON インターフェース上のサブネットがネットワーク・ユーティリティー内の OSPF 内にインポートされた上で、ネットワークに伝送されます。これが必要なのは、ネットワーク・ユーティリティーが MPC+ 接続を通して OSPF 更新を送信する場合に、ホストでエラー・メッセージが生じるのを防ぐためです。ホストの TCP/IP では、 OSPF ルーターからのリンク状態公示を (まだ) サポートしていません。
8. この例のあて先 MAC アドレスは、265ページの図42 のキャンパス・バックボーンの右側のローカル・ルーターです。このルーターも APPN ネットワーク・ノードとして構成されています。

第16章 データ・リンク交換

概説

ここでは、データ・リンク交換 (DLSw) について概説し、ネットワーク・ユーティリティーに実装されている DLSw 機能の概要を示します。

DLSw とは

DLSw とは、IP バックボーン・ネットワークを通して、SNA および NetBIOS を始めとする、コネクション型プロトコルをトランスポートするための、IBM 考案の標準テクノロジーです。IP ネットワークの端にある DLSw ルーターが、ネイティブ SNA および NetBIOS エンド・ステーションからのリンク確立要求をさばき、ピア DLSw ルーター間でターゲット・エンド・ステーションにサービスするピア・ルーターを探索し、そのピア・ルーターを通してエンド・ステーション間にパスおよび中継アプリケーション・データをセットアップします。

DLSw ルーター間を流れるプロトコルについては、RFC 1795、「Data Link Switching: Switch to Switch Protocol」に文書化されています。このプロトコルおよびマルチキャスト IP ベースの拡張容易性機能強化の説明は、 RFC 2166、「DLSw v2.0 Enhancements」に文書化されています。

多くの DLSw インプリメンテーションが備えている *ローカル DLSw* 機能では、1 つのルーター内の 2 つのリンクを接続し、これは IP ネットワークを通して、ルーター内の 2 つのリンクを別の DLSw ルーターに接続する場合とは異なります。関与する DLC のタイプによって異なりますが、この機能は、FRAD または X.25 PAD の機能に匹敵する場合があります。

ネットワーク・ユーティリティーの DLSw 機能

ネットワーク・ユーティリティーに実装されている DLSw は、機能的には IBM 2210 および 2216 ルーターの場合とほぼ同じです。次のようなエンド・ステーション・プロトコルを処理することができます。

- SNA
  - PU 4/5 - PU 2.0 (および SDLC 上の IBM 5394) 間
  - T2.1 - T2.1 間
  - PU 4/5 - PU 4/5 間
- NetBIOS
  - ポイント・ポイント・セッション
  - 同報通信データグラム・トラフィック
- LAN ネットワーク・マネージャー
  - LNM - ブリッジ・サーバー (例えば、LBS、CRS、REM) 間
  - LNM - 8235 インテリジェント・ハブ間
  - LNM - LAN ステーション・マネージャー間

ネットワーク・ユーティリティーの DLSw は、次のようなデータ・リンク制御 (DLC) タイプを通して、エンド・ステーションと通信することができます。

- 802.2 LLC

  LLC は、次のようなインターフェース・タイプのいずれを介しても伝達できます。
  - トークンリング
  - イーサネット (10 Mbps または 10/100 Mbps アダプター)
  - FDDI
  - リモート・ブリッジング用として使用可能にされた PPP リンク
  - リモート・ブリッジング用として使用可能にされたフレーム・リレー PVC および SVC (RFC 1490/2427 ブリッジド・フレーム・フォーマット)
  - ATM LAN エミュレーション
  - ATM ネイティブ・ブリッジング (RFC 1483 ブリッジド・フレーム・フォーマット)
- SDLC

  DLSw では、分岐回線上の 1 次ステーション、複数の 2 次ステーション、またはポイント・ポイント回線上の単一の完全折衝可能ステーションを表すことができます。
- QLLC

  DLSw は、単一の X.25 インターフェース上の QLLC PVC と SVC のどんな組み合わせでもサポートします。非構成 SVC からの着信コールだけでなく、同じリモート DTE アドレスへのパラレル・バーチャル・サーキットも処理できます。
- APPN

  APPN が同じネットワーク・ユーティリティー内に常駐する DLSw 機能に接続するように構成することができます。したがって、APPN は、DLSw ネットワーク内のどの PU 2.0 または T2.1 SNA エンド・ステーションとでもリンクをもつことができ、その場合に、リモート (特に、事業所) ルーター内に APPN が存在する必要はありません。
- チャネル LSA

  DLSw は、同じネットワーク・ユーティリティー内に常駐する ESCON およびパラレル・チャネル LSA 機能への内部インターフェースをサポートします。したがって、ホストは、 DLSw ネットワーク内のどの SNA エンド・ステーションとでもリンクをもつことができ、その場合に、別々のチャネル・ゲートウェイおよび中央側 DLSw ルーター・プロダクトの必要はありません。

リモート DLSw (IP を通して別のルーターへの) によって、ネットワーク・ユーティリティーの DLSw では、 TCP DLSw フレームからサポートされている DLC タイプのいずれへの変換もサポートします。ローカル DLSw がサポートされるのは、ここに示すように、特定の組み合わせの DLC タイプの場合だけです。

```
          LLC     SDLC    QLLC    APPN    Channel-LSA
LLC       (1)      x       x                 x
SDLC       x       x       x       x         x
QLLC       x       x       x       x         x
APPN               x       x                 x
CHANNEL    x       x       x       x
Note:
1 - You should use bridging for local LLC-to-LLC connectivity.  The
    only exception supported by local DLSW is LLC to a Frame Relay
    bridge port that is configured as a Boundary Access Node (BAN) port.
```

次のリストには、IBM ネットワーク・ユーティリティーの DLSw のその他の機能およびフィーチャーの一部が要約してあります。

- すべての DLSw プロトコル標準に対する動的互換性

  IBM DLSw では、RFC 1434+、RFC 1795 (DLSw バージョン 1)、および RFC 2166 (DLSw バージョン 2) をサポートします。事前構成を伴わないそれぞれのパートナー・ルーターのプロトコル・レベルを動的に検出し、異なるプロトコル・レベルのパートナーを同時に処理することができます。
- 動的およびオンデマンド・パートナー

  IBM DLSw では、非構成パートナーによるサービスを受けるエンド・ステーションのディスカバリー、および構成済みパートナーへの TCP 接続のオンデマンド立ち上げだけでなく、そのような TCP 接続の必要時立ち上げもサポートします。
- マルチキャスト IP ディスカバリー

  マルチキャスト IP アドレスまたはグループの簡単な構成によって、 IBM DLSw では、エンド・ステーションとパートナーの両方のマルチキャスト探索を実行することができます。IBM DLSw には、DLSw バージョン 2 標準を拡張する機能が数多く備えられており、それには、資源登録およびグループ構成の単純化も含まれています。
- トラフィックの優先順位付け

  SNA と NetBIOS の間の優先順位付けだけでなく、個々の回線順位の制御も行うことができる構成オプションがあります。これは、インターフェース・レベルのトラフィックの優先順位付けに対する、帯域幅予約システム (BRS) の拡張サポートに追加されるものです。
- 拡張フィルター項目および静的キャッシュ項目

  IBM DLSw には、MAC アドレスと NetBIOS 名のリスト、および静的キャッシュに対する拡張サポートが組み込まれているので、優先されるリモート・パートナーだけでなく、資源の探索に使用されるリンクについても、制御を行うことができます。
- 負荷平衡と耐障害性

  IBM DLSw では、リモート・パートナーをキャッシュし、近隣優先順位に基づいて、その中から最大フレーム・サイズ・サポート、または最初の応答先を選択することができます。また、近隣優先順位フィーチャーを使用すると、 1 つの中央側ルーターが別のルーターのバックアップとしてしか使用されないようにすることができます。

  重複 MAC アドレスを伴う構成の場合は、近隣優先順位フィーチャーを使用不可にするか、重複 MAC アドレスにアクセスする場合に使用されるパスを制御するように、キャッシュ・パラメーターを設定することができます。

構成例

ここでは、ネットワーク・ユーティリティーのデータ・リンク交換フィーチャーを使用する 3 つのサンプル構成について説明します これらの構成は、次のとおりです。

- DLSw LAN キャッチャー
- DLSw LAN チャネル・ゲートウェイ
- DLSw X.25 チャネル・ゲートウェイ

DLSw LAN キャッチャー

この事例は、図43 に図示してあります。この事例では、リモート・サイトの SNA トラフィックは、DLSw を使用してデータ・センターに戻ります。

ネットワーク・ユーティリティーは、バックボーン LAN セグメント上のデータ・センターにあります。それぞれのリモート・ルーターの DLSw パートナーであり、したがって、それぞれとの TCP セッションが必要です。この方法の利点は、このような TCP セッションの管理および DLSw 接続の終了に必要な CPU サイクルのすべてが、ネットワーク・ユーティリティー内に集中されている点にあります。ネットワーク・ユーティリティーがない場合は、ローカル・ルーターやホスト・ゲートウェイ (DLSw 対応可能の場合) は、この作業負荷による消費の対象となる可能性があります。

ホストの観点から見れば、SNA LLC2 トラフィックは、ホスト・ゲートウェイからネットワーク・ユーティリティー内にブリッジされます。ホスト・ゲートウェイは、IBM 3745/46、IBM 3746、マルチアクセス・エレクロージャー (MAE) 付き、 IBM 2216 のいずれかです。

ネットワーク・ユーティリティー内の 2 ポート・トークンリング・アダプターを活用して、1 つのポート上に IP カプセル化トラフィックを取り込み、もう 1 つのトークンリング・ポート上に LLC2 SNA トラフィックを送り出すことができます。こうすれば、使用可能な帯域幅が 2 倍になり、IP トラフィックと SNA トラフィックを別々のリング上に分離できる利点が加わります。ネットワーク・ユーティリティーでは、それぞれの LLC 接続ごとに、ホストに LLC ローカル確認 (スプーフィング) を提供するので、大規模ネットワーク環境では、キャンパス・バックボーンからのトラフィックが相当量除去されます。

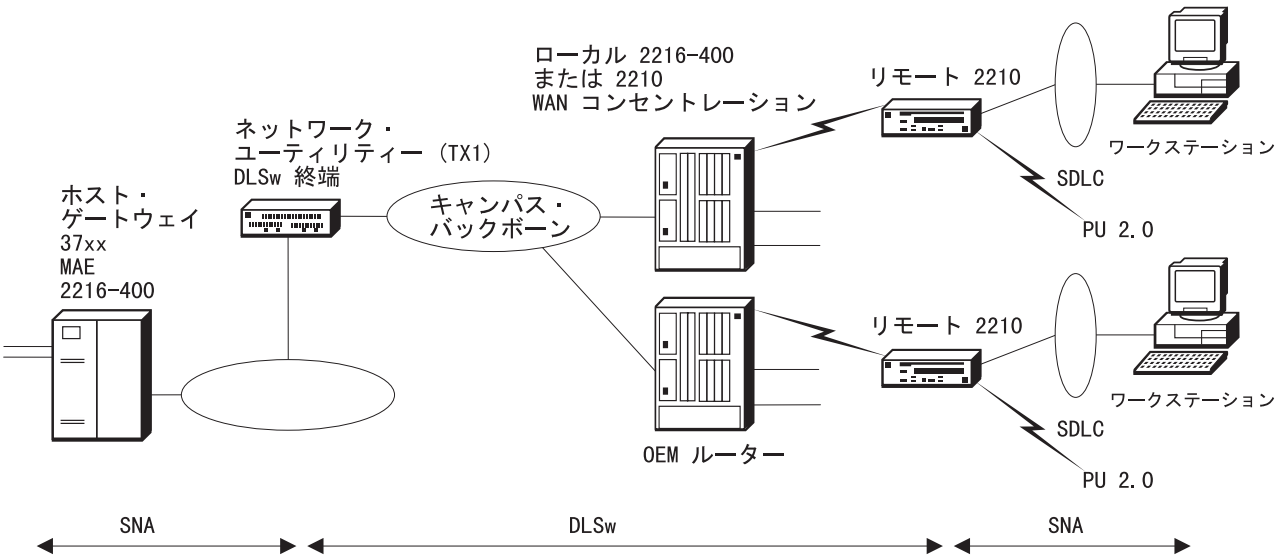


図 43. DLSw LAN キャッチャー

構成のかぎ

大体において、これが標準 DLSw 構成です。ただし、ネットワーク・ユーティリティーを DLSw LAN キャッチャーとして構成するにあたっては、以下の点を心得ている必要があります

- この事例の場合は、リモート・ルーターのどれからの TCP セッションでも可能にするように、ネットワーク・ユーティリティーを構成する必要があります。これは、DLSw 動的近隣と呼ばれています。こうすることによって、ネットワーク・ユーティリティー上でそれぞれの DLSw パートナーの IP アドレスを定義しなくて済みます。動的近隣のデフォルト値は「Enabled (使用可能)」です。
- ネットワーク・ユーティリティーでは、探索フレームがどのように転送されるかを指定することができる、 IBM DLSw インプリメンテーションの新規パラメーターを導入しています。これが特に重要なのは、中央側からのアウトバウンド方向の場合です。このパラメーターは、*enable/disable forwarding explorers* と呼ばれ、これによって、以下のオプションのどれでも指定できる柔軟性が得られます。
  - Disable forwarding of explorer frames (探索フレーム転送の使用不可)

    このオプションを選択すれば、探索フレームの転送が完全に使用不可になります。
  - Forward explorer frames to the local TCP connection only (ローカル TCP 接続のみへの探索フレームの転送)

    探索フレームが WAN リンク上に出ていくのを阻止したい場合は、このオプションが指定できます。ネットワーク・ユーティリティーでは、これがデフォルト値です。
  - Forward explorer frames to all DLSw パートナー (すべての DLSw パートナーへの探索フレームの転送)

    このオプションを選択すると、探索フレームはすべての DLSw パートナーに送り出されます。

DLSw LAN キャッチャー事例で必要な構成パラメーターを詳しく検討したい場合は、286ページの表74 をごらんください。

DLSw LAN チャネル・ゲートウェイ

この事例は、276ページの図44 に図示してあります。DLSw LAN キャッチャー事例の場合と同様、ネットワーク・ユーティリティーでリモート・ルーターからの DLSw セッションが終端します。ただし、この場合は、ESCON チャネル・アダプターがネットワーク・ユーティリティー内にあります。したがって、この構成では、DLSw 機能からのトラフィックは、 LAN セグメント上にブリッジされるのではなく、ネットワーク・ユーティリティー内に構成されている LSA ループバック・インターフェース経由で、チャネルに直接渡されます。

この構成では、ネットワーク・ユーティリティーの使用によるローカル ・キャンパスからホストへの SNA トラフィックのサポートも実証されています。このトラフィックは、 LSA ループバック・インターフェースを通して、キャンパス・バックボーン外にブリッジされます。 ネットワーク内のすべての SNA 装置は、LSA ループバック・インターフェースの MAC アドレスである、同じホストあて先 MAC アドレスを

用いて構成されます。 これには、リモート・サイトの装置だけでなく、メイン・サイトの装置も含まれます。

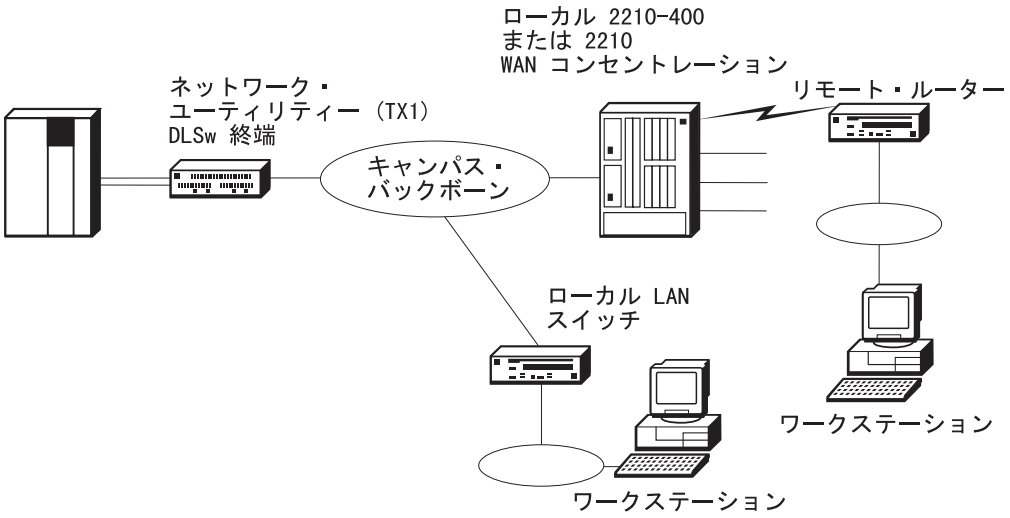


図 44. DLSw LAN チャネル・ゲートウェイ

注: この例に図示されているのは、DLSw トラフィック専用のチャネル・ゲートウェイとしてのネットワーク・ユーティリティーの使用です。ただし、 235 ページのチャネル・ゲートウェイ構成例に図示されている機能の多くは、有効なチャネル・ゲートウェイ構成内で、DLSw 終端と組み合わせることができます。

構成のかぎ

ネットワーク・ユーティリティーを DLSw LAN チャネル・ゲートウェイとして構成するにあたっては、以下の点に注意してください

- LSA インターフェースを構成する必要があり、このインターフェース上でループバックを使用可能にする必要があります。ループバックを使用可能にすると、ネットワーク・ユーティリティー内にバーチャル LAN が作成されます。この LAN 上に 2 つだけある装置が、ホストと DLSw 終端点です。チャネル上のホストを表す MAC アドレスが、LSA インターフェース上で定義されます。これは、ダウンストリーム装置内に構成されるあて先 MAC アドレスです。

  注: また、LSA 直接接続を定義して、トラフィックがローカル LAN セグメントからブリッジされて入ってくるようにすることもできます。このようにした場合は、これらのセグメント上の装置のあて先 MAC アドレスは、リモート装置とは異なるものとなります。LSA 直接インターフェースの MAC アドレスは、LSA ループバック・インターフェースとは異なるものになるからです。
- DLSw を構成するときは、トークンリング・インターフェースだけでなく、 LSA インターフェースの SNA SAP もオープンする必要があります。
- LSA インターフェースのサブチャネル構成は、ホスト内で構成されているパラメーターに一致する必要があります。サブチャネル・パラメーターの説明については、236ページの表68 を参照し、ホスト定義例については、 295ページの『第18章 サンプル・ホスト定義』を参照してください。この情報は、これらのパラメーターがどのように相関するかを見る場合に役立ちます。

- *ローカル TCP 接続* を構成する必要があります。これを行うには、IP アドレスがネットワーク・ユーティリティーの内部アドレスである DLSw パートナーを定義します。これは、ローカル LAN セグメントからホスト内にブリッジされるトラフィック用として使用されます。このトラフィックは、ブリッジされてネットワーク・ユーティリティー内で DLSw 内に入り、そこでローカル TCP 接続がトラフィックを LSA ループバック・インターフェースに渡します
- ネットワーク・ユーティリティーは、現在では、MAC アドレス/SAP ペア (例えば、あて先 MAC アドレス 400022AA0099 と SAP 04) 1 つにつき最大 2048 のリンク・ステーションをサポートします。 2048 を超えるワークステーションが必要な場合は、SAP または MAC アドレスが異なる別の LSA インターフェースを定義する必要があります。それぞれの LSA インターフェースごとに、ESCON チャネル・アダプター上で使用可能な 64 のサブチャネルの中の 1 つが必要であることを忘れないでください。また、対応する XCA 大ノードを定義して、それぞれの LSA インターフェースをサポートする必要もあります。

X.25 チャネル・ゲートウェイ

この事例は、278ページの図45 に図示してあります。ネットワーク・ユーティリティー内のローカル DLSw を使用して、X.25 アドレスと MAC アドレス/SAP ペアの間でマップします。 WAN を通るトランスポートは、固有の修飾論理リンク制御 (QLLC) で、SNA 装置が X.25 ネットワークをまたがって通信できるようにするプロトコルです。ネットワーク・ユーティリティーでは、ローカル DLSw が QLLC と LLC2 フレームの間でプロトコル変換を実行します。

リモート装置の観点から見れば、考慮の対象となる場合が 2 つあります。

1. 事業所ルーターに接続された LAN セグメント上の装置

   ワークステーション上で、SNA アプリケーションによって、ホストに送信したい LLC フレームが生成されます。事業所ルーターが IBM 2210 の場合は、この LLC フレームはブリッジされて、 2210 DLSw 機能に入り、そこで次の 3 つのことが行われます。

   a. LLC フレームから QLLC フレームへのプロトコル変換
   b. 該当する X.25 LCN (PVC) または DTE アドレス (SVC) への着信 MAC アドレス/SAP ペアのマッピング
   c. X.25 への QLLC フレームの受け渡し

   事業所ルーター内の X.25 PAD 機能は、LAPB リンク・レイヤー・パケットを作成して、PVC (または SVC) を通して送信します。

   IBM 2210 以外の製品が事業所ルーターの役割を務める場合は、これらの機能を実行する必要がありますが、そのためにローカル DLSw を使用しなくても構いません。

2. X.25 ネットワーク上に直接ある装置 (例えば、IBM 3174 制御装置、または広域コネクター・アダプター経由で接続された eNetwork 通信サーバー・ゲートウェイ・マシン)

   これらの装置上で、SNA は QLLC をネイティブ DLC タイプとして使用します。QLLC フレームを生成して、構成済み PVC (または SVC) を通して送り出します。

以上のいずれの場合も、ネットワーク・ユーティリティーでは、LAPB パケットが X.25 回線を通して受信され、まず QLLC に、次に DLSw に渡されます DLSw では、次の 2 つのことが行われます。

1. QLLC から LLC2 フレームへのプロトコル変換
2. LSA ローカル・ループバック・インターフェースの MAC アドレス/SAP への X.25 LCN (PVC) または DTE アドレス (SVC) のマッピング

次に、トラフィックは、ESCON チャネルを通るトランスポートに備えて、 LSA ループバック・インターフェースに渡されます。

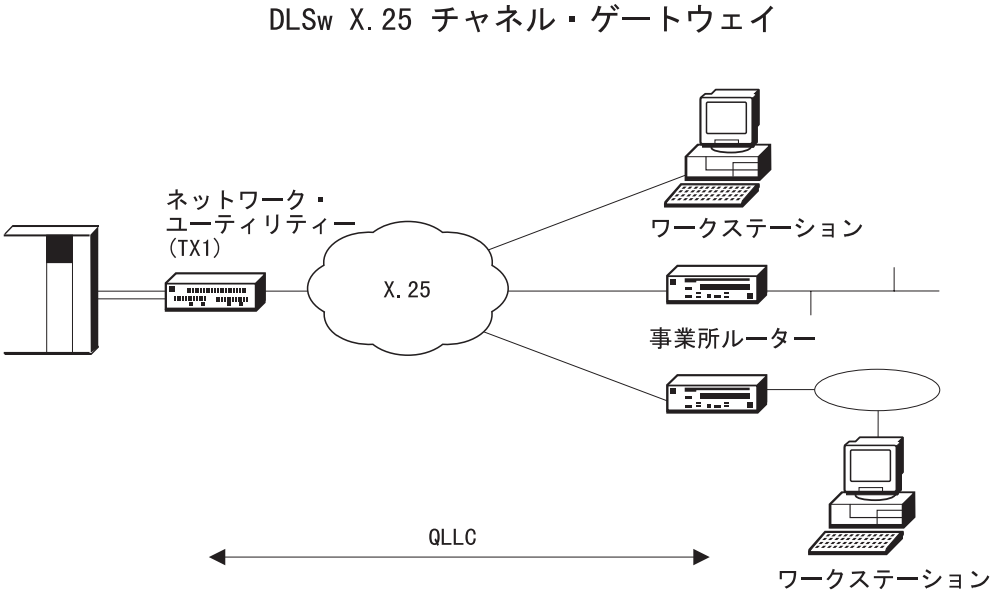


図 45. DLSw X.25 チャネル・ゲートウェイ

構成のかぎ

この事例の場合に実行する必要がある一般的な構成タスクを要約して、以下にリストにしてあります。詳細については、他の DLSw および LSA ループバック構成を参照してください。LSA ループバック・インターフェースは、 275ページの『DLSw LAN チャネル・ゲートウェイ』で同様にして構成されています。

- ESCON および LSA インターフェースを追加および構成します。
- X.25 インターフェースを追加および構成します。コマンド行から、 talk 6 で **net** コマンドを使用して、 X.25 Config (構成) サブプロセスに入り、その上で次のコマンドを使用します。
  - **set address** (ローカル DTE アドレスの設定)
  - **add protocol dlsw** (X.25 プロトコルとしての DLSw の追加)
  - **add pvc** または **add svc** (個々の PVC または SVC の範囲の追加)
- 他の例の場合と同様に IP 内部アドレスを構成します。
- DLSw を構成します。
  - 汎用 DLSw の構成 (使用可能、SRB セグメント、エクスプローラーのローカル転送)
  - DLSw ローカル TCP 接続の構成

– LSA ループバック用の DLSw の構成 (LSA インターフェースの SAP のオープン)

以上の一般的なタスクに加えて、X.25 アドレスを LSA ループバック MAC アドレスにマップするための、ネットワーク・ユーティリティーの DLSw を構成する必要があります。これには、次の 3 通りの方法があります。

- DLSw で、それぞれが独自のあて先 MAC アドレスをもつ、X.25 ステーションを個別に構成する。このオプションは、PVC と SVC の両方が対象になります。
- それぞれが独自のあて先 MAC アドレスをもつ、接続 ID のリストを構成する。X.25 ステーションには、コールする時に接続 ID を送信できるものがあり、ネットワーク・ユーティリティーでは、この値を構成済みリストに突き合わせます。このオプションの対象となるのは、SVC だけです。
- 接続 ID が含まれていない着信コールのデフォルトあて先 MAC アドレスを構成する。このオプションの対象となるのは、SVC だけです。

これ以降では、上記の 3 通りのアドレス・マッピング方式のそれぞれについて、その構成方法を説明します。

リモート X.25 ステーション数が相対的に少ない場合は、DLSw 内の各リモート X.25 装置が、それぞれ LSA ループバック MAC アドレスにマップされるように構成することができます。コマンド行を使用してこれを行う場合は、 * プロンプトで **talk 6** と入力して、次のように入力します。

- **protocol dls**
  – **add qllc station** (それぞれの X.25 ステーションごとに 1 回ずつ) システムがプロンプトを出して、以下の入力を指示してきます。
    - インターフェース番号 (X.25 インターフェース)
    - PVC または SVC
    - 論理チャネル番号 (PVC の場合) または DTE アドレス (SVC の場合)
    - 発信元 MAC および SAP (DLSw による生成可能)
    - あて先 MAC および SAP (LSA ループバック MAC アドレスの入力)
    - PU タイプ
    - XID ブロック/番号 (PU タイプが 2 の場合)

構成プログラムを使用してこれを行う場合は、次のようにします。

- プロトコル/DLSw/インターフェース/シリアル X25/QLLC ステーション
  – QLLC ステーションの追加 (上記と同じ情報の入力)

リモート X.25 ステーションが、コールする時に接続 ID を送信するように構成できる場合は[21]、 接続 ID 値をあて先 MAP アドレスにマップするように、 DLSw を構成することができます。コマンド行を使用してこれを行う場合は、 * プロンプトで **talk 6** と入力して、次のように入力します。

- **protocol dls**
  – **add qllc destination** (それぞれの有効な接続 ID ごとに 1 回ずつ)。システムがプロンプトを出して、以下の入力を指示してきます。
    - 接続 ID
    - あて先 MAC および SAP (LSA ループバック MAC アドレスの入力)

構成プログラムを使用してこれを行う場合は、次のようにします。

21. QLLC プロダクトでは、しばしば、このパラメーターが接続パスワードとして表示されます。

- プロトコル/DLSw/QLLC あて先
  - QLLC あて先の追加 (上記と同じ情報の入力)

最後になりましたが、それぞれのリモート X.25 ステーションの構成、または接続 ID の使用の実現可能性がない場合は、DLSw ANYCALL フィーチャーを使用して、着信する X.25 コールがあれば受け入れ、LSA ループバック MAC アドレスにマップすることができます。コマンド行を使用してこれを行う場合は、 * プロンプトで **talk 6** と入力して、次のように入力します。

- **protocol dls**
  - **add qllc destination** (1 回、ただし、希望する場合は、これに特定の接続 ID を追加することができる)。システムがプロンプトを出して、以下の入力を指示してきます。
    - 接続 ID (ワード 'ANYCALL' の使用)
    - あて先 MAC および SAP (LSA ループバック MAC アドレスの入力)

構成ツールを使用してこれを行う場合は、次のようにします。

- プロトコル/DLSw/QLLC あて先
  - QLLC あて先の追加 (上記と同じ情報の入力)

DLSw の管理

ここでは、DLSw 機能の監視および管理ができる方法の一部を紹介します。

コマンド行監視

DLSw では、状況の表示、構成パラメーターの動的監視、および接続の状態の能動的制御を行うための、広範囲にわたるコマンドのセットをサポートします。これらのコマンドについては、*MAS プロトコル構成と監視解説書 第 1 巻* の「DLSw の構成と監視」の章で詳述されています。これらのコマンドにアクセスする場合は、* プロンプトで **talk 5** と入力し、+ プロンプトで **protocol dls** と入力します。

状況を監視する上で特に有用なコマンドの一部に、次のようなものがあります。

list tcp sess

パートナー・ルーターへのすべての既知の TCP 接続の状況が表示されます。使用中の DLSw プロトコルのレベル、およびそれぞれの接続を使用する DLSw 回線数に関する要約統計を表示させて見ることができるだけでなく、TCP 接続がアップおよびダウンになるのに応じて、その状態を表示させて見ることもできます。DLSw が動的 (構成済みでない) パートナーからだけの TCP 接続を受け入れるように構成した場合は、このコマンドによって、構成がリモート・ルーターによって開始される状況が表示されます。リモート・ルーターが能動的に TCP 接続をアップにしていない場合は、状況はないことになります。

「ローカル TCP 接続」がローカル DLSw 機能を使用可能にするように構成した場合は、この構成にはコマンド出力でそのようにフラグが付けられるので、リモート・パートナー接続とは区別することができます。

list dls sess all

すべてのアクティブ DLSw セッションの状況が表示されます。セッションは、回線とも呼ばれ、MAC および SAP アドレスの 4 タプルで定義され、

SNA LU-LU セッションではなく、SNA リンクに対応します。セッションは、通常、 SNA エンド・ステーションによる駆動でアップおよびダウンになるので、このコマンドの出力は動的です。すべてのセッションについて、それぞれその識別 MAC および SAP アドレス、状態、セッションの接続に介在するパートナー、および詳細を入手する場合に、 **list dls sess detail** コマンドで使用できる識別子を表示させて見ることができます。ローカル DLSw セッション (このルーターだけが関与するセッション) が、このコマンドからの 2 行の出力として表示されます。

ネットワーク・ユーティリティーでは、アクティブ・セッションの数が簡単に何百何千にも達する可能性があるため、**list dls session** コマンドをさまざまに変えて使用し、そのサブセットだけを表示させることができます。例えば、「all」というキーワードの代わりに別のキーワードを使用して、特定のパートナーを介する回線だけを表示させたり、特定の状態の回線だけを表示させたりします。セッションを選択するために定義されているキーワードが 10 ほどあります。このようなコマンドすべての出力は、画面がいっぱいになると一時停止して、継続するか終了するかを指示するキーストロークを待ちます。したがって、次の画面に表示される出力を見たい場合は、スペース・バーを押します。

list dls mem

DLSw メモリーのさまざまなプールの状況、ならびにすべてのアクティブ・セッションのメモリー輻輳 (ふくそう) 状況が表示されます。

list llc sess all

LLC をルーターとエンド・ステーションの間のプロトコルとして使用するすべての DLSw セッションに関する、802.2 LLC 特定状況情報が表示されます。これには、LAN、チャネル、ATM、およびリモート・ブリッジ WAN インターフェースを通して実行されるセッションが含まれます。コマンド出力には、詳細な状態情報、ならびに、該当する場合は、エンド・ステーションへのソース・ルートが含まれます。

list sdlc sess all

SDLC をルーターとエンド・ステーションの間のプロトコルとして使用するすべての DLSw セッションに関する、SDLC 特定状況情報が表示されます。コマンド出力には、SDLC アドレス情報、ならびに状態情報が含まれます。SDLC 装置を使用する作業の場合は、汎用コマンドである **list dls sess** よりも、このコマンドの方が有用です。

list qllc sess

「QLLC over X.25」をルーターとエンド・ステーションの間のプロトコルとして使用するすべての DLSw セッションに関する、QLLC 特定状況情報が表示されます。コマンド出力には、QLLC アドレス情報、ならびに詳細な状態情報が含まれます。ルーターでは着信動的 SVC をサポートするため、構成済みと動的の両方の QLLC PVC および SVC の状態を表示させて見る場合は、このコマンドが欠かせません。

DLSw では、talk 6 のもとで構成できるパラメーターの大多数について、talk 5 のもとでの動的変更をサポートします。DLSw は標準モデルに従います。つまり、 talk 5 のもとで行われた変更は即時に有効となりますが、ボックス・リブートが行われる

と消失し、talk 6 のもとで行われた変更は、ボックス・リブートが行われて初めて有効になります。 talk 5 **list** コマンドでは、実行プロダクト内で現在アクティブの値が表示されます。

talk 5 コマンド **delete** および **disable** を使用すると、既存の DLSw 接続を切断することができます。例えば、 **delete dls** *session number* を使用すれば、ハング・セッションを終結処理し、エンド・ステーションにそれを再駆動させることができます。 **Delete/add** と **disable/enable** のシーケンスは、構成済み TCP、SDLC、および QLLC 接続のリサイクルを行うための強力な方式となります。

イベント・ログ・サポート

DLSw には、正常なイベントに関する通知メッセージから重大なエラー条件の警告に至るまで、何百もの ELS メッセージが定義されています。ELS メッセージが生成される可能性がある DLSw イベントのタイプの一部を、以下に挙げておきます。

- 初期化および構成のエラー
- パートナー TCP 接続および機能フレームの送信または受信
- 特定の MAC アドレスまたは NetBIOS 名に関する探索フレームの送信または受信
- 回線設定/切断フレームの送信または受信
- DLC リンク設定/切断フレームの送信または受信
- アクティブ回線でのデータ・フレームの送信または受信
- アクティブ回線での「ペーシング」ウィンドウの変更
- メモリー割り振りエラー
- 予期しないプロトコル・フロー、フレームの廃棄
- フレーム・フローの構成との不一致

このようなメッセージは、第一義的には、確かにソフトウェア・エンジニアが問題の解決にあたって使用するものには違いありませんが、DLSw プロトコルや DLC リンク起動フローについて基本的な知識があれば、ユーザーでもその意味を理解し、簡単な構成間違いのデバッグを行うことができるはずです。これらの ELS メッセージをアクティブにし、talk 2 を使用して出力を監視すれば、少なくとも「Is anything happening?」という質問には応答できるはずです。

「DLS」は、ELS 内で名前が付けられている サブシステム の 1 つです。標準的なエラー・メッセージのセットをアクティブにする場合は、talk 6 と talk 5 のどちらかのもとで、イベント・メニューで **disp sub dls** と入力します。すべての DLSw メッセージをアクティブにする場合は、 **disp sub dls all** と入力します。メッセージを非アクティブにするための対応するコマンドは、いずれも始めが **nodisp** になります。ELS メッセージの制御および表示に関する全般的な説明については、100ページの『イベント・メッセージの監視』を参照してください。

リンク起動試行のトレースを試みている場合は、DLSw メッセージだけでは全体像の完全な把握はできない場合があります。基礎にある DLC タイプに関する ELS メッセージは、次のようにしてアクティブにすることができます。

LLC disp sub llc all
SDLC disp sub sdlc all
QLLC disp sub qllc all
disp sub x253 all (X.25 レイヤー 3、パケット・レイヤー)
チャネル LSA
disp sub lsa all

個々のメッセージおよびその意味をすべて網羅したリストが必要な場合は、*イベント・ログ・システム・メッセージの手引き* (CD-ROM および 2216 Web ページ) を参照してください。

SNA 管理サポート

VTAM または NetView/390 オペレーター・コンソールから、111ページの『NetView/390』で説明しているように、DLSw にかかわるリンク、PU、および LU を制御することができます。

APPN の場合とは異なり、ネットワーク・ユーティリティーの DLSw が SNA アラートを送信することはありません。トラップを送信し (次の項で説明)、トラップを生成する可能性がある ELS メッセージを起動します。107ページの『IBM Nways Manager for AIX』で言及されているプロダクトを使用すれば、このようなトラップをアラートに変換することができます。

SNMP MIB およびトラップ・サポート

ネットワーク・ユーティリティーの DLSw には、RFC 2024 に文書化されている IETF 標準 DLSw MIB に対する完全な読み取り専用サポートと部分的な読み取り/書き込みサポートが備えられています。この大規模な MIB によって、RFC 1795 および 2166 を実装する製品が備えているはずの重要な構成、状況、および料金計算の情報のほとんどは、表示させて見ることができます。この情報には、以下のものがあります。

- 構成
  - ノード特性 (例えば、動的パートナーが使用可能になっている)
  - 構成済みパートナー情報
  - 構成済みディレクトリー/キャッシュ項目
- 状況
  - ノードがアップかダウンか、時間的長さ
  - アクティブ TCP 接続、時間的長さ、動的パートナー情報
  - 動的ディレクトリー/キャッシュ情報
  - アクティブ回線、時間的長さ、DLC 情報
- 統計および料金計算
  - TCP 接続のアップおよびダウン (正常およびエラー) のカウント
  - パートナー別のデータおよび制御フレームのカウント
  - 回線のアップおよびダウンのカウント
  - 回線別フレーム・カウントのための基礎 DLC MIB の索引
  - アクティブ回線のペーシング・カウント

ネットワーク・ユーティリティーの DLSw では、RFC 2024 に定義されているすべてのトラップをサポートし、以下のイベントを報告します。

- 機能交換障害または DLSw プロトコル違反による、 TCP 接続の終了
- TCP 接続のアップまたはダウン
- 回線のアップまたはダウン

DLSw はすべてがトラップ制御データ項目をサポートするので、管理ステーションでは、トラップが生成される条件を設定することができます。

ネットワーク・ユーティリティーの DLSw では、RFC 2024 に加えて、マルチキャスト IP ベースのグループおよび QLLC ステーションに関する、IBM 特定 DLSw MIB 拡張機能もサポートします。

ネットワーク管理アプリケーション・サポート

107ページの『IBM Nways マネージャー・プロダクト』で説明されている Nways マネージャー・プロダクトに実装されているネットワーク・ユーティリティーの Java ベースのアプリケーションには、標準 DLSw MIB および IBM 特定 DLSw MIB 拡張機能に対する統合サポートが備えられています。

これらのプロダクトを使用して、DLSw 資源およびその状況を表示させて見る場合は、 DLSw MIB およびその基礎の DLC レイヤー MIB (LLC、SDLC、または X.25) からの情報が表示される、特定のパネルを立ち上げます。また、内蔵ブラウザー・サポートを使用すれば、これらの MIB のいずれに入っている情報でも表示させて見ることができます。

Nways マネージャー・プロダクトからの DLSw トラップの発行を制御することができるので、特定のトラップについて、常時生成させることも、絶対に生成させないことも、特定の条件下でのみ生成させることもできます。

Nways Manager for AIX では、ネットワークの DLSw トポロジー・ビューが、 DLSw 接続、資源、および色分けされた状況を含めて表示されます。トポロジーは、新しいノードが検出されると最新表示されます。 このアプリケーションでは、DLSw IP マルチキャスト・グループのトポロジーは表示されません。

第17章 DLSw 構成例の詳細

この章には、271ページの『第16章 データ・リンク交換』の DLSw ネットワーク構成の例の幾つかに関する図と構成パラメーター表が挙げてあります。パラメーター値は、実際の作業テスト構成での値が示してあります。

構成パラメーター表の欄および規則の説明については、 144ページの『構成例表の規則』を参照してください。

ネットワーク・ユーティリティー ワールド・ワイド・ウェブ (WWW) ページには、ここに挙げてある構成パラメーター表に一致する 2 進構成ファイルが収められています。これらのファイルにアクセスする場合は、下記のアドレスから Download リンクをたどってください。

```
http://www.networking.ibm.com/networkutility
```

この章に記載されている構成は、次のとおりです。

表 73. 構成例情報の相互参照

構成記述	パラメーター表
274ページの『DLSw LAN キャッチャー』	286ページの表74
275ページの『DLSw LAN チャネル・ゲートウェイ』	291ページの表75

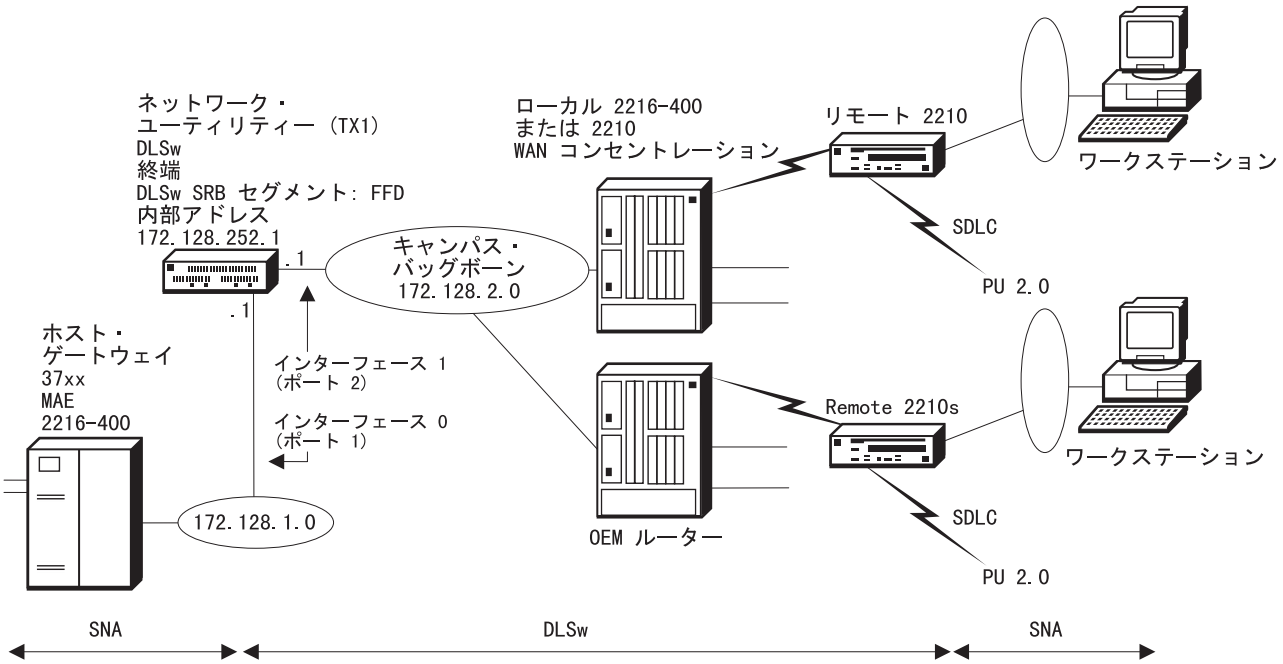


図 46. DLSw LAN キャッチャー

表 74. DLSw LAN キャッチャー. この構成の説明については 274 ページを、図については 285 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR	次の行の ″add device″ を参照	1
装置 アダプター ポート	スロット 1/ポート 1: インターフェース 0: TR スロット 1/ポート 2: インターフェース 1: TR	Config>**add dev tok** (ポート別に 1 回ずつ)	2
装置 インターフェース	インターフェース 0 MAC アドレス : 400022AA0001 パケット・サイズ : 4399 インターフェース 1 MAC アドレス : 400022AA0002 パケット・サイズ : 4399	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01** TKR config>**packet 4399** TKR config>**exit** Config>**net 1** TKR config>**set phy 40:00:22:AA:00:02** TKR config>**packet 4399**	
システム 一般	システム名 : NU_A ロケーション : XYZ 連絡先 : 管理者	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	3
プロトコル IP 一般	内部アドレス : 172.128.252.1 ルーター ID: 172.128.1.1	Config>**p ip** IP config>**set internal** IP config>**set router-id**	
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.1 サブネット・マスク : 255.255.255.0 インターフェース 1 (TR スロット 1 ポート 2) IP アドレス : 172.128.2.1 サブネット・マスク : 255.255.255.0	IP config>**add address** (インターフェース 1 つにつき 1 回)	4

表 74. DLSw LAN キャッチャー (続き). この構成の説明については 274 ページを、図については 285 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf**	5
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック) インターフェース 1 OSPF (チェック)	OSPF Config> **set interface** Interface IP address **172.128.1.1** Attaches to area **0.0.0.0** (他のデフォルトを受け入れる) OSPF Config>**set interface** Interface IP address **172.128.2.1** Attaches to area **0.0.0.0** (他のデフォルトを受け入れる)	
プロトコル DLSw 一般 一般	DLSw (チェック) SRB セグメント : FFD エクスプローラーの転送 : 使用不可	Config>**p dls** DLSw Config>**enable dls** DLSw Config>**set srb** DLSw Config>**disable forward all**	6
プロトコル DLSw 一般 動的近隣	動的近隣 (チェック)	DLSw Config>**enable dynamic**	7
プロトコル DLSw インターフェース	インターフェース 0 (TR スロット 1 ポート 1) SAP タイプ : SNA (SAP 0、4、8、C)	DLSw Config>**open 0 sna**	8
プロトコル ブリッジング 一般	ブリッジング (チェック) DLSw (チェック)	Config>**p asrt** ASRT config>**enable br** ASRT config>**enable dls**	9

表 74. DLSw LAN キャッチャー (続き). この構成の説明については 274 ページを、図については 285 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル ブリッジング インターフェース	インターフェース 0 (TR スロット 1 ポート 1) ブリッジング・ポート (チェック) インターフェース・サポート : SRB セグメント番号 : 001 MTU サイズ : 4399	('enable br' が前提) ASRT config>**disable transp 1** ASRT config>**enable source 1** ASRT config>**delete port 2**	10

注：

1. **add dev** で定義するのは、単一のポートであり、アダプターではありません。
2. 構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。 コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。
3. 書き込み対応可能 SNMP コミュニティーが必要なのは、構成ファイルを構成プログラムからルーターに直接ダウンロードしたい場合だけです。ルーターへの構成ファイルの TFTP を実行する場合は、SNMP は必要ありません。
4. DLSw がこの例で正しく機能するためには、インターフェース 1 だけが IP 用として構成される必要があります。インターフェース 0 がここで構成されているのは、ボックス管理の目的だけのためです。
5. OSPF の代わりに RIP を使用することもできます。
6. 汎用フィルターとしてのリモート・エクスプローラーの転送を使用不可にするのは、バックボーン LAN トラフィックがリモート・サイトへの WAN リンク上で、DLSw 探索メッセージを生成しないようにするためです。 つまり、すべての回線が、リモート・ルーターによって開始される必要があることを意味します。ネットワークで、ホストがリモート・サイトへの接続を開始できることを必要とする場合は、このパラメーターを「forward to all DLSw peers」に変更します。

   リモート・ルーターが IBM ルーターである場合は、MAC アドレスおよび NetBIOS 名のリストを使用して、受信したい探索メッセージを制御するように、個別に構成することができます。また、*connectivity setup type* パラメーターを使用して、それぞれがいつでもネットワーク・ユーティリティーへのその TCP 接続を立ち上げるか、使用しないときに除去するかを構成することもできます。
7. 動的近隣の使用可能がデフォルト値なので、このパネルの変更もこのコマンドの発行も必要ありません。ここでこれを示したのは、このパラメーターを使用すれば、リモート DLSw パートナー (近隣) がこのネットワーク・ユーティリティーへの TCP 接続を確立することができ、ユーザーがここで IP アドレスを定義する必要はないことを指摘するためです。 それぞれのリモート・ルーターごとに、このネットワーク・ユーティリティーの内部 IP アドレス (172.128.252.1) をそのパートナー・アドレスとして、構成する必要があります
8. インターフェース 1 では SAP をオープンする必要はありません。このインターフェースが伝達するのは IP トラフィックだけで、LLC トラフィックは伝達しないからです。
9. ″enable br″ では、両方のトークンリング・インターフェース用の TB ブリッジ・ポートが自動的に作成されます。ブリッジ・ポート番号は、 1 および 2 で、アダプター・ポート番号からは独立しています。
10. 「disable」および「enable」コマンドで、ブリッジ・ポート 1 は、 TB から SRB に切り替わります。「delete port」コマンドでは、インターフェース 1 (ブリッジ・ポート 2) でのブリッジングがオフになります。 このインターフェースでのブリッジングが必要になるのは、キャンパス・バックボーンからホストへの、ローカル・エンド・ステーション・トラフィックのブリッジングをサポートする場合です。

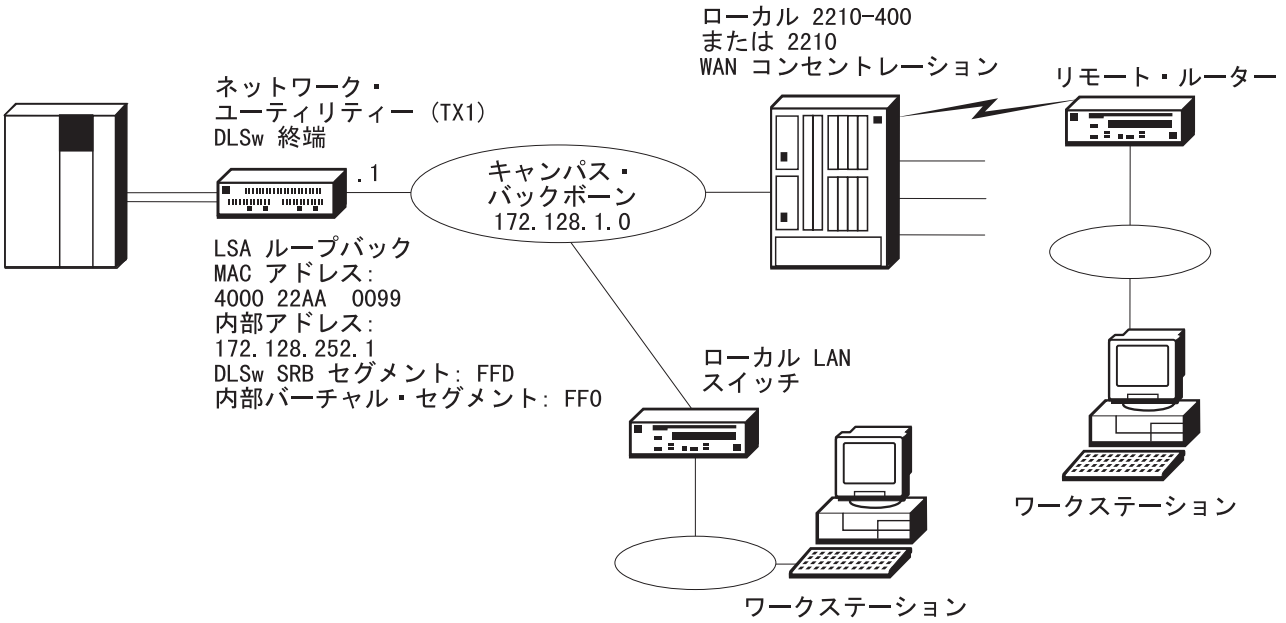


図 47. DLSw LAN ゲートウェイ

表 75. DLSw LAN ゲートウェイ. この構成の説明については 275 ページを、図については 290 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
装置 アダプター スロット	スロット 1: 2 ポート TR スロット 2: ESCON	次の行の ″add device″ を参照	1
装置 アダプター ポート	スロット 1/ポート 1: インターフェース 0: TR スロット 2/ポート 1: インターフェース 1: ESCON	Config>**add dev tok** Config>**add dev escon**	2
装置 インターフェース	インターフェース 0 MAC アドレス : 400022AA0001	Config>**net 0** TKR config>**set phy 40:00:22:AA:00:01**	
装置 チャネル・アダプター ESCON インターフェース ESCON インターフェース	基本ネットワーク番号 : 1 プロトコル・タイプ : LSA (これを最初に行う) ループバック (チェック - これを 2 番目に行う) LAN タイプ : トークンリング 最大データ・フレーム : 2052 MAC アドレス : 400022AA0099	Config>**net 1** ESCON Config>**add lsa** (インターフェース 2 として追加) ESCON Add Virtual>**enable loopback** ESCON Add Virtual>**mac 40:00:22:AA:00:99** ESCON Add Virtual>**lan tok** ESCON Add Virtual>**maxdata 2052** (次の行との同一セッション内で継続)	3
装置 チャネル・アダプター ESCON インターフェース ESCON サブチャネル	インターフェース 2、基本ネットワーク 1、 プロトコル LSA 装置アドレス : E4 サブチャネル・タイプ : 読み取り/書き込み リンク・アドレス : EF	ESCON Add Virtual>**subchannel add** (継続) ESCON Add LSA Subchannel>**device E4** ESCON Add LSA Subchannel>**link EF** (**exit** を 2 回入力した上で、 **list all** と入力)	
システム 一般	システム名 : NUA_SC1C ロケーション : XYZ 連絡先 : Admin	Config>**set host** Config>**set location** Config>**set contact**	
システム SNMP Config (構成) 一般	SNMP (チェック)	Config>**p snmp** SNMP Config>**enable snmp**	

表 75. DLSw LAN ゲートウェイ (続き). この構成の説明については 275 ページを、図については 290 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
システム SNMP Config (構成) コミュニティー 一般	コミュニティー名 : admin アクセス・タイプ : 読み取り/書き込みトラップ コミュニティー・ビュー : All	SNMP Config>**add community** SNMP Config>**set comm access write**	4
プロトコル IP 一般	内部アドレス : 172.128.252.1 ルーター ID: 172.128.1.1	Config>**p ip** IP config>**set internal** IP config>**set router-id**	
プロトコル IP インターフェース	インターフェース 0 (TR スロット 1 ポート 1) IP アドレス : 172.128.1.1 サブネット・マスク : 255.255.255.0	IP config>**add address**	
プロトコル IP OSPF 一般	OSPF (チェック)	Config>**p ospf** OSPF Config>**enable ospf**	5
プロトコル IP OSPF エリア構成 一般	エリア番号 : 0.0.0.0 スタブ・エリア (チェックしない)	OSPF Config>**set area**	
プロトコル IP OSPF インターフェース	インターフェース 0 OSPF (チェック)	OSPF Config>**set interface** Interface IP address **172.128.1.1** Attaches to area **0.0.0.0** (他のデフォルトを受け入れる)	
プロトコル DLSw 一般 一般	DLSw (チェック) SRB セグメント : FFD エクスプローラーの転送 : ローカル TCP 接続のみ	Config>**p dls** DLSw Config>**enable dls** DLSw Config>**set srb** DLSw Config>**enable forward local**	6
プロトコル DLSw 一般 動的近隣	動的近隣 (チェック)	DLSw Config>**enable dynamic**	7

表 75. DLSw LAN ゲートウェイ (続き). この構成の説明については 275 ページを、図については 290 ページを参照してください。

構成プログラム・ナビゲーション	構成プログラム値	コマンド行コマンド	注
プロトコル DLSw TCP 接続	(追加) 近隣 IP アドレス : 172.128.252.1 (これはルーター内部 IP アドレス)	DLSw Config>**add tcp** DLSw neighbor IP address: **172.128.252.1** (他のデフォルトを受け入れる)	8
プロトコル DLSw インターフェース	インターフェース 0 (TR スロット 1 ポート 1) SAP タイプ : SNA (SAP 0、4、8、C) インターフェース 2 (ESCON-LSA) SAP タイプ : SNA (SAP 0、4、8、C)	DLSw Config>**open 0 sna** DLSw Config>**open 2 sna**	9
プロトコル ブリッジング 一般	一般タブ : ブリッジング (チェック) DLSw (チェック) SRB タブ : 内部バーチャル・セグメント : FF0	Config>**p asrt** ASRT config>**enable br** ASRT config>**enable dls**	10
プロトコル ブリッジング インターフェース	インターフェース 0 (TR スロット 1 ポート 1) ブリッジング・ポート (チェック) インターフェース・サポート : SRB セグメント番号 : 001 MTU サイズ : 2052	('enable br' が前提) ASRT config>**disable transp 1** ASRT config>**enable source 1**	11

注：

1. **add dev** で定義するのは、単一のポートであり、アダプターではありません。
2. 構成プログラムでは、1 つのアダプターのすべてのポートにインターフェース番号を自動的に割り当てるので、使用したくないものは削除します。 コマンド行からは、使用したいそれぞれのポートごとに、 **add dev** コマンドを入力すると、インターフェース番号 (「ネット番号」とも呼ばれる) がコマンドの出力として表示されます。
3. この LSA ループバック・インターフェースを表す MAC アドレスは、 DLSw ネットワーク内のすべてのエンド・ステーションが、ネットワーク・ユーティリティーを介してホストにアクセスする場合に使用する、ターゲット MAC アドレスです
4. 書き込み対応可能 SNMP コミュニティーが必要なのは、構成ファイルを構成プログラムからルーターに直接ダウンロードしたい場合だけです。ルーターへの構成ファイルの TFTP を実行する場合は、SNMP は必要ありません。
5. OSPF の代わりに RIP を使用することもできます。
6. ローカル転送を使用可能にして、ローカル・キャンパスのエンド・ステーションがホストにアクセスできるようにします。汎用フィルターとしてのリモート・エクスプローラーの転送を使用不可にするのは、バックボーン LAN トラフィックがリモート・サイトへの WAN リンク上で、DLSw 探索メッセージを生成しないようにするためです。つまり、すべてのリモート回線が、リモート・ルーターによって開始される必要があることを意味します。ネットワークで、ホストがリモート・サイトへの接続を開始できることを必要とする場合は、このパラメーターを「forward to all DLSw peers」に変更します。

   リモート・ルーターが IBM ルーターである場合は、MAC アドレスおよび NetBIOS 名のリストを使用して、受信したい探索メッセージを制御するように、個別に構成することができます。また、*connectivity setup type* パラメーターを使用して、それぞれがいつでもネットワーク・ユーティリティーへのその TCP 接続を立ち上げるか、使用しないときに除去するかを構成することもできます。
7. 動的近隣の使用可能がデフォルト値なので、このパネルの変更もこのコマンドの発行も必要ありません。ここでこれを示したのは、このパラメーターを使用すれば、リモート DLSw パートナー (近隣) がこのネットワーク・ユーティリティーへの TCP 接続を確立することができ、ユーザーがここで IP アドレスを定義する必要はないことを指摘するためです。 それぞれのリモート・ルーターごとに、このネットワーク・ユーティリティーの内部 IP アドレス (172.128.252.1) をそのパートナー・アドレスとして、構成する必要があります
8. 近隣としての内部 IP アドレスの追加が必要なのは、 DLSw が ESCON/LSA インターフェースからバックボーン LAN へトラフィックを伝達できるようにする場合です。
9. SAP がインターフェース 0 でオープンされるのは、ローカル LAN スイッチへの LLC フローを使用可能にする場合で、リモート DLSw が動作するためには必要ありません。
10. ″enable br″ では、トークンリング・インターフェース用の TB ブリッジ・ポートが自動的に作成されます。 ブリッジ・ポート番号は 1 で、アダプター・ポート番号およびボックス・インターフェース番号からは独立しています。
11. 「disable」および「enable」コマンドで、ブリッジ・ポート 1 は、 TB から SRB に切り替わります。このインターフェースでのブリッジングが必要になるのは、キャンパス・バックボーンからホストへ、DLSw を通ってループするローカル・エンド・ステーション・トラフィックをサポートする場合です。

第18章 サンプル・ホスト定義

この章には、本書で使用している構成のネットワーク・ユーティリティーに関するホスト定義の例が示してあります。

特に、次の環境の場合の定義が紹介してあります。
- LSA
- LCS
- MPC+

さらに、ネットワーク・ユーティリティーに ESCON チャネル・アダプターが使用されている場合と、パラレル・チャネル・アダプターが使用されている場合の相違点が強調してあります。

ホストに対するネットワーク・ユーティリティーの定義について詳しくは、*IBM 2216 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*、SC88-6699 を参照してください。

概説

ホストに対してチャネル接続ネットワーク・ユーティリティーを定義する手順には、次の 3 つのステップがあります。

1. ホスト・チャネル・サブシステムに対してネットワーク・ユーティリティーを定義する。

   使用している MVS バージョンに応じて、入出力構成プログラム (IOCP) とハードウェア構成定義 (HCD) のいずれかから行います (HCD の場合は、MVS/ESA SP バージョン 4.2 以降、 APAR# OY67361 付きが必要です)。

   ESCON チャネル接続装置とパラレル・チャネル接続装置とでは、定義ステートメントが多少異なっています。これらの定義の例は、 296ページの『サンプル・ホスト IOCP 定義』に示してあります。
2. ホスト・オペレーティング・システムに対してネットワーク・ユーティリティーを制御装置として定義する。

   ほとんどのシステムで、ESCON チャネル・アダプターの場合もパラレル・チャネル・アダプターの場合も、定義は同じです。明らかに、使用しているオペレーティング・システムしだいです。これらの定義の例は、299ページの『オペレーティング・システムでのネットワーク・ユーティリティーの定義』に示してあります。
3. ホスト TCP/IP または VTAM に対してネットワーク・ユーティリティーを定義する。

   ネットワーク・ユーティリティー上で定義するインターフェースが LSA (SNA) であるか、 LCS (TCP/IP) であるか、MPC+ (SNA または TCP/IP、あるいはその両方) であるかによって、定義は異なります。 301ページの『VTAM 定義』の節に、必要な VTAM 定義の例が示してあります。307ページの『ホスト IP 定義』の節に、必要な TCP/IP 定義の例が示してあります。

チャネル・サブシステム・レベルでの定義

このレベルでの定義は、IOCP を経由して、または HCD を用いて行います。HCD が使用可能であれば、これを使用したいと考えるでしょう。HCD によって、システム・ハードウェア構成の定義方式が改善されました。HCD を使用すれば、ハードウェア構成データの入力に必要な幾つかの複雑なステップが、対話式ダイアログを使用して実行できます。この章では、HCD から生成される IOCP マクロだけを紹介します。

サンプル・ホスト IOCP 定義

ネットワーク・ユーティリティーが ESCON アダプターを使用して構成される場合に、入出力構成プログラム (IOCP) で必要とされる定義の例が、 図48 に示してあります。

```
CHPID                PATH=((05)),TYPE=CNC
CNTLUNIT             CUNUMBR=1E0,PATH=05,CUADD=0,
                     UNITADD=((E0,32)),LINK=3C,UNIT=3172
IODEVICE             UNIT=3172,ADDRESS=((1E0,32)),
                     CUNUMBR=1E0
```

図 48. ネットワーク・ユーティリティー (ESCON) に関するサンプル・ホスト IOCP 定義

以下の各項では、ホストでネットワーク・ユーティリティーを定義する場合に必要な IOCP マクロについて説明します。

RESOURCE ステートメント

これは、名前および番号でホストの論理区画 (LPAR) を識別します。*上記の例の場合*のように、ホストが区画に分割されていない場合は、このステートメントは表示されません。

- PART=((name1,x),(name2,y)...(nameX,z))

  名前は LPAR を識別し、チャネル・パス定義の残りで使用されます。番号は、対応する LPAR 番号です。LPAR 番号は、ネットワーク・ユーティリティー上でのサブチャネルの定義に使用されます。ホストが区画に分割されていない場合は、LPAR 番号は常に 0 です。

チャネル・パス ID (CHPID) ステートメント

CHPID では、チャネル接続のタイプとその使用者を識別します。

- PATH=x

  こうしてチャネル・パスを固有に識別します。この値は、「CHPID 番号」と呼ばれる場合があります。

- TYPE=CNC

  チャネルが ESCON チャネルであることを示しています。チャネル・タイプは、CNC で ESCON を表し、BL でブロック・マルチプレクサー (パラレル・チャネル・アダプター) を表します。

- SWITCH=x

このパス内にある ESCON ディレクターを識別します。ディレクターが使用されていない場合は、このパラメーターは省略されます。

- SHARED

  CHPID が複数の LPAR で同時に使用できることを示しています。表示されていない場合は、CHPID を使用できる LPAR は、一度に 1 つだけです。

- PARTITION=(name1,name2,...,nameX)

  PARTITION パラメーターの 1 つの形式であり、このチャネルにアクセスできる区画を示す、 LPARS のアクセス・リストが含まれています。名前は、 RESOURCE ステートメントに組み込まれている必要があります。

- PARTITION=((name1,...,nameX),(name2,...,nameY))

  PARTITION パラメーターのもう 1 つの形式です。この形式では、上記のように、最初の名前のグループがアクセス・リストに入っています。2 番目のグループは、オペレーターがチャネルにアクセスできるように構成できる可能性のある LPAR のリストです。2 番目のグループには、少なくとも最初のグループと同数の LPAR があり、追加の LPAR が指定される場合もあります。

制御装置 (CNTLUNIT) ステートメント

このステートメントは、IODEVICE ステートメントと共に、ホストからネットワーク・ユーティリティーへのパスを定義します。CNTLUNIT と IODEVICE ステートメントは、ペアで使用されます。複数の LPAR が単一の CHPID を使用するように定義される場合は、それぞれの LPAR ごとに CNTLUNIT と IODEVICE ステートメントが必要です。

- CUNUMBR=x

  制御装置定義を表す識別子です。

- PATH=x

  この番号では、使用されている CHPID を識別します。

- UNIT=3172

  チャネルの他端の制御装置のタイプを識別します。値は、ネットワーク・ユーティリティーへの talk 時には常に 3172 です IBM 3172 は、ネットワーク・ユーティリティーの ESCON チャネル機能の先駆けとなったものです

- CUADD=x

  この値では、ネットワーク・ユーティリティーの制御装置アドレスを識別します。0 がデフォルト値です。

- UNITADD=((*addr*,*number*))

  この制御装置用として予約されるアドレスの範囲を定義します。ただし、次のとおりです。

  addr この制御装置に割り当てられる最初のサブチャネルの 16 進数のアドレスです。

  number
  この制御装置に割り当てられるサブチャネルの数を表す 10 進数です。

  上記の例では、32 の範囲の制御装置アドレス、つまり、サブチャネルが、 16 進数の E0 から始めて昇順に定義されています。ネットワーク・ユーティリティーの LCS、 LSA、または MPC+ インターフェース定義上で指定される装置アドレスは、

この範囲内からであることが必要です。ネットワーク・ユーティリティーでは、最大 64 のサブチャネルが使用できます。

- LINK=xx

  LINK パラメーターの値は、ネットワーク・ユーティリティー が接続される、ESCON ディレクター (ESCD) のポートに設定される必要があります。ESCD はスイッチであるため、リンク・パラメーターについては、ホストがスイッチを通してネットワーク・ユーティリティーにアクセスする場合に使用する、電話番号とみなすことができます。

IODEVICE ステートメント

このステートメントは、CNTLUNIT ステートメントと共に、ホストへのネットワーク・ユーティリティー接続を識別します。

- ADDRESS=(*addr*,*number*)

  このパラメーターでは、ホストの残りへのアドレスの範囲を識別します。ただし、次のとおりです。

  addr　予約される最初のアドレスに ***割り当てられる***、 16 進数のアドレスです。

  number
  予約されるサブチャネルの数を表す 10 進数です。

  このアドレスは、UNITADD とは異なっています。TCP/IP プロファイル (LCS の場合)、 VTAM XCA 大ノード定義 (LSA の場合)、および VTAM TRL (MPC+ 場合) で、使用されるサブチャネルを識別する場合に使用します。

- CUNUMBR=x

  この IODEVICE ステートメントに対応する CNTLUNIT ステートメントを識別します。このパラメーターの値は、CNTLUNIT と IODEVICE の両マクロで同じであることが必要ですが、他のパラメーターのいずれにも関連する必要はありません。ただし、IODEVICE マクロ内の ADDRESS パラメーターで定義されている同じ値にするのは、考え方として優れています。CUNUMBR の値は、チャネル・パス定義外では意味をもちません。

- UNIT=3172

  ダウンストリームの装置のタイプを識別します。ネットワーク・ユーティリティーが制御装置である場合は、常に 3172 である必要があります。ホスト内の IOCP ソフトウェアがこのフィールドを調べることはありません。3172 からネットワーク・ユーティリティーへの移行である場合は、既存の IOCP ステートメントに UNIT=SCTC の値が入っている可能性があります。ネットワーク・ユーティリティーの場合は、これは 3172 に変更する必要があります。

- PARTITION=(name)

  これは、装置候補リストであり、装置にアクセスできる 1 つまたは複数の LPAR のリストが含まれます。このリストは、CHPID ステートメントで指定されている、LPAR のリストのサブセットであり、これらの装置を使用することができる、チャネル候補リスト内の LPAR を制限する場合に使用されます。ホストが区画に分割されていない場合は、このフィールドは表示されません。

図49 には、パラレル・チャネル・アダプター (PCA) を使用するネットワーク・ユーティリティーを定義するための、IOCP ステートメントの例が示してあります。

```
CHPID                PATH=((05)),TYPE=BL
CNTLUNIT             CUNUMBR=640,PATH=05
                     PROTOCL=S4,UNIT=3172
                     SHARED=N,UNITADD=((40,32))
IODEVICE             UNIT=3172,ADDRESS=((640,32))
                     STADET=N,CUNUMBR=640,TIMEOUT=Y
```

図 49. ネットワーク・ユーティリティー (PCA) に関するサンプル・ホスト IOCP 定義

PCA を使用するネットワーク・ユーティリティーの場合の IOCP ステートメントに関する以下の点に注意してください。

- TYPE は BL で、ブロック・マルチプレクサーを表します。
- PROTOCL パラメーターは、装置機能に応じて、次の値に設定することができます。

  D 直結インターロック (DCI) モード

  S 最大 3.0 Mbps データ・ストリーム速度

  S4 最大 4.5 Mbps データ・ストリーム速度

  ネットワーク・ユーティリティーの場合は、値は S4 に設定します。転送モードおよびチャネル・パラメーターは、転送モードおよびチャネル転送速度に関する PCA 設定に適合する必要があります。
- CNTLUNIT および IODEVICE ステートメントの UNIT パラメーターは、3172 に設定する必要があります。
- CHPID TYPE パラメーターは、チャネル・パスが ESCON コンバーターである場合は、CVC に設定する必要があり、それ以外の場合は、BL に設定します。

オペレーティング・システムでのネットワーク・ユーティリティーの定義

以下の各項では、さまざまなオペレーティング・システムの場合に必要な定義について説明します。

VM/SP の場合のネットワーク・ユーティリティー定義

ネットワーク・ユーティリティーを VM/SP オペレーティング・システムに対して定義する場合は、 RDEVICE および RCTLUNIT マクロ内のネットワーク・ユーティリティーに関する項目を用いて、実入出力構成ファイル (DMKRIO) を更新することによって行う必要があります。次の例で、640 が基本装置アドレスであり、 アドレス範囲のサイズが 32 です。

```
RDEVICE ADDRESS=(640,32),DEVTYPE=3088
RCTLUNIT ADDRESS=640,CUTYPE=3088,FEATURE=32-DEVICE
```

VM/XA と VM/ESA の場合のネットワーク・ユーティリティー定義

ネットワーク・ユーティリティーを VM/拡張アーキテクチャー (VM/XA または VM/ESA) オペレーティング・システムに対して定義する場合は、RDEVICE マクロ内のネットワーク・ユーティリティーに関する項目を用いて、実入出力構成ファイル (HCPRIO) を更新することによって行う必要があります。次の例では、640 および 2A0 が 基本制御装置アドレスです。UCW または IOCP で定義されているアドレス範囲サイズは、両方の例のいずれでも 8 です。

次の例は、VM/XA HCPRIO 定義です。

```
RDEVICE ADDRESS=(640,8),DEVTYPE=CTCA
```

次の例は、VM/ESA HCPRIO 定義です。

```
RDEVICE ADDRESS=(2A0,8),DEVTYPE=CTCA
```

MVS/XA と MVS/ESA (HCD なし) の場合のネットワーク・ユーティリティー定義

ネットワーク・ユーティリティーを IBM 多重仮想記憶/拡張アーキテクチャー (MVS/XA) または MVS/ESA オペレーティング・システムに対して定義する場合は、IODEVICE マクロ内のネットワーク・ユーティリティーに関する項目を用いて、MVS 制御プログラムを更新することによって行う必要があります。

ESCON チャネルの場合は、IODEVICE マクロの例は次のとおりです。

```
IODEVICE UNIT=3172,ADDRESS(540,8)
```

パラレル・チャネルの場合は、IODEVICE マクロの例は次のとおりです。

```
IODEVICE UNIT=CTC,ADDRESS(640,8)
```

540 と 640 が基本制御装置アドレスです。 UCW または IOCP で定義されているアドレス範囲サイズは、両方の例のいずれでも 8 です。

MVS/ESA (HCD 付き) の場合のネットワーク・ユーティリティー定義

MVS/ESA SP バージョン 4.2 および 4.3 (APAR #OY67361 付き) のハードウェア構成定義 (HCD) コンポーネントによって、ネットワーク・ユーティリティーに関するシステム・ハードウェア構成を定義する方式が改善されました。ハードウェア構成データの入力に必要な幾つかの複雑なステップが、HCD での対話式ダイアログを使用して実行できます。

ネットワーク・ユーティリティーに関する必須構成データは、次のとおりです。

- HCD を APAR # OY67361 と共に使用するときは、ネットワーク・ユーティリティーを (UNIT=3172) として定義します。次にその例を挙げます。

  ```
  IODEVICE UNIT=3172,ADDRESS(740,8)
  ```

- HCD がない場合は、ネットワーク・ユーティリティーは次のように定義します。
  - パラレル・チャネルの場合は、3088 装置 (UNIT = 3088 または CTC) として定義する。

    ```
    IODEVICE        UNIT=CTC,ADDRESS(840,8)
    ```

– ESCON チャネルの場合は、シリアル CTC 装置 (UNIT = SCTC) として定義する。

```
IODEVICE        UNIT=SCTC,ADDRESS(A40,8)
```

注:

1. MVS バージョン 4 の HCD を使用して、ESCON ホスト接続を定義する場合は、装置定義 (UNIT=3172) に対する UIM サポートを得るためには、APAR # OY67361 が必要になります。
2. IOCP 定義およびオペレーティング・システム定義を HCD 環境に移行する場合は、すべてのネットワーク・ユーティリティー装置ステートメントを装置タイプ (UNIT=3172) に変更することが重要になります。

VSE/ESA の場合のネットワーク・ユーティリティー定義

ネットワーク・ユーティリティーを VSE/ESA オペレーティング・システムに対して定義する場合は、初期プログラム・ロード (IPL) 時に、それぞれのチャネル装置アドレスごとに、 ADD ステートメントを指定して行う必要があります。次の例に示すように、 ADD ステートメント上で装置タイプを CTCA,EML とコーディングします。

```
ADD 640,CTCA,EML
```

この例では、640 が基本制御装置アドレスです。追加されるチャネル装置アドレスの数については、IOTAB ストーレッジ・マクロをこのカウントだけ増分します。

VTAM 定義

ここでは、XCA 大ノード、MPC+ ローカル PU およびトランスポート資源リスト (TRL) 大ノードに関するサンプル VTAM 定義と、APPN および DLUR サポートに関する VTAM 定義の例を示します。また、TN3270 サーバー内の PU に関する交換回線大ノードの例も示してあります。ただし、ここでは、この主題のすべてに言及するつもりはありません。VTAM の構成について詳しくは、 *CS OS/390 Resource Definition Reference*、SC31-8565 を参照してください。

VTAM XCA 大ノード定義

LSA を使用するチャネル・ゲートウェイを VTAM に対して定義する場合は、外部通信アダプター (XCA) に関する定義が必要です。この定義は、IBM 3172 に使用されているものと同じです。例は、302ページの図50 に示してあります。

```
*************************************************************************
RAINETU VBUILD TYPE=XCA     1

**
**
RANETUP  PORT  ADAPNO=0,     2                      * X
               CUADDR=285,     3                   * X
               MEDIUM=RING,      4                 * X
               SAPADDR=4,          5               * X
               TIMER=60
**
*************************************************************************
RANETUG1 GROUP DIAL=YES,CALL=INOUT,DYNPU=YES
*
RANETUL1 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP1 PU   ISTATUS=ACTIVE
RANETUL2 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP2 PU   ISTATUS=ACTIVE
RANETUL3 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP3 PU   ISTATUS=ACTIVE
RANETUL4 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP4 PU   ISTATUS=ACTIVE
RANETUL5 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP5 PU   ISTATUS=ACTIVE
RANETUL6 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP6 PU   ISTATUS=ACTIVE
RANETUL7 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP7 PU   ISTATUS=ACTIVE
RANETUL8 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP8 PU   ISTATUS=ACTIVE
RANETUL9 LINE ANSWER=ON,ISTATUS=ACTIVE
RANETUP9 PU   ISTATUS=ACTIVE
```

図 50. LSA 直接接続の場合の XCA 大ノード定義サンプル

注:

1 TYPE は、 XCA であることが必要です。

2 ADAPNO は、ネットワーク・ユーティリティー・インターフェースの LAN 番号です。この値は、ネットワーク・ユーティリティーの LSA インターフェースの作成時に割り当てられます。この値は、talk 6 メニューでインターフェースの構成をリストして、ネットワーク・ユーティリティーから得ることもできるし、ESCON コンソールから Talk 5 で、 **list nets** コマンドを入力して検索することもできます。 LSA 構成で単一のエラーとして最もよく起こるのが、このパラメーターに誤った値を使用することであることに注意してください。

3 CUADDR では、ネットワーク・ユーティリティーとの通信に使用されるサブチャネルを指定します。この値は、IOCP 定義内の IODEVICE ステートメントで指定されている値の範囲内であることが必要です。

4 LSA インターフェースが接続される物理 LAN トポロジーを指定します。ネットワーク・ユーティリティー・インターフェースの LAN タイプに指定されている値に対応します。トークンリングの場合は MEDIUM=RING、イーサネットの場合は MEDIUM=CSMACD、ファイバー分散データ・インターフェース (FDDI) の場合は MEDIUM=FDDI が、有効な値です。

5 SAPADDR は、 VTAM がネットワーク・ユーティリティー上でオープンしようとする、サービス・アクセス・ポイント番号です。 SOURCE SAP であって、

DESTINATION SAP ではないことに注意してください。複数のアクティブ XCA 大ノードが同一の LAN を参照する場合は、すべての XCA 大ノードで異なる SAP を使用する必要があります。

LINE ステートメント

CALL フィールドは、次のいずれか 1 つになります。
- IN では、接続を確立できるのはリモート装置だけであることを意味します。
- OUT では、接続を開始できるのは、VTAM だけであることを意味します。
- INOUT 接続は、両端のどちらでも開始できます。

VTAM がダイヤルアウトする場合は、交換回線大ノード定義では、 PATH ステートメントを用いてあて先を指定する必要があります。

1 桁目のアスタリスクは、ステートメントがコメント化されているので、無視する必要があることを示します。最後の桁の文字は、次の行がその行の続きであることを示します。

MPC+ 接続の場合の VTAM 定義

MPC+ 接続では、2 つの VTAM 制御ブロックに項目が必要です。
- ローカル大ノード
- トランスポート資源リスト (TRL) 大ノード

図51 には、ネットワーク・ユーティリティーの MPC+ 接続に関するローカル SNA 大ノードのサンプル定義が示してあります。これは、TRL に定義されているチャネル接続をサポートする VTAM 内に常駐するローカル PU です。接続タイプは APPN であることが必要であり、HPR を使用可能にする必要もあります。

```
LOCNETU  VBUILD TYPE=LOCAL
MPCNETUP PU     TRLE=MPCNETU,
                XID=YES,
                CONNTYPE=APPN,
CPCP=YES,       HPR=YES
```

図 51. VTAM ローカル大ノード定義

注:

1. TYPE は、VBUILD ステートメントの LOCAL に等しいことが必要です。
2. TRLE では、使用されている TRL を識別します。名前は、既存の TRL の名前に一致する必要があります。
3. XID では、XID が交換されるかどうかを示します。XID=YES であることが必要です。
4. CONNTYPE は CONNTYPE=APPN に設定する必要があります。VTAM が MPC+ 接続で使用する唯一のプロトコルは、APPN であるからです。
5. CPCP では、APPN による CP-CP 接続が、この MPC+ 接続を通して確立できることを指定します。APPN トポロジーに応じて、YES と NO のどちらにも設定できます。

6. HPR では、APPN HPR トラフィックがこの MPC+ 接続を通って流れることができることを指定します。HPR は、通常、デフォルトで使用されますが、この値を YES に設定すれば、それが保証されます。このことが重要なのは、MPC+ 接続では RTP (および HPR) が必要であるからです。

次に、ネットワーク・ユーティリティーからの MPC+ 接続に関するトランスポート資源リストが必要です。定義例が 図52 に示してあります。

```
        VBUILD TYPE=TRL
MPCNETU TRLE   LNCTL=MPC,
               MAXBFRU=9,
               READ=280,
               WRITE=281,
               MPCLEVEL=HPDT,
               REPLYTO=3.0
```

図 52. VTAM トランスポート資源リスト (TRL) 定義

注:

1. TYPE は TRL である必要があります。
2. MPCNETU は、TRL を識別する名前です。ローカル大ノード定義の TRLE= フィールドでの指定に一致する必要があります (303ページの図51 を参照してください)。
3. LNCTL では、接続タイプを識別します。LCNTL=MPC であることが必要です。
4. MAXBFRU は、読み取りサブチャネルごとに 4K ページという数です。
5. READ/WRITE では、MPC+ グループ内のサブチャネル数を指定し、その方向を示します。サブチャネル数は、IOCP 定義内の IODEVICE ステートメントで指定されているアドレスの範囲内である必要があります。TRLE ステートメントには、複数の READ および WRITE パラメーターがあって構いませんが、それぞれが少なくとも 1 つずつは必要です。

   注: ここでの READ および WRITE の指定は、HOST の観点によるものです。ネットワーク・ユーティリティーの MPC+ 定義では、指定はネットワーク・ユーティリティーの観点によります。したがって、ホストで READ に指定されるサブチャネルは、ネットワーク・ユーティリティーでは WRITE に指定される ***必要*** があり、逆も同様です。
6. REPLYTO は、秒単位の応答タイムアウト値です。

APPN の場合の VTAM 定義

VTAM が DLUS 用として構成される場合は、APPN ネットワーク・ノードである必要があります。VTAM を APPN ネットワーク・ノードとして構成するには、特定のパラメーターが、VTAM 始動パラメーターの中で指定される必要があります。これが 305ページの図53 に示してあります。CONNTYPE を APPN に、NODETYPE をネットワーク・ノード (NN) に設定します。

```
ASYDE=TERM,IOPURGE=5M,
CONFIG=I0,
CONNTYPE=APPN,
CPCP=YES,
CSALIMIT=0,
DYNADJCP=YES,
ENCRYPTN=NO,
GWSSCP=YES,
HOSTPU=ISTPUS18,
HOSTSA=18,
HPR=RTP,
NETID=USIBMRA,
NODETYPE=NN,
NOTRACE,TYPE=VTAM,IOINT=0
PPOLOG=YES
SORDER=APPN,
SSCPDYN=YES,
SSCPID=18,
SSCPNAME=RAI,
SSCPORD=PRIORITY,
SUPP=NOSUP,
TNSTAT,CNSL,
VRTG=YES
OSITOPO=LLINES,
OSIMGMT=YES
XNETALS=YES
```

図 53. VTAM 始動パラメーター

TN3270 資源の VTAM 静的定義

TN3270E サーバーで使用される PU の場合は、VTAM 定義が必要です。TN3270E サーバー内の各 PU ごとに、それぞれ交換回線大ノード定義が必要です。例えば、TN3270E サーバー内の各 PU では、それぞれ最大 253 の LU をサポートすることができます。500 の 3270 セッションが必要な場合は、ルーター内に 2 つの PU と、VTAM 内に 2 つの PU 定義が必要になります。

図54 には、TN3270E サーバー PU が DLUR および APPN を経由して接続される場合の、VTAM 交換回線大ノード定義の例が示してあります。

```
LOCNETU  VBUILD TYPE=SWNET
MNETUA   PU     ADDR=01,ISTATUS=ACTIVE,VPACING=0,                       *
                DISCNT=NO,PUTYPE=2,SSCPFM=USSSCS,USSTAB=US327X,         *
                IDBLK=077,IDNUM=02216,IRETRY=YES,MAXDATA=521,           *
                MAXOUT=7,MAXPATH=8,PASSLIM=7,PACING=0,ANS=CONTINUE
*********************************************************************
PNETUA   PATH   PID=1,DLCADDR=(1,C,INTPU),DLCADDR=(2,X,07702216),       *
                DLURNAME=MNETUA
*********************************************************************
JC7LU2   LU     LOCADDR=2
JC7LU3   LU     LOCADDR=3
JC7LU4   LU     LOCADDR=4
```

図 54. TN3270E サーバー PU (DLUR/APPN) に関する VTAM 定義

306ページの図55 には、TN3270E サーバー PU がホストへのサブエリア接続を使用する場合の、VTAM交換回線大ノードの例が示してあります。

```
LSAP08T VBUILD TYPE=SWNET
PUPS08T PU ADDR=01,IDBLK=077,IDNUM=12244,MAXOUT=7,PACING=0,VPACING=0,
               DLOGMOD=B22NNE,PUTYPE=ANY,
               SSCPFM=USSSCS,MAXDATA=2000,MODETAB=LMT3270
PT08LU2 LU LOCADDR=02,LOGAPPL=TSO
PT08LU3 LU LOCADDR=03,LOGAPPL=TSO
PT08LU4 LU LOCADDR=04,LOGAPPL=TSO
PT08LU5 LU LOCADDR=05,LOGAPPL=TSO
PT08LU6 LU LOCADDR=06,LOGAPPL=TSO
```

図 55. TN3270E サーバー PU (サブエリア) に関する VTAM 定義

以下の各項では、交換回線大ノード定義内のステートメントについて概説します。

VBUILD ステートメント

TYPE フィールドは、TYPE=SWNET であることが必要です。

PU ステートメント

このステートメントでは、データ・フローとあて先を定義します。関連するパラメーターは、次のとおりです。

- ADDR は識別子です。
- MAXDATA は、VTAM がこのインターフェース上でサポートする最大パケット・サイズです。この値は、XID 交換時にネットワーク・ユーティリティーとの間で下方折衝されます。
- IDBLK/IDNUM では、VTAM が PU 2.0 (従属) 装置と通信するするときの、リモート装置を識別します。

LU ステートメント

これらのステートメントでは、この PU を通して接続できる論理装置 (LU) を定義します。それぞれのステートメントの左側の名前は、ホストがそれぞれの LU にアドレスする場合に使用する名前です。LOCADDR は、ネットワーク・ユーティリティーが VTAM 内で正しい LU を識別する場合に使用します。

PATH ステートメント

VTAM がダイヤルアウトする場合は、交換回線大ノード定義では、 PATH ステートメントを用いてあて先を指定する必要があります。パス・ステートメントは、TN3270E サーバーがサブエリアを経由して接続するか、 DLUR/APPN 接続を経由して接続するかによって異なります。

サブエリア接続の場合は、次のようなフォーマットです。

```
PATH DIALNO=xxyyzzzzzzzzzzzz
```

ただし、次のとおりです。

- *xx* はプレースホルダー
- *yy* はあて先 SAP 番号
- *zz* はあて先 MAC アドレス

306ページの図55 の例には PATH ステートメントがありません。この例では、VTAM が装置にダイヤルアウトするのではなく、ダウンストリーム PU が VTAM に接続するからです。

305ページの図54 の例には、TN3270E サーバー PU が DLUR を使用してホストに接続する場合の、PATH ステートメントが示されています。ここでは、 PATH ステートメントが、DLURNAME パラメーターによって、ネットワーク・ユーティリティー (MNETUA) の CP 名を識別しています。この必要があるのは、DLUR と DLUS の間の LU6.2 会話が確立されるためです。このセッションが確立されると、VTAM と TN3270E サーバーの間の SSCP-PU セッションが、DLCADDR=(2,X,07702216) によって指定されている IDBLK/IDNUM 値を使用して確立されます。

TN3270 資源の VTAM 動的定義

最新情報については、167ページの『従属 LU の動的定義』をごらんください。

ホスト IP 定義

TCP/IP 接続のホストに対してネットワーク・ユーティリティーを定義する場合は、ホストの TCP/IP プロファイルに変更を加える必要があります。ここでは、変更する必要がある関連ステートメントについて概説します。

DEVICE ステートメント

このステートメントでは、TCP/IP によって使用されるサブチャネル・ペアを定義します。フォーマットは、次のとおりです。

```
DEVICE  name  LCS  subchannel
```

ただし、次のとおりです。

- *name* では、使用されるサブチャネル・パスを識別します。ローカルでしか意味がなく、何でも構いません。
- *subchannel* では、この接続に使用される偶数サブチャネルを識別します。この値は、IOCP 定義内の IODEVICE ステートメントのものです。指定すると、そのサブチャネルと次のサブチャネルの両方が使用されます。

TCP/IP プロファイルには、使用されるそれぞれのサブチャネル・ペアごとに、 1 つずつ DEVICE ステートメントが必要です。

LINK ステートメント

このステートメントでは、特定のサブチャネル・ペアで使用される、ネットワーク・ユーティリティー上の LCS インターフェースを識別します。形式は、次のとおりです。

```
LINK name lantype lannumber devicename
```

ただし、次のとおりです。

- *name* では、LCS インターフェースを識別します。ローカルでしか意味がなく、何でも構いません。
- *lantype* では、ネットワーク・ユーティリティーの LCS インターフェースがエミュレートする LAN インターフェースのタイプを識別します。使用できる値は、次のとおりです。
  - IBMTR (トークンリングの場合)
  - ETHERNET (イーサネット V2 の場合)
  - 802.3 (イーサネット (IEEE 802.3) の場合)
  - ETHERor802.3 (受け入れられているイーサネット・フォーマットのいずれかの場合)
  - FDDI (FDDI の場合)
- *lannumber* では、使用されるネットワーク・ユーティリティー上の LCS インターフェースを識別します。*lannumber* は、LCS インターフェースを追加すると、ネットワーク・ユーティリティー上のそれぞれの *lantype* ごとに順次生成されます。*lannumber* は、 ESCON コンソールから talk 5 で **list nets** と入力して、表示させることができます。*lannumber* は、ネットワーク番号では ***ない*** ことに注意してください。LCS 構成で単一のエラーとして最もよく起こるのが、誤った *lannumber* の使用です。
- *devicename* では、LCS インターフェースをサブチャネル・ペアに相関付けます。前に定義した DEVICE ステートメントに一致する必要があります。

複数の LINK ステートメントを単一の DEVICE ステートメントに対応付けることができます。それぞれの LINK ステートメントごとに、ネットワーク・ユーティリティー上に LCS インターフェースが必要です。

HOME ステートメント

このステートメントでは、ホストの TCP/IP スタックの IP アドレス (複数の場合もある) を指定します。フォーマットは、次のとおりです。

```
HOME     ipaddress1     link1
         ipaddress2     link2
```

ただし、次のとおりです。

- *IpaddressX* では、ホスト上の IP アドレスを指定します。
- *LinkX* では、この IP アドレスに対応付けられるリンクを指定します。

各 LINK ステートメントごとに、それぞれ HOME アドレスが 1 つだけ必要です。HOME アドレスは、ネットワーク・ユーティリティー内の LCS インターフェースの IP アドレスと同じ IP サブネット内にある必要がありますが、***異なるアドレスであることが必要です***。

GATEWAY ステートメント

このステートメントでは、ホストに関する IP ルーティング情報を識別します。これは 3 つのセクションに分かれています。

- 直接ルートとは、ホストに直接接続されているルートのことです。ネットワーク・ユーティリティーの LCS インターフェースを含むサブネットは、直接ルートです。

- 間接ルートとは、ルーターを経由してアクセスできるルートのことです。例えば、ネットワーク・ユーティリティー上の LAN のサブネットは、間接ルートです。
- デフォルト・ルートとは、IP アドレスへの直接ルートも間接ルートもホストにない場合に使用されるルートのことです。

直接ルート

直接ルートのフォーマットは、次のとおりです。

```
network firsthop linkname pktsize submask subvalue
```

ただし、次のとおりです。

- *network* は、IP アドレスの非サブネット化部分です。
- *firsthop* では、IP ネットワーク内のネクスト・ホップの IP アドレスを示します。直接ルートの場合は、これは等号 (=) である必要があります。
- *linkname* では、ホストがこのルート上のアドレスにアクセスする場合に使用する必要があるリンクを識別します。ネットワーク・ユーティリティーを経由してアクセスできるルートの場合は、このサブネット上の LCS インターフェースに対応する LINK ステートメントからの名前である必要があります。
- *pktsize* は、インターフェース上で使用される最大フレーム・サイズです。これは、ネットワーク・ユーティリティー上の LCS 構成で定義されているパケット・サイズ以下である必要があります。DEFAULTSIZE の値では、デフォルトのパケット・サイズが使用されることを示します。
- *submask* では、このリンク上で使用されるサブネット・マスクを指定します。サブネット・マスクは、ネットワーク・ユーティリティー上の IP 構成で LCS インターフェースに関して定義されているサブネット・マスクに対応する必要があります。このフィールドは、HOST に設定されて、ポイント・ポイント接続を識別する場合もあります。この場合は、ネットワーク・フィールドに、LCS インターフェースのフル IP アドレスが入る必要があります。
- *subvalue* では、IP アドレスのサブネット化部分を指定し、ネットワーク・フィールドと共に、この LCS インターフェースに対応する IP サブネットを完全に指定する必要があります。

間接ルート

間接ルートのフォーマットは、次のとおりです。

```
network firsthop linkname pktsize submask subvalue
```

ただし、次のとおりです。

- *network* は、IP サブネットのフル・アドレスです。
- *firsthop* では、IP ネットワーク内のネクスト・ホップの IP アドレスを示します。ネットワーク・ユーティリティーを経由してアクセスできる間接ルートの場合は、これは、ネットワーク・ユーティリティーの LCS インターフェースの IP アドレスである必要があります。
- *linkname* では、ホストがこのルート上のアドレスにアクセスする場合に使用する必要があるリンクを識別します。ネットワーク・ユーティリティーを経由してアク

セスできるルートの場合は、このサブネット上の LCS インターフェースに対応する LINK ステートメントからの名前である必要があります。

- *pktsize* は、直接ルートの場合と同じ値です。
- *submask* は 0 であるか、ネットワーク・フィールドにフル・サブネット・アドレスが入っている場合は、ブランクである必要があります。
- *subvalue* は、サブネット・マスクが指定されていない場合は、ブランクのままにしておく必要があります。

デフォルト・ルート

デフォルト・ルートのフォーマットは、次のとおりです。

```
network firsthop linkname pktsize submask subvalue
```

ただし、次のとおりです。

- *network* は、DEFAULTNET である必要があります。
- *firsthop* では、IP ネットワーク内のネクスト・ホップの IP アドレスを示します。ネットワーク・ユーティリティーへのデフォルト・ルートの場合は、これは、ネットワーク・ユーティリティーの LCS インターフェースの IP アドレスである必要があります。
- *linkname* では、ホストがこのルート上のアドレスにアクセスする場合に使用する必要があるリンクを識別します。ネットワーク・ユーティリティーを経由してアクセスできるルートの場合は、このサブネット上の LCS インターフェースに対応する LINK ステートメントからの名前である必要があります。
- *pktsize* は、直接ルートの場合と同じ値です。
- *submask* は、0 とブランクのどちらかである必要があります。
- *subvalue* は、ブランクである必要があります。

START ステートメント

このステートメントによって、指定されているサブチャネルが開始されます。フォーマットは、次のとおりです。

```
START devicename
```

ただし、*devicename* は、上記の DEVICE ステートメント上の名前です。

TCP/IP の開始時に装置を起動したい場合は、すべての DEVICE ステートメントのそれぞれに 1 つずつ START ステートメントが必要です。START ステートメントがここにない場合は、装置は、OBEY ファイルを使用して開始することができます。ここでの名前は、DEVICE ステートメントのものであって、LINK ステートメントからではないことに注意してください。また、START が TCP/IP から発行されるまでは、ネットワーク・ユーティリティーの LCS インターフェースは、DOWN 状態のままであることにも注意してください。

LCS に関するホスト TCP/IP 定義

ここでは、LCS 接続を定義している場合に必要な、上記のステートメントの例を示します。

1. DEVICE ステートメント

   ```
   DEVICE LCS1 LCS 210
   ```

   ただし、LCS1 は定義されている装置名であり、LCS は装置のタイプであり、210 はこの定義で使用されるホストの読み取り (ネットワーク・ユーティリティーの書き込み) サブチャネルです。

2. LINK ステートメント

   ```
   LINK ETHLCS1 802.3 0 LCS1
   ```

   ただし、ETHLCS1 はリンク名であり、 802.3 は、LCS インターフェースがネットワーク・ユーティリティー上で接続する LAN タイプであり、 0 は、ネットワーク・ユーティリティーに割り当てられている LAN 番号であり、LCS1 は装置の名前 (上記の DEVICE ステートメントからのもの) です。

   注: LAN 番号は、LCS インターフェースの定義時に、ネットワーク・ユーティリティーによって自動的に割り当てられることに注意してください。これは、ネットワーク・ユーティリティー・コンソールでの talk 6 プロセスで、ESCON Config> プロンプトで `list all` コマンドを出して表示させることができます。

3. HOME コマンド

   ```
   HOME 9.24.106.72 ETHLCS1
   ```

   ただし、9.24.106.72 はこの LCS インターフェースの IP アドレスであり、ETHLCS1 はリンクの名前です。

4. GATEWAY コマンド

   ```
   GATEWAY 9.24.106   9.24.106.1   ETHLCS1   4096  0
   ```

   ただし、9.24.106 はネットワークの IP アドレスであり、9.24.106.1 はデフォルトのルーターの IP アドレスであり、ETHLCS1 は、上記の LINK ステートメントで定義されているリンク名であり、4096 は MTU サイズであり、0 はサブネット・マスクであり、サブネット値はブランクのままになっています。

5. TCP/IP プロファイルの起動

   ステップ 1 で定義された装置を起動する場合は、次のようにコマンドを発行します。

   ```
   start lcs1
   ```

MPC+ に関するホスト TCP/IP 定義

MPC+ 接続の場合にホスト内で TCP/IP を構成する手順のステップは、LCS 接続の場合と同じです。ただし、装置コマンドおよびリンク・コマンドのコマンド構文は、多少異なっています。MPC+ 接続の場合は、装置コマンドの構文は次のとおりです。

```
DEVICE IPTRL1 MPCPTP
```

ただし、IPTRL1 はこの接続で使用する TRL の名前であり、MPCPTP では、 MPC ポイント・ポイント・リンクを指定します。

リンクを定義する場合は、構文は次のようになります。

```
LINK LINK1 MPCPTP IPTRL1
```

ただし、LINK1 はリンク名であり、他の 2 つのパラメーターは、 DEVICE ステートメントで使用されているものと同じです。

第19章 VPN (仮想私設ネットワーク)

インターネットが低コストのバックボーン・インフラストラクチャーとして普及してきました。これを利用すれば世界中に手が届くという強みがあるため、この公衆インターネットを介して安全な VPN (仮想私設ネットワーク) の構築を考える企業や団体 (以後、便宜上企業という用語で代表させる) が多くなっています。今日のグローバルなビジネス環境に見合う VPN の設計にあたっては、企業内通信と企業間通信の両方に公衆インターネット・バックボーンを利用しながら、従来からの私設専用管理ネットワークが備えていた機密保護性と信頼性を確保することが、最大の課題になります。

この章では、VPN について定義し、VPN を実装することによって得られる利点について説明します。また、セキュリティー上の考慮事項と計画上の諸面についても説明し、今日の市場で調達できる VPN ソリューションについても触れます。

VPN の概要と利点

インターネットの爆発的な普及に伴って、企業では、「*自社の業務にインターネットを生かす最善の利用法*」を問い始めています。企業が自社の Web サイトを設ける目的は、当初は、企業のイメージや製品やサービスの売り込みにありました。今日では、インターネットの可能性は無限に広がり、焦点は e-business に移りました。すなわち、世界中どこにでも手の届くインターネットの特性を利用して、従来の I/T システムに存在している重要なビジネス・アプリケーションとデータに簡単にアクセスしようというわけです。今や、企業では、安全な VPN ソリューションの実装を通じて、自らが持つアプリケーションとデータの到達する範囲を全世界に、安全かつ費用効果的に広げることができます。

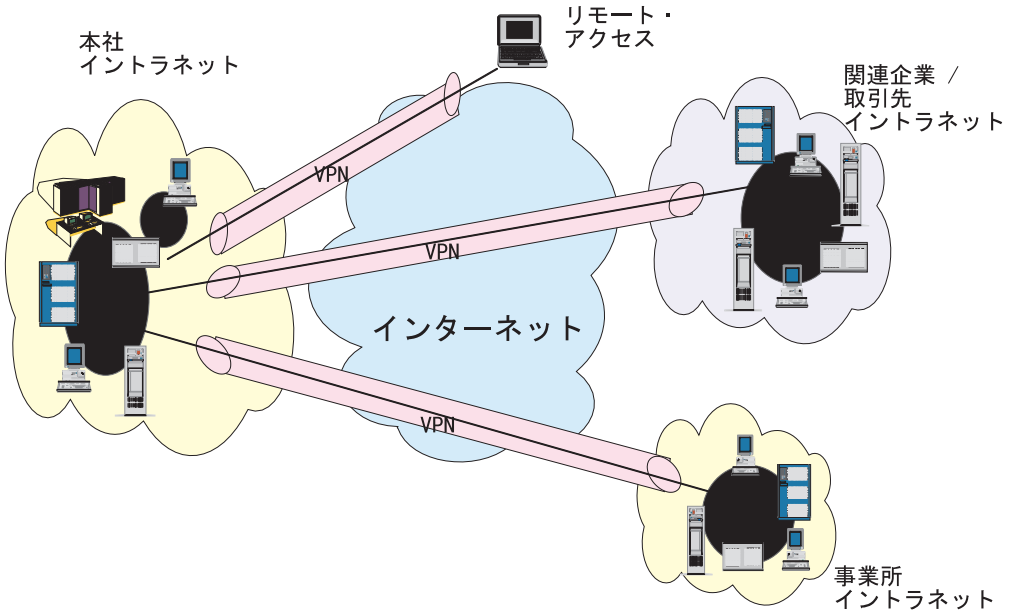


図 56. VPN (仮想私設ネットワーク)

VPN とは、エンタープライズの私設イントラネットがインターネットなどの公衆ネットワークにまたがって拡張し、それによって、本質的には私設トンネルを通る安全な専用接続を創設するものです。VPN では、313ページの図56 に示されているように、遠く隔たったユーザーや事業所や関連企業などを接続して、拡張された私設ネットワークに組み込むことによって、インターネットを通して安全に情報を伝達します。インターネット・サービス・プロバイダー (ISP) によって、費用効果性に優れたインターネットへのアクセスが提供される (直接回線や加入者電話番号を通して) ので、企業では、これまでの高価な専用線、長距離通信、フリーダイヤルなどの必要がなくなります。

IETF の IP セキュリティー・フレームワーク

階層化通信プロトコル・スタック・モデル内では、ネットワーク層 (TCP/IP スタックの場合の IP) が、エンド・エンド・セキュリティーを確保できる層として、最も費用のかからない層です。ネットワーク層セキュリティー・プロトコルでは、 IP データグラムのペイロードで搬送される上位層アプリケーション・データすべてを対象とする包括的な保護が得られます。

ソリューションの基盤になっているのは、IETF の IPSec 作業グループによって定義された、IP セキュリティー・アーキテクチャー (IPSec) のオープン・フレームワークです。IPSec がフレームワークと呼ばれているのは、ネットワーク層セキュリティーを確保するための安定した長期的な基盤を提供するからにほかなりません。今日の暗号アルゴリズムに対処できるだけでなく、さらに強力なアルゴリズムが新たに使用可能になっても、それにも対処できます。IPSec をサポートするには、IPv6 の実装が必要であり、IPv4 の実装をぜひともお勧めします。 IPSec によって、インターネットに関する基本セキュリティー機能が得られるだけでなく、堅ろうで安全な VPN の構築に使用できる柔軟性の高い基礎単位も提供されます。

IPSec 作業グループでは、次のような幾つかの主要領域を対象とするプロトコルの定義を集中的に行ってきました。

- データ発信元認証：それぞれのデータグラムが請求先送信元によって発信され、否認できないことを検証します。
- データ保全性：データグラムの内容が、故意にせよ、ランダム・エラーが原因にせよ、転送中に変更されなかったことを検証します。
- データ機密性：平文テキストのメッセージを、一般的には、暗号化の使用によって秘匿する。
- 再生保護：ハッカーがデータグラムを代行受信し、後刻検出を免れて再生することができないようにします。
- 暗号キーの自動管理とセキュリティー・アソシエーション (SA)：企業の VPN ポリシーの実装が、人手による構成をほとんどまたはまったく伴わず、拡張ネットワーク全般にわたって便利かつ正確に行えるようにします (このような機能があればこそ、VPN の規模を業務の必要に応じて容易に拡張することが可能になります)。

以下に基本 IPSec プロトコルを挙げておきます。

- IP 認証ヘッダー (IP Authentication Header) (AH) では、データ発信元認証、データ保全性、再生保護が提供されます。

- IP カプセル化セキュリティー・ペイロード (IP Encapsulating Security Payload) (ESP) では、データ機密性、データ発信元認証、データ保全性、再生保護が提供されます。
- インターネット・セキュリティー・アソシエーション/キー管理プロトコル (Internet Security Association and Key Management Protocol) (ISAKMP) では、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、その暗号キーを管理するための方式が提供されます。
- Oakley では、ISAKMP で使用される暗号キー管理プロトコルが提供されます。
- インターネット・キー交換 (Internet Key Exchange) (IKE) では、共用キーやディジタル・シグニチャーとの併用で、キー管理の自動化を実現するので、人手による手動キー生成の必要はありません。フェーズ 1 交渉時に、暗号キーが交換され、ユーザーがそれぞれ相手側の ID を認証します。この時点で、ISAKMP 機能では、Oakley 暗号キー管理プロトコルを使用して、ルーター間で交換される ISAKMP メッセージを保護して安全なデータ交換に備えます。
- パブリック・キー・インフラストラクチャー (Public Key Infrastructure) (PKI) は、ユーザー用のキーを配布し検査する証明権限 (CA) による取り決めです。
- 証明 (Certificate) は、それぞれのネットワーク・ユーザーのコード化 ID (ディジタル・シグニチャー) をそのパブリック/プライベート・キーにバインドするデータ域です。
- ディジタル・シグニチャー (Digital Signature) は、証明の一部になるユーザーのコード化 ID が入るデータ域です。

認証ヘッダー

IP 認証ヘッダー (AH) では、IP データグラムに関するコネクションレス保全性 (つまり、パケット単位) とデータ発信元認証が提供されます。また、再生に対する保護も提供されます。データ保全性は、メッセージ確認コード (例えば、 MD5) によって生成されるチェックサムによって保証され、データ発信元認証は、認証の対象となるデータに秘密共用キーを組み込むことによって保証され、再生保護は、AH ヘッダー内の順序番号フィールドの使用によって確保されます。IPSec 用語では、この 3 つの別々の機能をひとまとめにして、単に認証という名前で呼んでいます。

AH では、できるだけ多くの IP データグラムを認証します。IPheader (IP ヘッダー) 内のフィールドには途中で変更されるものがあり、そのようなフィールドの値は、受信側で予期することはできません。こうしたフィールドは可変性と呼ばれ、AH による保護の対象になりません。可変性 IPv4 フィールドには、次のようなフィールドがあります。

- サービス・タイプ (TOS)
- フラグ
- フラグメント・オフセット
- 活動時間 (TTL)
- ヘッダー・チェックサム

AH は、IANA によって割り当てられたプロトコル番号 51 によって識別されます。プロトコル・ヘッダー (IPv4、IPv6、またはエクステンション) が AH ヘッダーの直

前に付いていて、そのプロトコル (IPv4) フィールドかネクスト・ヘッダー (IPv6、エクステンション) フィールドにこの値が入っています。

AH 処理が適用されるのは、非分割 IP パケットの場合だけです。ただし、AH が適用されている IP パケットは、中間ルーターで分割できます。この場合は、あて先では、まずパケットを再組み立てし、その上で AH 処理を適用します。フラグメントと思われる IP パケット (オフセット・フィールドが非ゼロであるか、「More Fragments」ビットが設定されている) が AH 処理に入力された場合は、廃棄されます。したがって、偽造パケットを作成して、強制的にファイアウォールを通過させるために、フラグメント再組み立てアルゴリズムを誤用する、いわゆるオーバーラップ・フラグメント・ハッキングを防止できます。

認証に外れたパケットは廃棄され、上位層に送達されることは決してありません。したがって、偽のパケットのフラッディングによって、ホストやゲートウェイの通信を妨害する目的をもつサービス・ハッキングの否認が成功する可能性は、この動作モードによって大幅に減少します。

AH は、トランスポート・モードとトンネル・モードという 2 つのモードで使用できます。トランスポート・モードは、ゲートウェイではなく、ホストで使用されます。トランスポート・モードをサポートするには、ゲートウェイは必須ではありません。トランスポート・モードでは、処理オーバーヘッドは少なくて済みますが、可変性フィールドは認証できません。

IPv4 フィールドの保護が必要なときは、トンネリングを使用する必要があります。IP パケットのペイロードは非可変性とみなされ、常に AH によって保護されます。

SA の両端のどちらか一方でもゲートウェイの場合は、必ずトンネル・モードを使用します。したがって、2 つのファイアウォール間では、常にトンネル・モードが使用されます。ゲートウェイが必須なのは、トンネル・モードをサポートする場合だけですが、ゲートウェイがトランスポート・モードをサポートする場合もあります。このモードが使用できるのは、ゲートウェイがホストになるときで、例えば、トラフィックのあて先がゲートウェイ自体である場合などです。SNMP コマンドや ICMP エコー要求がその例です。

トンネル・モードでは、外部ヘッダーの IP アドレスが内部ヘッダーのアドレスと同じである必要はありません。例えば、2 つのセキュリティー・ゲートウェイによって接続されているネットワーク間の全トラフィックの認証に使用される AH トンネルを、その 2 つのセキュリティー・ゲートウェイで動作させることができます。これは非常に一般的な動作モードです。トンネル・モードをサポートするのに、ホストは必須ではありませんが、ホストがトンネル・モードをサポートする場合もあります。

トンネル・モードでは、カプセル化された IP データグラムの全的保護と、専用アドレスを使用する可能性が得られます。ただし、このモードに対応する特別の処理オーバーヘッドが生じます。

注: RFC 1825 による本来の AH 仕様には、トンネル・モードは要件として挙げられていません。そのため、RFC に基づく IPSec 実装には、トンネル・モードの AH をサポートしないものがあります。このことが、特定の事例を実現できるかどうかにかかわってきます。

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) では、データ機密性 (暗号化)、コネクションレス保全性 (つまり、パケット単位)、データ発信元認証、再生に対する保護が提供されます。ESP で必ず提供されるのは、データ機密性であり、データ発信元認証、データ保全性検査、再生保護は、オプションで提供できるものです。ESP を AH と比較してみれば分かるように、ESP でしか得られないのは暗号化だけであり、認証や保全性検査や再生保護は、どちらでも得られます。

ESP が認証機能を提供する場合は、使用するアルゴリズムは AH プロトコルで使用されるものと同じですが、対象範囲が異なります。

プロトコルの組み合わせ

ESP も AH も、適用にあたっては、それぞれ単独で使用することも、両者を組み合わせて使用することも、それぞれをそれ自体の別のインスタンス内にネストして使用することもできます。このような組み合わせによって、一対の交信ホスト間、一対の交信ファイアウォール間、またはホストとファイアウォールの間で、認証と暗号化がそれぞれ、または併せて得られます。

インターネット・キー交換 (IKE)

SA には、通信中のシステムが AH や ESP などの IPSec プロトコルを実行するために必要とする、すべての関連情報が入ります。例えば、SA では、使用される暗号アルゴリズム、keying 情報、関与するユーザーの ID を識別します。ISAKMP で、SA の交渉をサポートする標準化フレームワーク、すべての暗号キーの初期生成、これらのキーのその後のリフレッシュを定義します。Oakley は、ISAKMP フレームワーク内で使用される必要がある必須キー管理プロトコルです。ISAKMP では、SA の自動化交渉、暗号キーの自動化された生成とリフレッシュをサポートします。こうした機能を人手によるマシンの構成をほとんど、またはまったく伴うことなく実行できることが、VPN が規模を拡大していく重要な要素になっています。

キーの安全な交換が、安全な通信環境を確立する上で最も重要な要因になります。認証や暗号化がどれほど強力でも、キーが漏えいしていては、すべて無価値です。ISAKMP 手順は、キーの初期設定を処理するので、セキュリティーがまったく施されていないリンク上でも実行できる必要があります。つまり、IPSec プロトコルのブートストラップに使用されます。したがって、IPSec プロトコル・スイートの中で、ISAKMP プロトコルが最も複雑で、プロセッサー集中性の高い操作を使用します。

ISAKMP では、すべての情報交換に暗号化と認証を必要とします。だれにもキー keying 材料を傍受させないし、keying 材料の交換は、認証されたユーザー間でしか行われません。

VPN のユーザー事例

この節では、VPN ソリューションの実装に適した最も可能性の高いビジネス事例の中から次の 3 つを選んで説明します。

- 事業所接続ネットワーク
- 関連企業/業者ネットワーク
- リモート・アクセス・ネットワーク

以下の各項では、これらの事例のそれぞれについて簡単に概説します。

事業所接続ネットワーク

事業所事例では、組織内の 2 つのトラステッド・イントラネットを安全に接続します。そこで、セキュリティー上の焦点は、自社のイントラネットを外部の侵入から保護することと、自社のデータが公衆インターネット上を流れている間の保護の両方に集まります。したがって、次の項で説明する関連企業/業者ネットワークで、自社のイントラネット内のデータに関連企業がアクセスできるようにすることに焦点が置かれるのとは異なります。

本社では、事業所との通信によって生じる費用を最小限に抑制したいと考えているものとします。現在は、交換回線と専用線のどちらか、または両方を使用しているにしても、それよりも安価で、安全で、グローバルにアクセスできる他のオプションを、内部機密データの伝送用として試みたいと考えているものとします。インターネットを利用することによって、事業所接続 VPN を確立すれば、このような企業のニーズには簡単に応えることができます。

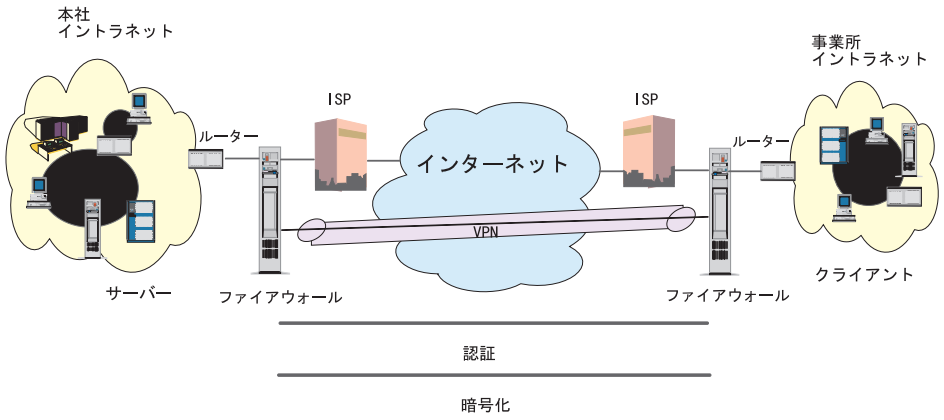


図 57. 事業所接続ネットワーク

本社と事業所の 1 つの間にこの VPN を実装する手段の 1 つとして、 図57 に示されているように、ISP (例えば、 IBM Global Services) からインターネット・アクセスを購入する方法があります。ファイアウォール機能が内蔵された IBM eNetwork ルーターやファイアウォールか、場合によっては、IPSec 機能を備えた IBM サーバーを、それぞれのイントラネットの境界に配して、自社トラフィックをインターネット・ハッカーから保護します。この事例では、クライアントやサーバーが IPSec テクノロジーをサポートする必要はありません。必要なデータ・パケットの認証と暗号

化は、 IPSec 対応可能ルーター (または、ファイアウォール) によって提供されるからです。この方法によれば、ルーターやファイアウォールが、潜在的にハッカーとなる可能性があるものに対してはアクセスを否認するので、機密情報はすべてアントラステッド・インターネット・ユーザーから秘匿されます。

事業所接続 VPN が確立されれば、事業所がローカルであろうと遠方にあろうと、本社では事業所との間で安全で費用効果的に交信できます。VPN テクノロジーによって、それぞれの事業所でも、それぞれが既存のイントラネットの範囲を拡張して、他の事業所のイントラネットを統合し、拡張された全社的規模の企業ネットワークを構築できます。

こうなれば、オープン IPSec テクノロジーの使用を通じて、新たに作成された環境をさらに拡大して、関連企業、業者、リモート・ユーザーを統合することも簡単にできます。

関連企業/業者ネットワーク

業界の主導的地位にある企業では、関連企業、系列企業、取引先などと安価で安全に通信できる必要があります。この交信を実現するために、多くの企業では、交換回線と専用線のどちらか、または両方の実装を選択してきました。しかし、これでは費用が高価につく場合がしばしばあり、到達範囲が地理的に限定される場合もあります。VPN テクノロジーでは、これに代わるものとして、インターネットやその他の公衆網を利用して、企業などが全世界を到達範囲とする費用効果性の高い私設拡張専用ネットワークを構築する方法を提供します。

例えば、完成品メーカー相手の主要部品業者の場合を想定してみましょう。特定の部品の特定数量を、完成品メーカーが必要とする時期に正確に納入することが要求されるため、完成品メーカーの在庫状況と生産スケジュールを常時把握している必要があります。現時点では、この交信は手動で処理していると考えられますが、当事者としては、時間がかかり、費用も高くつき、不正確であるとさえ感じている可能性があります。そこで、もっと簡単で高速で、効果的な通信手段を見つけたいと考えるはずです。しかし、このような情報には機密性を伴い、時間が重要な意味をもつことから、完成品メーカー側としては、データを自社の Web ページで発表したり、月次報告書などで情報を外部に配布することを承知しません。

そこで、部品業者と完成品メーカーは、320ページの図58 に図示されているような VPN を実装すれば、このような問題を解決できます。VPN は、部品業者のイントラネット内で、クライアント・ワークステーションとの間に構築してもよいし、完成品メーカーのイントラネット内にあるサーバーに対して直接構築することもできます。クライアントは自らの認証を、完成品メーカーのイントラネットを保護するルーターやファイアウォールに対して行うことも、完成品メーカーのサーバーに対して直接行う (自らが申し立てている本人に相違ないことを検証する) ことも、その両方を行うこともできますが、そのどれにするかは、セキュリティー・ポリシーによって決まります。そうすると、トンネルが確立できて、クライアントからインターネットを通して必要なサーバーに送信されるデータ・パケットがすべて暗号化されます。

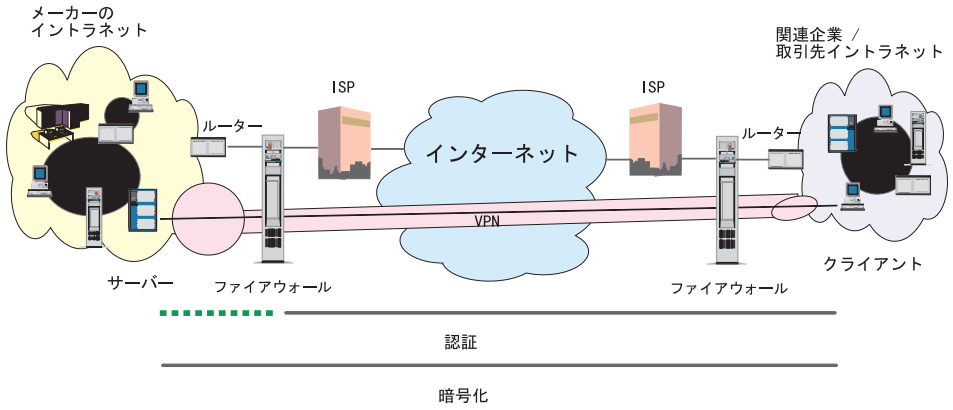


図 58. 関連企業/業者ネットワーク

この事例を実現する手段の 1 つとしては、企業が ISP (例えば、IBM Global Services) からインターネット・アクセスを購入する方法があります。その上で、インターネットにセキュリティー不備があれば、IPSec 対応可能ルーターか、 IBM eNetwork ファイアウォールか、IPSec 機能を備えた IBM サーバーを必要に応じて配備して、イントラネットを外部の侵入から保護することができます。エンド・エンド保護が必要な場合は、クライアント・マシンとサーバー・マシンの両方も、IPSec 対応可能にする必要があります。

この VPN テクノロジーの実装によって、完成品メーカーでは、既存の自社イントラネットの到達範囲を拡張して、1 社または複数社の部品業者を組み込み (本質的には、拡張私設ネットワークの構築になる)、同時にインターネットをそのバックボーンとして使用する費用効果性の高い利点を享受できます。こうなれば、オープン IPSec テクノロジーの柔軟性によって、この完成品メーカーがさらに多くの外部業者を統合する能力は無限に広がります。

VPN の実装にあたっては、一連のセキュリティー構成基準を設定する必要があります。それぞれの IPSec 対応可能ボックスが使用するセキュリティー・アルゴリズムやキーをリフレッシュする時期などの決定は、すべてポリシー管理の局面になります。キー・テクノロジーに関しては、今日普及しているセキュリティー・プロトコルのほとんどすべては、パブリック・キー暗号の使用で始まっています。各ユーザーには、それぞれ固有のパブリック・キーが割り当てられています。ディジタル・シグニチャーの形式をとる証明によって、ユーザーの ID と暗号化キーの認証性が検証されます。

このような証明は、保護 DNS などのようなパブリック・キー・データベース (これは、LDAP などのようなシンプル・プロトコル経由でアクセスできる) に保管できます。

リモート・アクセス・ネットワーク

リモート・ユーザーの場合は、自宅にいたり移動中であるときでも、自社の私設イントラネットに安全で費用効果的に連絡したい場合があります。

今日ではまだ高価な長距離やフリーダイヤル電話番号を使用している場合が多いのですが、インターネットを利用すれば、この費用は大幅に節減できます。例えば、

自宅にいたり移動中であるにもかかわらず、自社のイントラネット内のサーバーに入っている機密ファイルが必要になったとします。ISP (例えば、 IBM Global Services など) へのダイヤルイン接続の形式でインターネットにアクセスすることによって、自社のイントラネット内の該当のサーバーと交信し、必要なファイルにアクセスできます。

この事例を実現する手段の 1 つとして、図59 に図示されているように、eNetwork VPN IPSec 対応可能のリモート・クライアントと、ルーターやファイアウォールを使用する方法があります。クライアントは、ISP へのダイヤル呼び出しを経てインターネットにアクセスした上で、イントラネット境界にあるルーターやファイアウォールと自分自身の間に、認証と暗号化を経たトンネルを確立します。

リモート・クライアントとルーターやファイアウォールの間で認証を適用することによって、望ましくないばかりか、悪意のある可能性がある IP パケットからイントラネットを保護できます。さらに、リモート・ホストとルーターやファイアウォールの間を流れるトラフィックを暗号化することによって、部外者による情報の傍受を防止できます。

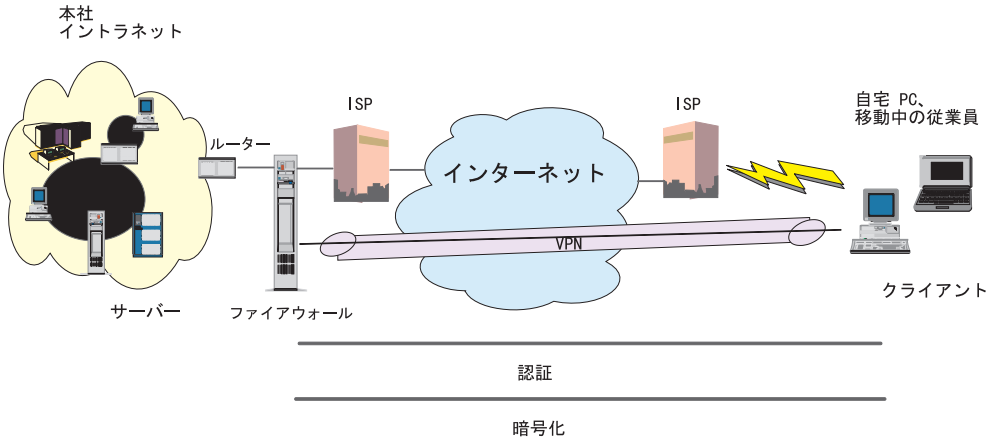


図 59. リモート・アクセス・ネットワーク

この節で説明した上記の 3 事例は、本書に記載されている IPSec の実装と構成の例の基礎になるものです。以下では、IBM ルーターを使用して IPSec トンネルを構成するための順次手順について説明します。

ポリシー・ベース・ネットワーキング

ポリシー・ベース・ネットワーキングとは、ルーティング以外のアクションを受信トラフィックに適用する必要があるかどうかを、ネットワーク装置が判別するアーキテクチャーのことです。例えば、トラフィックを IP セキュリティーによって保護する必要があるかとか、トラフィックに特殊なサービス品質 (QOS) 要件があるかなどといったことです。ネットワーク装置がポリシーに基づいて決定を行うためには、そうするように構成されている必要があります。大規模ネットワークへの拡張が難しいのは、複数の装置の構成です。共通の構成オブジェクトを保管し、検索し、配布する方式を開発すれば、こうした複数構成の管理は容易に行えるようになりま

す。構成データを保管し、検索し、共用する方式として受け入れられた方式は、ポリシー・データベースに入れておきます。

ポリシーを開発するためには、まず最初に、トラフィックのセキュリティーとパフォーマンスなどの要件を定義する必要があります。トラフィック処理要件の例として、*インターネットを通して事業所と本社の間を往来するトラフィックを保護する必要がある* とします。この要件を使用して、**ポリシー** と呼ばれているものを定義します。前記の要件がある場合は、ネットワーク装置では、受信するパケットのうちで、該当の事業所を発信元とし、本社をあて先とするものを識別できる必要があります。そこで、IP 発信元アドレスとあて先アドレスやプロトコルなどの属性に基づいて、***プロファイル*** が作成されて、受信パケットと突き合わせされます。パケットの属性がプロファイルの属性に一致すると、**アクション** 定義に規定されている方法で、パケットが処理されます。アクションでは、当然、暗号化や QOS の方式などが定義されることになります。

ポリシー、プロファイル、アクションのすべては、データベースに保管されます。したがって、データベースを使用すれば、特定のプロファイルやアクションを再使用し、さまざまに組み合わせて、複数のポリシーが作成できるので、それぞれのポリシーを装置構成で個々に作成する必要はありません。オブジェクトに変更を加える場合は、変更を 1 回加えれば、そのオブジェクトを使用するすべてのポリシーに変更が波及するので、変更管理が容易になります。例えば、複数の VPN トンネルで共通の暗号化方式が使用できます。そして、これらのトンネルのすべてについて暗号化方式を変更したい場合でも、変更を行うのは 1 つだけで済むことになります。

ポリシー・データベースは、4 つのプロトコルで使用できます。これらのプロトコルは、データが繰り返し型 (装置内で繰り返し型であり、ネットワークを通しても繰り返し型と考えられる) のプロトコルです。サポートされるプロトコルは、次のとおりです。

- RSVP
- DiffServ
- IKE
- IPSec

すべてのポリシーには、それぞれトラフィック・プロファイルと使用可能期間があります。ポリシーについては、特定のインターフェースによって発着するトラフィックにだけ適用されることを指定できます。IKE アクションを指定する場合は、ユーザーを識別する必要があるだけです。

IPSec アクションでは、除去、受け渡し、または保護のアクションを指定できます。アクションが除去であれば、このポリシーに一致するパケットはすべて除去されます。アクションがセキュリティーなしの受け渡しであれば、パケットはすべて平文テキストで受け渡されます。これに対して、アクションがセキュリティー付きの受け渡しであれば、パケットはすべて、このアクションで指定された SA を使用して保護されます。また、 IPSec アクションには、IPSec トンネルと IKE SA のトンネル・エンドポイントの IP アドレスも含まれます。

手動定義ポリシー

ポリシーをデータベース内に入れる場合のオプションの 1 つとして、手動による各装置の構成があります。IBM ルーター上で、コマンド行インターフェース (talk 6) や構成プログラムを使用して、ポリシー、プロファイル、有効期間、 IPSec アクションなどのオブジェクトや、セキュリティーとパフォーマンスに関連するその他のオブジェクトを追加します。すでに説明したように、このようなオブジェクトの一部には、さまざまなポリシーで再使用できるものがあるので、手動構成の手間が省けます。この方式は、ネットワークの規模が小さい場合は、受け入れられるし、望ましい場合さえありますが、大規模ネットワークでは、うまく機能しません。

LDAP サーバーからのポリシー

ネットワーク装置をそれぞれ構成するという方式に代わる代替策としては、ポリシーをすべて中央サーバーに入力しておき、装置に配布するという方法があります。IETF では、中央サーバーを LDAP サーバーとし、各ネットワーク装置をそれぞれ LDAP クライアントとすることを提唱しています。ただし、現時点では、 LDAP サーバーでポリシーの保管と配布ができることだけ理解していれば十分です。 図60 では、右側のポリシーが LDAP サーバーによって配布されています。

このトピックについて詳細を知りたい場合は、Web ブラウザーで下記のアドレスにアクセスしてください。

`http://www.networking.ibm.com/support/networkutility/downloads`

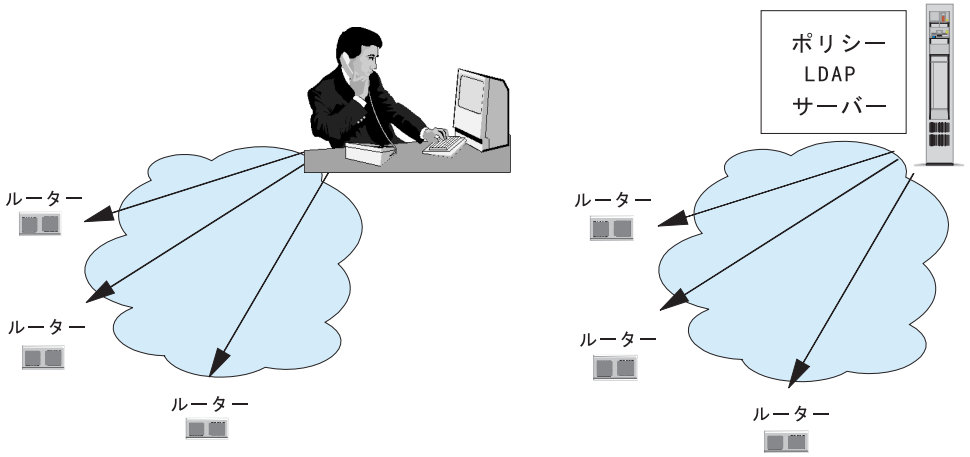


図 60. 手動と LDAP サーバーによるポリシーの配布

IKE

IKE では、IPSec 用の手動トンネルの問題に対処します。手動トンネルでは、 SA 特性とキーの難しい手動構成が必要です。

IKE は、以前は ISAKMP/Oakley キー・レゾリューションと呼ばれていたもので、 SA の自動化交渉、すべての暗号キーの初期生成と以後のリフレッシュをサポートするための、標準化されたフレームワークを定義します。交渉された SA と keying 材料を使用して、IKE 交換だけでなく、AH や ESP など、その他のセキュリティー機能

も保護します。キーの安全な交換が、安全な通信環境を確立する上で最も重要な要因になります。IKE ではキーの初期設定を扱うので、セキュリティーが施されていないリンク上でも使用できる必要があります。したがって、IPSec プロトコル・スイートの中で、IKE プロトコルが最も複雑で、プロセッサー集中性の高い操作を使用します。

IKE では、すべての情報交換に暗号化と認証の両方を必要とします。また、次のように幾つかの既知の表出に対する防護設計も行われています。

- **Denial of Service:** プロセッサー集中性の高い暗号操作を実行しなくても、無効メッセージを即時に識別して拒否できる、固有の Cookies を使用して、メッセージが構成されます。
- **Man-in-the-middle:** メッセージの削除、メッセージの変更、送信元へのメッセージの折り返し、古いメッセージの再生、予定外の受信先へのメッセージの転送など、よく発生するハッキングに対する保護が提供されます。
- **Perfect Forward Secrecy (PFS):** 過去のキーの折衷では、他のキーが見破られたのがキーの折衷の前でも後でも、そこから有用な手掛かりを得られません。

IKE 事前共用キーとディジタル証明

IKE には 2 つのフェーズがあります。フェーズ I では、暗号操作のプロセッサー集中性が最も高くなりますが、セキュリティーが正しく施されていないときは、「マスター・シークレット」を交換するように、このフェーズが設計されているからです。マスター・シークレットは、ユーザーのトラフィックを保護するために使用されるキーを派生させる場合に使用します。フェーズ I は、IKE メッセージ自体の保護の組の確立だけにかかわり、ユーザー・データを保護するためのキーの SA を確立することはありません。フェーズ I 操作は、頻繁に行う必要はなく、フェーズ I 交渉を 1 回使用すれば、複数回のフェーズ II 交換をサポートできます。図61 に、フェーズ I で交換されるメッセージが示してあります。この 6 つのメッセージで、メイン・モードでの 2 対間の交換が示されます。

メイン・モード:

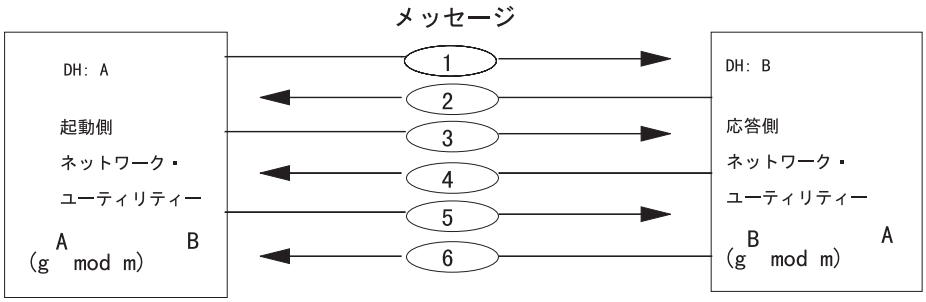


図 61. IKE メイン・モードでのフェーズ I メッセージ交換

メッセージ 1 が、ISAKMP トンネルの確立を望む IKE ピアによって送信されます。最初のメッセージは、標準 IP ヘッダーと UDP ヘッダーで構成されています。ISAKMP メッセージはすべて、あて先ポート 500 を指定した UDP パケットに入れて搬送されます。UDP ペイロードは、ISAKMP ヘッダーと SA ペイロードと、1 つまたは複数の提案/変換ペイロードで構成されています。

メッセージ 2 には、応答側で受け入れを望む単一提案/変換が入っています。

メッセージ 3 とメッセージ 4 では、暗号キーが最終的に派生される元になる情報を交換します。情報はすべて平文で交換されます。メッセージには、キー交換ペイロードと nonce ペイロードが含まれます。キー交換ペイロードには、Diffie-Hellman (DH) 公開値が入っています。指数は DH 秘密値で、これは常に秘密に保たれます。nonce ペイロードには、非常に厳密な数学的指針に従って生成される大きな乱数が入ります。このペイロードは、接続の存在の保証と、再生ハッキングに対する保護のために使用されます。

これで、両方の IKE 装置とも、それぞれ相手側の DH 公開値とそれ自体の独自のキーをもちました。 DH 計算を実行して、共用秘密を生成できます。共用秘密は、DH 公開値のプライベート・キー乗です。324ページの図61 では、 DH 秘密値は A と B です。この場合は、共用秘密は、DH 値 A と B の使用によって派生した、両方のルーターで等しい数です。*g* の値は、メッセージ 1 と 2 でルーターによってすでに合意されています。

この時点以降は、キーはすでに交換され確立されている情報を使用して生成できます。これで、両方のルーターには、次のことが分かっています。

- 2 つの nonce 値 N-i と N-r
- それぞれの独自の DH 秘密値
- それぞれの相手側の DH 公開値 pk-i と pk-r
- 起動側 Cookies と応答側 Cookies
- 合意されたハッシュ・アルゴリズム
- 共用秘密 -- DH 計算の結果

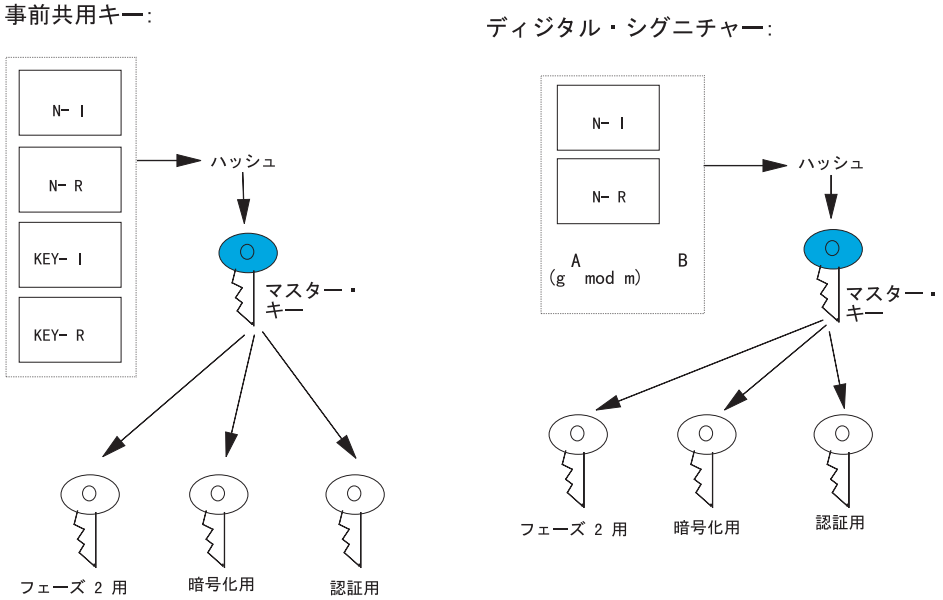


図 62. キーの生成

325ページの図62 に示されているように、両方の装置はここで、SKEYID と呼ばれるマスター・キーを生成します。これは、実際の実暗号キーが派生される keying 材料です。マスター・キーを生成する方式は、メッセージ 2 で同意された認証に応じて異なります。オプションは、次のとおりです。

事前共用キー
マスター・キーは、起動側からの nonce (N-I) と応答側からの nonce (N-R) による事前共用キーのハッシュから派生します。

ディジタル・シグニチャー
マスター・キーは、起動側からの nonce (N-I) と応答側からの nonce (N-R) による共用秘密 (DH 計算の結果) のハッシュから派生します。

メッセージ 5 の目的は、応答側が起動側を認証できるようにすることにあり、メッセージ 6 では、起動側が応答側を認証できるようにします。メッセージの形式は、IKE ピア間での合意が、事前共用キーによる認証かディジタル・シグニチャーによる認証かに応じて異なります。

この時点で、フェーズ I メッセージがメイン・モードで完了です。各ピアは、それぞれ相手側ピアに対してそれ自体を認証し、両方が ISAKMP SA の特性について合意し、同じ一組の keying 材料を派生させました。

積極モード:
フェーズ I でのもう 1 つの方法が積極モードです。積極モードは、プロセッサー集中性が低く、メッセージ交換が 6 回ではなく 3 回だけです。ただし、積極モードでは安全性が低くなります。

積極モードでのメッセージ 1 は、同位に ISAKMP SA を自由に選択させるという点で、メイン・モードでのメッセージ 1 に似ています。これには、キー交換ペイロード、nonce ペイロード、識別ペイロードも含まれています。これらは、メイン・モードでは、メッセージ 3 と 5 で送信されたものです。つまり、積極モードでは、発信側の ID は平文で送信されることを意味し、暗号化されているメイン・モードの場合とは異なります。

積極モードでのメッセージ 2 では、応答側が受け入れを望む ISAKMP SA を示します。応答側では、メイン・モードではメッセージ 2、メッセージ 4、メッセージ 6 に挿入していたペイロードを、この応答に組み込みます。

つまり、応答側では、認証についてはディジタル・シグニチャーを使用する場合でも、識別、証明、シグニチャーは平文で送信することを意味します。認証に事前共用キーを使用する場合は、識別とハッシュのペイロードは平文で伝送されます。なお、メイン・モードでのメッセージ 6 では、認証材料は送信前に暗号化されています。

メッセージ 3 は、暗号化され、応答側で起動側を認証できるようにするために送信されます。起動側では、応答側にハッシュ・ペイロード (事前共用キー) か証明/シグニチャー・ペイロード (ディジタル・シグニチャー・モード) を送信します。ペイロードの内容については、メイン・モードの項で説明しています。応答側では、メイン・モードでのメッセージ 5 について説明したように、提供された情報を使用して起動側を認証します。

フェーズ II の交換では、ユーザー・データ交換を保護するために使用される、 SA とキーを交渉します。フェーズ II の IKE メッセージは、フェーズ I で生成された IKE SA で保護されます。フェーズ II の交渉は、一般的に、フェーズ I の場合よりも頻繁に行われ、フェーズ I では、1 日に 1 回程度しか行われない場合があるのに対して、通常は数分に 1 回の頻度で行われます。

フェーズ II では、メッセージ交換は起動側からの申しいでで始まります。メッセージ 1 で、図63 に示されているように、起動側が共用キーを計算するためのオプションと情報を提供します。これには、公開 DH (pk-i)、起動側 nonce 値 (大きな乱数 (N-i)) があります。この情報はすべて、暗号化された形式で転送されます。

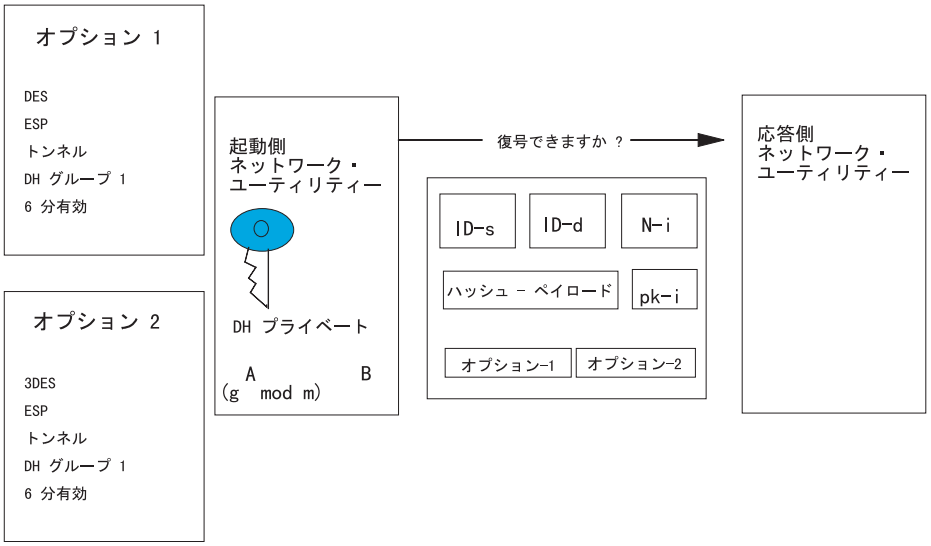


図 63. フェーズ II のメッセージ 1

メッセージ 2 では、応答側が起動側からの情報に加えて、類似情報 (N-r、pk-r) を起動側に提供します。応答側では、提供されたオプションから 1 つを選択します。

これで、各ネットワーク・ユーティリティーには、それぞれ相手側について次のことが分かりました。

- 相手側の nonce N-I と N-R
- 相手側のパブリック・キー (つまり、DH 公開値)
- セキュリティー・パラメーター索引 (SPI) : 2 つのセキュリティー・アソシエーションのどちらか一方 (インバウンドかアウトバウンド) を固有に識別する任意の 32 ビット値
- 合意されたプロトコル
- フェーズ I で計算された SKEYID_d (これは、マスター・キーと 2 つの Cookies と DH 共用秘密のハッシュ)

DH 計算は、フェーズ II の共用秘密を生成するために実行されます。応答側から起動側に向かうトラフィックに関する keying 材料は、 SKEYID_d と共用秘密とプロトコルと起動側の SPI と 2 つの nonce のハッシュです。

これで、必要な keying 材料はすべて交換されました。メッセージ 3 では、接続が活動していることを実証します。

トンネリング・プロトコル

次のプロトコルの詳しい説明については、*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* を参照してください。

レイヤー 2 トンネリング

レイヤー 2 トンネリング・プロトコル (L2TP) は、IP ネットワークをまたがってポイント・ポイント・プロトコル (PPP) トラフィックをトンネル伝送するための、 IETF 標準のトラック・プロトコルです。 L2TP では、トンネル・セットアップ・メッセージ用と、エンドポイント間での PPP データのトランスポート用の両方として、UDP トランスポートを使用します。 L2TP は、クライアントが L2TP アクセス・コンセントレーター (LAC) と呼ばれ、サーバーが L2TP ネットワーク・サーバー (LNS) と呼ばれる、クライアント・サーバー・アーキテクチャーです。

レイヤー 2 転送

レイヤー 2 転送 (L2F) は、Cisco Systems, Inc によって開発されたトンネリング・プロトコルであり、L2TP の場合と同じソリューションが得られます。IETF では、L2TP の開発にあたって、Cisco 社の L2F と Microsoft 社の PPTP の一部を再利用しました。IBM ルーターには、Cisco ルーターとの相互運用の場合は、L2F が実装されます。IBM ルーター間では L2TP が使用されますが、理由はそれが IETF 標準であるからです。

L2F では、2 つの装置 -- NAS とホーム・ゲートウェイを定義します。

ポイント・ポイント・トンネリング・プロトコル

ポイント・ポイント・トンネリング・プロトコル (PPTP) は、目的が L2TP の場合と同じで、IP ネットワークをまたがって PPP パケットをトンネル伝送することにあります。L2TP は、IETF によって開発されましたが、その基になっているのは PPTP と L2F (Cisco 社の同等品) です。Microsoft 社の装置とのトンネルを確立する場合は、IBM ルーターで PPTP をサポートする必要があります。

PPTP は、クライアントが PPTP ネットワーク・アクセス・コンセントレーター (PAC) と呼ばれ、サーバーが PPTP ネットワーク・サーバー (PNS) と呼ばれる、クライアント・サーバー・アーキテクチャーです。このアーキテクチャーでは、PAC は一般的にワークステーションで、 PNS はサーバーです。

PPTP による自発的トンネリング

自発的トンネリングは、クライアント開始モデルです。クライアント/PAC が NAS にダイヤルインし、IP アドレスを入手し、正規のネットワーク・アクセスを確立します。その後で、別のダイヤル呼び出しセッションをオープンし、これが PPTP トンネルを確立します。IBM ルーターが自発的トンネリング PPTP で使用できる事例は 2 つあります。IBM ルーターでは、トンネルを終端するすることも、トンネルを開始す

ることもできます。これでトンネルを終端する場合は、トンネルを開始するクライアントは、PPTP 対応可能である必要があり、NT か Windows の装置、または PPTP をサポートするそれ以外の装置が使用できる必要があります。2 番目の事例では、ルーターから PPTP 装置 (例えば、NT サーバーなど) にトンネルを逆に確立できます。

L2TP による強制的トンネリング

強制的トンネリングは、ルーター開始モデルです。この事例では、クライアントは L2TP に関知しません。クライアントが LAC にダイヤルインし、LAC が逆に LNS への L2TP トンネルを開始します。この場合は、LAC は、LNS に着信コール・リクエストを送信します。クライアントと LAC はすでに LCP と部分認証を交渉しているので、LAC が、この情報をプロキシー認証と呼ばれるもので LNS に渡します。コール設定後に、LNS では PPP 認証と、新しく形成されたトンネルを通るクライアントとのネットワーク・フェーズを完了します。

VPN イベント・ログ・サポート (ELS)

次の 4 つのサブシステムを使用すると、デバッグと VPN 構成の状況の判別に役立ちます。

L2 サブシステム

L2 サブシステムには、L2F、L2TP、PPTP を含めて、レイヤー 2 トンネリング・プロトコルのすべてに関する ELS メッセージが入っています。このサブシステムでは、トンネルとコールの設定と終了についての情報を表示します。また、L2 トンネルを通して送受信されるパケットについての情報も表示します。トンネルの交渉が正常に行われなかった場合のエラー・メッセージも表示されます。

PLCY サブシステム

PLCY サブシステムに関する ELS メッセージでは、ポリシー・データベース・リフレッシュの状況、データベース内にロードされた規則の数、ポリシー・データベースの構築時に発生した可能性があるエラーについての情報が分かります。パケット情報を調べれば、ポリシー・データベース照会、このような照会の結果の規則やアクション、ポリシー・データベースに関する交渉に関係のあるエラーやその他の情報が得られます。

IPSP サブシステム

IPSP サブシステムには、ルーター内の IPSec モジュールに関するメッセージが入っています。IPSP サブシステムでは、パケットの暗号化と復号についての情報、使用されているアルゴリズム、障害のためパケットが廃棄された結果のエラー・メッセージを表示します。

IKE サブシステム

IKE サブシステムでは、最終的には 2 つのセキュリティー・ゲートウェイまたはホストの間に安全な IPSec トンネルをセットアップする、フェーズ I とフェーズ II の

交渉についての情報を表示します。事前共用キーの不一致、セキュリティー提案の不一致、ポリシー・エラーなどのため、交渉が正常に行われなかった結果のエラーがあれば、すべて表示されます。

第20章 VPN (仮想私設ネットワーク) の例

この章では、次のような例を示して、基本 VPN ソリューションを実際に則して説明します。

- 事前共用キーの使用による IPSec ルーター間 VPN
- ディジタル証明の使用によるルーター間 VPN
- IBM ルーターを終端とする自発的 PPTP トンネル
- IBM ネットワーク・ユーティリティー開始の自発的 PPTP トンネル
- IBM ネットワーク・ユーティリティー開始の自発的 L2TP トンネル
- IBM ネットワーク・ユーティリティー LNS で終端する L2TP トンネル

事前共用キーの使用による IPSec ルーター間 VPN

この例では、自動キー生成と事前共用キーによる IPSec を使用します。 図64 では、保護トンネルがゲートウェイ間に作成されています。このトンネルでは、特定のホストからのトラフィックの認証と暗号化を行い、それ以外のトラフィックはすべて除外します。データにトンネルを通過させることができるのは、トンネルのどちらの端のどのホストであるかは、プロファイルに正確に記述されています。ポリシーで許可できるのは、どちらかの端の 1 つのホストか、どちらかの端の 1 つまたは複数のサブネットか、その両方の任意の組み合わせです。ゲートウェイ間トンネリングには、LAN 上では認証も暗号化も行われないという制限があります。したがって、このソリューションでは、LAN 上でのセキュリティーは得られません。

この例で使用されているネットワーク (図64) は、2 つのトークンリング・セグメントが 2 台の IBM 2210 ルーターで接続された構成です。実際の事例では、ルーター間のシリアル・リンクは、広域ネットワーク (WAN) であれば、私設ネットワークでも公衆ネットワークでも構いません。

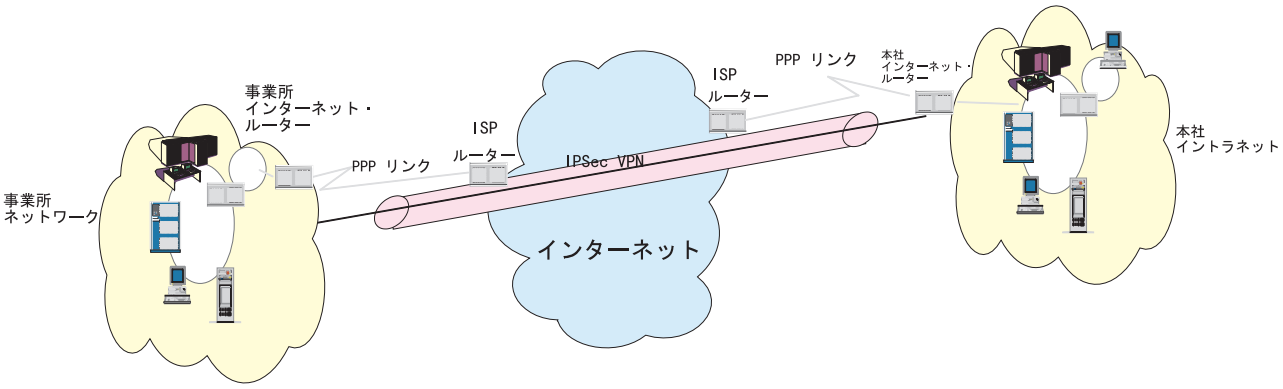
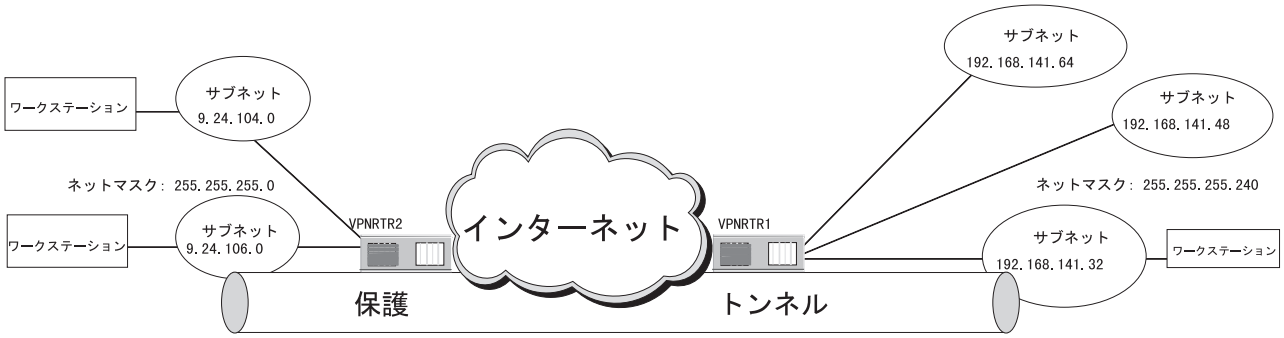


図 64. 構成例を示すために使用した物理ネットワーク

332ページの図65 では、トンネルでサブネット 9.24.106.0 (事業所ルーター VPNRTR2 と本社ルーター VPNRTR1 を経由) とサブネット 192.168.141.32 の間のすべてのトラフィックを認証し暗号化する必要があります。それ以外のサブネットからのそれ以外のトラフィックが、この 2 つのルーター間のリンクを通過することはできません。

認証では、トンネルが正しいエンドポイント間にセットアップされていることを保証し、暗号化では、データが WAN 通過中に傍受されることがないよう保護します。



ルーター IP アドレス:
VPNRTR2 - トークンリング 9.24.106.8
- シリアル 192.168.141.17
VPNRTR1 - トークンリング 192.168.141.33
- シリアル 192.168.141.18

図 65. 事前共用キーによる IPSec を示すために使用したサンプル・ネットワーク

VPNRTR1 用として IPSec トンネルに関するポリシーを作成する

次の手順に従って、ルーターを構成します。

1. IP セキュリティーを使用可能にする。
2. 事前共用キーを作成する。
3. ポリシーを追加する。
4. プロファイルを追加する。
5. 有効期間を追加する。
6. IPSec アクションを追加する。
7. IPSec 提案を追加する。
8. ESP 変換を追加する。
9. ISAKMP アクションを追加する。
10. ISAKMP 提案を追加する。

IP セキュリティーを使用可能にする

Talk 6 コマンド行インターフェースから、ボックス・レベルで IP セキュリティーを使用可能にします。

表 76. IP セキュリティーを使用可能にする

```
VPNRTR1  *TALK 6
Gateway user configuration
VPNRTR1 Config>feature ipsec
IP Security feature user configuration
IPsec config>ipv4
VPNRTR1 IPV4-IPsec config>ENABLE IPSEC
It is necessary to restart the router for IPsec to be active.
VPNRTR1 IPV4-IPsec config>EXIT
VPNRTR1 IPsec config>EXIT
```

事前共用キーを作成する

すべてのリモート・ユーザーに、それぞれ事前共用キーを構成する必要があります。したがって、事前共用キーは余り拡張が容易ではありません。ただし、事前共用キーは定期的にリフレッシュされるので、手動トンネル方式よりも優先されます。

Talk 6 **Add User** コマンドを使用して、キーを構成します。

表 77. PPP ユーザーを追加する

```
VPNRTR1 Config>FEATURE Policy
IP Network Policy configuration VPNRTR1 Policy config>ADD USER
Choose from the following ways to identify a user:      1
        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]? 1
Enter the IP Address that distinguishes this user
 [0.0.0.0]? 192.168.141.17                          2
Group to include this user in []?
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]? 1
Mode to enter key (1=ASCII, 2=HEX) [1]? 1
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (3 characters) in ascii:       3


Here is the User Information you specified...

Name      = 192.168.141.17
Type      = IPV4 Addr
        Group     =
        Auth Mode =Pre-Shared Key
        Key(Ascii)=key                                  3
Is this correct? [Yes]:
```

1. ルーターには、リモート IKE 同位と事前共用キーを認識する方法が分かる必要があります。
2. この例では、選択された識別子は、「IP Address」でした。これは、リモート・ルーターのトンネル・エンドポイントのアドレス (この例では、 VPNRTR2 の WAN インターフェースの IP アドレス) である必要があります。
3. キーは、妥当性検査のために 2 回入力する必要があり、トンネル・エンドポイントのそれぞれのルーターで正確に同じである必要があります。この例では、ワード **key** を使用しています。128 文字を上限として、どんなキーでも使用できます。ただし、それぞれのルーターで、正確に同じキーを 2 回ずつ入力する必要が

あります。これについては、テキスト・エディターにキーを入力しておいて、そのキーを Talk 6 プロンプトの入力フィールドに切り貼りするのが最も簡単な方法です。

ポリシーを追加する

ポリシーとは、ルーターに出入りするトラフィックを処理する方法を記述するためのフレームワークです。アクセス制御がなければ、ルーターではルーティングの決定を行うだけです。ポリシーの使用によって、ルーターでは、パケットにインターフェースを通過させるかどうか、パケットは認証の必要があるかどうか、パケットは暗号化か復号の必要があるかなどの決定を行います。ポリシーでは、他のオブジェクトを結合します。この例では、**Add Policy** コマンドを最初に使用しています。その理由は、すべての必要な情報を正しい順序で入力するように指示するプロンプトが出されるので、最初のポリシーを作成する最も簡単な方法と考えられるからです。

ポリシーがセキュリティー・トンネルを作成する場合は、プロファイルに一致するパケットだけが暗号化され転送されます。プロファイルに一致しないそれ以外のパケットは、別のポリシーで明示的に除去されない限り、平文で渡されます。複数のポリシーがルーター上に存在しているときは、優先順位番号によるポリシーの評価が行われます。

着信パケットを複数のポリシーと突き合わせて評価する方法については、 図66 をごらんください。パケットがポリシー #1 のプロファイルに一致すれば、IPSec に送られて処理されます。パケットがポリシー #1 のプロファイルに一致しない場合は、ポリシー #2 のプロファイルと突き合わせて評価されます。プロセスがこのようにして続き、着信パケットはすべてのポリシーと突き合わせて評価されます。パケットがどのプロファイルにも一致しなかった場合は、平文でルーティング・プロトコルに送られて処理されます。

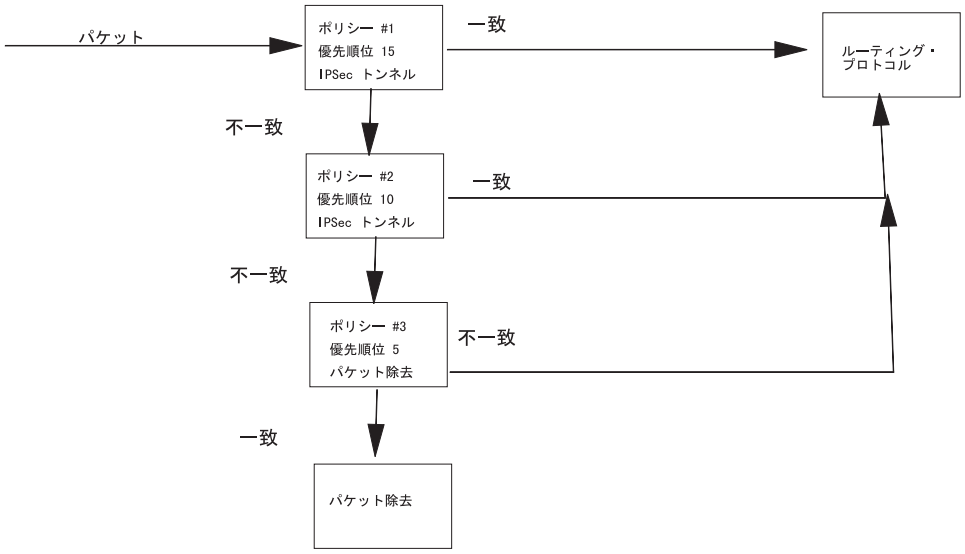


図 66. ポリシーが複数の場合の効果

表 78. 新規ポリシーを作成する

```
VPNRTR1 Policy config>ADD POLICY
Enter a Name (1-29 characters) for this Policy []? ike-pre-32-106
Enter the priority of this policy (This number is used to determine
the policy to enforce in the event of policy conflicts) [5]? 15              1
List of Profiles:
       0: New Profile                  2
```

1. ポリシーの優先順位では、複数のポリシーについて評価の順序を指定します。優先順位番号が大きいポリシーほど先に評価されます。複数のポリシーが定義されているときのパケット評価の流れについては、 334ページの図66 をごらんください。
2. ポリシーが追加されたら、そのポリシーに対応するプロファイルを作成する必要があります。このルーターではプロファイルがまったく作成されていなかったので、新規プロファイルの作成を指示するプロンプトが出されています。

プロファイルを追加する

プロファイルでは、パケットをポリシーによる作用の対象とする必要があるかどうかを判別する場合に使用する、基準を記述します。この基準としては、発信元とあて先のアドレス、プロトコル、ポート・タイプ、差異化サービス (DS/TOS) バイトがあります。

表 79. プロファイルを追加する

```
List of Profiles:
       0: New Profile
Enter a Name (1-29 characters) for this Profile []? 32-106        1
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?        2
Enter IPV4 Source Address [192.168.141.32]?
Enter IPV4 Source Mask [255.255.255.240]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [9.24.106.0]?
Enter IPV4 Destination Mask [255.255.255.0]?

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

Select the protocol to filter on (1-4) [3]?         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]?        4
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]: YES         5
Enter local identification to send to remote
     1)  Local Tunnel Endpoint Address
     2)  Fully Qualified Domain Name
     3)  User Fully Qualified Domain Name
     4)  Key ID (any string)
Select the Identification type (1-4) [1]?
Any user within profile definition allowed access? [Yes]:
Limit this profile to specific interface(s)? [No]:


...continued on next screen
```

1. ここでは、記述名 106-32 が使用されています。
2. この例では、一方のサブネット上のホストであれば、他方のサブネット上のホストには必ずアクセスできる必要があります。
3. さらにサービスを制限したい場合は、特定のプロトコルと特定のポートだけが使用できるように、プロファイルを構成できます。例えば、TCP ポート 23 だけを許容することによって、Telnet だけが使用できて、FTP は使用できなくすることができます。
4. DS バイトは、QOS や優先順位付けに関連します。プロファイルに一致するトラフィックを、優先順位によって選択できます。
5. ISAKMP に関してローカルとリモートの ID を構成するこのステップは、相手側ピアがユーザーの IP アドレス以外のものでユーザーを識別する必要がある場合以外は、オプションです。

表 80. プロファイルを確認する

```
Here is the Profile you specified...


Profile Name    = 32->106
        sAddr:Mask= 192.168.141.32: 255.255.255.240 sPort=    0 : 65535
        dAddr:Mask= 9.24.106.0 : 255.255.255.0   dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
        Remote Grp=All Users
Is this correct? [Yes]:
List of Profiles:
        0: New Profile
        1: 32->106

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

有効期間を追加する

有効期間とは、ポリシーが有効である時間枠です。有効期間を構成して、ポリシーが有効である期間を指定してもよいし、月、曜日、時刻を指定することもできます。このように柔軟性があるので、ネットワーク管理者は、ポリシーがいつ有効であるか指定できます。例えば、「常時」、「今年の 1 月と 2 月だけ」、「月曜日から金曜日の午前 9 時から午後 5 時までだけ」で要件になります。このような要件が、**Add Validity Period** コマンドを使用して構成値に変換されます。

表 81. 有効期間を追加する

```
List of Validity Periods:              1
        0: New Validity Period

Enter number of the validity period for this policy [0]?
Enter a Name (1-29 characters) for this Policy Valid Profile []? always
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   = always                       2
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day
Is this correct? [Yes]:
List of validity periods:
        0: New Validity Period
        1: always
Enter number of the validity period for this policy [1]?
```

1. 新規ポリシーの作成中なので、プロンプトによって有効期間の作成を指示されます。以前作成された有効期間を再使用できる場合もあります。既存の有効期間が使用されている場合が、この章の後出の例で見られます。この概念は、ポリシー・データベース・オブジェクトのすべてに該当します。どんなオブジェクトでも、適宜再使用できます。
2. この例での有効期間は、常時有効に構成されています。

IPSec アクションを追加する

ポリシーは、プロファイルと有効期間に加えて、IPSec アクションと手動 IPSec と DiffServ アクションのどれかにも対応づける必要があります。この事例では、IPSec アクションが構成されています。

IPSec アクションでは、除去、受け渡し、または保護のアクションを指定できます。アクションが除去であれば、このポリシーで使用されるプロファイルに一致するパケットはすべて除去されます。アクションがセキュリティーなしの受け渡しであれば、パケットはすべて平文テキストで受け渡されます。アクションがセキュリティー付きの受け渡しであれば、パケットはすべて、このアクションで指定された SA によって保護されます。また、IPSec アクションには、 IPSec トンネルと IKE SA のトンネル・エンドポイントの IP アドレスも含まれます。

表 82. IPSec アクションを追加する

```
Should this policy enforce an IPSEC action? [No]: y
IPSEC Actions:
        0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
Enter a Name (1-29 characters) for this IPsec Action []? tunnel_vpnrtr1-vpnrtr2
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
 [192.168.141.18]?
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
 [0.0.0.0]? 192.168.141.17
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:        1
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):           2
     1)  Copy
     2)  Set
     3)  Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?          3
Do you want to negotiate the security association at
system initialization(Y-N)? [No]: y          4
```

1. 次に、交渉された IPSec トンネルが別のトンネル内にも流れ込むかどうかについて尋ねられます。これは、最初は V3.2 のコードに入れて出荷されたトンネル内トンネル機能に関連しています。トンネル内トンネルに関する事例は、図67 に図示してあります。

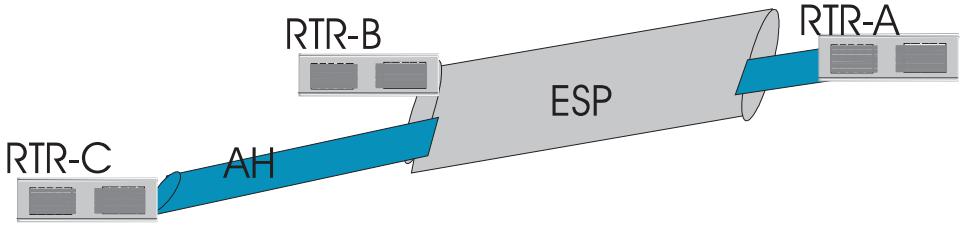


図 67. トンネル内のトンネル

RTR-A と RTR-C の間を往来するトラフィックは、すべてに認証が必要ですが、RTR-A と RTR-B の間のトラフィックは、すべて暗号化が必要です。トンネル内トンネルの特質は、トンネルの開始点は同じであるが、終了点が異なることにあります。この例の場合は、応答は「No」です。

2. IPSec ヘッダーが作成されると、IP ヘッダーのフィールドの多くは、保護されているパケットのヘッダーからコピーされます。「**don't fragment**」フィールドの設定方法を制御できます。元のパケットからコピーし、 DF ビットを設定するか、それが元のパケットでオンになっている場合は、オフにすることができます。DF ビットの設定には、IPSec にとって重要な意味が潜在しています。次の図について、考えてみましょう。

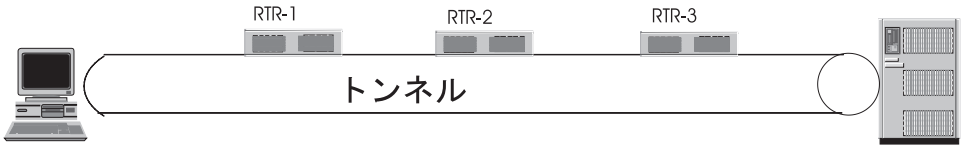


図 68. DF ビットについて

トラフィックは左側の装置から右側の装置に流れています。RTR-2 は、パケットを分割する必要がありますが、DF ビットが設定されているため、そうすることができません。RTR-2 では、「ICMP パケット大き過ぎ」メッセージを生成して、それをパケットの送信側である RTR-1 に送信します。そこで、 RTR-1 では、パケットが大き過ぎることを送信側に通知する必要があります。しかし、これが RTR-1 にとって問題の原因になる可能性があります。(a) ICMP パケットに入る元のパケットの部分が少な過ぎて、送信側を判別できなくなったり、 (b) IP アドレスが暗号化されたりする可能性があるからです。RTR-1 が送信側を判別できない場合は、トンネル情報を保管して、そのトンネルに関して別のパケットが到着するのを待ちます。そのパケットが到着すると、 RTR-1 では、必要なら、「ICMP パケット大き過ぎ」メッセージを生成します。したがって、DF ビットの設定については慎重に考慮する必要があります。

この例では、 DF ビットを copy (デフォルト) に設定しました。

3. 「**Enable replay prevention**」では、受信パケット上で順序番号をチェックする必要があるかどうか定義します。
4. このパラメーターでは、システム始動時にこの SA を作成する必要があるかどうかについて制御します。「**no**」と指定すると、この SA を交渉する必要があるのは、ポリシーに一致するパケットが受信されたときだけであることを示します。

このステップが終了すると、IPSec 提案の選択を指示するプロンプトが出されます。以前の提案は存在していないので、新規提案を作成する以外のオプションはありません。

IPSec 提案を追加する

IPSec 提案には、フェーズ II ISAKMP 交渉時に提案または照合チェックする ESP 変換、AH 変換 (または、その両方) についての情報が入ります。フェーズ II 交渉の説明については、323ページの『IKE』 をごらんください。 PFS (Perfect Forward Secrecy) を必要とする場合は、 IPSec 提案では、使用する DH (Diffie-Hellman) グループを識別します。IPSec 提案が参照する変換は送信され、指定されている順序と照合チェックされます。リスト内の最初の ESP または AH 変換は、使用に最も適したものである必要があります。リスト内に複数の変換がある場合は、各変換をピアの変換リストと比較して、一致を見つけます。構成済み変換のどれもがピアのリストに一致しない場合は、交渉は正常に行われません。IPSec 提案には、 AH 変換と ESP 変換の組み合わせがリストされている場合がありますが、有効な組み合わせは次のものだけです。

- AH だけ (トンネル・モードかトランスポート・モード) のリスト
- ESP だけ (トンネル・モードかトランスポート・モード) のリスト
- AH (トランスポート・モード) のリストと ESP (トンネル・モード) のリスト

– AH (トランスポート・モード) + ESP (トランスポート・モード) では、トランスポート・モードを定義する。
– AH (トンネル・モードかトランスポート・モード) + ESP (トンネル・モードかトランスポート・モード) では、トンネル・モードを定義する。

表 83. IPSec 提案を追加する

```
You must choose the proposals to be sent/checked against during phase 2
negotiations.  Proposals should be entered in order of priority.

List of IPSEC Proposals:         1
        0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
Enter a Name (1-29 characters) for this IPsec Proposal []? esp-prop1
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]: y         2
```

1. IPSec アクションを指定したため、新規提案の作成を指示するプロンプトが出されます。
2. 「**y**」とタイプして ESP 変換を入力すると、変換の追加を指示するプロンプトが出されます。

IPSec 変換を追加する

IPSec 変換の属性には、IPSec の暗号化と認証のパラメーターについての情報が入り、キーがリフレッシュされる頻度も指定されます。変換は AH (認証だけ) と ESP (暗号化、認証、またはその両方) のどちらかであり、トンネル・モードとトランスポート・モードのどちらかで動作するように構成できます。

表 84. IPSec 変換を追加する

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

Enter the Number of the ESP transform [0]?
Enter a Name (1-29 characters) for this IPsec Transform []? esp-trans1
List of Protocol IDs:
     1)  IPSEC AH
     2)  IPSEC ESP

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

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

Select the ESP Authentication Algorithm (0-2) [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]?           3
Security Association Lifesize, in kilobytes (1024-65535) [50000]?           4
Security Association Lifetime, in seconds (120-65535) [3600]?


Here is the IPSec transform you specified...


Transform Name  = esp-trans1
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES
Is this correct? [Yes]: y
List of ESP Transforms:
        0: New Transform
        1: esp-trans1

Enter the Number of the ESP transform [1]?
Do you wish to add another ESP transform to this proposal? [Yes]: n
```

1. トランスポート・モードは、2 つのエンド・ステーション間に定義された SA です。トンネル・モードが使用されるのは、装置の少なくとも一方がセキュリティー・ゲートウェイ (例えば、ルーター) のときです。2 つのルーター間の SA なので、トンネル・モードを選択しました。
2. これは認証方式です。HMAC_SHA の方が HMAC_MD5 よりも安全性が大です。
3. 暗号化方式を選択します。なお、ESP 3DES は米国以外では使用できません。
4. SA lifetime/lifesize を設定します。SA の有効期限が切れると、IKE がフェーズ II の計算を実行して、キーをリフレッシュします。デフォルトの 3600 秒に設定されています。つまり、何者かがパケットの 1 つを代行受信しようとしても、 1 時間以内にコードを見破る必要があることを意味します。大学生のグループによって、DES 暗号化をたった 1 つ見破るのに 22 時間かかることが実証された例があります。

IPSec 変換を追加し終わると、IPSec 提案の確認を指示するプロンプトが出されます。

表 85. IPSec 提案を確認する

```
Here is the IPSec proposal you specified...


Name  = esp-prop1
        Pfs   = N
        ESP Transforms:
                esp-trans1
Is this correct? [Yes]: y
List of IPSEC Proposals:
        0: New Proposal
        1: esp-prop1

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

IPSec 変換と提案の作成が終われば、IPSec アクションを終了できます。確認画面が表示され、ポリシーに対応づけるアクションの選択を指示するプロンプトが出されます。

表 86. IPSec アクションを確認する

```
Here is the IPSEC Action you specified...

IPSECAction Name = tunnel_vpnrtr1-vpnrtr2
        Tunnel Start:End         = 192.168.141.18 : 192.168.141.17
        Tunnel In Tunnel         =              No
        Min Percent of SA Life   =              75
        Refresh Threshold        =              85 %
        Autostart                =             Yes
        DF Bit                   =            COPY
        Replay Prevention        =        Disabled
        IPSEC Proposals:
                esp-prop1
Is this correct? [Yes]:
IPSEC Actions:
        0: New IPSEC Action
        1: tunnel_vpnrtr1-vpnrtr2

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

ISAKMP アクションを追加する

保護 IPSec アクションが指定されたので、ISAKMP アクションの作成を指示するプロンプトが自動的に出されます。ほとんどの場合は、ISAKMP アクションが 1 つと ISAKMP アクションが 1 つで、セキュリティー・ポリシーのすべてで十分です。選択するアルゴリズムと方式は、戦略的でエンタープライズ全般にわたるパラメーターになる可能性が大です。例えば、最大暗号化レベル間での選択やプライバシーとパフォーマンスの間のバランスなど、企業のセキュリティー要件を基にして、決定することになります。どんなセキュリティー設計の場合についても言えることですが、元の構成の監査と監視を行って、それが正しく意図に沿うものかどうか確認する必要があります。ISAKMP アクションでは、フェーズ I に関する重要な管理情報を指定します。フェーズ I とフェーズ II の交渉の説明については、 323ページの『IKE』をごらんください。

表 87. ISAKMP アクションを追加する

```
ISAKMP Actions:
        0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
Enter a Name (1-29 characters) for this ISAKMP Action []? ike-1

List of ISAKMP Exchange Modes:            1
     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]?        2
ISAKMP Connection Lifetime, in seconds (120-65535) [30000]?
Do you want to negotiate the security association at
system initialization(Y-N)? [Yes]:           3
```

1. 交換モードは、フェーズ I の交渉時のセキュリティーのレベルに関係します。積極モードの方が、交換されるメッセージの数が少ないので高速ですが、起動側の ID が平文で送信されるため、安全性は低くなります。アクションがメイン・モードで行われるように選択します。
2. 「Connection Lifesize」と「Connection Lifetime」では、新規 SA の交渉時点を制御します。このキーのリフレッシュには何秒もかかる可能性があるので、数が小さいほど、リフレッシュの頻度が高くなります。セキュリティーに関する選択の多くについて言えることですが、パフォーマンスとセキュリティー要件の間で上手にバランスをとることが必要です。
3. トンネルをまたがって行われる初期トランザクションのパフォーマンスの向上を図るため、ここではシステム初期化時の SA 交渉を選択しました。

ISAKMP 提案を追加する

ISAKMP 提案では、フェーズ I の SA の暗号化と認証の属性を指定します。また、キーを生成する場合に使用する DH グループと、フェーズ I のセキュリティーの存続期間も指定します。

表 88. ISAKMP 提案を追加する (画面 2 の 1)

```
You must choose the proposals to be sent/checked against during phase 1
negotiations.  Proposals should be entered in order of priority.
List of ISAKMP Proposals:
        0: New Proposal

Enter the Number of the ISAKMP Proposal [0]? 0
Enter a Name (1-29 characters) for this ISAKMP Proposal []? ike-prop1

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

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

List of Hashing Algorithms:
     1)  MD5
     2)  SHA

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

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

Select the Cipher Algorithm (1-2) [1]? 1

...continued
```

表 89. ISAKMP 提案を追加する (画面 2 の 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]?        1


Here is the ISAKMP Proposal you specified...

Name = ike-prop1
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC
Is this correct? [Yes]:
List of ISAKMP Proposals:
        0: New Proposal
        1: ike-prop1

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

1. 事前共用キーの場合は、1 を選択します。認証用として証明を使用したい場合であれば、RSA-SIG を選択することになります。

保護トンネル・ポリシーに必要なオブジェクトのすべてが作成されると、ポリシーの要約が表示されます。定義済みポリシー (ike-pre-32-106) は、優先順位番号が 15 で、192.168.141.32 サブネットと 9.24.106.0 サブネットの間に保護トンネルをセットアップします。IPSec アクションでは、有効期間で指定されているように常時有効で

ある保護トンネルを指定します。トンネルに入ることを許可されるパケットは、2 つのサブネットを記述するプロファイルによって判別されます。認証方式と暗号化方式は、ISAKMP アクションと ISAKMP 提案の中で指定されます。

表 90. ISAKMP を確認する

```
Here is the ISAKMP Action you specified...


ISAKMP Name     = ike-1
        Mode                    =            Main
        Min Percent of SA Life  =              75
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =             Yes
        ISAKMP Proposals:
                ike-prop1
Is this correct? [Yes]: y
ISAKMP Actions:
        0: New ISAKMP Action
        1: ike-1

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

ポリシーを確認する

ISAKMP のアクションと提案を確認し終えると、DiffServ アクションの構成が必要になる場合があります。その場合は、確認のためにポリシーの要約が表示されます。

表 91. ポリシーを確認する

```
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     = ike-pre-32-106
        State:Priority =Enabled    : 15
        Profile        =32-106
        Valid Period   =always
        IPSEC Action   =tunnel_vpnrtr1-vpnrtr2
        ISAKMP Action  =ike-1
Is this correct? [Yes]:   Y
```

このポリシーでは、ルーターに入るパケットすべてを評価し、プロファイルに一致するパケットを暗号化のため IPSec に転送します。これ以上はポリシーが作成されていない場合は、プロファイルに一致しないパケットはすべて平文で、該当するインターフェースに向けてルーティングされます。

ただし、この事例の目的上、VPN を通過するのは、2 つのサブネット間のトラフィックだけである必要があります。この目的を達成するためには、指定されている 2 つのサブネットのどちらからでもないトラフィックをすべて除去するためのポリシーを作成することが必要になります。

公衆トラフィックを除去するためのポリシーを VPNRTR1 上に作成する

以下のステップは、IPSec トンネル・ポリシーに指定されているサブネットのどちらからでもない公衆トラフィックを除去するためのポリシーを作成する手順です。このポリシーを構成する手順は、ステップ数が少ないという点を除けば、トンネル・ポリシーの場合に似ています。

1. ポリシーを追加する。
2. プロファイルを追加する。
3. インターフェースを指定する。
4. 有効期間を追加する。
5. IP セキュリティー・アクションを追加する。
6. ポリシーを確認する。

ポリシーを追加する

表 92. 公衆トラフィックを除去するためのポリシーを追加する

```
VPNRTR1 Config>FEATURE Policy
IP Network Policy configuration
VPNRTR1 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]?          1
```

1. 上記のポリシーでは、優先順位番号 15 が割り当てられました。次回は、優先順位番号 5 が割り当てられることになります。したがって、着信パケットは、最初にトンネル・ポリシーのプロファイルと突き合わせて評価されます。そのプロファイルに一致しなければ、このプロファイルと突き合わせて評価されます。したがって、トンネル・プロファイルに一致しないパケットはすべて、このプロファイルに一致するので、除去されるという結果になります。

プロファイルを追加する

このプロファイルは、すべてのトラフィックに一致するように設計されます。

表 93. すべてのトラフィックに一致するためのポリシーを追加する

```
List of Profiles:
        0: New Profile
        1: 32->106

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

インターフェース・ペアを指定する

発信元とあて先の IP アドレスがまったく指定されなかったので、ポリシーの適用対象となるインターフェースを指定する必要があります。

表 94. 公衆トラフィックを阻止するためのインターフェースを定義する

```
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.
Limit this profile to specific interface(s)? [No]: yes
Interface Pair Groups:
        0: New Ifc Pair
Number of Ifc Pair Group [1]? 0
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]? 192.168.141.18
Interface Pair Groups:
        0: New Ifc Pair
        1) Group Name: inOutPublic
                  In:Out=255.255.255.255 : 192.168.141.18
```

表 95. 指定されたインターフェースを検証する

```
Number of Ifc Pair Group [1]? 0
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]? 192.168.141.18
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 : 192.168.141.18
                  In:Out= 192.168.141.18 : 255.255.255.255

Number of Ifc Pair Group [1]? 1


Here is the Profile you specified...


Profile Name    = allPublicTraffic
        sAddr:Mask=        0.0.0.0 : 0.0.0.0   sPort=    0 : 65535        1
        dAddr:Mask=        0.0.0.0 : 0.0.0.0   dPort=    0 : 65535        2
        proto     =              0 : 255
        TOS       =            x00 : x00              3
Remote Grp=All Users
        1.  In:Out=255.255.255.255 : 192.168.141.18
        2.  In:Out= 192.168.141.18 : 255.255.255.255
Is this correct? [Yes]:
```

1. すべてがゼロでは、どの発信元からのトラフィックもプロファイルに一致することを示します。
2. すべてがゼロでは、あて先がどこのトラフィックもプロファイルに一致することを示します。
3. デフォルトの TOS を x00 のままにしておくと、優先順位レベルがどのトラフィックもプロファイルに一致することを示します。

有効期間を追加する

インターフェースが指定されたら、プロファイルと有効期間を選択する必要があります。以前の構成済み「**always**」記述が使用できるので、新規有効期間を作成する必要はありません。

表 96. 有効期間 ALWAYS を再使用する

```
List of Profiles:
        0: New Profile
        1: 32->106
        2: allPublicTraffic

Enter number of the profile for this policy [1]? 2
List of Validity Periods:
        0: New Validity Period
        1: always

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

IPSec アクションを追加する

allPublicTraffic プロファイルに一致するトラフィックすべてを除去するためのセキュリティー・アクションを記述します。この優先順位の方がトンネル・ポリシーの場合よりも低く設定されているので、正しいトラフィックがトンネルに入り、それ以

外のトラフィックはすべて除去されることになります。言い換えれば、各着信パケットは、まず最初にトンネル・プロファイルと突き合わせてテストされ、最後に公衆プロファイルと突き合わせてテストされるということになります。

表 97. 公衆トラフィックを除去するための IPSec アクションを追加する

```
Should this policy enforce an IPSEC action? [No]: yes
IPSEC Actions:
        0: New IPSEC Action
        1: tun-32->106

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]: yes
IPSEC Actions:
        0: New IPSEC Action
        1: tun-32->106
        2: dropTraffic

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

ポリシーが正しいことを確認する

「**Yes**」と入力して、ポリシーを確認します。

表 98. トラフィックを除去するためのポリシーを確認する

```
Here is the Policy you specified...


Policy Name     = dropAllPublicTraffic
        State:Priority =Enabled    : 1
        Profile        =allPublicTraffic
        Valid Period   =always
        IPSEC Action   =dropTraffic
Is this correct? [Yes]:   Y
```

これで VPNRTR1 での構成は完了します。IBD、構成プログラム内に構成のコピーを作成するか、TFTP サーバーに送信します。

VPNRTR2 用として IPSec トンネルに関するポリシーを作成する

この例でのネットワーク図と IP アドレスについては、332ページの図65 をごらんください。ルーターを構成する手順は、次のようになります。

1. セキュリティーを使用可能にする。
2. 事前共用キーを作成する。
3. ポリシーを追加する。

4. プロファイルを追加する。
5. 有効期間を追加する。
6. IPSec アクションを追加する。
7. IPSec 提案を追加する。
8. ESP 変換を追加する。

VPNRTR2 のポリシーを作成する手順は、VPNRTR1 の場合と同じですが、次の点が異なっています。

- VPNRTR2 のトンネル・ポリシーのプロファイルは、VPNRTR1 で使用した sAddr:Mask と dAddr:Mask が逆になる。
- VPNRTR2 の除去ポリシーのプロファイルでは、指定されたインターフェースが逆になる。
- VPNRTR2 の IPSec アクションでは、トンネル開始/終了点が逆になる。
- VPNRTR2 の場合に定義されるユーザーは、VPNRTR1 のトンネル・エンドポイントである。

注: 事前共用キーは、両方のルーターで必ず同じものにします。ここための簡単な方法の 1 つに、キーの切り貼りがあります。また、入力されたキーが Telnet セッション画面の文字幅より長い場合は、確認画面が表示されたとき、キー全体は見えない可能性があります。

表99 には、VPNRTR2 の構成の完了後の、 Talk 6 **list all** コマンドの出力です。VPNRTR1 のポリシーの場合と異なる値については、それぞれの図の下に注釈を付けてあります。

表 99. VPNRTR2 の場合のポリシー・データベース・オブジェクトのすべてをリストする

```
VPNRTR2 Policy config>LIST ALL

Configured Policies....

Policy Name     = ike-pre-106->32              1
        State:Priority =Enabled    : 15
        Profile        =106->32                2
        Valid Period   =always
        IPSEC Action   =ike-1
        ISAKMP Action  =ike-1

Policy Name     = dropAllPublicTraffic
        State:Priority =Enabled    : 5
        Profile        =allPublicTraffic
        Valid Period   =always
        IPSEC Action   =dropTraffic

Configured Profiles....

Profile Name    = 106->32      3
        sAddr:Mask=     9.24.106.0 : 255.255.255.0   sPort=     0 : 65535
        dAddr:Mask= 192.168.141.32 : 255.255.255.240 dPort=    0 : 65535
        proto     =              0 : 255
        TOS       =            x00 : x00
```

1. ポリシーの名前は、参照のために過ぎません。意味のある名前を使用するようにしてください。
2. プロファイル用として意味のある名前を使用します。

3. プロファイル・アドレスは、トンネルの反対側のエンドポイントのルーターの場合と逆になります。

表 100. VPNRTR2 の場合のポリシー・データベース・オブジェクトをリストする (画面 4 の 1)

```
Remote Grp=All Users

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 : 192.168.141.17       1
        2.  In:Out= 192.168.141.17 : 255.255.255.255

Configured Validity Periods

Validity Name   = always
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day

Configured DiffServ Actions....
No DiffServ Actions configured
```

1. WAN ポートのアドレス

表 101. VPNRTR2 の場合のポリシー・データベース・オブジェクトをリストする (画面 4 の 2)

```
Configured IPSEC Actions....

IPSECAction Name = ike-1
        Tunnel Start:End         = 192.168.141.17 : 192.168.141.18           1
        Tunnel In Tunnel         =             No
        Min Percent of SA Life   =             75
        Refresh Threshold        =             85 %
        Autostart                =             No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
                esp-prop1

IPSECAction Name = dropTraffic
        Action   = Drop

Configured IPSEC Proposals....

Name  = esp-prop1
        Pfs   = N
        ESP Transforms:
                esp-trans1
```

1. このルーターの IPSec アクションの場合は、トンネルの開始点と終了点は、反対側のエンドポイントのルーターの場合の正確に逆になる必要があります。

表 102. VPNRTR2 の場合のポリシー・データベース・オブジェクトをリストする (画面 4 の 3)

```
Configured IPSEC Transforms....

Transform Name  = esp-trans1
        Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
        Auth =SHA   Encr =DES

Configured ISAKMP Actions....

ISAKMP Name     = ike-1
        Mode                    =            Main
        Min Percent of SA Life  =              75
        Conn LifeSize:LifeTime  =            5000 : 30000
        Autostart               =             Yes
        ISAKMP Proposals:
                ike-prop1
```

表 103. VPNRTR2 の場合のポリシー・データベース・オブジェクトをリストする (画面 4 の 4)

```
Configured ISAKMP Proposals....
Name = ike-prop1
        AuthMethod = Pre-Shared Key
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC

Configured Policy Users....
Name      = 192.168.141.18         1
Type      = IPV4 Addr
        Group     =
        Auth Mode =Pre-Shared Key
        Key(Ascii)=key
Configured Manual IPSEC Tunnels....

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

   ID         Name        Local IPv4 Addr  Rem IPv4 Addr    Mode    State
 ------  ---------------  ---------------  ---------------  -----  --------
VPNRTR2 Policy config>
```

1. VPNRTR2 の場合の構成済みユーザーは、VPNRTR1 の IP アドレスになります。

公衆トラフィックを除去するためのポリシーを VPNRTR2 上に作成する

以下のステップは、IPSec トンネル・ポリシーに指定されているサブネットのどちらからでもない公衆トラフィックを除去するためのポリシーを作成する手順です。

注: ステップごとの正確な説明については、346ページの『公衆トラフィックを除去するためのポリシーを VPNRTR1 上に作成する』をごらんください。唯一の違いは、「**インターフェースを指定する**」ステップで、インターフェース・アドレスが、VPNRTR2 の場合は WAN ポートの IP アドレスになります。

1. ポリシーを追加する。
2. プロファイルを追加する。
3. インターフェースを指定する。
4. 有効期間を追加する。

5. IP セキュリティー・アクションを追加する。
6. ポリシーを確認する。

ポリシーの監視/トラブルシューティング

ポリシー・データベースでは、ポリシーを受け継ぎ、IPSec に必要な規則を生成します。ポリシーでは、x.x.x.x から x.x.x.x に流れるトラフィックが、トンネル *tunnelname* を使用して保護されることを定義しました。過去には、x.x.x.x から x.x.x.x へのトラフィックが、トンネル *tunnelname* で保護されていたことを確認する場合は、パケット・フィルターも構成する必要がありました。ポリシー・フィーチャーが代わってこのフィルターを作成してくれます。生成されているポリシーを知りたい場合は、talk 5 からポリシー・フィーチャーに入り、 **list policy generated** と入力します。ユーザーが定義したポリシーすべてが、ルーターによって表示されます。該当する番号を選択すると、そのポリシーに関して生成された規則が、ルーターによって示されます。

表 104. 生成されたポリシーをリストする

```
VPNRTR2 *TALK 6
VPNRTR2 Config>FEATURE Policy
IP Network Policy configuration
VPNRTR2 Policy console>LIST POLICY GENERATED
1: (Enabled,Valid)      dropAllPublicTraffic
2: (Enabled,Valid)      ike-pki-106-32
Number of Policy to display [0]? 2
Rules generated for policy ike-pki-106-32:
Rule 1.  ike-pki-106-32.p1in
Rule 2.  ike-pki-106-32.p1out
Rule 3.  ike-pki-106-32.p2in
Rule 4.  ike-pki-106-32.traffic
Rule 5.  ike-pki-106-32.inBoundTunnel
```

これらの規則について知りたい場合は、コマンドが 2 つあり、一方のコマンドでは、要約が表示され、もう一方のコマンドでは、詳細が表示されます。「**List rule basic**」では、1 つの規則についての基本情報 (優先順位、どのようにして生成されたか、どのように使用されているか) が示されます。

表 105. List Rule Basic

```
VPNRTR2 Policy console>LIST RULE BASIC
1: (Enabled,Valid)      ike-pki-106-32.p2in
2: (Enabled,Valid)      ike-pki-106-32.p1out
3: (Enabled,Valid)      ike-pki-106-32.p1in
4: (Enabled,Valid)      ike-pki-106-32.traffic
5: (Enabled,Valid)      ike-pki-106-32.inBoundTunnel
11: (Enabled,Valid)     dropAllPublicTraffic
Number of Rule to display (0 for All) [0]? 1
Policy Name: ike-pki-106-32.p2in
Loaded from: Local
State:       Enabled and Valid
Priority:    94
Hits:        0
Profile:     106->32.p2in
Validity:    always
IPSEC:       ike-1
```

「**List rule complete**」では、該当の規則の詳細が表示されます。この規則は、192.168.141.18 から 192.168.141.17 へのトラフィックが、正しいトンネル定義を使用して保護されたことを確認する場合に使用されます。

表 106. List Rule Complete

```
VPNRTR2 Policy console>LIST RULE COMPLETE
1: (Enabled,Valid)      ike-pki-106-32.p2in
2: (Enabled,Valid)      ike-pki-106-32.p1out
3: (Enabled,Valid)      ike-pki-106-32.p1in
4: (Enabled,Valid)      ike-pki-106-32.traffic
5: (Enabled,Valid)      ike-pki-106-32.inBoundTunnel
11: (Enabled,Valid)     dropAllPublicTraffic
Number of Rule to display (0 for All) [0]? 1
Policy name:                            ike-pki-106-32.p2in
Policy Loaded from:                     Local Configuration
Policy state:                           Enabled and Valid
Policy Priority:                        94

Profile Name    = 106->32.p2in
        sAddr:End = 192.168.141.18 : 192.168.141.18  sPort=  500 : 500
        dAddr:End = 192.168.141.17 : 192.168.141.17  dPort=  500 : 500
        proto     =             17 : 17
        TOS       =            x00 : x00
Remote Grp=All Users

Validity Name   = always
        Duration  = Forever
        Months    = ALL
        Days      = ALL
        Hours     = All Day

IPSECAction Name = ike-1
        Tunnel Start:End         = 192.168.141.17 : 192.168.141.18
        Tunnel In Tunnel         =              No
        Min Percent of SA Life   =              75
        Refresh Threshold        =              85 %
        Autostart                =              No
        DF Bit                   =           COPY
        Replay Prevention        =       Disabled
        IPSEC Proposals:
        ----------------
        1:Name = esp-prop1
                Pfs   = N
                ESP Transforms:
                --------------
                1:Name = esp-trans1
                        Mode     = Tunnel
                        LifeSize = 50000
                        LifeTime = 3600
                        Authent  = SHA          Encr =DES
VPNRTR2 Policy console>
```

その他に、次のようなコマンドが通常使用されます。

- >TALK 5
- >+FEATURE IPSec
- IPSec>IKE
- VPNRTR2 IKE>LIST TUNNEL
- VPNRTR2 IKE>LIST ALL
- VPNRTR2 IKE>STATS

ディジタル証明の使用によるルーター間 VPN

ディジタル証明を使用して認証を実行する場合は、証明権限 (CA) が必要になります。これは、一般的には、PC か UNIX プラットフォームで稼働するソフトウェア・パッケージです。今回のリリースでは、CA は 1 つしかサポートされないので、ネットワーク全体に関する証明のすべてが、同じインスタンスのソフトウェア・パッケージによって発行される必要があります。CA ソフトウェアを販売している企業は、例えば、Entrust Technologies, Inc. や VeriSign など、数多くあります。

証明を入手する場合は、ルーターにプライベート・キーとパブリック・キーが必要です。これらのキーは、talk 5 から証明要求 (認証要求) が発行されると生成されます。キーが生成されると、ルーターでは証明要求パケットを形成します。これには、ルーターのパブリック・キーと識別子が入ります。次に、この要求がネットワーク内のどこかにある TFTP サーバーに送信されます。証明要求は、次に CA に渡され、 CA で読み取られ処理されます。CA が証明を発行することになります。証明には、ルーターのパブリック・キー、ルーターによって送信された識別子、有効期間が入っています。証明には、CA のプライベート・キーによるシグニチャーがあります。

次に、ルーターでは、TFTP 経由と LDAP 経由のどちらかで、この証明を検索する必要があります。ルーターが証明をダウンロードするときは、証明内でパブリック・キーとパートナーになっているプライベート・キーは、まだルーターの実行メモリー内にあることが必要です。ダウンロードされた証明は、それに一致するプライベート・キーがルーターになくなっていては、役に立ちません。つまり、証明要求の発行時点から証明のダウンロード時点まで、ルーターの再始動や再ロード、キャッシュのクリア、新規証明要求の発行を行うことはできないことを意味します。これらの操作のどれが行われても、プライベート・キーは破棄されます。証明が検索されたら、キーと証明をただちに保管する必要があります。

ルーターには、CA の証明のコピーも必要です。ルーターが同位の証明を検証するときは、その同位の証明に CA のプライベート・キーのシグニチャーがあったことを確認する必要があります。これができるためには、CA のパブリック・キーが含まれている CA の証明がルーターにあることが必要です。IKE を実行する各ルーターは、それぞれ TFTP と LDAP のどちらかを使用して、CA の証明をダウンロードする必要があります。この証明も保管する必要があります。

この例では、ディジタル・シグニチャーを使用して認証を提供する、自動キー交渉による IP セキュリティーのために、IBM ルーターを構成する方法について説明します。トンネルはルーター間です。このトンネルでは、特定のホストからのトラフィックの認証と暗号化を行い、それ以外のトラフィックはすべて除外します。データにトンネルを通過させることができるのは、トンネルのどちらの端のどのホストであるかは、***プロファイル*** に正確に記述されます。***ポリシー*** で許可できるのは、どちらかの端の 1 つのホストか、どちらかの端の 1 つまたは複数のサブネットか、その両方の任意の組み合わせです。ゲートウェイ間トンネリングには、LAN 上では認証も暗号化も行われないという制限があります。したがって、このソリューションでは、LAN 上でのセキュリティーは得られません。

物理ネットワーク接続については、331ページの図64 をごらんください。論理ネットワーク図と IP アドレッシングについては、332ページの図65 をごらんください。説

明と画面取りについては、パラメーターが 331ページの『事前共用キーの使用による IPSec ルーター間 VPN』の例とは異なっている場合にだけ示します。

注: この場合は、ユーザーを定義する必要はありません。認証はディジタル証明によって提供されます。

VPNRTR1 用として IPSec トンネルに関するポリシーを作成する

この例の手順は、332ページの『VPNRTR1 用として IPSec トンネルに関するポリシーを作成する』で説明されている手順に非常によく似ています。この構成を作成する場合は、「**IPSecurity を使用可能にする**」というステップから開始し、「**ISAKMP アクションを追加する**」というステップで終了します。次のステップ「**ISAKMP 提案を追加する**」は異なります。

ステップに注記がある場合を除いて、以下のステップは、332ページの『VPNRTR1 用として IPSec トンネルに関するポリシーを作成する』に示されている事前共用キーの例の場合と同じです。この方式を使用するときは、 **Add User** コマンドを使用して、ユーザーとキーを作成することがないようにします。プロファイルの作成時には、前記の例の場合と同様に構成できますが、必ず注記を考慮する必要があります。

1. セキュリティーを使用可能にする。
2. ポリシーを追加する。
3. プロファイルを追加する。

   注: プロファイルの追加時には、プロンプトが出て、ISAKMP 用としての ID の構成を指示されます。相手側同位がユーザーを識別できるようにするために、これは行う必要があります。ここで選択する方式は、**subject-alt-name** タイプと、359ページの表109 に示されている **CERT-REQ** コマンドで入力された情報に一致する必要があります。また、情報は 361ページの図70 に示されているように、証明権限に送信される内容にも一致する必要があります。
4. 有効期間を追加する。
5. IPSec アクションを追加する。
6. IPSec 提案を追加する。
7. ESP 変換を追加する。
8. ISAKMP アクションを追加する。

以下のステップは、事前共用キーの例の場合とは異なることになります。新規 ISAKMP 提案を追加することから始めて、認証方式 RSA SIG を指定します。RSA SIG は、ディジタル証明に関する用語です。次に、ルーター証明と CA 証明を要求しロードします。

1. ISAKMP 提案を追加する。
2. 証明をロードするために TFTP サーバーを構成する。
3. ルーター証明を要求する。
4. ルーター証明をロードする。
5. ルーター証明を保管する。
6. CA 証明を取得する。
7. CA 証明をロードする。

8. CA 証明を保管する。

ISAKMP 提案を追加する

ISAKMP 提案では、フェーズ I の SA の暗号化と認証の属性を指定します。また、キーを生成する場合に使用するための Diffie-Hellman グループと、フェーズ I のセキュリティーの存続期間も指定します。

表 107. ディジタル証明に関する ISAKMP 提案を追加する

```
VPNRTR1 Policy config>ADD ISAKMP-PROPOSAL
Enter a Name (1-29 characters) for this ISAKMP Proposal []? cert1      1

List of Authentication Methods:         2
     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]?

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

Select the Cipher Algorithm (1-2) [1]?
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 = cert1
        AuthMethod = RSA SIG
        LifeSize   = 1000
        LifeTime   = 15000
        DHGroupID  = 1
        Hash Algo  = MD5
        Encr Algo  = DES CBC
Is this correct? [Yes]:
```

1. ISAKMP 提案に名前が付けられます。
2. ディジタル証明を使用するように指定します。

証明をロードするために TFTP サーバーを構成する

Load Certificate コマンドを使用するためには、 TFTP サーバーが事前定義されている必要があります。**Add Server** コマンドを使用して、名前と IP アドレスを割り当てます。証明ロード操作を試みるにあたっては、その前にルーターとサーバーの間の接続をチェックしておく方が賢明です。

表 108. 証明をロードするために TFTP サーバー記述を追加する

```
VPNRTR1 Config>FEATURE IPSec
IP Security feature user configuration
VPNRTR1 IPsec config>PKI
VPNRTR1 PKI config>ADD SERVER
Name ? (max 65 chars) []? TFTPServer
Enter server IP Address []? 9.24.106.146
Transport type (Choices: TFTP/LDAP)  [TFTP]?
VPNRTR1 PKI config>EXIT
```

ルーター証明を要求する

証明を要求するにあたっては、その前に、証明をロードする先のルーターのクロックが、CA システムのクロックに近いが、それよりも遅れてはいないことを確認しておくことが大切です。証明権限の説明については、 313ページの『第19章 VPN (仮想私設ネットワーク)』をごらんください。CA が証明を発行すると、開始日時と終了日時として表された有効期間によるタイム・スタンプが施されます。ルーターの時刻は、証明の開始時刻よりも後で、その終了時刻よりも前である必要があります。証明がユーザーの制御下にないホストによって発行されている場合は、証明のタイム・スタンプを確認する方法は、ルーターへのロードの試行を要求する以外にはありません。ルーターの時刻が有効期間外である場合は、次のようなメッセージが ELS ログで表示されます。

```
PKI.009 Validity check: failed Current date 1999/3/5, Time 9:38.21.
Cert valid date: 1999/3/5 10:14:38 -- 1999/6/5 10:14:38
```

このメッセージは、ルーター時刻が有効証明時刻前であることを通知するものです。このメッセージが表示された場合は、時刻を表示するための T 6 コマンド **time list** と、時刻を調整するためのコマンド **time set** を使用して、ルーター時刻をチェックします。

CA に送信される証明要求を作成する場合は、 **CERT-REQ** コマンドを使用します。

表 109. 証明を要求する

```
VPNRTR1  *TALK 5
VPNRTR1 +FEATURE IPSec
VPNRTR1 IPSP>PKI
VPNRTR1 PKI Console>CERT-REQ
Enter the following part for the subject name
   Country Name(Max 16 characters) []? us
   Organization Name(Max 32 characters) []? cert
   Organization Unit Name(Max 32 characters) []?
   Common Name(Max 32 characters) []? VPNRTR1        1
Key modulus size (512|768|1024)
 [512]?
Certificate subject-alt-name type:     2
   1--IPv4 Address
   2--User FQDN
   3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 192.168.141.18       3
Generating a key pair. This may take some time. Please wait ...
Cert Request format: 1--DER;2--PEM      4
 [1]? 2
PKCS10 message successfully generated
Enter tftp server IP Address []? 9.24.106.146
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]? test.req
Memory transfer starting.
.Memory transfer completed - successfully.
Certificate request TFTP to remote host sucessfully.     5
Generated private key stored into cache
Please download router certificate and save
both router certificate and its private key ASAP.
VPNRTR1 PKI Console>
```

1. この名前は、実際の構成済みルーター・システム名に一致する必要があります。
2. タイプは、プロファイル内で指定された ID タイプに一致する必要があります。
3. これは、ローカル・トンネル・エンドポイント・アドレスである必要があります。シリアル・インターフェースの IP アドレスは、インターネット上に直接あります。
4. 証明要求形式は、CA が証明を作成する場合に使用する形式に一致する必要があります。DER はディジタル形式であり、PEM は ASCII 形式です。
5. これで、証明要求が TFTP サーバー上に test.req としてできています。

CA から証明を取得する

証明要求は CA サーバーに送信される必要があり、そこで要求が検証され、証明が発行されます。証明には、ルーターのパブリック・キーと、ユーザーが入力した情報が入ります。CA がプライベート・キーによるシグニチャーを証明に施し、これでトラステッド・ディジタル情報になります。

360ページの図69 に示されているような、ワード・パッド内の *test.req* 文書をオープンします。

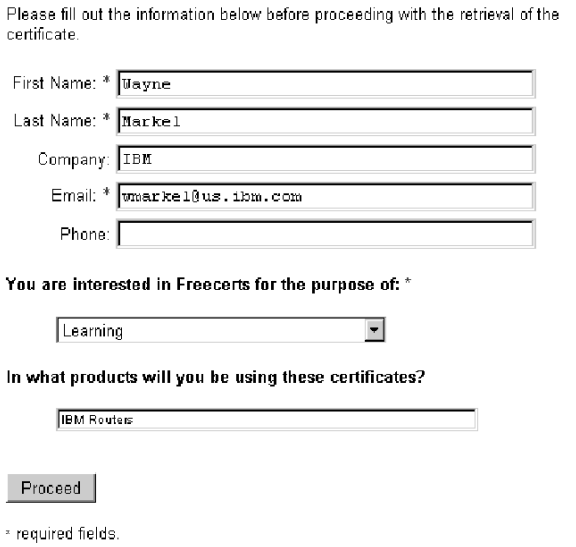


図 69. ルーターによって作成された証明要求

この例の場合は、Entrust Technologies が使用されましたが、どんな証明権限を使用しても構いません。ただし、証明を入手する手順は、ここに示すステップとは異なる場合もあります。

なお、切り貼りを行うときは、ヘッダーとフッターとその間の文字を切り貼りするだけにします。ただし、ヘッダーは先頭がダッシュで始まり、フッターは末尾がダッシュで終わる必要があります。

企業の Web サイトで、「**Request a VPN Certificate**」を選択します。特記事項書式に記入し、「**PROCEED**」をクリックします。その次の書式で、359ページの表109 に示されているような入力域までスクロールダウンし、共通名 (この例では、VPNRTR1) を記入します。「**Encode certificate in PKCS7 certificates only message**」というラベルが付いているボックスのチェック・マークを消します。359ページの表109 の参照 2 に一致する必要がある代替名を入力します (この例では、192.168.141.18 を入力しました)。切り貼り域の事前入力テキストを削除します。ワード・パッドを使用して、*test.req* ファイルをオープンし、Web ページに設けられているウィンドウ内に証明要求を切り貼りします。証明の切り貼りに改行は伴いません。

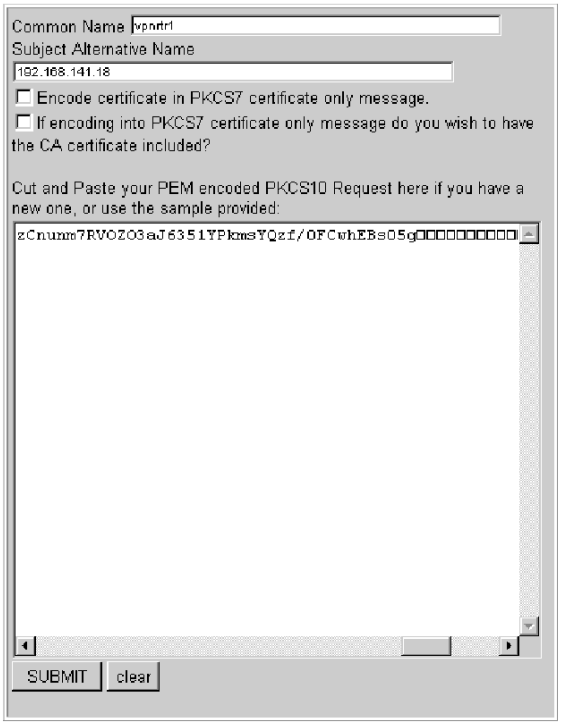


図 70. 証明要求書式に記入する

証明は、図71 に示されているように、Web ブラウザー内に戻されます。

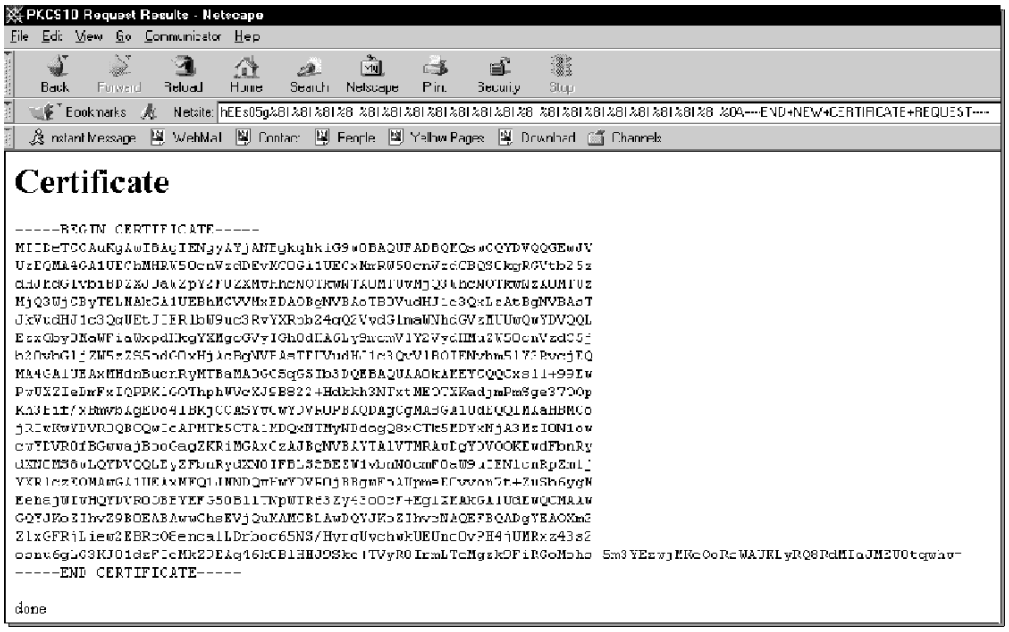


図 71. ルーター証明がブラウザーに戻される

証明をワード・パッド内の新規テキスト文書内に切り貼りします。最初の行、最終行の前の行、最終行の行末のスペースを削除します。証明を TFTP サーバーのアップロード・ディレクトリーに保管します。この例の場合は、証明ファイルには *cert.txt* という名前が付けられています。

ルーター証明をロードする

ここで、証明を LDAP か TFTP を介して検索する必要があります。次の事例では、TFTP を使用して証明を検索しています。表110 に示されているように、ルーターの証明を検索する場合は、**Load Certificate** コマンドを使用します。検索の対象がルーターの証明なので、証明のタイプにはデフォルト・オプションを選択します。そうすると、証明についてディジタル形式 (オプション 1) か ASCII 形式 (オプション 2) かを尋ねられます。オプション 2 を選択します。次は、サーバー名を尋ねられます。これは、talk 6 から追加した TFTP サーバーの名前です。最後に、サーバー上のファイルの名前を尋ねられます。次は、ルーターが証明を検索し、その実行メモリーに保管します。

表 110. ルーター証明をロードする

```
VPNRTR1 PKI Console>LOAD CERTIFICATE
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]? 2
Server info name []? TFTPServer
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? cert.txt

Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - succesfully.
Router Certificate  loaded into run-time cache
VPNRTR1 PKI Console>
```

ルーター証明を保管する

証明と対応するキーを即時に保管します。証明の保管が正常に行われず、しかもルーターが再始動した場合は、証明プロセスを繰り返す必要があります。保管しようとしている証明がどれなのか、それをどんな名前で呼びたいのか、ルーターの始動時に、この証明がルーターのメモリーにロードされるようにしたいのかについて尋ねられます。

表 111. ルーター証明を保管する

```
VPNRTR1 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 []? r1cert.txt
Load as default router certificate at initialization? [No]: y
Both Router Certificate and private key saved into SRAM successfully
VPNRTR1 PKI Console>
```

CA 証明を取得する

証明要求の発行の直前に生成されたプライベート・キーとパブリック・キーが、これでルーターに備えられました。ルーターの証明を検索したばかりです。そこで、IKE ピアの証明の有効性を検証できるようにするために、今度は CA の証明が必要です。CA がピアの証明にシグニチャーを施したかどうかをチェックすることが、有効性の確認の一部になります。したがって、CA の証明が必要です。別の CA によって発行された証明をチェックするメカニズムは備えられていないため、ピアの証明には同じ CA のシグニチャーが必要です。

次に、「**Retrieve PEM Encoded Certificate**」が、 Entrust Web サイトで選択されました。図72 に示されているように、CA 証明がブラウザーに戻されました。この特定のテストでは、ヘッダーもフッターも CA 証明に付けて送信されませんでした。

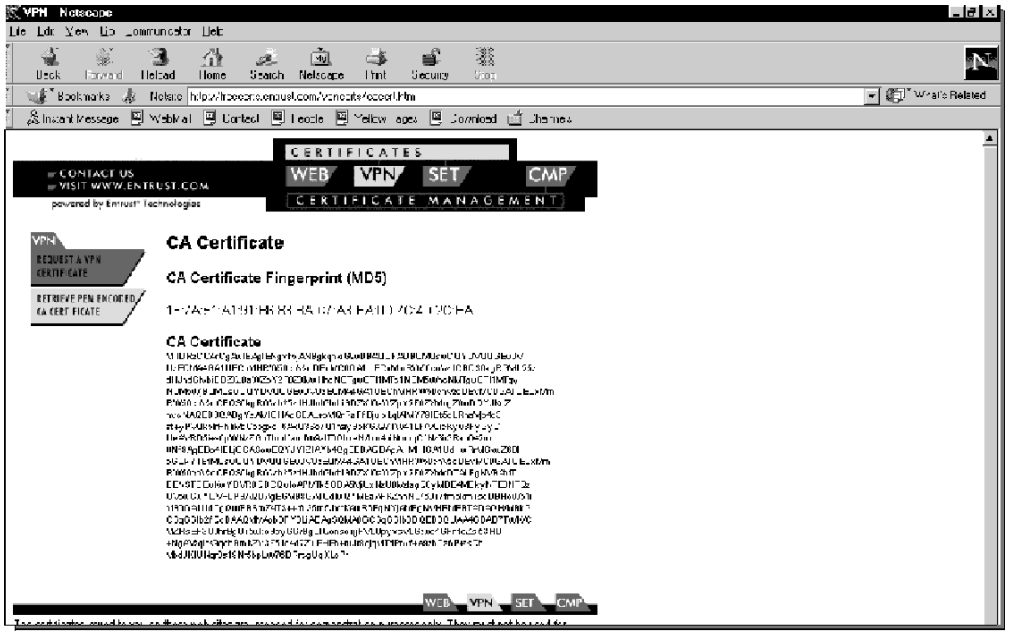


図 72. CA 証明が Web ブラウザーに戻される

この例では、″CA Certificate″ の後に続くテキストがワード・パッドのテキスト文書に切り貼りされました。ヘッダーもフッターも CA 証明に付けて送信されませんでした(これは、CA 証明の取得方法によって異なる可能性があります)。この例のルーターが証明を受け入れるためには、すでに受信されたルーター証明からのヘッダーとフッターが文章に切り貼りされる必要があったので、CA 証明のテキストは、 364ページの図73 に示されているように、そのヘッダーとフッターの間に切り貼りされました。

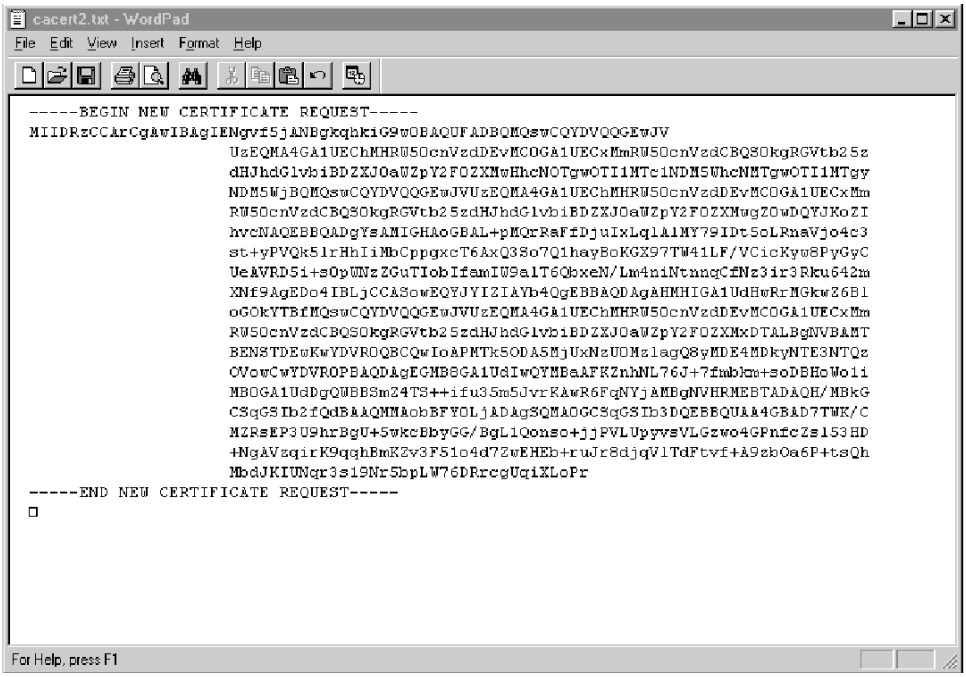


図 73. CA 証明にヘッダーとフッターを追加する

証明を文書として TFTP サーバーのアップロード・ディレクトリーに保管します。この例の場合は、ファイルには *cert.txt* という名前が付けられました。

CA 証明をロードする

CA の証明は、TFTP を介して、**Load Certificate** コマンドを使用し、証明のタイプとしてオプション 1 を選択してロードすることもできます。

表 112. ルート証明をキャッシュにロードする

```
VPNRTR1 PKI Console>LOAD CERTIFICATE
Enter the type of the certificate:
Choices:  1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]? 1
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]? 2
Server info name []? TFTPServer
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? cacert.txt

Attempting to load certificate file. Please wait ...
Memory transfer starting.
.Memory transfer completed - successfully.
Root CA Certificate  loaded into run-time cache
VPNRTR1 PKI Console>
```

CA 証明を保管する

表 113. ルート証明をルーター構成に保管します。

```
VPNRTR1 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]? 1
SRAM Name to store Root Certificate? []? cacert
Load as default root certificate at initialization? [No]: y
Root Certificate saved into SRAM successfully.
VPNRTR1 PKI Console>
```

CA 証明を保管してしまえば、VPNRTR1 トンネル・ポリシーの構成は完了です。

公衆トラフィックを除去するためのポリシーを VPNRTR1 上に作成する

このポリシーを構成する手順のステップは、346ページの『公衆トラフィックを除去するためのポリシーを VPNRTR1 上に作成する』に示されている例でのステップとまったく同じです。

1. ポリシーを追加する。
2. プロファイルを追加する。
3. インターフェースを指定する。
4. 有効期間を追加する。
5. IP セキュリティー・アクションを追加する。
6. ポリシーを確認する。

これで VPNRTR1 での構成は完了です。時間をかけてこれを再度行いたくはないでしょうから、構成のコピーを保管しておきます。

VPNRTR2 用として IPSec トンネルに関するポリシーを作成する

IP セキュリティー・トンネルを作成する場合は、次の手順に従います。

1. セキュリティーを使用可能にする。
2. ポリシーを追加する。
3. プロファイルを追加する。
4. 有効期間を追加する。
5. IPSec アクションを追加する。
6. IPSec 提案を追加する。
7. ESP 変換を追加する。
8. ISAKMP アクションを追加する。
9. ISAKMP 提案を追加する。
10. 証明をロードするために TFTP サーバーを構成する。
11. ルーター証明を要求する。
12. ルーター証明をロードする。
13. ルーター証明を保管する。
14. CA 証明を取得する。

15. CA 証明をロードする。
16. CA 証明を保管する。

上記の手順は、356ページの『VPNRTR1 用として IPSec トンネルに関するポリシーを作成する』に示されている場合と同じステップですが、次のような違いがあります。

- VPNRTR2 のトンネル・ポリシーのプロファイルは、VPNRTR1 で使用した sAddr:Mask と dAddr:Mask が逆になる。
- VPNRTR2 の IPSec アクションでは、トンネル開始/終了点が逆になる。

公衆トラフィックを除去するためのポリシーを VPNRTR2 上に作成する

このポリシーを作成するための手順は、352ページの『公衆トラフィックを除去するためのポリシーを VPNRTR2 上に作成する』 の場合と同じステップです。

Talk 5 からの監視/トラブルシューティング

この例での監視の操作と統計は、事前共用キーの例の場合と同じです。353ページの『ポリシーの監視/トラブルシューティング』をごらんください。

IBM ルーターを終端とする自発的 PPTP トンネル

PPTP に関する追加情報については、328ページの『ポイント・ポイント・トンネリング・プロトコル』をごらんください。

Microsoft Windows 装置では PPTP しかサポートしないので、それとのインターオペラビリティーを確保するために、IBM ルーターでは PPTP をサポートします。Microsoft の発表によれば、同社では NT 5.0 で L2TP の実装を計画しているようです。

367ページの図74 は、PPTP 自発的トンネリングを使用するリモート・アクセス VPN の一例です。IBM ルーターが PPTP トンネルのエンドポイントとして構成されることになります。クライアントである Windows/98、Windows/95、または Windows NT ダイヤルアップ・ネットワーキング (DUN) クライアントが、 ISP ルーターにダイヤルインします。クライアントが PPP 接続を確立し、 9.24.104.0 サブネット上で IP アドレスを与えられます。この時点では、クライアントは、本社インターネット・ルーターの WAN インターフェースも含めて、インターネット IP クラウド内のどこにでも IP 接続できます。そこで、クライアントでは、192.168.141.18 (本社インターネット・ルーターの IP アドレス) へのトンネルを確立します。PPTP トンネルのユーザー ID とパスワードは *sg245281* であり、IP アドレスは 192.168.141.38 です。これらは、本社ルーターによって割り当てられます。トンネルが確立されると、本社 LAN 上のリモート・アクセス・サーバーに直接ダイヤルインした場合と同じ接続になります。

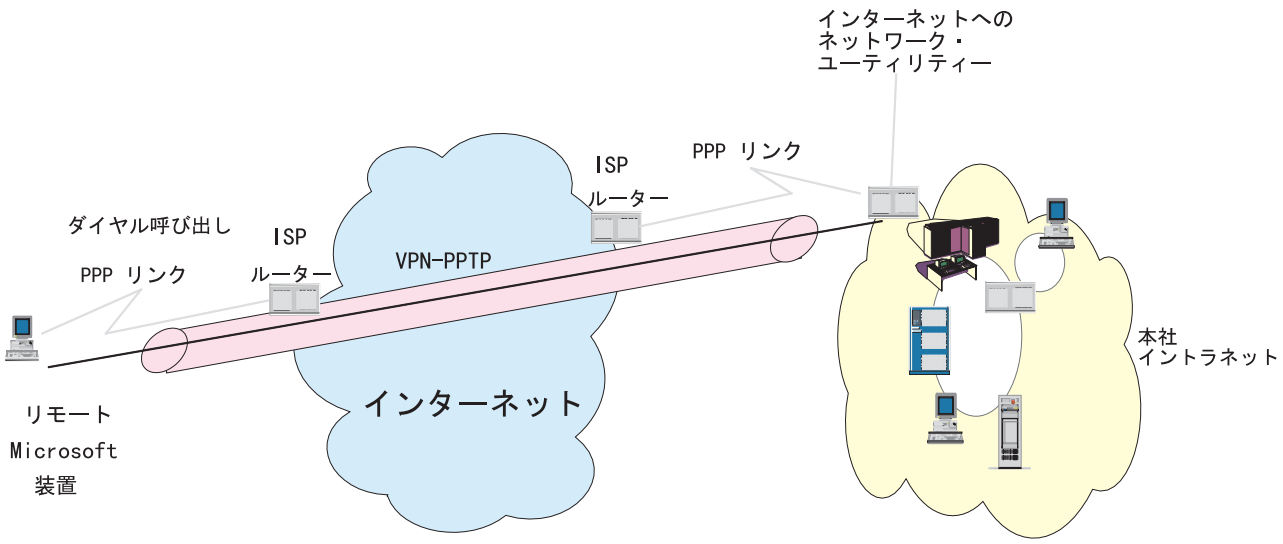


図 74. ワークステーションとゲートウェイ間の PPTP トンネル

ネットワーク・ユーティリティーの構成

以下の手順を完了する前に、ネットワーク。ユーティリティーに適正なインターフェースを必ず構成しておきます。また、PPP インターフェースがインターネットへの静的ルートと動的ルートのどちらかを確保できるように、IP も構成しておきます。イントラネット・インターフェースは、インターネット上に公示しないようにします。この例で使用されたネットワークの IP アドレッシングについては、368ページの図75 をごらんください。

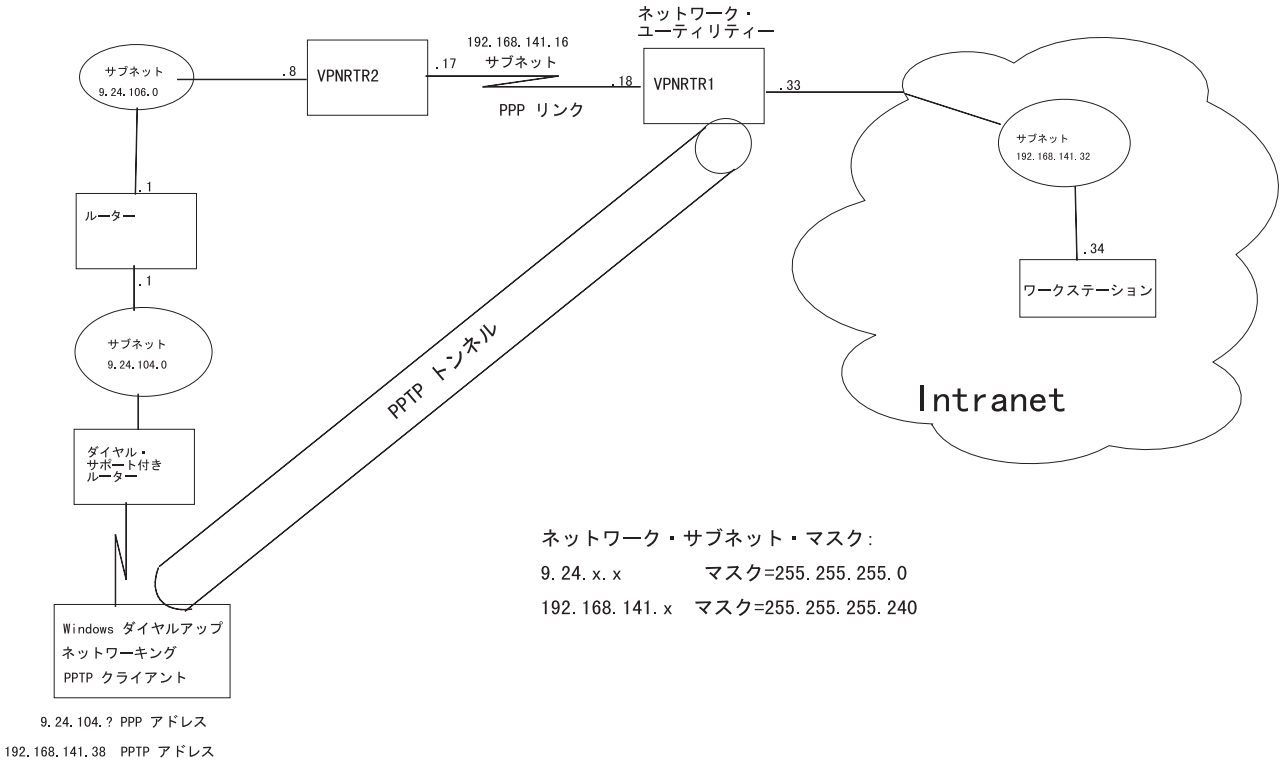


図 75. IP アドレッシング方式

367ページの図74 に図示されているような本社インターネット・ルーターを構成する場合は、次の手順に従います。

- PPTP を使用可能にする。
- L2 ネットを追加する。
- mschap と mppe を使用可能にする。
- PPP USER を追加する。
- ARP サブネット・ルーティングを使用可能にする。
- ダイヤルアップ・ネットワーキング (DUN) クライアントを構成する。

PPTP を使用可能にする

表 114. PPTP を使用可能にする

```
VPNRTR1  *TALK 6
VPNRTR2 Config>FEATURE Layer-2-Tunneling
VPNRTR2 Layer-2-Tunneling Config>ENABLE PPTP

 Restart system for changes to take effect.
```

レイヤー 2 ネットを追加する

最大数の同時接続をサポートする場合に必要な数のレイヤー 2 ネットを追加します。この例では、3 つのネットが追加されます。IPX や透過ブリッジングを使用可能にする必要はありません。

表 115. レイヤー 2 ネットを追加する

```
VPNRTR1  *TALK 6
VPNRTR2 Config>FEATURE Layer-2-Tunneling
VPNRTR2 Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 3       1
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 6
Defaulting Data-link protocol to PPP
Adding device as interface 7
Defaulting Data-link protocol to PPP
Adding device as interface 8
Defaulting Data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.
VPNRTR2 Layer-2-Tunneling Config>
```

1. 同時に接続される PPTP クライアントの予定最大数に等しいネットの数を追加します。

mschap と mppe を使用可能にする

Microsoft Windows ダイヤルアップ・ネットワーキング (DUN) PPTP クライアントでは、MPPE を使用して暗号化を実行します。このプロトコルは、L2Net 上で使用可能にする必要があります。任意のだれかからのインバウンドとして構成された L2Net (デフォルト) では、レイヤー・フィーチャー内のテンプレートから、 PPP デフォルトを引き継ぎます。**encapsulator** コマンドによってプロンプトが表示されるので、そこからすべての PPP デフォルトが調整できます。

MPPE を使用する場合は、MS-CHAP を使用可能にする必要があります。MPPE を使用可能にすると、MPPE の動作が必須モードか任意選択モードかを尋ねられます。動作が必須モードの場合は、MPPE を交渉する必要があります。必須モードでは、送信側が前に送信側自体とルーターの間に MPPE を確立した場合でも、新規接続が要求されると、ルーターはその度に強制的に MPPE を再交渉させられます。MPPE の動作が任意選択モードの場合は、MPPE の交渉を強制されることはありません。任意選択モードでは、初期交渉後、ルーターがルーター自体と送信側の間で MPPE を保持する結果になり、新規接続ごとに MPPE を再交渉することはありません。次に、キーが stateful か stateless かを尋ねられます。 キーが stateless の場合は、パケットが送信される度に、キーが変更されるのに対して、stateful では、 255 パケットが送信されて初めてキーが生成されます。stateless は、非可逆ネットワークの場合にお勧めであり、PPTP 接続の場合に使用する必要があります。 MPPE ヘッダーの一部に、キーがリフレッシュされたかどうか示す部分があるので、クライアントが使用しているのが stateless モードか stateful モードかが、ルーターに分かります。

Microsoft には、独自の圧縮アルゴリズム MPPC もあります。MPPE は、 MPPC オプションとして交渉されます。圧縮を希望し、MPPE を使用している場合は、 MPPC を使用する必要があります。この場合は、通常は PPP リンクの場合に使用可能な Stac-LZS アルゴリズムは使用できません。MPPC を使用しないことにした場合は、ルーター・コードによって、MPPE を使用できるようにする機能の交渉が部分的にできます。MPPE と MPPC を使用することにした場合は、これらのプロトコルでは同じ PPP ヘッダーが共用されるので、 1 回のパスでデコードされます。

表 116. MSCHAP と MPPE を使用可能にする

```
VPNRTR1 Layer-2-Tunneling Config>ENCAPSULATOR
Point-to-Point user configuration
VPNRTR1 PPP-L2T Config>ENABLE MSCHAP
Rechallenge Interval in seconds (0=NONE)  [0]?
Enabling MSCHAP
VPNRTR1 PPP-L2T Config>ENABLE MPPE
mandatory or optional [optional]?
stateful or stateless [stateful]? stateless      1
Enabling encryption

** Note ** : To view the MPPE configuration, please enter a 'list ccp'
            command since MPPE is negotiated within the CCP protocol.
VPNRTR1 PPP-L2T Config>
```

1. キーが stateless の場合は、パケットが送信される度に、キーが変更されるのに対して、stateful では、255 パケットが送信されて初めてキーが生成されます。stateless は、非可逆ネットワークの場合にお勧めであり、 PPTP 接続の場合に使用する必要があります。

PPP ユーザーを追加する

この例では、ユーザーが 2 つ構成されるので、少なくとも 2 つの同時接続がテストされます。各ユーザーには、それぞれ静的 IP アドレスが割り当てられています。 IP アドレスを PPP クライアントに割り当てる方法としては、これは最も簡単ですが、柔軟性も拡張容易性も最も低くなります。IP アドレスを割り当てる方式としては、その他に IP アドレス・プールの使用や、DHCP サービスの使用があります。

最初に *sg245281* という名前のユーザーが追加されます。パスワード記入項目は画面には表示されません。

表 117. PPP ユーザーを追加する

```
VPNRTR2 Config>ADD PPP-USER
Enter name:  []? sg245281
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]? 192.168.141.38       1
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]

     PPP user name: sg245281
   User IP address: 192.168.141.38
     Netroute Mask: 255.255.255.255
          Hostname:       Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
    Account Expiry:    Password Expiry:
Is information correct? (Yes, No, Quit): [Yes]

User 'sg245281' has been added
VPNRTR2 Config>
```

1. PPTP クライアントの手動割り当て IP アドレス。

同じパラメーターを使用して、*salesman* という名前の別の PPP ユーザーを追加してから、すべての PPP ユーザーをリストします。

表 118. PPP ユーザーをリストする

```
VPNRTR2 Config>LIST PPP-USERS addr
List  (Name, Verb, User, Addr, VCon, Call, Time, Dial, Encr): [User] addr

PPP user name      User IP address     Netroute Mask       Hostname
-----------------  ------------------  ------------------  ---------------
salesman           192.168.141.39      255.255.255.255     <undefined>
sg245281           192.168.141.38      255.255.255.255           <undefined>
2 PPP records displayed.
```

ARP サブネット・ルーティングを使用可能にする

ARP サブネット・ルーティングは、プロキシー ARP とも呼ばれています。本社ネットワーク上のホストが、同じサブネット上に IP アドレスをもつ PPTP ホストにデータグラムを送信する場合は、送信側では、データグラムをデフォルト・ルートに送信しないで、それ自体の ARP キャッシュ内に項目を予期します。ARP キャッシュ内に項目がない場合は、送信側では、あて先 IP にあてた ARP 同報通信を送信します。あて先 IP アドレス (リモート PPTP クライアント) は物理ネットワーク上にはないので、応答することはありません。ARP サブネット・ルーティングの使用によって、

ローカル・ルーターがリモート・クライアントに代わって、ARP 同報通信に応答できます。そうすると、データグラムがルーターによってコピーされ、インターネットをまたがって転送されます。

表 119. ARP サブネット・ルーティングを使用可能にする

```
VPNRTR2 Config>PROTOCOL
Protocol name or number [IP]?
Internet protocol user configuration
VPNRTR1 IP config>ENABLE ARP-SUBNET-ROUTING
VPNRTR1 IP config>
```

DUN クライアントを構成する

Microsoft プラットフォームを使用して PPTP 接続を確立する場合は、2 つの DUN セッションが必要です。1 つはインターネット -- ISP のルーターへのセッションで、もう 1 つはネットワーク・ユーティリティーへのセッションです。最初に、インターネット接続を確立する PPP ダイヤル呼び出し接続を立ち上げ、次に、PPTP 接続を立ち上げて、ネットワーク・ユーティリティーへのトンネルを作成します。IBM ネットワーク・ユーティリティーの PPP インターフェースは、インターネット上でアクセス可能である必要があります。

注: DUN 1.2 以降がインストールされている必要があります。バージョン 1.2 以降かどうか確認する場合は、DUN フォルダー内の「**Make a New Connection**」ウィンドウをオープンします。「**Select a Device**」ドロップダウン・ウィンドウに、Microsoft VPN アダプターが表示されているかチェックします。

Microsoft PPTP クライアントを構成するには、次の手順に従います。

- DUN クライアントを追加する。モデムを使用して ISP ルーターにダイヤルインするように構成します。
- 2 番目の DUN クライアントを追加する。VPN アダプターを使用して本社ルーターの WAN インターフェースの IP アドレスに接続するように構成します。「**Make a New Connection**」をクリックすると、アダプターについての詳細を尋ねられます。Microsoft VPN アダプターを使用する必要があります。次の画面で、ホスト名か IP アドレスを要求されます。このボックスには、IP クラウドを経由して到達可能な IBM ルーターの IP アドレスを入力します。その DUN 接続を立ち上げると、367ページの『ネットワーク・ユーティリティーの構成』に示されているようにルーター構成で、 **add ppp-user** コマンドで構成された詳細に一致する必要がある、ユーザー ID とパスワードを要求します。

手動で定義された PPP ユーザーを使用するときは、手動で構成されたユーザーのそれぞれごとに静的 IP アドレスが必要です。

各ユーザーごとに PPP ユーザー/IP アドレスを定義し、DUN 上でサーバー割り当て IP アドレスを使用するように指定できます。そうでない場合は、 PPP ユーザーを 1 つもち、DUN 上でローカル割り当ての静的 IP アドレスを使用するように指定できます。

Properties/Server Type/TCP/IP 設定のもとでの DUN クライアントでは、リモート・ネットワーク上でデフォルト・ルートを使用するかどうか指定できます。ここで指

定することは、PPTP クライアントがリモート・サブネット上の資源にだけアクセスしているのかどうかということ、または他のネットへの接続も必要かどうかということによって異なります。

監視

構成が正しいか検証する場合は、次の PING テストを行うことができます。まず最初に、DUN クライアント上で PPP リンクを開始し、ネットワーク・ユーティリティーのインターネット・インターフェースを PING します。PING は正常に行われるはずです。次に、イントラネット・インターフェースの PING を試みます。PING は正常に行われないはずです。そこで、PPTP DUN 定義を立ち上げて、 PPTP トンネルを開始します。今度は、イントラネット上のすべてのホストを PING できるはずです。

Talk 5 プロンプトで、**NETWORK 6** コマンドを発行してから、 **LIST ALL** コマンドを実行して、PPP 接続についての膨大な量の情報を表示させます。統計とユーザー ID と接続の IP アドレスが、トラブルシューティングを行う上で最も役立ちます。

表120 に示されているように、**CALL STATE** コマンドを使用します。**CALL STATE** コマンドを発行する前に、2 つの PPP ユーザーとのセッションを確立しました。

表 120. レイヤー 2 セッションを表示させる

```
VPNRTR1 Layer-2-Tunneling Console> CALL STATE
CallID | Serial # | Net # |     State     | Time Since Chg | PeerID | TunnelID
 55285 |        0 |     8 | Established |     0:37:10    |      0 |     6084
 38142 |        0 |     7 | Established |     0: 4:35    |      0 |    24721
VPNRTR1 Layer-2-Tunneling Console>
```

監視とトラブルシューティングの場合は、次のコマンドを使用します。

- VPNRTR1 Layer-2-Tunneling Console> **TUNNEL TRANSPORT**
- **DISPLAY SUBSYSTEM L2 ALL ALL** によって ELS をセットアップした後で、**TALK 2** コマンドを発行する。

表121 では、**TALK 2** コマンドの出力に、 CallID が情報に一致する 2 つの PPP ネットが示されています。

表 121. サブシステム L2 の表示のためにイベントを設定した Talk 2 の出力

```
00:41:55   L2.024: PPTP PAYLOAD SEND 38 bytes, net=7, callid=38142
00:41:55   L2.041: SND PPTP:F=3081,L=54,Tid=0,Cid=0,NS=115,NR=117,O=0
00:41:55   L2.040: RCV PPTP:F=3081,L=38,Tid=24721,Cid=38142,NS=118,NR=115,O=0
00:41:55   L2.022: PPTP PAYLOAD RCVD 38 bytes, net 7, callid=38142
00:42:00   L2.024: PPTP PAYLOAD SEND 38 bytes, net=8, callid=55285
00:42:00   L2.041: SND PPTP:F=3081,L=54,Tid=0,Cid=0,NS=264,NR=274,O=0
00:42:00   L2.040: RCV PPTP:F=3081,L=38,Tid=6084,Cid=55285,NS=275,NR=264,O=0
00:42:00   L2.022: PPTP PAYLOAD RCVD 38 bytes, net 8, callid=55285
00:42:03   L2.084: PPTP Tunnel 6084/0 EVENT Rcv-ECHO,state=Established
```

LIST ALL コマンドの部分リストについては、 374ページの表122 をごらんください。

表 122. List All コマンドの部分出力

```
VPNRTR1 +NETWORK 8
Point-to-Point Console
       VPNRTR1 PPP 8>LIST ALL

Interface Statistic        In                        Out
-------------------        --                        ---
Packets:                   81                        70
Octets:                    3316                      2581
..
.Remote Username:           sg245281
.
..IPCP Option                Local                     Remote
-----------                -----                     ------
IP Address                 0.0.0.0                   192.168.141.38
Compression Slots          None                      None
```

IBM ネットワーク・ユーティリティー開始の自発的 PPTP トンネル

今度の例は、375ページの図76 に図示されている PPTP の事例で、IBM ルーターが PPTP トンネルを開始し、そのトンネルが Microsoft NT リモート・アクセス・サーバー (RAS) (これが PPTP ピア) で終端しています。NT サーバーには、アダプターが 2 つあり、1 つには、IP クラウド経由で到達可能な IP アドレスがあり、もう 1 つは私設ネットワーク上にあります。NT ホストには、動的ルーティング・プロトコルは構成されていませんが、IP 転送機能があります。

この事例では、事業所の IP ホストと本社ネットワーク内の単一のサブネット上のホストとの接続が可能になります。NT RAS は、DMZ と呼ばれる場合があるものの中に配されています。インターネットからのアクセスが可能であり、本社ファイアウォールでは保護されていません。RAS 自体が、インターネットをまたがってアクセスされる本社サブネットにとって、ファイアウォールになります。

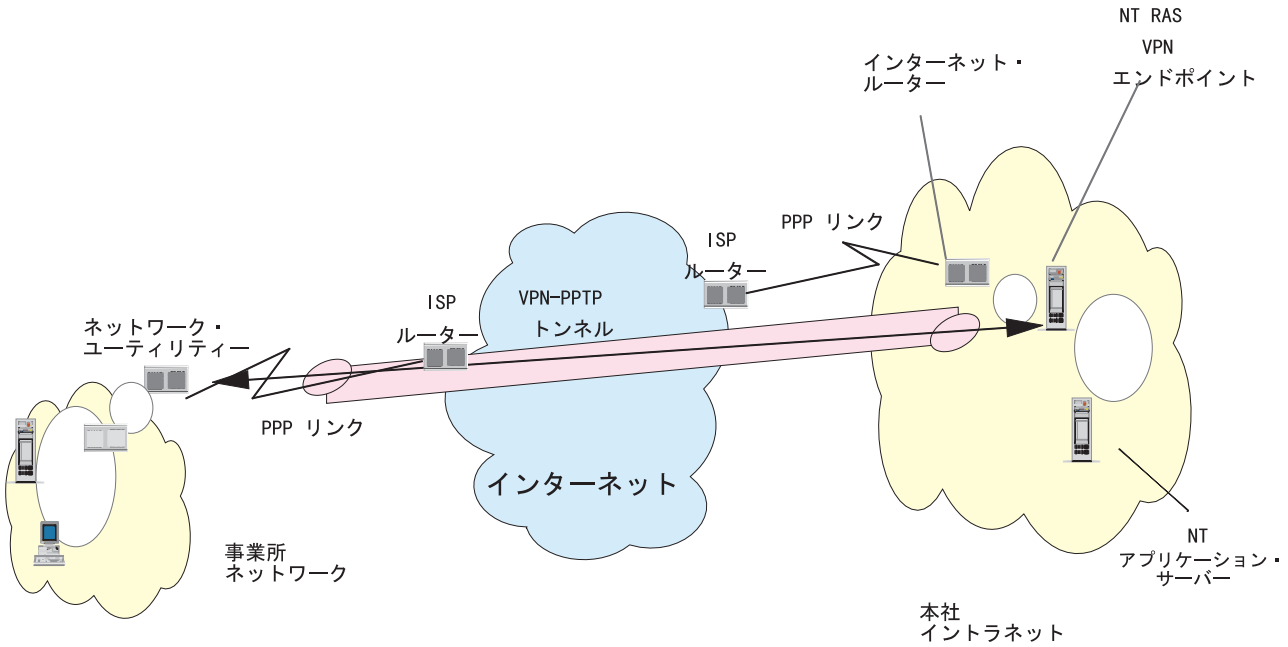


図 76. IBM ルーター開始の PPTP トンネル

この例で使用されている LAB ネットワークは、1 つの PPP リンクと、2 台の IBM 2210 ルーターで接続された 3 つのトークンリング・セグメントで構成されています。ルーターには VPNRTR1 と VPNRTR2 という名前を付けました。LAB 内のルーターは、 56 Kbps PPP リンクで接続されています。実際の事例では、ルーター間のリンクは、広域ネットワーク (WAN) であれば、私設ネットワークでも公衆ネットワークでも構いません。

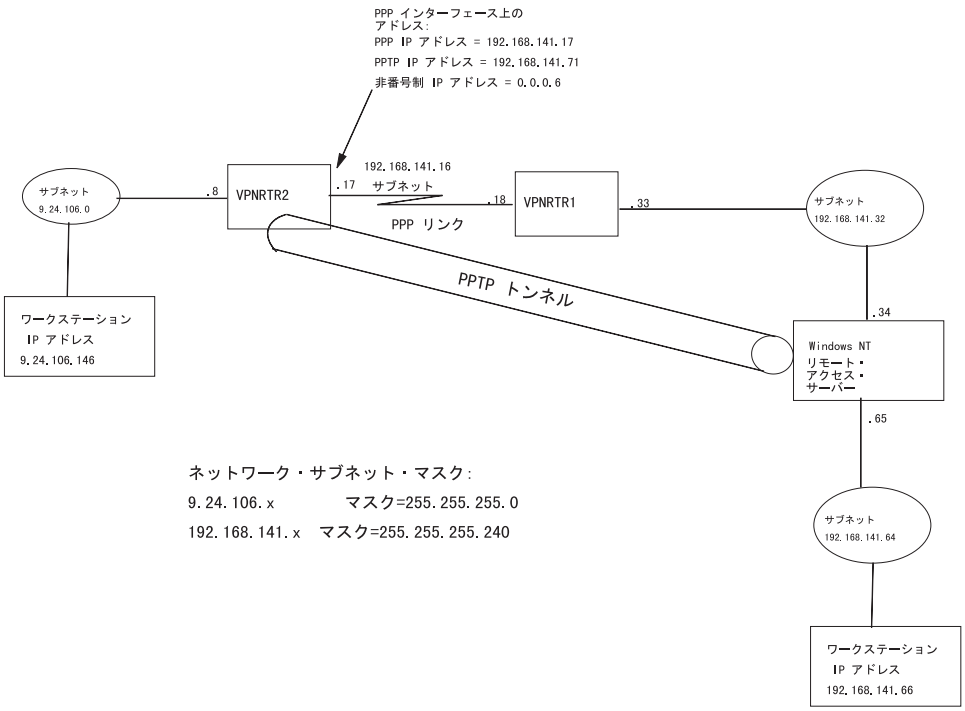


図 77. LAB ネットワークの IP アドレッシング

本社 LAN IP ネットワーク 192.168.141.64 に送信したいデータが、事業所ネットワーク 9.24.106.0 上の装置にあると、PPTP トンネルが確立されます。 192.168.141.64 ネットワークは、IP クラウド内には公示されていません。本社ネットワーク上のホストは私設アドレスであり、IP クラウドは ISP のネットワークです。

VPNRTR2 は、375ページの図76 に図示されている事業所インターネット・ルーターを表し、192.168.141.64 ネットワークあてのトラフィックを指定し、バーチャル・インターフェースを経由してルーティングされる必要がある、静的ルートを使用して構成されます。データがインターフェース上で受信されると、ルーターが PPTP トンネルを確立します。ルーターでは、L2Net とトンネル定義を調べて、PPTP 同位 192.168.141.34 (NT リモート・アクセス・サーバーと VPN エンドポイントとして図示されている) の IP アドレスを見つけます。ルーターは、インターネット経由でこのアドレスへの TCP 接続を確立します。NT が PPTP 接続を受け入れたら、事業所ルーターがその L2Net に関する PPP パラメーターを交渉します。NT サーバーでは、その PPTP インターフェースのために構成されたアドレスのプールから IP アドレスを 1 つ戻します。この IP アドレスは、本社 LAN インターフェースと同じサブネット内にある必要があります。L2Net は、その IP アドレスを IPCP 経由で受信するように構成する必要があります。

事業所ルーターを構成する

事業所ルーターを構成する手順の基本ステップは、次のとおりです。

- PPTP を使用可能にする。
- トンネル・プロファイルを追加する。
- IP アドレッシングと認証に関する定義を設定する。
- ネットワーク・アドレス変換を構成する。

- パケット・フィルターを作成する。

PPTP をルーター上で使用可能にし、バーチャル・インターフェースを追加します。トラフィックがこのインターフェース上で受信されると、ルーターが PPTP トンネルを開始します。

表 123. レイヤー 2 ネットワークを追加する

```
VPNRTR2 *TALK 6

VPNRTR2 Config>FEATURE Layer-2-Tunneling
VPNRTR2 Layer-2-Tunneling Config>ENABLE PPTP

 Restart system for changes to take effect.
VPNRTR2 Layer-2-Tunneling Config>
Layer-2-Tunneling Config>add l2-nets
Additional L2 nets: [0]? 1
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 6         1
Defaulting data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or
[No]):
Bridge configuration was not changed.
Restart router for changes to take affect.
Layer-2-Tunneling Config>exit
VPNRTR2 Config>
```

1. 非番号制 IP アドレスを追加するように指定したので、0.0.0.6 が割り当てられたのは、L2Net がインターフェース 6 であるためです。表124 に示されているように、IP Config> コマンド・プロンプトで、**list addr** コマンドを使用して、アドレスを検証できます。このアドレスは、 379ページの表128 に示されているように、**enable dynamic** コマンドのパラメーターとして使用されます。

表 124. List Address コマンドで PPTP インターフェースの IP アドレスを検証する

```
VPNRTR2 Config>PROTOCOL IP
VPNRTR2 IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0                                      IP disabled on this interface
   intf     1  192.168.141.17   255.255.255.240  Local wire broadcast, fill 1
   intf     2                                      IP disabled on this interface
   intf     3                                      IP disabled on this interface
   intf     4                                      IP disabled on this interface
   intf     5  9.24.106.8       255.255.255.0    Local wire broadcast, fill 1
   intf     6  0.0.0.6          0.0.0.0          Local wire broadcast, fill 1
                                                  DYNAMIC-ADDRESS Enabled
VPNRTR2 Config>EXIT
```

次のステップでは、PPTP トンネル・エンドポイントを定義します。**add tunnel-profile** コマンドを使用して、トンネルを定義します。プロンプトによって入力を指示される名前は、リモートと PPTP の名前です。これは、ローカルでの識別目的だけのためのものです。PPTP 交換時に送信されることはありません。トンネル・サーバー・エンドポイント・アドレスを尋ねられますが、これは、IP クラウド経由で到達可能な NT サーバーのアドレス内にあります。

表 125. トンネルを追加する

```
VPNRTR2 Config>ADD TUNNEL-PROFILE
Enter name:  []? NT
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP] PPTP
Tunnel-Server endpoint address: [0.0.0.0]? 192.168.141.34

       Tunnel name: NT
          TunnType: PPTP
          Endpoint: 192.168.141.34

Tunnel 'NT' has been added
```

次のステップでは、NT と呼ばれるピアにバーチャル・インターフェースを結合します。デフォルトでは、L2Net はすべてどの装置からでもインバウンドです。これをアウトバウンドに変更する必要があります。そうすると、プロンプトによってリモート装置の名前の入力を指示されます。つまり、トラフィックがこのバーチャル・インターフェース (インターフェース 6) にルーティングされると、ルーターが ″NT″ と呼ばれるピアへのトンネルを確立することを意味します。″NT″ トンネル定義を調べて、192.168.141.34 への PPTP トンネルであることを検出します。

ルーターでは、そのルーティング・テーブルを調べて、そのアドレスに至る方法 (この例では、192.168.141.17 経由) を判別します。ルーターは、静的ルーティング・プロトコルと動的ルーティング・プロトコルのどちらかによって、 192.168.141.34 に至る方法が分かるように構成する必要があります。

表 126. バーチャル・インターフェースを構成する

```
VPNRTR2 Config>NETWORK 6
Session configuration
VPNRTR2 L2T config:   6>SET CONNECTION-DIRECTION OUTBOUND     1
Enter remote tunnel hostname:  []? NT
VPNRTR2 L2T config:   6>
```

L2Net がインバウンドからアウトバウンドに変更されると、PPP のデフォルトがその L2Net 上に構成されます。**encapsulator** コマンドを使用して、PPP 構成プロンプトにアクセスできます。この例では、ルーターは、プロンプトが出ると、名前 rtr-1 を送信するように構成されます。この L2Net は、その IP アドレスを NT ボックスから受信するようになっています。これが送信されるのは、IPCP 交渉時であり、ルーターは、NT ボックスにその IP アドレスを要求するように構成する必要があります。これを行うには、**set ipcp** コマンドを使用し、「yes」と応答して IP アドレスを要求します。

表 127. L2net が名前を送信するように構成し、インターフェースが IPCP 経由で IP アドレスを受信できるようにする

```
VPNRTR2 Config>NETWORK 6
Session configuration
VPNRTR2 L2T config:   6>ENCAPSULATOR
Point-to-Point user configuration
VPNRTR2 PPP 6 Config>SET NAME
Enter Local Name:  []? rtr-1
Password:rtr-1            1
Enter password again:rtr-1
PPP Local Name = rtr-1


VPNRTR2 PPP 6 Config>
VPNRTR2 PPP 6 Config>SET IPCP
IP COMPRESSION [no]:
Request an IP address [no]: yes      2
Interface remote IP address to offer if requested (0.0.0.0 for none) [0.0.0.0]?

VPNRTR2 PPP 6 Config>EXIT
VPNRTR2 L2T config:   6>EXIT
VPNRTR2 Config>
```

1. パスワードは画面には表示されません。ここには図示による説明の便宜上示してあるだけです。この名前とパスワードは、ユーザー・マネージャー機能のもとで NT リモート・アクセス・サーバー内で設定されているユーザーとパスワードに一致する必要があります。
2. 「yes」と応答して、NT に L2Net に関する IP アドレスを送信させます。

ルーター L2net が NT トンネルから IP アドレスを受信するためには、IP アドレスを動的 IP 用として使用可能にする必要があります。そうすれば、NT は IPCP 経由で事前構成アドレス・プールからアドレスを送信できます。

表 128. L2Net 上に IP を構成する

```
VPNRTR2 Config>PROTOCOL IP
Internet protocol user configuration
VPNRTR2 IP config>ENABLE DYNAMIC-ADDRESS
Interface address []? 0.0.0.6   1
VPNRTR2 IP config>
```

1. **add l2-nets** コマンドによって、 377ページの表123 に示されているように割り当てられた IP アドレスを入力します。

NT RAS ホスト上で動的ルーティング・プロトコルが使用されていないので、本社サブネットへの静的ルートが追加される必要があります。

表 129. 静的ルートを私設網に追加する

```
VPNRTR2 IP config>ADD ROUTE
IP destination []? 192.168.141.64       1
Address mask [255.255.255.0]? 255.255.255.240
Via gateway 1 at []? 0.0.0.6
Cost [1]?
Via gateway 2 at []?
VPNRTR2 IP config>EXIT
VPNRTR2 Config>
```

1. これは、NT RAS が配されているネットワークのアドレスとサブネット・マスクです。

ルーターは本社ネットワーク上の単一のユーザーとして表示されることになり、本社ネットワークでは事業所ネットワークについてまったく関知しないので、ネットワーク・アドレス/ポート変換 (Network Address and Port Translation) (NAPT) を使用する必要があります。NAPT は、元もとは IBM ルーターの V3.1 に付属していた NAT の機能を強化したものです。NAT フィーチャーから使用可能にし、構成することができます。

表 130. NAT を構成する

```
VPNRTR2 Config>FEATURE NAT
Network Address Translation (NAT) user configuration
VPNRTR2 NAT config>ENABLE NAT

Complete! NAT set to ENABLED.
VPNRTR2 NAT config>
```

次のステップでは、パケットの変換先としたいアドレスを定義します。これには **reserve** コマンドを使用します。アドレスが IPCP 経由で取得できるか尋ねられたときは、「Yes」と応答します。インターフェースは 6、 L2Net です。次に、ルーターがプール名を要求します。これは、変換する必要があるアドレスを定義するとき、参照として使用します。また、ルーターは、IP パケット・フィルターを構成して、変換される NAT フィーチャーにパケットを渡す必要があることも指示してきます。ルーターがユーザーに IP パケット・フィルターを構成するように念を押するのは、このときが最初になります。

表 131. LAN アドレスの変換方法を定義する

```
VPNRTR2 NAT config>RESERVE
Dynamically allocate address via IPCP? [No]: yes
Network number to get dynamic address. [0]? 6
Reserve Pool name..................... []? dyn-nat

Complete! NAT Reserve Pool defined.

NOTE: The associated TRANSLATE RANGE for this RESERVE POOL
      must still be configured.
      It must have a pool name of: dyn-nat

NOTE: You must have a corresponding INBOUND IP Access Control rule
      applied to your designated NAT interface.
      The rule should include the following information:
          Type=IN (include + NAT)
          DESTINATION_Addr=0.0.0.0
          DESTINATION_Mask=0.0.0.0

VPNRTR2 NAT config>
```

次のステップでは、変換する必要があるアドレスを定義します。コマンドは、″Translate all packets with a source address in the 9.24.106.0 network to have an address in the dyn-nat pool″ になります。 直前のステップで、 dyn-nat プールがインターフェース 6 上で IPCP が受信するアドレスであることを定義しました。ルーターはユーザーに対して、フィルターを構成して、パケットが変換のために NAT/NAPT に渡されるようにする必要があることを念押しします。

表 132. 変換する必要がある LAN アドレスを定義する

```
VPNRTR2 NAT config>TRANSLATE
Base (private) IP address to translate [0.0.0.0]? 9.24.106.0
Translate Range mask.................. [255.255.255.0]?
Associated Reserve Pool name.......... [dyn-nat]?

Complete! NAT Translate Range defined.

NOTE: The associated RESERVE POOL for this TRANSLATE RANGE has been found.

NOTE: You must have a corresponding OUTBOUND IP Access Control rule
      applied to your designated NAT interface.
      The rule should include the following information:
          Type=IN (include + NAT)
          SOURCE_Addr=9.24.106.0
          SOURCE_Mask=255.255.255.0
VPNRTR2 NAT config>EXIT
VPNRTR2 Config>
```

ここで IP パケット・フィルターを作成する必要があります。 表133 には、アクセス制御が使用可能にされてから、L2Net に接続されているフィルターが作成され、out-6 と in-6 という名前が付けられることが示されています。

表 133. パケット・フィルターを追加する

```
VPNRTR2 Config>PROTOCOL IP
Internet protocol user configuration
VPNRTR2 IP config>SET ACCESS-CONTROL ON
VPNRTR2 IP config>

VPNRTR2 IP config>ADD PACKET-FILTER
Packet-filter name []? out-6
Filter incoming or outgoing traffic? [IN]? out
Which interface is this filter for [0]? 6

VPNRTR2 IP config>ADD PACKET-FILTER
Packet-filter name []? in-6
Filter incoming or outgoing traffic? [IN]?
Which interface is this filter for [0]? 6
VPNRTR2 IP config>
```

パケット・フィルターが作成されたら、**update packet-filter** コマンドを使用して、フィルターを定義します。out-6 フィルターの目的は、サブネット 9.24.106.0 から出てインターネットに向かうパケットをすべて、ネットワーク・アドレス変換機能に向かわせることにあります。

表 134. アウトバウンド・パケット・フィルターを更新する

```
VPNRTR2 IP config>UPDATE PACKET-FILTER
Packet-filter name []? out-6
VPNRTR2 Packet-filter 'out-6' Config>ADD ACCESS-CONTROL
Access Control type [E]? N      1
Internet source [0.0.0.0]? 9.24.106.0
Source mask [255.255.255.0]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Starting protocol number ([0] for all protocols) [0]?
Starting DESTINATION port number ([0] for all ports) [0]?
Starting SOURCE port number ([0] for all ports) [0]?
Filter on ICMP Type ([-1] for all types) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]?
Enable logging? [No]:
VPNRTR2 Packet-filter 'out-6' Config>exit
```

1. タイプ N では、データグラムが NAT 機能に送信される必要があることを指定します。

in-6 フィルターの目的は、インターネットから出て サブネット 9.24.106 に向かうパケットをすべて、ネットワーク・アドレス変換機能に向かわせることにあります。

表 135. インバウンド・パケット・フィルターを更新する

```
VPNRTR2 IP config>UPDATE PACKET-FILTER
Packet-filter name []? in-6
VPNRTR2 Packet-filter 'in-6' Config>ADD ACCESS-CONTROL
Access Control type [E]? N
Internet source [0.0.0.0]?
Source mask [0.0.0.0]?
Internet destination [0.0.0.0]?
Destination mask [0.0.0.0]?
Starting protocol number ([0] for all protocols) [0]?
Starting DESTINATION port number ([0] for all ports) [0]?
Starting SOURCE port number ([0] for all ports) [0]?
Filter on ICMP Type ([-1] for all types) [-1]?
TOS/Precedence filter mask (00-FF - [0] for none) [0]?
TOS/Precedence modification mask (00-FF - [0] for none) [0]?
Enable logging? [No]:
VPNRTR2 Packet-filter 'in-6' Config>exit
VPNRTR2 IP config>EXIT
VPNRTR2 Config>
```

これで事業所ルーターの構成は完了です。毎度のことながら、構成プログラムと TFTP サーバーのどちらかに構成を保管しておくのが賢明な策です。

NT リモート・アクセス・サーバーを構成する

NT リモート・アクセス・サーバーを構成する場合は、次の手順に従います。

- インターネット・アクセス可能トークンリング上の IP = 192.168.141.34 / 255.255.255.240
- イーサネット上の IP = 192.168.141.65 / 255.255.255.240
- VPN インターフェースが最小限 1 つの PPTP プロトコルを追加する。
- リモート・アクセス・サービスで、RAS 装置を追加する。
- VPN インターフェースを RAS サーバーにリンクする。
- IP プール 192.168.141.70 〜 192.168.141.73 を構成する。

NT ユーザー名 **rtr-1** とパスワード **rtr-1** を追加します。これは、379ページの表127で構成した値に一致する必要があります。 ″change password on first logon″ オプションを使用不可にし、パスワードを「never age」に設定します。

NT ボックスには IP クラウド経由で到達可能である必要があります。悪意のある活動を防止するためには、IP クラウドに接続されているインターフェース上で PPTP フィルターを使用可能にすることができます。つまり、PPTP サーバーが受け入れるのは、認証されたユーザーからの PPTP パケットだけであることを意味します。ユーザー (この例では、リモート・ルーター) は、NT 内の「ユーザーを管理する」機能を使用して定義します。非 PPTP パケットや未認証ユーザーからの PPTP トラフィックは、すべて除去されます。

PPTP サーバーのセットアップに関する説明については、Microsoft Web ページ、http://www.microsoft.com/NTServer/commserv/deployment/planguides/installing_pptp.asp にアクセスしてください。

構成の監視/トラブルシューティング

PPTP トンネルを動的に監視する場合は、ELS を使用します。**NODISPLAY SUBSYSTEM ALL** コマンドを発行し、それに続けて **DISPLAY SUBSYSTEM L2 ALL ALL** コマンドを発行して、 ELS がサブシステム L2 だけを表示するように構成します。その上で、 表136 に示されているように、**TALK 2** コマンドを発行します。

なお、たとえ他にトラフィックがない場合でも、30 秒ごとに「キープアライブ」タイプのトラフィックが生じます。

表 136. L2 サブシステムに関する ELS 出力

```
VPNRTR2 *TALK 2

40:19:49   L2.024: PPTP PAYLOAD SEND 38 bytes, net=6, callid=55253
40:19:49   L2.041: SND PPTP:F=3081,L=54,Tid=0,Cid=0,NS=121,NR=122,O=0
40:19:49   L2.040: RCV PPTP:F=3081,L=38,Tid=20169,Cid=55253,NS=123,NR=121,O=0
40:19:49   L2.022: PPTP PAYLOAD RCVD 38 bytes, net 6, callid=55253
40:19:59   L2.024: PPTP PAYLOAD SEND 38 bytes, net=6, callid=55253
40:19:59   L2.041: SND PPTP:F=3081,L=54,Tid=0,Cid=0,NS=122,NR=123,O=0
40:19:59   L2.040: RCV PPTP:F=3081,L=38,Tid=20169,Cid=55253,NS=124,NR=122,O=0
40:19:59   L2.022: PPTP PAYLOAD RCVD 38 bytes, net 6, callid=55253
```

この例の場合は、Talk 5 Protocol IP プロンプトで **INTERFACE** コマンドを発行すると、PPP/4 インターフェースにトンネルの他端のサブネット上の IP アドレスが割り当てられたことが示されます。NT RAS が 192.168.141.70 で始まり、192.168.141.73 で終わるプールから IP アドレスを割り当てるように構成したことを思い出しましょう。

NT RAS ホストでは、そのトンネル・エンドポイント・アドレスに .70 をとり、もう一方のトンネル・エンドポイントのネットワーク・ユーティリティーに .71 を割り当てました。

表 137. インターフェース情報を表示させる

```
VPNRTR2 *TALK 5

CGW Operator Console
VPNRTR2 + PROTOCOL IP
VPNRTR2 IP>INTERFACE
Interface    MTU   IP Address(es)   Mask(s)         Address-MTU
  PPP/0     2044   192.168.141.17   255.255.255.240 Unspecified
  TKR/0     4082   9.24.106.8       255.255.255.0   Unspecified
  PPP/4     1500   192.168.141.71   255.255.255.255 Unspecified
VPNRTR2 IP>EXIT
```

表138 に示されているように、 FEATURE Layer-2-Tunneling プロンプトで、**call state** コマンドと **call statistics** コマンドを使用して、トンネル活動を検査します。

表 138. トンネルの状況と統計を表示させる

```
VPNRTR2 +FEATURE Layer-2-Tunneling
Layer-2-Tunneling Information
VPNRTR2 Layer-2-Tunneling Console> CALL STATE
CallID │ Serial # │ Net #  │    State    │ Time Since Chg │ PeerID │ TunnelID
 64985 │        0 │      6 │ Established │     0:13:46    │      0 │    19704

VPNRTR2 Layer-2-Tunneling Console> CALL STATISTICS
CallID │ Serial # │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │  ATO
 64985 │        0 │      95 │     3440 │      97 │     3415 │     0 │
0
VPNRTR2 Layer-2-Tunneling Console>
```

注: >FEATURE Layer-2-Tunneling プロンプトでは、次の順序で一連のコマンドを使用できます。=>T5、=>NET 6、=>LIST ALL

IBM ネットワーク・ユーティリティー開始の自発的 L2TP トンネル

次のステップを例外として、IBM ネットワーク・ユーティリティー開始の自発的 PPTP トンネル の手順どおりにします。

- L2TP を使用可能にする。
- トンネル・プロファイル内で L2TP を指定する。

注: このステップでは、プロンプトが多少異なっています (385ページの表139 をごらんください)。

表 139. トンネル・プロファイル内で L2TP を指定する

```
add tunnel-profile
Enter name: [ ]? L2TP peer
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP]
Enter local host name: [ ] netU
Set shared secret? (Yes, No): [No] y
Shared secret for tunnel authentication: * will not appear
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0] 192.168.141.34

      Tunnel name: L2TP peer
      Tunn Type 3: L2TP
      Endpoint: 192.168.141.34
      Local Hostname: netU
Tunnel 'NT' has been added
```

IBM ネットワーク・ユーティリティー LNS で終端する L2TP トンネル

L2TP 事例のサンプルでは、L2TP トンネリングを使用して、事業所内のリモート・ダイヤル呼び出しユーザーと本社のネットワーク・ユーティリティーの間に接続を確立します。 図78 のサンプル・ネットワーク図をごらんください。

ダイヤルイン・リモート・ユーザーを接続する

インターネットなどの公衆 IP ネットワークを通して、リモート・ダイヤルイン・ユーザーを中央側に接続する場合にも、VPN が応用できます。リモート・アクセス・サーバーは、 ISP かユーザーの企業が管理します。この事例では、IBM Nways 2210/ネットワーク・ユーティリティーの L2TP とLAN へのダイヤルイン・アクセス (DIALs) を使用して、 IBM Nways 2210/ネットワーク・ユーティリティーをリモート LAN アクセス (RLAN) サーバーとして使用する方法を実証します。

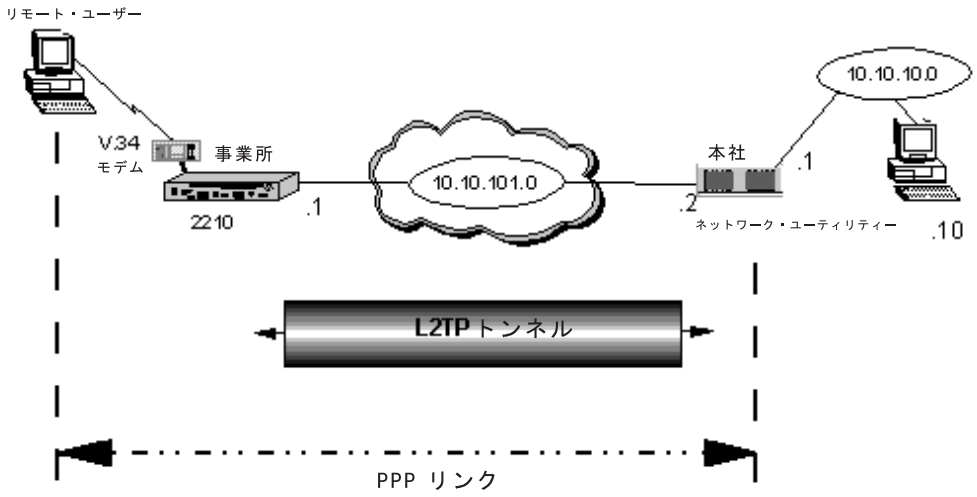


図 78. L2TP のサンプル構成

この例では、IBM Nways 2210/ネットワーク・ユーティリティーが使用され、事業所内の 2210 がリモート・ダイヤルイン・ユーザーの RLAN アクセス・サーバーとなります。 L2TP トンネルが事業所ルーターとデータ・センターのネットワーク・ユーティリティーの間にセットアップされるので、リモート・ユーザーは、ネットワーク・ユーティリティー内の RLAN 機能を使用して、本社イントラネット上の資源にアクセスできます。L2TP 接続は IP ベースであるので、IPSec も構成されている場合は、このトラフィックは IPSec トンネルを通しても送信できます。この代替方法では、L2TP は IPSec トンネル内にあります。

事業所ルーターをダイヤルイン・アクセス・サーバー用として構成する

事業所ルーターは、リモート・ユーザーが、V.34 ダイヤル呼び出しモデムを経由して事業所ルーターにアクセスした上で、次のことができるように構成しました。つまり、L2TP を使用して、事業所の 2210 から 中央側の IBM ネットワーク・ユーティリティーにセッションをトンネル伝送することによって、インターネットなどの IP ネットワークを通して、リモート・ユーザーのセッションを本社データ・センターの場所まで拡張します。

注:

1. リモート・ユーザー・アクセス用としての V.34 の使用については、この事例で実証されています。ただし、2210 では V.34、ISDN BRI、V.25bis をサポートします。V.34 のサポートについては、WAN ポートに接続された外付けモデム経由か、V.34 モデムが内蔵されている、4 ポートまたは 8 ポートのダイヤル・アクセス・アダプター経由になります。
2. IP ネットワークは、IP ベースのネットワークであれば、インターネットや公衆フレーム・リレー・ネットワークなど、何でも構いません。この事例では、IP ネットワークは、 PPP シリアル WAN リンクで表してあります。

RLAN 構成の最初のステップでは、V.34 インターフェースを追加します。これは、表140 に示してあります。

表 140. V.34 アドレスを追加し、V.34 インターフェースを構成する

```
Branch *t 6
Gateway user configuration
Branch Config>add V34-ADDRESS
Assign address name [1-23] chars []? local
Assign network dial address [1-30 digits] []? 9193013461
Branch Config>set data v34
Interface Number [0]? 4
Branch Config>net 4
V.34 Data Link Configuration
Branch V.34 System Net Config 4>set local-address
Local network address name []? local
```

V.34 ポートを V.34 アドレスにマップする必要があります。また、モデム初期化ストリングと速度も設定できますが、この例では、デフォルトのパラメーターを使用しています。構成したパラメーターについては、**'list all'** コマンドを使用して、387ページの表141 に示されているようにチェックできます。

表 141. V.34 ポートの構成を一覧表示させる

```
Branch V.34 System Net Config   4>LIST all

         V.34 System Net Configuration:

Local Network Address Name    = local
Local Network Address         = 9193013461

Non-Responding addresses:
Retries                       = 1
Timeout                       = 0 seconds

Mode                          = Switched

Call timeouts:
Command Delay                 = 0 ms
Connect                       = 60 seconds
Disconnect                    = 2 seconds

Modem strings:
Initialization string         =

Speed (bps)                   = 115200
```

次のステップでは、ダイヤルイン接続用として使用するバーチャル・インターフェースを作成します。 RLAN ユーザーは、「ダイヤルイン回線」と呼ばれている特殊なダイヤル回線を使用します。この事例では、単一の RLAN テスト・ユーザー用として、バーチャル・インターフェースを 1 つ作成しています。ただし、さらに多くのバーチャル・インターフェースを作成しても構いません。実用上の上限は、ルーター上で使用可能な非同期ポートの数です。

ダイヤルイン・インターフェースは、次の図に示されているように、 **talk 6 Config>** プロンプトで追加します。

表 142. バーチャル・ダイヤルイン・インターフェースを作成する

```
Branch Config>ADD DEVICE DIAL-IN
Enter the number of PPP Dial-in Circuit interfaces [1]?
Adding device as interface 6
Base net for this circuit [0]? 4
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.
Defaulting Data-link protocol to PPP
Add more dial circuit interface(s)?(Yes or [No]):
Use "net " command to configure circuit parameters

Branch Config>LIST DEVICES
Ifc 0     Ethernet            CSR  81600, CSR2  80C00, vector 94
Ifc 1     WAN PPP             CSR  81620, CSR2  80D00, vector 93
Ifc 2     WAN PPP             CSR  81640, CSR2  80E00, vector 92
Ifc 3     WAN PPP             CSR 381620, CSR2 380D00, vector 125
Ifc 4     V.34 Base Net       CSR 381640, CSR2 380E00, vector 124
Ifc 5     Token Ring          CSR 6000000, vector 95
Ifc 6     PPP Dial-in Circuit

Branch Config>NETWORK 6
Circuit configuration
Branch Dial-in Circuit config:   6>LIST all

Base net                       = 4
Circuit priority               = 8
```

注: V.34 を通してサポートされるのは、PPP だけです。ただし、DIALs を使用すれば、複数のプロトコル (IP、IPX、NetBIOS、802.2、LLC) が PPP 接続を通してサポートできます。

それぞれのダイヤルイン回線ごとに、ユーザーが構成できるパラメーターは数多くありますが、一般的には、デフォルト値のままにしておいて構いません。

V.34 インターフェースを通して IP をルーティングするためには、インターフェースに IP アドレスを割り当てる必要があります。クライアントがダイヤルインすると、ルーターでは、そのルーティング・テーブルに自動的に静的ルートを追加し、これによって、リモート・ユーザーのネクスト・ホップが V.34 バーチャル・インターフェースの IP アドレスであることを示します。

アドレスは、あて先 LAN セグメントとは異なるサブネット上にある必要があります。実 IP アドレスを使用することも、非番号制 IP を使用することもできます。非番号制 IP の場合は、アドレスの形式は 0.0.0.n (ただし、n はインターフェース番号) となります。表143 に、この事例でのダイアログが示してあります。インターフェース 6 が、テスト・ダイヤルイン・ユーザーの場合のバーチャル・インターフェースです。

表 143. バーチャル・インターフェース上に IP アドレスを構成する

```
Branch IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0                                IP disabled on this interface
   intf     1  10.10.101.1 255.255.255.0     Local wire broadcast, fill 1
   intf     2                                IP disabled on this interface
   intf     3                                IP disabled on this interface
   intf     4                                IP disabled on this interface
   intf     5  10.10.1.1   255.255.255.0     Local wire broadcast, fill 1
   intf     6                                IP disabled on this interface

Branch IP config>add address
Which net is this address for [0]? 6
New address []? 0.0.0.6
Address mask [0.0.0.0]? 255.255.255.0
```

あて先へのネクスト・ホップが、ARP 要求を受信しているインターフェースとは異なるインターフェースを介しているとき、ルーターが ARP に応答できるようにするためには、ARP サブネット・ルーティングが使用可能にされている必要があります。これに該当するのは、クライアント IP アドレスはルーターの LAN インターフェースと同じサブネット上にあるが、ネクスト・ホップ (V.34 インターフェース) は別のサブネット上にあるような、RLAN の場合です。 ARP サブネット・ルーティングは、表144 に示されているようにして使用可能にします。

表 144. ARP サブネット・ルーティングを使用可能にする

```
Branch IP config>ENABLE ARP-SUBNET-ROUTING

Branch IP config>LIST ADDRESSES
IP addresses for each interface:
   intf     0                                IP disabled on this interface
   intf     1  10.10.101.1 255.255.255.0     Local wire broadcast, fill 1
   intf     2                                IP disabled on this interface
   intf     3                                IP disabled on this interface
   intf     4                                IP disabled on this interface
   intf     5  10.10.1.1   255.255.255.0     Local wire broadcast, fill 1
   intf     6  0.0.0.6     255.255.255.0     Local wire broadcast, fill 1
```

これで、基本 DIAL 機能用としての事業所ルーターの構成は完了です。そこで、表145 に示されているようにして、ルーターを再始動して、変更をアクティブにします。

表 145. ルーターを再始動する

```
Branch config>
Branch *res
Are you sure you want to restart the gateway? (Yes or [No]): yes
```

L2TP を事業所ルーターで構成する

この例では、事業所にある 2210 とデータ・センターのネットワーク・ユーティリティーの間に L2TP をセットアップすることによって、ダイヤルイン・ユーザーの PPP 接続が拡張できます。エンド・ユーザーは、ネットワーク・ユーティリティー内の RLAN 機能を使用して、データ・センター内の資源に接続できる必要があります。

L2TP は、L2TP 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) の間のトンネルに関与するメカニズムです。この事例では、事業所の 2210 が LAC として構成され、ネットワーク・ユーティリティーが LNS として構成されます。最初のステップでは、L2TP を LAC 内で使用可能にします。 表146 をごらんください。

表 146. L2TP を LAC (事業所ルーター) 内で使用可能にする

```
Branch Config> FEATURE Layer-2-Tunneling
Branch Layer-2-Tunneling Config>ENABLE L2TP

 Restart system for changes to take effect.
Branch Layer-2-Tunneling Config>EXIT
```

次に、LAC 内でトンネルが作成されます。これについては、 390ページの表147 に示してあります。

表 147. L2TP トンネルを LAC (事業所ルーター) 内で作成する

```
Branch 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:
Passwords do not match.
...try again
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 10.10.101.2

       Tunnel name: lns.org
          TunnType: L2TP
          Endpoint: 10.10.101.2
    Local Hostname: lac.org

Tunnel 'lns.org' has been added

Branch Config>LIST TUNNEL-PROFILES
TunnType  Endpoint         Tunnel name            Hostname

L2TP      10.10.101.2      lns.org                lac.org

1 TUNNEL record displayed.
```

以下の注記は、LAC トンネル構成に関するものです。

Tunnel name
この名前は、LNS (ネットワーク・ユーティリティー) 上で構成されるホスト名に一致する必要があります。

Hostname
LAC のホスト名です。

Tunnel-Server endpoint
トンネルのエンドポイントの IP アドレス。このアドレスは、LAC から到達可能である必要があります。インターフェース・アドレスでもよいし、ネットワーク・ユーティリティー上の内部 IP アドレスでも構いません。ここでは、トンネルのエンドポイントであるインターフェースのアドレスが使用されています。

Shared secret
このパラメーターを設定する必要があるのは、トンネル上で認証が使用される場合であり、ここでの値は、LNS で構成された値に一致する必要があります。デフォルトでは、L2TP トンネル認証が使用可能にされます。

以上の変更をアクティブにするには、ルーターを再始動する必要があります。

L2TP をネットワーク・ユーティリティー内で構成する

2216 が L2TP ネットワーク・サーバー (LNS) として構成されています。最初に、L2TP が LNS 内で使用可能にされました。これについては、 391ページの表148 に示してあります。

表 148. L2TP を LNS 内で使用可能にする

```
Corp Config>FEATURE Layer-2-Tunneling
Corp Layer-2-Tunneling Config>ENABLE L2TP

 Restart system for changes to take effect.
Corp Layer-2-Tunneling Config>EXIT
```

次に、トンネルが LNS 内で作成されて、LAC の IP アドレスと名前を指し示します。これについては、表149 に示してあります。

表 149. L2TP トンネルを LNS (本社ネットワーク・ユーティリティー) 内で作成する

```
Corp 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]? 10.10.101.1

       Tunnel name: lac.org
          TunnType: L2TP
          Endpoint: 10.10.101.1
    Local Hostname: lns.org
Tunnel 'lac.org' has been added

Corp Config>LIST TUNNEL-PROFILES
TunnType  Endpoint         Tunnel name            Hostname

L2TP      10.10.101.1      lac.org                lns.org

1 TUNNEL record displayed.
```

注: 共用秘密を使用する場合は、キーは LAC 内で構成したキーに一致する必要があります。

L2TP トンネルに関する PPP パラメーターは変更できます。ただし、これらのパラメーターについては、LAC と LNS の間で交渉されます。LAC は、クライアント PC のプロキシーとして PPP 交渉に当たります。L2TP トンネルに関して、認証プロトコルが使用可能にされる必要があります。この事例では、LNS 上のデフォルトの PPP パラメーターが使用されました。

次に、PPP 接続が終端されるバーチャル・インターフェースが追加されました。DIALs 機能用としての構成時に事業所ルーター内で追加されたダイヤルイン・インターフェースに類似しています。ただし、この場合は、ユーザーの着信が通るのは、V.34 インターフェースではなく、 L2TP トンネルです。

LNS 内では、バーチャル・インターフェースは、L2TP フィーチャー構成プロンプトで追加します (LAC 内では、talk 6 メイン・プロンプトで追加しました)。これについては、392ページの表150 に示してあります。

表 150. バーチャル・インターフェースを追加する

```
Corp Config>FEATURE Layer-2-Tunneling
Corp Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets:  [0]? 2
Add unnumbered IP addresses for each L2 net? [Yes]:
Adding device as interface 6
Defaulting Data-link protocol to PPP
Adding device as interface 7
Defaulting Data-link protocol to PPP
Enable IPX on L2T interfaces?(Yes or [No]):
Enable transparent bridging on L2T interfaces?(Yes or [No]):
Bridge configuration was not changed.

Restart router for changes to take affect.
Corp Layer-2-Tunneling Config>EXIT
```

L2 ネットを通して IP をルーティングするためには、インターフェースに IP アドレスを割り当てる必要があります。クライアントが L2TP トンネルを通して PPP 接続を確立すると、ルーターでは、そのルーティング・テーブルに自動的に静的ルートを追加し、これによって、リモート・ユーザーのネクスト・ホップが L2TP バーチャル・インターフェースの IP アドレスであることを示します。アドレスは、あて先 LAN セグメントとは異なるサブネット上にある必要があります。

これらのインターフェースの IP アドレスは、インターフェースの作成時に追加されます。デフォルトでは、非番号制 IP アドレスです。アドレスの形式は 0.0.0.n (ただし、 n はインターフェース番号) となります (例えば、インターフェース 7 の場合は、非番号制 IP アドレスは 0.0.0.7 になります)。

注: L2TP ネットに対応するデフォルトの IP アドレスは、 talk 6 の IP config プロンプトで変更できます。ただし、RLAN では、非番号制 IP アドレッシングが非常によく機能します。L2TP ネットへのユーザーの接続が任意であり、L2TP ネットに対応する特定の IP アドレスが余り重要ではないためです。

あて先へのネクスト・ホップが、ARP 要求を受信しているインターフェースとは異なるインターフェースを介しているとき、ルーターが ARP に応答できるようにするためには、ARP サブネット・ルーティングが使用可能にされている必要があります。これに該当するのは、クライアント IP アドレスはルーターの LAN インターフェースと同じサブネット上にあるが、ネクスト・ホップ (L2TP バーチャル・インターフェース) は別のサブネット上にあるような、RLAN の場合です。 ARP サブネット・ルーティングは、表151 に示されているようにして使用可能にします。

表 151. ARP サブネット・ルーティングを使用可能にする

```
Corp config>protocol ip
Corp IP config>ENABLE ARP-SUBNET-ROUTING
Corp IP config>EXIT
```

次に、クライアントが IP アドレスを取得するための方式を定義します。ネットワーク・ユーティリティー内の DIALs サーバーは、ユーザーが L2TP トンネルを通してトンネリングインするのではなく、ISDN や V.34 経由でダイヤルインしている場合と同じように構成する必要があります。 DIALs ユーザーには、接続したい LAN インターフェースと同じサブネット上にある IP アドレスが割り当てられる必要があります。使用可能な方式には、次の 5 つがあります。

Client (クライアント)
IP アドレスがクライアント上で構成されます。

User ID (ユーザー ID)
IP アドレスがユーザー ID 定義の一部としてルーター上で構成され、クライアントには認証時に送信されます。この場合は、IP アドレスは特定のユーザーに対応します。

Interface (インターフェース)
IP アドレスがインターフェース内で構成されて、クライアントに送信されます。この場合は、IP アドレスが対応するのは、ユーザー ID ではなく、インターフェースです。

DHCP Proxy (DHCP プロキシー)
IP アドレスは DHCP サーバーによって提供され、ルーターがクライアントの DHCP プロキシーを務めます。

IP Pool (IP プール)
IP プーリングを使用すると、プールに保管される IP アドレスのブロックをセットアップできます。クライアントが接続して、IP アドレスを要求すると、ルーターがプールからアドレスを検索します。

クライアントが IP アドレスを取得する方式は、グローバル DIALs メニューから構成します。クライアント、ユーザー ID、インターフェース、IP プールの各方式が使用可能にされます。ルーターは、最初に使用可能にされる (列挙されている順序) 方式を使用します。アドレスが IPCP 交渉時にクライアントに渡される、 1 次と 2 次のドメイン・ネーム・サーバーを定義することもできます。これについては、表152 に示してあります。

表 152. IP アドレスを取得するための方式を一覧表示させる

```
Corp Config>FEATURE DIALs
Dial-in Access to LANs global configuration
Corp Config>FEATURE DIALs
Dial-in Access to LANs global configuration
Corp DIALs config>LIST IP-ADDRESS-ASSIGNMENT
DIALs client IP address assignment:
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
```

この事例では、IP プールからの DIALs ユーザーの IP アドレスを割り振ります。これについては、表153 に示してあります。

表 153. DIALs ユーザー用の IP プールを追加する

```
Corp Config>FEATURE DIALs
Dial-in Access to LANs global configuration
Corp DIALs config>ADD IP-POOL
Base address []? 10.10.10.11
Number of addresses [1]? 20
Corp DIALs config>LIST IP-POOLS
Configured IP address pools:
     Base Address      Last Address        Number
     ------------      ------------        ------
      10.10.10.11       10.10.10.30            20
```

この時点では、トンネルは LNS と LAC の両方で構成され、DIAL フィーチャーは LNS 内で構成されています。ここでは、LNS にトンネリングする PPP ユーザーを構成する必要があります。トンネリングされる PPP ユーザーを構成する方法には、次の 2 通りがあります。

- **Rhelm ベースのトンネリング：** この方式を使用すると、ユーザーは LNS で定義するだけで済みます。形式は、username@domain を使用する必要があります (ただし、domain は LNS のホスト名)。クライアントが username@domain 形式 (例えば、Sharif@lns.org) を使用して LAC にダイヤルインすると、LAC が特定のドメイン (lns.org) へのトンネルを作成し、 PPP 接続が希望のあて先にトンネリングされます。この方式では、ドメイン名が同じユーザーは、すべて同じあて先にトンネリングされます。
- **ユーザー・ベースのトンネリング：** この方式では、ユーザーのプロファイルが LAC と LNS の両方で構成される必要があり、 username@domain 形式は使用しません。LAC では、ユーザーのプロファイル内で終端あて先を指定します。LNS では、通常のダイヤル呼び出しユーザーを構成します。

表154 には、データ・センターのネットワーク・ユーティリティーでの Rhelm ベースのユーザーの定義が示してあります。

表 154. Rhelm ベースの L2TP ユーザーを追加する

```
Corp Config>ADD PPP-USER
Enter name:  []? sharif@lns.org
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]?
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]


     PPP user name: sharif@lns.org
   User IP address: Interface Default
     Netroute Mask: 255.255.255.255
          Hostname:       Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
    Account Expiry:    Password Expiry:
Is information correct? (Yes, No, Quit): [Yes]

User 'sharif@lns.org' has been added
```

ユーザー・ベースのトンネリングの場合は、ID は LAC と LNS の両方で定義します。 表155 には、事業所の 2210 でのユーザー・ベース ID の定義が示してあります。このユーザーは、トンネリングされる設定で、ユーザーがダイヤルインすると、ルーターに L2TP トンネルのセットアップが指示されます。トンネルのもう一方のエンドポイントのあて先 IP アドレスが、トンネルの作成時に使用する 2210 のホスト名と共に指定されます。

表 155. 2210 (LAC) 内でユーザー・ベースのトンネリング・ユーザーを追加する

```
Branch Config>ADD PPP-USER
Enter name:  []? shoma
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No] y
Tunneling Protocol?  (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 10.10.101.2

     PPP user name: shoma
          TunnType: L2TP
          Endpoint: 10.10.101.2
    Local Hostname: lac.org

Is information correct? (Yes, No, Quit): [Yes] y

User 'shoma' has been added
```

注: ユーザーがトンネリングされることを指定すると、DIAL 機能がこのユーザーの場合に使用可能になっている必要があるのかについても、クライアントの IP アドレスはどれである必要があるかについても、 DIAL ユーザーの定義時にプロンプトで要求されるその他のパラメーターのどれについても、ルーターには尋ねようがありません。このユーザーの場合の DIAL 機能は、ネットワーク・ユーティリティーによって提供されているためです。2210 では、ネットワーク・ユーティリティーにゲートウェイ・サービスを提供しているだけです。

396ページの表156 には、データ・センターの 2216 での同じユーザー・ベース ID の定義が示してあります。ここでは、通常の DIAL ユーザーが定義されています。このユーザーは、トンネリングされたユーザーではありません。認証されるまでに、DIAL 機能によって認証され、L2TP ヘッダーはすべてはぎ取られ、パケットは通常の PPP パケットです。これで LNS の構成は完了です。

表 156. ネットワーク・ユーティリティー (LNS) でユーザー・ベースのトンネリング・ユーザーを追加する

```
Corp Config>ADD PPP-USER
Enter name:  []? shoma
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route?  (hostroute, netroute): [hostroute]
Number of days before account expires [0-1000] [0]?
Number of grace logins allowed after an expiration [0-100] [0]?
IP address: [0.0.0.0]?
Enter hostname: []?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No]
Disable user ? (Yes, No): [No]


     PPP user name: shoma
   User IP address: Interface Default
     Netroute Mask: 255.255.255.255
          Hostname:       Virtual Conn: disabled
      Time alotted: Box Default
     Callback type: disabled
          Dial-out: disabled
        Encryption: disabled
            Status: enabled
    Login Attempts: 0
    Login Failures: 0
  Lockout Attempts: 0
    Account Expiry:    Password Expiry:
Is information correct? (Yes, No, Quit): [Yes] y

User 'shoma' has been added
```

以上の変更をアクティブにするためには、ネットワーク・ユーティリティーを再始動する必要があります。

L2TP を監視する

構成が整ったので、L2TP と RLAN の構成がテストできます。L2TP は、最初に Rhelm ベースのユーザー ID を使用し、次にユーザー・ベースの ID を使用して、リモート PC からダイヤルインすることによってテストできます。

IP 接続は、PC クライアントからネットワーク・ユーティリティーへの PING を使用してテストできます。L2TP は、disp sub l2 all を使用して、ELS から監視できます。ネットワーク・ユーティリティー LNS からのサンプル talk 2 セッションが、397ページの表157 に示してあります。

表 157. ELS から L2TP を監視する

```
Corp *TALK 2
00:04:27   L2.052: Tunnel 7042/0 has 15 seconds to establish itself
00:04:27   L2.050: EVENT Rx-SCCRQ,tid=7042/0,state=Idle
00:04:27   L2.048: RCV l2tpGetHostname, tid=7042/0
00:04:27   L2.058: Peer TunnelID = 48802
00:04:27   L2.060: Peer Hostname = lac.org
00:04:27   L2.047: Tunnel 7042/48802 State Changed Idle -> Authorizing
00:04:27   L2.074: Upcall from AAA subsystem, request SUCCESS
00:04:27   L2.050: EVENT Continue-SCCRQ,tid=7042/48802,state=Authorizing
00:04:27   L2.048: RCV SCCRQ, tid=7042/48802
00:04:27   L2.058: Peer TunnelID = 48802
00:04:27   L2.060: Peer Hostname = lac.org
00:04:27   L2.058: Peer Rcv Window = 4
00:04:27   L2.058: Peer Challenge = 0
00:04:27   L2.049: SEND SCCRP, tid=7042/48802
00:04:27   L2.035: Tunnel Auth Create Challenge, Tid=7042/48802, Len=16
00:04:27   L2.035: Tunnel Auth Create Challenge Response, Tid=7042/48802,
Len=16
00:04:27   L2.044: Allocating UDP port 1026 for tunnelid=7042
00:04:27   L2.041: SND L2TP:F=C802,L=121,Tid=48802,Cid=0,NS=0,NR=1,O=0
00:04:27   L2.047: Tunnel 7042/48802 State Changed Authorizing -> Wait-ctl-cnn
00:04:27   L2.040: RCV L2TP:F=C800,L=42,Tid=7042,Cid=0,NS=1,NR=1,O=0
00:04:27   L2.050: EVENT Rx-SCCCN,tid=7042/48802,state=Wait-ctl-cnn
00:04:27   L2.048: RCV SCCCN, tid=7042/48802
00:04:27   L2.057: Processing Challenge Response from Peer 4.7.3.3
00:04:27   L2.039: NOTE:SCCCN: Tunnel Authenticated
00:04:27   L2.047: Tunnel 7042/48802 State Changed Wait-ctl-cnn -> Established
00:04:27   L2.040: RCV L2TP:F=C800,L=48,Tid=7042,Cid=0,NS=2,NR=1,O=0
00:04:27   L2.007: LNS Allocated L2 net 8
00:04:27   L2.020: RCV Inbound-Call-Request, callid=25642, net=8
00:04:27   L2.021: SEND Inbound-Call-Reply, callid=25642, net=8
00:04:27   L2.041: SND L2TP:F=C802,L=44,Tid=48802,Cid=1156,NS=1,NR=3,O=0
00:04:27   L2.013: L2TP Call 25642 State Changed Idle -> Wait Connect
00:04:27   L2.030: LNS Forcing LCP option ACFC
00:04:27   L2.039: NOTE:Proxy-LCP Callback received
00:04:27   L2.009: Call Rcv Proxy-Auth-Type AVP,attr=29,val=4,len=8,flag=8008
00:04:27   L2.009: Call Rcv SEQUENCING_REQUIRED AVP,attr=39,val=0,len=6,flag=800
00:04:27   L2.013: L2TP Call 25642 State Changed Wait Connect -> Established
00:04:27   L2.015: Call Established-LNS,net=8,speed=115200,flags=4802
00:04:27   L2.017: Using Proxy-LCP AUTH on net 8
00:04:27   L2.021: SEND Set-Link-Info, callid=25642, net=8
00:04:27   L2.041: SND L2TP:F=C802,L=36,Tid=48802,Cid=1156,NS=2,NR=4,O=0
00:04:27   L2.040: RCV L2TP:F=C800,L=12,Tid=7042,Cid=0,NS=4,NR=3,O=0
00:04:32   L2.022: L2TP PAYLOAD RCVD 53 bytes, net 8, callid=25642
00:04:32   L2.024: L2TP PAYLOAD SEND 6 bytes, net=8, callid=25642
00:04:32   L2.041: SND L2TP:F=6902,L=18,Tid=48802,Cid=1156,NS=1,NR=2,O=0
00:04:32   L2.024: L2TP PAYLOAD SEND 8 bytes, net=8, callid=25642
```

L2TP トンネル状態は、398ページの表158 に示されているように、talk 5 からチェックできます。

表 158. L2TP を Talk 5 から監視する

```
Branch *TALK 5

Branch +FEATURE Layer-2-Tunneling
Layer-2-Tunneling Information
Branch Layer-2-Tunneling Console> TUNNEL STATE
Tunnel ID │ Type │ Peer ID │    State    │ Time Since Chg │ # Calls │ Flags
    35589 │ L2TP │   58774 │ Established │     0: 1:24    │       1 │  TL
 F
Branch Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID │ Type │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │  ATO
    35589 │ L2TP │     108 │     7883 │     104 │     5388 │     5 │     5


Corp *TALK 5
Corp +FEATURE Layer-2-Tunneling
Layer-2-Tunneling Information
Corp Layer-2-Tunneling Console> TUNNEL STATE
Tunnel ID │ Type │ Peer ID │    State    │ Time Since Chg │ # Calls │ Flags
    58774 │ L2TP │   35589 │ Established │     0: 2: 9    │       1 │  TL
 F
Corp Layer-2-Tunneling Console> TUNNEL STATISTICS
Tunnel ID │ Type │ Tx Pkts │ Tx Bytes │ Rx Pkts │ Rx Bytes │  RTT  │  ATO
    58774 │ L2TP │     108 │     5540 │     112 │     8035 │     5 │     5
```

これで、IBM 2210 とネットワーク・ユーティリティーを使用するリモート LAN アクセスのための L2TP の構成と監視は完了しました。

第4部 付録および後付け

付録A. 特記事項

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

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

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

本書のオンライン・バージョンのご使用条件

弊社は、お客様に対して以下のことを許諾します。

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

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

情報処理装置等電波障害自主規制協議会 (VCCI) 表示

電波障害自主規制 届出装置の記述

注意:

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

商標

次の用語は、米国またはその他の国において IBM 社の商標です。

AIX	Microsoft	Parallel Sysplex
eNetwork	Nways	Presentation Manger
ESCON	NetView	VM/ESA
IBM	OS/2	

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

Java および Java ベースのすべての商標およびロゴは、米国およびその他の国における Sun Microsystems, Inc. の商標または登録商標です。

Microsoft、Windows、Windows NT、および Windows ロゴは、米国およびその他の国における Microsoft Corporation の商標です。

その他の会社名、製品名、およびサービス名は他社の商標またはサービス・マークになっている場合があります。

付録B. 安全上の注意

⚠ 危険

導入作業を開始する前に、安全に関する小冊子 **SD21-0030** の「最初にお読みください」**(Read This First)** の項をお読みください。この小冊子は、電気機器の安全な配線と接続の手順について説明しています。

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］

［ワ行］

［数字］

A

C

D

E

H

I

L

M

N

P

S

T

V

W

X

［特殊文字］

Printed in Japan

GA88-6548-01

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