

Tru64 UNIX

ネットワーク管理ガイド: 接続編

Part Number: AA-RQ30B-TE

2002 年 11 月

ソフトウェア・バージョン: Tru64 UNIX バージョン 5.1B 以上

本書では、ネットワークで動作するようにシステムを構成する方法、ネットワーク・サービスの構成方法、ネットワーク、ネットワーク・インタフェース、ネットワーク・サービスに関する日常管理作業について説明します。本書では、ネットワークおよびネットワーク・サービスに関する問題が発生した場合の解決方法についても説明しています。本書は、経験のあるシステム管理者またはネットワーク管理者を対象としています。

© 2002 日本ヒューレット・パッカード株式会社

本書の著作権は日本ヒューレット・パッカード株式会社が保有しており、本書中の解説および図、表は日本ヒューレット・パッカードの文書による許可なしに、その全体または一部を、いかなる場合にも再版あるいは複製することを禁じます。

日本ヒューレット・パッカードは、弊社または弊社の指定する会社から納入された機器以外の機器で対象ソフトウェアを使用した場合、その性能あるいは信頼性について一切責任を負いかねます。

本書に記載されている事項は、予告なく変更されることがありますので、あらかじめご承知おきください。万一、本書の記述に誤りがあった場合でも、弊社は一切その責任を負いかねます。

本書で解説するソフトウェア(対象ソフトウェア)は、所定のライセンス契約が締結された場合に限り、その使用あるいは複製が許可されます。

COMPAQ, Compaq ロゴ, Digital ロゴは U.S. Patent and Trademark Office に登録されています。Alpha, AlphaServer, NonStop, TruCluster, および Tru64 は米国 Compaq Computer Corporation の商標です。

Microsoft, Windows および Windows NT は米国 Microsoft 社の登録商標です。Intel は米国 Intel 社の登録商標です。Motif, OSF/1, UNIX, The Open Group および X/Open は、The Open Group の米国ならびに他の国における商標です。

このドキュメントに記載されているその他の会社名および製品名は、各社の商標または登録商標です。

原典 Network Administration: Connections (AA-RH9CD-TE)
Copyright ©2002 Hewlett-Packard Company

目次

まえがき

1 ネットワーク管理の概要

1.1	本書の概要	1-1
1.2	管理手法	1-2
1.2.1	SysMan Menu	1-3
1.2.1.1	クイック・セットアップ	1-4
1.2.1.2	ネットワーク・セットアップ・ウィザード	1-6
1.2.1.3	コマンド行の統合	1-7
1.2.2	Compaq Insight Manager	1-8
1.2.3	その他のインタフェース	1-9
1.2.4	構成ファイルの手動による編集	1-9
1.2.5	インストレーションと構成のクローニング	1-10

2 基本的なネットワーク接続

2.1	ネットワーク環境	2-2
2.1.1	ネットワーク・インタフェース	2-2
2.1.1.1	サブネットとの多重インタフェース接続	2-3
2.1.1.2	NetRAIN	2-5
2.1.1.3	リンク・アグリゲーション	2-7
2.1.2	ルーティング	2-9
2.2	構成の準備	2-10
2.2.1	インタフェースとデーモンのための情報	2-10
2.2.1.1	ネットワーク・インタフェース	2-11
2.2.1.2	Token Ring インタフェース	2-15
2.2.1.3	NetRAIN インタフェース	2-15

2.2.1.4	LAG インタフェース	2-15
2.2.1.5	rwhod デーモン	2-15
2.2.1.6	routed デーモン	2-16
2.2.1.7	gateways ファイル	2-17
2.2.1.8	gated デーモン	2-18
2.2.1.9	IP ルータ	2-19
2.2.2	ネットワーク・ファイルのための情報	2-19
2.2.2.1	スタティック・ルート・ファイル (/etc/routes)	2-20
2.2.2.2	ホスト・ファイル (/etc/hosts)	2-21
2.2.2.3	ホスト等価ファイル (/etc/hosts.equiv)	2-22
2.2.2.4	networks ファイル (/etc/networks)	2-23
2.3	ネットワーク構成要素の構成	2-23
2.3.1	ネットワーク・インタフェースの構成	2-24
2.3.2	rwhod デーモンの構成	2-27
2.3.3	routed デーモンの構成	2-27
2.3.4	gated デーモンの構成	2-29
2.3.5	IP ルータとしてのシステムの構成	2-30
2.3.6	スタティック・ルート・ファイルの構成	2-31
2.3.7	hosts ファイルの構成	2-33
2.3.8	hosts.equiv ファイルの構成	2-33
2.3.9	networks ファイルの構成	2-34
2.3.10	IP 別名の構成	2-35
2.4	多重ネットワーク・インタフェースの管理	2-36
2.4.1	NetRAIN の構成	2-36
2.4.2	NetRAIN の動作状況の監視	2-41
2.4.3	リンク・アグリゲーション・グループの構成	2-42
2.5	インタフェースでのアクセス・フィルタリングの設定	2-45
2.6	FDDI パラメータの表示と変更	2-45
2.7	トークン・リングのソース・ルーティングの管理	2-47

2.8	トークン・リング IP MTU のサイズの表示と変更	2-50
2.9	ネットワークのサービス品質の管理	2-51
2.9.1	トラフィック制御サブシステムの管理	2-52
2.9.2	RSVP の管理	2-53
2.9.2.1	rsvdpd の起動および終了	2-53
2.9.2.2	ネットワーク・インタフェースの追加および削除	2-54
2.9.2.3	RSVP セッション情報の表示	2-54

3 IPv6 (Internet Protocol Version 6)

3.1	IPv6 の歴史的背景	3-1
3.2	用語	3-2
3.3	IPv6 のアドレッシング	3-3
3.3.1	アドレスのテキスト表記	3-3
3.3.2	アドレスの種類	3-4
3.3.2.1	ユニキャスト・アドレス	3-5
3.3.2.2	エニーキャスト・アドレス	3-9
3.3.2.3	マルチキャスト・アドレス	3-9
3.3.3	アドレス・プレフィックス	3-11
3.3.4	アドレスの自動構成	3-11
3.3.5	アドレス解決	3-12
3.3.6	アドレス割り当て	3-13
3.3.6.1	集約可能グローバル・ユニキャスト・アドレス・ フォーマット	3-13
3.3.6.2	集約可能テスト・アドレス・フォーマット	3-15
3.4	トンネルを用いた IPv6 の展開	3-16
3.4.1	自動トンネル	3-16
3.4.2	6to4 トンネル	3-17
3.4.3	構成済みトンネル	3-18
3.5	IPv6 の環境	3-19

3.6	IPv6 のプランニング	3-24
3.6.1	カーネル内の IPv6 サポートの確認	3-24
3.6.2	構成の準備	3-25
3.6.2.1	DNS/BIND	3-29
3.6.2.2	6to4 トンネル	3-29
3.6.2.3	構成済みトンネル	3-30
3.6.2.4	ルータ	3-31
3.6.2.5	手動経路	3-32
3.6.3	IPv6 構成例のシステムの構成	3-32
3.6.3.1	シンプルなホスト対ホスト構成	3-32
3.6.3.2	ホスト対ホスト構成 (ルータあり)	3-33
3.6.3.3	IPv6 ネットワーク対 IPv6 ネットワーク構成 (ルータあり)	3-35
3.6.3.4	複数の IPv6 ネットワークと複数のルータがある構成	3-35
3.6.3.5	ホスト対ホスト構成 (IPv4 構成済みトンネルあり)	3-36
3.6.3.6	ホスト対ルータ構成 (IPv4 構成済みトンネルあり)	3-37
3.6.3.7	IPv6 ネットワーク対 IPv6 ネットワーク構成 (IPv4 構成済みトンネルあり)	3-39
3.6.3.8	6to4 トンネルの構成	3-41
3.7	システム上での IPv6 の構成	3-43
3.7.1	IPv6 ホストの構成	3-46
3.7.2	IPv6 ルータの構成	3-54
3.8	構成後の作業	3-62
3.8.1	6bone ネットワークへの接続	3-63
3.8.2	IPv6 用の新しいインタフェースの初期化	3-63
3.8.2.1	IPv6 インタフェース識別子の設定	3-64
3.8.3	インタフェースからの IPv6 の削除	3-64
3.8.4	構成済みトンネルの作成	3-65
3.8.5	インタフェースへのアドレスの追加	3-65

3.8.6	インタフェースからのアドレスの削除	3-66
3.8.7	省略時のルータの追加または削除	3-66
3.8.8	オンリンク・プレフィックス用の経路の手動追加	3-67
3.8.9	カーネルのルーティング・サポートの構成	3-67
3.8.10	実行時構成ファイルの編集	3-68
3.8.11	ルータ構成ファイルの編集	3-70
3.8.12	カーネル・サブシステムのチューニング	3-71
3.9	IPv6 デーモンのログ・ファイル	3-71

4 IPsec

4.1	IPsec 環境	4-1
4.1.1	ホスト対ホストの構成	4-2
4.1.2	セキュア・ゲートウェイ対セキュア・ゲートウェイの構成	4-2
4.1.3	ホスト対セキュア・ゲートウェイの構成	4-3
4.1.4	制限	4-4
4.2	セキュア接続	4-4
4.2.1	IPsec プロトコル	4-5
4.3	セキュリティ・アソシエーション	4-9
4.4	鍵交換	4-10
4.4.1	手動鍵交換	4-10
4.4.2	IKE	4-11
4.4.2.1	フェーズ 1 交換	4-11
4.4.2.2	フェーズ 2 交換	4-12
4.5	証明書	4-13
4.5.1	証明書のエンコーディング	4-14
4.5.2	証明書の使用に関するガイドライン	4-15
4.6	IPsec の計画	4-17
4.6.1	IPsec サブセットがインストールされていることの確認 ..	4-18
4.6.2	システムのネットワーク・トラフィックの記録	4-18

4.6.3	TruCluster への IPsec の実装	4-18
4.6.4	IPsec 実装ガイドラインへの準拠	4-19
4.6.5	システムの性能に対する IPsec の影響の削減	4-19
4.6.6	構成の準備	4-20
4.6.6.1	IPsec 接続のワークシート	4-22
4.6.6.2	IPsec プロポーザルのワークシート	4-25
4.6.6.3	IPsec カスタム・プロポーザルのワークシート	4-29
4.6.6.4	IKE プロポーザルのワークシート	4-32
4.6.6.5	IKE カスタム・プロポーザルのワークシート	4-35
4.6.6.6	IKE 認証のワークシート	4-37
4.6.6.7	公開鍵証明書のワークシート	4-40
4.6.6.8	IKE オプションのワークシート	4-42
4.6.6.9	手動鍵のワークシート	4-44
4.6.7	IPsec 構成例でのシステム構成	4-47
4.6.7.1	ホスト対ホスト接続の構成	4-47
4.6.7.2	セキュア・ゲートウェイ対セキュア・ゲートウェイ接 続の構成	4-50
4.6.7.3	ホスト対セキュア・ゲートウェイ接続の構成	4-54
4.6.7.4	特定のトラフィックに対する接続の構成	4-58
4.7	IPsec の構成	4-59
4.7.1	ホストの構成	4-59
4.7.2	セキュア・ゲートウェイの構成	4-63
4.8	構成後の作業	4-68
4.8.1	IPsec デーモンの管理	4-68
4.8.2	セキュリティ・アソシエーションのモニタリング	4-69
4.8.3	IPsec のモニタリング	4-71

5 Mobile IPv6

5.1	Mobile IPv6 の経緯	5-2
-----	-----------------------	-----

5.2	Mobile IPv6 の環境	5-2
5.3	Mobile IPv6 の動作	5-3
5.4	Mobile IPv6 の準備	5-7
5.4.1	カーネルでの IPv6 サポートの確認	5-8
5.4.2	カーネルでの Mobile IPv6 サポートの確認	5-8
5.5	Mobile IPv6 の構成	5-8
5.5.1	コレスポンデント・ノードの構成	5-9
5.5.2	コレスポンデント・ノードおよびルータの構成	5-9
5.6	Mobile IPv6 環境のモニタリング	5-10
5.6.1	tcpdump の使用	5-10
5.6.2	netstat の使用	5-10
5.6.3	IPv6 デーモンのログ・ファイル	5-11

6 ATM

6.1	ATM 環境	6-1
6.1.1	Classical IP 環境	6-2
6.1.2	LAN Emulation 環境	6-3
6.1.3	IP スイッチング	6-4
6.2	ATM の計画	6-6
6.2.1	ATM サブセットがインストールされていることの確認 ..	6-6
6.2.2	ATM のカーネルへの構成	6-7
6.2.3	構成の準備	6-8
6.2.3.1	アダプタに関する情報	6-8
6.2.3.2	Classical IP に関する情報	6-10
6.2.3.3	LAN エミュレーションに関する情報	6-13
6.2.3.4	IP スイッチングに関する情報	6-15
6.3	ATM の構成	6-17
6.3.1	ATM アダプタの構成	6-18
6.3.2	Classical IP の構成	6-19

6.3.2.1	ATM スイッチへの PVC マッピングの作成	6-20
6.3.2.2	atmhosts ファイルへのサーバの追加	6-20
6.3.2.3	hosts データベースへのホストの追加	6-21
6.3.2.4	ATM 設定アプリケーションの実行	6-22
6.3.2.5	Classical IP 論理インタフェースの構成	6-23
6.3.2.6	スタティック・ルートの追加 (SVC のみ)	6-24
6.3.2.7	PVC の構成の確認 (PVC のみ)	6-24
6.3.3	LAN エミュレーションの構成	6-24
6.3.3.1	atmhosts ファイルへのサーバの追加	6-24
6.3.3.2	hosts データベースへのホストの追加	6-25
6.3.3.3	ATM 設定アプリケーションの実行	6-25
6.3.3.4	LAN エミュレーション論理インタフェースの構成 ...	6-27
6.3.4	IP スwitチングの構成	6-27
6.3.4.1	hosts ファイルへの IP アドレスの追加	6-27
6.3.4.2	ATM 設定アプリケーションの実行	6-28
6.3.4.3	IP スwitチング論理インタフェースの構成	6-29
6.3.4.4	ルートの追加	6-29
6.4	ATM 環境の管理	6-30
6.4.1	ATM ネットワークと , ATM ネットワークに関する情報の 表示	6-30
6.4.2	シグナリング・モジュール	6-31
6.4.3	Classical IP 環境	6-31
6.4.4	LAN Emulation 環境	6-32
6.4.4.1	LAN Emulation Client の管理	6-32
6.4.4.2	LE-ARP テーブルの表示	6-32
6.4.5	IP スwitチング	6-32
6.4.6	ATM サブシステムのメッセージ	6-33

7 DHCP

7.1	DHCP 環境	7-2
7.1.1	DHCP パラメータの割り当て	7-3
7.1.2	DHCP とセキュリティ	7-5
7.2	DHCP の計画	7-5
7.2.1	DHCP ソフトウェアのインストールの確認	7-5
7.2.2	構成の準備	7-5
7.2.2.1	サーバ/セキュリティ・パラメータ	7-5
7.2.2.2	基本的な DHCP パラメータ	7-10
7.3	DHCP サーバの構成	7-14
7.3.1	サーバ/セキュリティ・パラメータの構成	7-15
7.3.2	IP レンジの構成	7-15
7.3.3	ホスト名リストの構成	7-16
7.3.4	サブネットワークの構成	7-17
7.3.5	DHCP クライアント・ノードの構成	7-17
7.3.6	グループ・パラメータの設定	7-19
7.3.7	DHCP サーバの起動 (joind)	7-20
7.4	DHCP の管理	7-21
7.4.1	DHCP クライアントの起動	7-22
7.4.2	DHCP クライアント構成のモニタリング	7-23
7.4.3	クライアント IP アドレスの永久的なマッピング	7-24
7.4.4	DHCP サーバへのアクセスの制限	7-25
7.4.5	BOOTP クライアントの構成	7-25
7.4.6	DHCP アドレス割り当ての無効化	7-26

8 ポイント・ツー・ポイント接続

8.1	SLIP (Serial Line Internet Protocol)	8-1
8.1.1	SLIP 環境	8-1

8.1.2	SLIP の計画	8-2
8.1.2.1	ハードウェアの確認	8-3
8.1.2.2	構成の準備	8-4
8.1.3	SLIP の構成	8-8
8.1.3.1	ダイヤル・イン・システムの構成	8-9
8.1.3.2	ダイヤル・アウト・システムの構成	8-10
8.1.4	SLIP ダイヤル・アウト接続の終了	8-12
8.2	PPP (Point-to-Point Protocol)	8-13
8.2.1	PPP 環境	8-13
8.2.1.1	chat スクリプト	8-15
8.2.1.2	PPP オプション	8-17
8.2.1.3	認証	8-18
8.2.2	PPP の準備	8-22
8.2.2.1	ハードウェアの確認	8-22
8.2.2.2	カーネルでの PPP サポートの確認	8-22
8.2.2.3	構成の準備	8-22
8.2.2.3.1	基本的な接続オプション	8-23
8.2.2.3.2	認証オプション	8-27
8.2.3	PPP を使用したダイヤル・アウト・システムの構成	8-30
8.2.3.1	ダイヤル・アウト・システムの初期通信の設定	8-30
8.2.3.2	ダイヤル・アウト・システムの options ファイルの作成	8-32
8.2.3.3	シークレット・ファイルの作成	8-33
8.2.3.3.1	PAP-secrets ファイルのエントリの作成	8-33
8.2.3.3.2	CHAP-secrets ファイルのエントリの作成	8-34
8.2.3.4	メッセージ・ロギングの設定	8-35
8.2.3.5	PPP 接続の開始	8-36
8.2.3.6	Microsoft Windows Remote Access Server への接続 ..	8-36
8.2.3.6.1	RAS サーバの構成	8-37

8.2.3.6.2	Microsoft CHAP の認証の問題の解決	8-38
8.2.4	PPP でのダイアル・イン・システムの構成	8-38
8.2.4.1	ダイアル・イン・システムの初期通信の設定	8-39
8.2.4.2	ダイアル・イン・システムの options ファイルの作成	8-40
8.2.5	PPP 接続のモニタリングと終了	8-41
8.3	モデム使用時のガイドライン	8-43
8.3.1	正しいモデム・ケーブルの使用方法	8-43
8.3.2	ダイアル・イン・アクセス用のシステムの構成	8-44
8.3.2.1	ダイアル・イン・アクセス用モデムの設定	8-45
8.3.3	ダイアル・アウト・アクセス用のシステムの構成	8-47
8.3.3.1	/etc/remote ファイルのエントリの作成	8-48

9 LAT 接続

9.1	LAT 環境	9-1
9.1.1	LAT 接続のタイプ	9-2
9.1.2	LAT ネットワークでのアクセス制御方法	9-3
9.1.3	リモート・サービスのパスワードの指定方法	9-4
9.1.4	負荷分散	9-5
9.2	LAT の計画	9-5
9.2.1	LAT サブセットがインストールされていることの確認 ...	9-5
9.2.2	カーネルでの DLB サポートの確認	9-5
9.2.3	構成の準備	9-6
9.3	LAT の構成方法	9-7
9.3.1	latsetup による LAT の構成	9-8
9.3.2	LAT のスタートおよび停止	9-9
9.3.3	LAT スタートアップ・ファイルの作成	9-9
9.3.4	inittab ファイルのカスタマイズ	9-11
9.3.5	特定のネットワーク・アダプタでの LAT の実行	9-12
9.4	LAT 接続の構成	9-12

9.4.1	プリンタの設定方法	9-12
9.4.1.1	ターミナル・サーバでのプリンタの設定方法	9-13
9.4.1.2	ポート構成のテスト方法	9-14
9.4.1.3	プリンタ用のサービス・ノードの設定方法	9-14
9.4.1.4	サービス・ノードでのプリント・スプーラの設定方法	9-15
9.4.1.5	プリンタのテスト方法	9-16
9.4.2	ホスト側が開始する接続の設定方法	9-16
9.4.2.1	ホスト側が開始する接続用のシステムの設定方法	9-16
9.4.2.2	プログラム・インタフェース	9-17
9.4.3	発信接続の設定方法	9-18
9.4.3.1	発信接続用のシステムの設定方法	9-18
9.4.3.2	プログラム・インタフェース	9-19
9.4.4	LAT/Telnet ゲートウェイの設定方法	9-19
9.4.5	専用またはオプションのサービスの作成方法	9-20
9.4.6	端末の専用 tty デバイスの提供	9-22
9.4.6.1	専用 tty デバイスの設定方法	9-22
9.4.6.2	専用 tty デバイスの削除方法	9-23

10 ネットワークおよびネットワーク・サービスに関する問題の解決

10.1	診断マップの使用方法	10-1
10.2	準備	10-2
10.3	IPv4 ネットワークに関する問題の解決	10-5
10.4	IPv6 ネットワークに関する問題の解決	10-10
10.4.1	IPv6 ホストに関する問題の解決	10-12
10.4.2	IPv6 ルータに関する問題の解決	10-19
10.4.3	Mobile IPv6 に関する問題の解決	10-26
10.5	IPsec に関する問題の解決	10-27
10.6	ATM に関する問題の解決	10-33
10.6.1	CLIP に関する問題の解決	10-35

10.6.2	LANE に関する問題の解決	10-38
10.6.3	IP スイッチに関する問題の解決	10-41
10.7	DHCP に関する問題の解決	10-44
10.8	SLIP に関する問題の解決	10-47
10.9	PPP に関する問題の解決	10-51
10.10	LAT に関する問題の解決	10-53
11	問題解決ツールの使用	
11.1	ネットワーク・インタフェースに関する情報の表示	11-1
11.2	ネットワーク・インタフェースの障害の検出	11-5
11.2.1	NIFF の構成と構成解除	11-6
11.2.2	NIFF イベントの表示	11-7
11.3	インターネット・ネットワーク・ホストへの接続テスト	11-8
11.4	ネットワーク統計情報の表示	11-11
11.5	インターネット (IPv4) アドレスから MAC アドレスへのアドレス変換テーブルの表示および変更	11-12
11.6	ネットワーク・ホストまでのデータグラムの経路の表示	11-13
11.7	ネットワーク上のパケット・ヘッダの表示	11-16
11.8	エラー・ログ・ファイルの表示	11-16
11.9	syslogd デーモンのメッセージ・ファイルの表示	11-17
12	ネットワークに関する問題の報告	
12.1	一般情報の収集	12-2
12.2	ハードウェア・アーキテクチャに関する情報の収集	12-2
12.3	ソフトウェア・アーキテクチャに関する情報の収集	12-3
A	ネットワーク・インタフェースの監視	
A.1	イーサネット・インタフェースの監視	A-1
A.2	FDDI インタフェースの監視	A-4

A.2.1	FDDI カウンタ	A-6
A.2.2	FDDI の状態	A-9
A.2.3	FDDI の特性	A-17
A.3	トークン・リング・インタフェースの監視	A-19
A.3.1	トークン・リング・カウンタ	A-21
A.3.2	トークン・リングおよびホストの情報	A-24

B IPsec のメッセージ

B.1	正常なステータス・メッセージ	B-1
B.2	起動時のエラー・メッセージ	B-1
B.2.1	一般的な起動時のエラー・メッセージ	B-1
B.2.2	手動鍵接続のエラー・メッセージ	B-4
B.3	IKE 折衝のエラー・メッセージ	B-7
B.3.1	フェーズ 1 のエラー・メッセージ	B-7
B.3.2	フェーズ 2 のエラー・メッセージ	B-9
B.4	ipsecd デモンのメッセージ	B-11

用語集

索引

例

2-1	単独の NetRAIN セットの作成	2-39
2-2	2 つの NetRAIN セットの作成	2-40
2-3	リンク・アグリゲーション・ステートメントの例	2-44
3-1	IPv6 ホストの構成変数の例	3-69
3-2	IPv6 ルータの構成変数の例	3-69
3-3	ip6rtrd.conf ファイルの例	3-70
9-1	/etc/latstartup.conf ファイルの例	9-10



1-1	SysMan Menu	1-4
1-2	Quick Setup	1-5
1-3	ネットワーク・セットアップ・ウィザード	1-6
1-4	Compaq Management Agents	1-8
2-1	シングル・インタフェース構成の例	2-2
2-2	1つのサブネット内での多重インタフェースの使用例	2-3
2-3	NetRAIN 構成の例	2-6
2-4	リンク・アグリゲーション構成の例	2-9
2-5	インタフェースおよびデーモン・ワークシート	2-11
2-6	ネットワーク・ファイル・ワークシート	2-20
3-1	MAC アドレスに基づくインタフェース ID の作成	3-6
3-2	シンプルなホスト対ホスト構成	3-19
3-3	ホスト対ホスト構成 (ルータあり)	3-20
3-4	IPv6 ネットワーク対 IPv6 ネットワーク構成 (ルータあり)	3-20
3-5	複数の IPv6 ネットワークと複数のルータがある構成	3-21
3-6	ホスト対ホスト構成 (構成済みトンネルあり)	3-21
3-7	ホスト対ルータ構成 (トンネリングあり)	3-22
3-8	IPv6 ネットワーク対 IPv6 ネットワーク構成 (構成済みトンネルあり)	3-23
3-9	6to4 構成	3-24
3-10	IPv6 構成ワークシート 1	3-26
3-11	IPv6 構成ワークシート 2	3-27
4-1	ホスト対ホストの構成例	4-2
4-2	セキュア・ゲートウェイ対セキュア・ゲートウェイの構成例	4-3
4-3	ホスト対セキュア・ゲートウェイの構成例	4-3
4-4	一般的な IPv4 パケット (保護なし)	4-6
4-5	一般的な IPv6 パケット (保護なし)	4-6

4-6	AH トランスポート・モードと AH トンネル・モードのパケット (IPv4)	4-7
4-7	AH トランスポート・モードと AH トンネル・モードのパケット (IPv6)	4-7
4-8	ESP トランスポート・モードと ESP トンネル・モードのパケット (IPv4)	4-8
4-9	ESP トランスポート・モードと ESP トンネル・モードのパケット (IPv6)	4-8
4-10	1 つのプロトコルに対して作成された SA	4-10
4-11	2 つのプロトコルに対して作成された SA	4-10
4-12	ワークシートの流れ図	4-21
4-13	IPsec 接続ワークシート	4-22
4-14	IPsec プロポーザル・ワークシート	4-26
4-15	IPsec カスタム・プロポーザル・ワークシート	4-30
4-16	IKE プロポーザル・ワークシート	4-33
4-17	IKE カスタム・プロポーザル・ワークシート	4-35
4-18	IKE 認証ワークシート	4-37
4-19	IPsec 公開鍵証明書ワークシート	4-40
4-20	IKE オプション・ワークシート	4-42
4-21	IPsec 手動鍵ワークシート	4-45
5-1	ホーム位置にあるモバイル・ノードとの通信	5-4
5-2	ホームから離れているモバイル・ノードとの通信 - その 1	5-5
5-3	ホームから離れているモバイル・ノードとの通信 - その 2	5-6
6-1	ATM ネットワークでの Classical IP	6-3
6-2	ATM ネットワークでのエミュレート LAN	6-4
6-3	ATM ネットワークでの IP スイッチング	6-6
6-4	ATM 設定ワークシート	6-9
6-5	ATM クラシカル IP ワークシート	6-11
6-6	ATM LAN エミュレーション・ワークシート	6-13
6-7	ATM IP スイッチング・ワークシート	6-16

7-1	DHCP の構成 (acme-net)	7-3
7-2	DHCP サーバ/セキュリティ・パラメータ・ワークシート	7-6
7-3	DHCP 基本パラメータ・ワークシート	7-10
8-1	単純な SLIP 構成のサンプル	8-2
8-2	ゲートウェイ・システムを使用した SLIP 構成	8-2
8-3	SLIP 設定ワークシート	8-4
8-4	単純な PPP の構成	8-14
8-5	ネットワーク PPP 構成	8-15
8-6	PPP 設定ワークシート	8-23
8-7	PPP 認証ワークシート	8-28
9-1	サンプルの LAT ネットワーク構成	9-2
9-2	LAT 設定ワークシート	9-6
10-1	診断マップの使用方法	10-2

表

2-1	多重インタフェース構成の比較	2-3
2-2	fddi_config コマンドのオプション	2-45
2-3	srconfig コマンドのオプション	2-48
3-1	周知のマルチキャスト・アドレス	3-11
3-2	IPv6 アドレス・タイプとプレフィックス	3-11
4-1	SysMan の省略時の接続	4-5
4-2	証明書のバイナリ・データをエンコードする方法	4-14
6-1	ATM カーネル・オプション	6-8
8-1	必須 startslip サブコマンド	8-6
8-2	オプションの startslip サブコマンド	8-7
8-3	slhosts ファイル・オプション	8-7
8-4	ダイヤル・アウト・アクセス用のモデム・コマンド	8-10
8-5	ダイヤル・イン・アクセス用のモデム・コマンド	8-46
9-1	LAT パラメータ	9-9

10-1	問題解決のスタート・ポイント	10-3
11-1	ping コマンドのオプション	11-9
11-2	netstat コマンドのオプション	11-11
11-3	tracert コマンドのオプション	11-13

まえがき

本書は、ネットワークのインタフェースとトランスポートを構成し、管理する方法、および Tru64 UNIX オペレーティング・システムが稼働しているシステムで発生するネットワーク関連の問題を解決する方法について説明します。

本書では、オペレーティング・システム・ソフトウェアおよび適切なネットワーク・サブセットがインストールされていることを前提としています。

本書の対象読者

本書は、ネットワーク・サービスの構成と管理を担当しているシステム管理者およびネットワーク管理者を対象にしています。管理者は、オペレーティング・システム概念、コマンド、および構成について理解する必要があります。また、伝送制御プロトコル/インターネット・プロトコル (TCP/IP) ネットワーク概念とネットワーク構成についての知識を持っていることも望まれます。本書は、TCP/IP ネットワークについて説明するためのものではありません。

新しい機能および変更された機能

『ネットワーク管理ガイド：接続編』の改訂内容は以下のとおりです。

- IPv6 (Internet Protocol Version 6) の章では、次のような変更があります。トンネル定義に関する新しい記述、エニーキャスト・アドレスに関する新しい項、自動トンネル、6to4 トンネル、構成済みトンネルを使用した IPv6 の導入に関する新しい項、構成ワークシートの変更、新しい 6to4 トンネル構成とそれに対応するワークシートの例、IPv6 ホストおよびルータを構成する手順の例の追加 (第 3 章)。
- IPsec (Internet Protocol Security) と IPsec をシステムに構成する方法に関する章が追加されました (第 4 章)。
- Mobile IPv6 と、コレスポンデント・ノードまたはルータ (またはその両方) としてシステムを構成する方法に関する章が追加されました (第 5 章)。

- ポイント・ツー・ポイント接続に関する章に、拡張構成ワークシートと PPP (Point-to-Point Protocol) オプションに関する説明が追加されました。
- 問題解決に関する章に Mobile IPv6 (10.4.3 項) と IPsec (10.5 節) に関する説明が追加されました。
- 問題解決ツールに関する章に、ネットワーク・インタフェースに関する情報の表示に関する節が追加されました (11.1 節)。
- IPsec メッセージを記載した付録が追加されました (付録 B)。

本書の構成

本書はいくつかの章から構成されており、各章でそれぞれ異なる接続やトランスポートの構成について説明します。その他、補足情報を記載した付録もあります。

次に、各章と付録の内容を示します。

- | | |
|--------|--|
| 第 1 章 | ネットワーク管理について説明し、本書で取り上げる各種の構成要素を紹介します。 |
| 第 2 章 | IPv4 (Internet Protocol Version 4) ネットワークでのネットワーク接続の基本的な管理作業について説明します。 |
| 第 3 章 | IPv6 (Internet Protocol Version 6) ネットワークの管理作業について説明します。 |
| 第 4 章 | IPsec (Internet Protocol Security) の管理作業について説明します。 |
| 第 5 章 | Mobile IPv6 の管理作業について説明します。 |
| 第 6 章 | ATM (Asynchronous Transfer Mode) ネットワーク接続の管理作業について説明します。 |
| 第 7 章 | DHCP (Dynamic Host Configuration Protocol) の管理作業について説明します。 |
| 第 8 章 | ポイント・ツー・ポイント接続の管理作業について説明します。 |
| 第 9 章 | LAT (Local Area Transport) の管理作業について説明します。 |
| 第 10 章 | ネットワークの問題を診断する方法について説明します。 |
| 第 11 章 | 問題解決に役立つ各種の診断ツールについて説明します。 |
| 第 12 章 | 問題をコンパックに報告する方法と、その際に用意すべき情報について説明します。 |

- 付録 A `netstat` コマンドを使用して、イーサネット、FDDI (Fiber Distributed Data Interface)、およびトークン・リングのネットワーク・インタフェースを監視する方法について説明します。
- 付録 B IPsec のエラー・メッセージとその原因について説明します。

関連情報

Tru64 UNIX のネットワーク機能および通信機能についての詳細は、以下のドキュメントを参照してください。

- 『ネットワーク管理ガイド：サービス編』
本書で取り上げる接続とトランスポートを使用するネットワーク・サービスについての情報を記載したマニュアルです。次に挙げるサービスとアプリケーションの構成と管理について説明しています。
 - DNS (Domain Name System)
 - NIS (Network Information Service)
 - NFS (Network File System)
 - UUCP (UNIX-to-UNIX Copy Program)
 - NTP (Network Time Protocol)
 - sendmail , POP (Post Office Protocol) および IMAP (Internet Message Access Protocol) を含むメール・システム
 - SNMP (Simple Network Management Protocol)
- 『Tru64 UNIX ユーザーズ・ガイド』
オペレーティング・システムのコマンドおよびシェルの基本的な使用方法について説明しています。
- 『JOIN Server Administrator's Guide』 -- Join Systems 社
ネットワークで Dynamic Host Configuration Protocol をインプリメントする方法について詳しく説明しています。このマニュアルは、Web ブラウザで次のファイルを開けば閲覧できます。
`/usr/doc/join/TOC.html`
- RFC (Request for Comments) 文書
本書では随所で、RFC 文書 (RFC 1577 など) をネットワーク関連トピックの詳しい参照先としています。RFC 文書では、インターネット標準、

新しい研究概念，およびインターネットに関するメモなどが発表されています。RFC の全文書と IETF (Internet Engineering Task Force) の詳細情報は，次の URL で閲覧できます。

<http://www.ietf.org>

- Best Practice

Tru64 UNIX の Best Practices ドキュメントでは，ネットワークに関するいくつかの概念と作業，およびその他のトピックについて説明しています。これらのドキュメントは，次の URL の Tru64 UNIX のドキュメント・サイトで閲覧できます。

<http://tru64unix.compaq.co.jp/document/>

公開鍵暗号化についての詳細は，『*Applied Cryptography: Protocols, Algorithms, and Source Code in C*』(second edition, John Wiley & Sons, Inc., 1996 by Bruce Schneier, ISBN 0-471-11709-9) を参照してください。

IPsec についての詳細は，『*IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*』(Prentice Hall, 1999 by Naganand Doraswamy and Dan Harkins, ISBN 0-13-011898-02) を参照してください。

本書の表記法

本書は，次の表記法を使用します。

%

\$

パーセント記号は，C シェルのシステム・プロンプトを表します。ドル記号は，Bourne シェル，Korn シェル，および POSIX シェルの場合のシステム・プロンプトを表します。

#

番号記号は root としてログインした場合のシステム・プロンプトを表します。

% cat

対話式の例における太字(ボールド体)は，ユーザが入力する文字を示します。

file

イタリック体(斜体)は，変数値，プレースホルダ，および関数の引数名を示します。

[|]
{ | }

構文定義では、大カッコはオプションの項目を示し、中カッコは必須項目を示します。大カッコまたは中カッコの中の項目を縦線で区切っている場合は、そこに併記されている項目の中から 1 つの項目を選択することを示します。

...

構文定義では、水平の反復記号は、前の項目を 1 回以上繰り返して使用できることを示します。

cat(1)

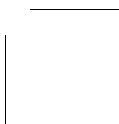
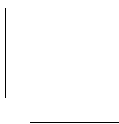
リファレンス・ページの参照には、該当するセクション番号をカッコ内に示します。たとえば、cat(1) は、cat コマンドについての情報が、リファレンス・ページのセクション 1 に記載されていることを示します。

Return

四角で囲まれたキー名はユーザがそのキーを押すことを示します。

Ctrl/x

この記号は、スラッシュの前に指定されているキーを押しながら、スラッシュの後のキーまたはマウス・ボタンを押すことを示します。例中では、このようなキーの組み合わせは、四角あるいは大カッコで囲まれて示されます(たとえば、Ctrl/C)。



ネットワーク管理の概要

ネットワーク管理には、ネットワーク・インタフェース、ソフトウェア、およびデーモンの設定と構成のための作業と、設定および構成されたインタフェース、ソフトウェア、デーモンの日常的な管理が含まれます。また、発生する問題の解決も、ネットワーク管理作業に含まれます。

この章では、次のトピックについて説明します。

- ネットワークの日常的な管理における本書の利用方法 (1.1 節)
- ネットワークの構成要素の管理に利用できる各種のユーティリティと手法 (1.2 節)

1.1 本書の概要

本書では、次の各項目の管理について説明します。

- イーサネット、トークン・リング、および FDDI (Fiber Distributed Data Interface) による基本的なネットワーク接続、ネットワーク・アダプタの自動フェイルオーバー (NetRAIN)、ネットワーク・デーモン (第 2 章)
- IPv6 (Internet Protocol Version 6) (第 3 章)
- IPsec (Internet Protocol Security) (第 4 章)
- Mobile IPv6 (第 5 章)
- ATM (Asynchronous Transfer Mode) (第 6 章)
- DHCP (Dynamic Host Configuration Protocol) (第 7 章)
- SLIP (Serial Line Internet Protocol)、PPP (Point-to-Point Protocol) などのポイント・ツー・ポイント接続 (第 8 章)
- LAT (Local Area Transport) (第 9 章)

ネットワーク・サービスとネットワーク・アプリケーションに関する情報は、別冊の『ネットワーク管理ガイド：サービス編』にまとめられています。

それぞれのネットワーク接続が備えている機能が異なるため、日常的な管理作業は、ネットワーク接続ごとに異なります。一般に、管理作業には、`/etc/hosts` ファイルへのホストの追加、新しい LAT デバイスの構成、状態情報の入手といった小規模な変更や調整が含まれます。本書の第 2 章～第 9 章では、これらの個々の作業を実施するための一般的な手順を、例や補足情報を交えて説明します。

本書には、ネットワークの接続とトランスポートの日常的な管理作業に関する情報に加え、発生する可能性がある問題の解決に役立つ情報も記載しています。問題の解決は毎日行わなければならない作業ではないため、管理作業とは分けて説明します。

管理の章とは異なり、問題解決の章は、問題別に構成されています。各問題の節には、その問題を解決するための手順を示します。

問題解決に成功する秘訣は、問題の原因を特定することです。複雑なネットワークや、ネットワーク・サービス間の相互作用によって、原因の特定が困難になることがよくあります。エラー・メッセージまたはイベント（たとえば遅いレスポンスなど）によって問題を検出した場合は、次の手順を実行してください。

1. 使用しているシステム、ネットワーク・インタフェース、およびネットワークへの接続部を調べます。
2. ネットワークを調べて、使用しているシステムがリモート・システムに接続できるかどうかを確かめます。

ほとんどの問題は、上記の 2 つの手順を実行すれば解決できます。それでも問題が解決できない場合は、該当する問題解決の節に進んで、その手順に従ってください。

1.2 管理手法

以下の各項では、オペレーティング・システムに含まれるネットワーク構成要素を管理するための手法を要約します。1.2.4 項で説明するように、ネットワーク構成作業に伴う構成ファイルの編集は、手作業で行うべきではありません。できる限り、SysMan Menu ユーティリティを使用してください。

1.2.1 SysMan Menu

SysMan Menu ユーティリティを使用すると、グラフィカル・ユーザ・インタフェース (GUI) またはコマンド行インタフェースを使用して、ローカルにシステムを管理することができます。さらに、World Wide Web を経由してシステムをリモート管理することも可能です。SysMan Menu ユーティリティでは、単独の階層型メニュー・インタフェースで Suitlet (統合ユーティリティ) を速やかに見つけて起動し、最も一般的な管理作業を実行することができます。

構成作業との関連で SysMan Menu ユーティリティについて言及している部分は、このユーティリティの起動方法をすでに理解していることを前提としています。CDE から SysMan Menu ユーティリティを起動するには、次の手順に従ってください。

1. CDE フロント・パネルの「アプリケーション・マネージャ」アイコンを選択します。
2. 「システム管理」アプリケーション・グループ・アイコンを選択します。
3. SysMan Menu を選択します。SysMan Menu が表示され、各種のシステム管理作業が一覧されます。

CDE を使用していない場合には、次のいずれかの方法で SysMan Menu を起動することができます。

```
# /usr/bin/sysman
```

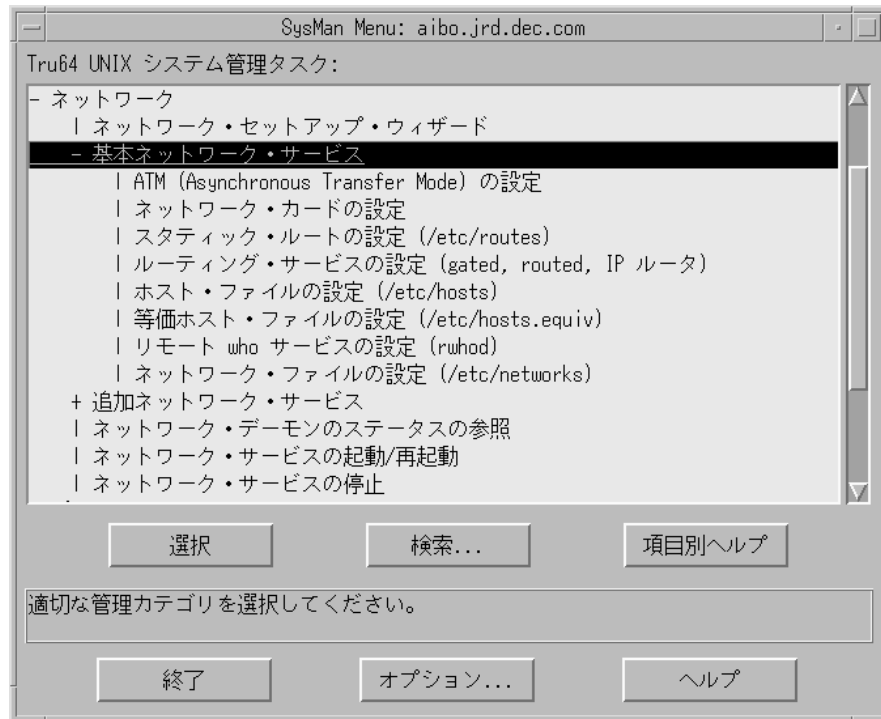
キャラクタセル端末または端末ウィンドウから curses モードで起動するには、次のように入力します。

```
# sysman -ui cui
```

SysMan Menu の起動後、メニュー項目を選択するには、その項目をダブルクリックします。グラフィック機能のないシステムで項目を選択するには、矢印キーと [Enter] キーを使用します。多くのメニュー項目では、さらに下位の選択項目が展開されます。適切な Suitlet が見つかるまで、メニュー操作を続けます。

図 1-1 では、[基本ネットワーク・サービス] メニュー項目が選択されています。このメニュー項目を展開すると、ネットワーク・アダプタや、その他の基本的なネットワーク構成要素を構成する Suitlet 群が表示されます。

図 1-1: SysMan Menu



SysMan Menu を終了するには、[終了] を選択します。グラフィック機能がないシステムでは、[Tab] キーを使用してカーソルを [終了] に移動し、[Enter] キーを押します。

SysMan Menu についての詳細は、『システム管理ガイド』，sysman(8)，およびオンライン・ヘルプを参照してください。

1.2.1.1 クイック・セットアップ

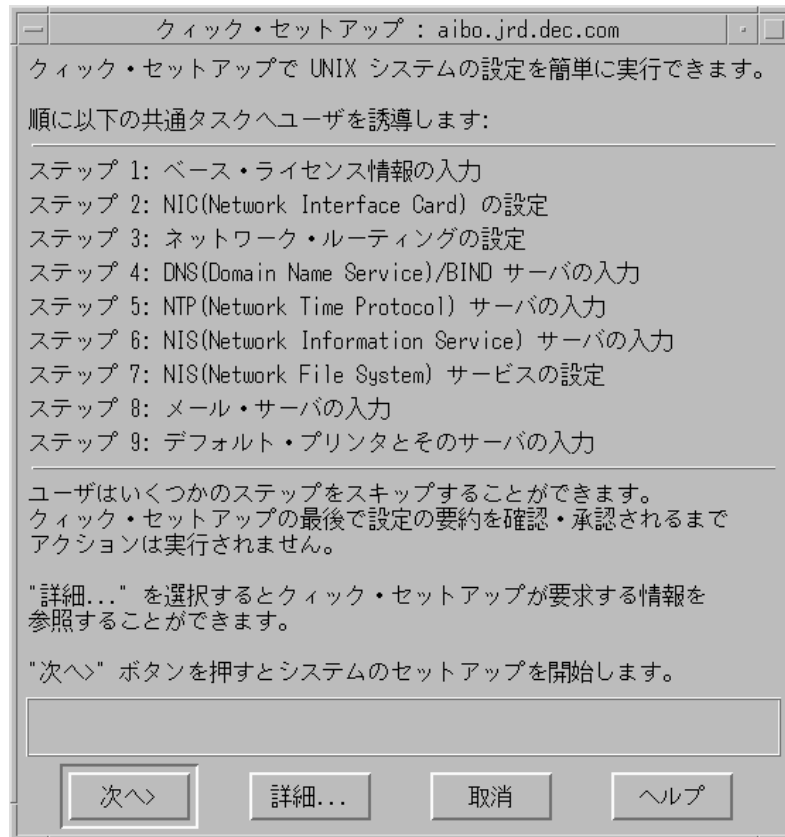
SysMan Menu には、クライアント・システムの基本的な構成要素とサービスを構成するために使用できるクイック・セットアップ・ユーティリティが含まれています。クイック・セットアップ・ユーティリティは、オペレーティング・システムのフル・インストール後にシステムをブートした場合に、自動的に起動されます。ただし、それ以外の場合にこのユーティリティを使用するには、SysMan Menu を起動して [一般的なタスク] → [クイック・セットアップ] を選択するか、次のコマンドをコマンド行に入力します。

```
# /usr/bin/sysman quicksetup
```

クイック・セットアップ・ユーティリティが表示されます (図 1-2 参照)。

1-4 ネットワーク管理の概要

図 1-2: Quick Setup



クイック・セットアップ・ユーティリティを使用すると、一連の構成手順が順を追って表示されます。これらの手順の多くは、システムをネットワーク上で稼働させる準備を行います。1つの手順から次の手順に進むには、情報を入力して[次へ]を選択します。入力していない情報があることに気付いた場合には、前の手順に戻ることができます。入力した情報は、最後の手順で[完了]を選択して構成を確定するまで保存されません。

クイック・セットアップ・ユーティリティの使用後には、必要に応じて他のコンポーネントを追加して構成したり、構成を変更することができます。クイック・セットアップ・ユーティリティについての詳細は、オンライン・ヘルプを参照してください。

1.2.1.2 ネットワーク・セットアップ・ウィザード

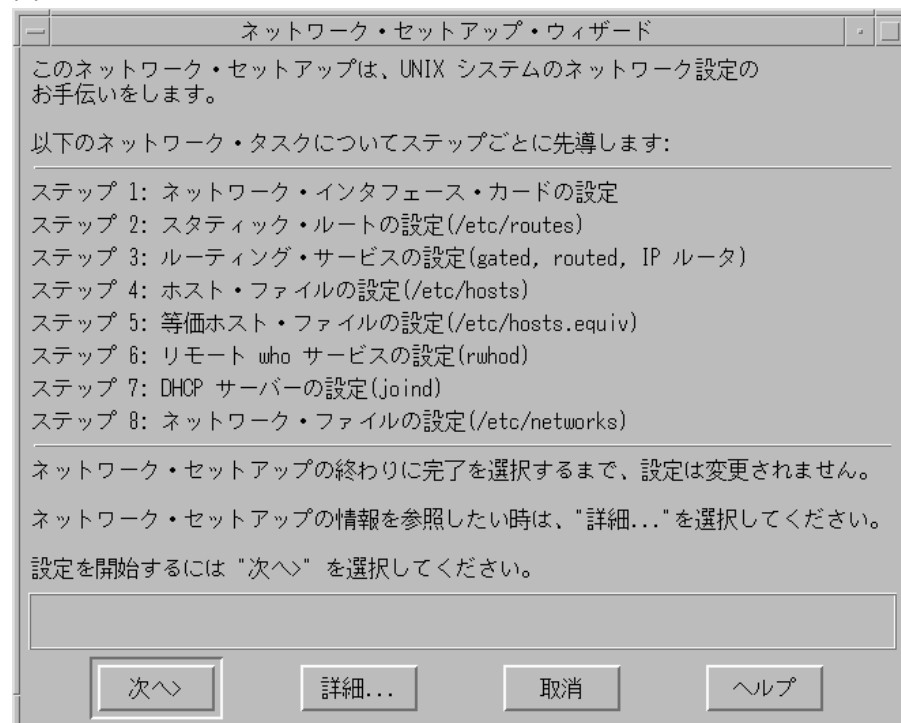
SysMan Menu には、システムのネットワーク構成要素の構成に使用できるネットワーク・セットアップ・ウィザード・ユーティリティもあります。SysMan Menu で構成 Suitlet を起動すれば、基本的なネットワーク・サービスを個別に構成できます。また、ネットワーク・セットアップ・ウィザードを使用すれば、基本的なネットワーク・サービスすべての設定処理を順を追って実行することができます。

ネットワーク・セットアップ・ウィザードを使用するには、SysMan Menu を起動して [ネットワーク → ネットワーク・セットアップ・ウィザード] を選択するか、またはコマンド行で次のコマンドを実行します。

```
# /usr/bin/sysman net_wizard
```

ネットワーク・セットアップ・ウィザード・ユーティリティが表示されます (図 1-3 を参照)。

図 1-3: ネットワーク・セットアップ・ウィザード



ネットワーク・セットアップ・ウィザード・ユーティリティを使用すると、一連の構成手順が順を追って表示されます。1つの手順から次の手順に進むには、情報を入力して [次へ] を選択します。入力していない情報があることに気付いた場合には、前の手順に戻ることができます。入力した情報は、最後の手順で [完了] を選択して構成を確定するまで保存されません。

さらに、ネットワーク・セットアップ・ウィザード・ユーティリティの使用後には、必要に応じて他の構成要素を追加して構成したり、構成を変更することができます。ネットワーク・セットアップ・ウィザード・ユーティリティについての詳細は、オンライン・ヘルプを参照してください。

1.2.1.3 コマンド行の統合

SysMan Menu では、さまざまな構成オプションにコマンド行から直接アクセスし、操作することができます。この機能は、管理者がサイト固有のシェール・スクリプトを作成して構成作業を実行する手段として、特に効果的です。

コマンド行インタフェースを使用するには、`sysman -cli` コマンドを実行します。このコマンドには引数として、処理対象の構成要素とグループ、および実行する処理を指定します。

たとえば、`/etc/hosts` ファイル内の全エントリを表示するとします。この処理は、次のコマンドで実行できます。

```
# sysman -cli -list values -comp networkedSystems \
-group hostMappings
```

`/etc/hosts` ファイルにホストを追加するには、次のコマンドを実行します。

```
# sysman -cli -add row -comp networkedSystems \
-group hostMappings -data "{queen} \
{DNS server} {18.240.32.40} {queen.abc.xyz.com}"
```

さらに、IP アドレスなど、`/etc/hosts` ファイル内の既存の値を変更することも可能です。変更を行うコマンドの例を、次に示します。

```
# sysman -cli -set val -comp networkedSystems \
-group hostMappings -attr networkAddress="18.240.32.45" \
-key1 queen.abc.xyz.com -key2 18.240.32.40
```

SysMan Menu のコマンド行インタフェースについての詳細は、『システム管理ガイド』および `sysman_cli(8)` を参照してください。

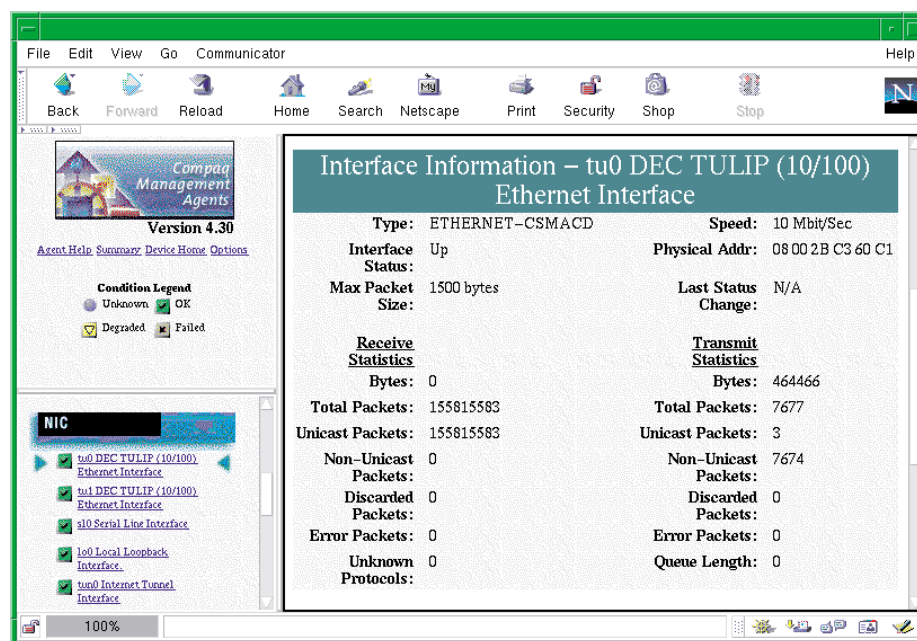
1.2.2 Compaq Insight Manager

Compaq Insight Manager は、Web ベースのシステム管理ユーティリティです。このユーティリティは Management Agents と Management Console という異なる 2 つの構成要素で構成されています。Management Agents は、Tru64 UNIX を含む多彩なオペレーティング・システム上で動作します。Management Console は、Microsoft Windows NT 専用です。

Tru64 UNIX システム上で Compaq Management Agents を有効にすると、システムと Web との間に通信経路が確立されます。一旦有効にすると、この経路により、任意のシステム上の Web ブラウザからシステムおよび周辺機器の構成に関する情報にアクセスできます。さらに、Java 対応の一部の Web ブラウザでは、このインターフェースを通して SysMan Menu を起動し、システムを管理することも可能です。

図 1-4 は、Management Agents を使用して、イーサネット・ネットワーク・アダプタの統計情報を入手する例です。

図 1-4: Compaq Management Agents



Compaq Insight Manager XE Management Console を使用すれば、システムだけでなく、プリンタやルータといった、ネットワーク上のさまざまな

スタンドアロン・デバイスの情報を参照したり管理することができます。Management Console は、サポートされているすべてのオペレーティング・システムや環境用の Management Agents と通信できるため、異種の環境を管理する手段として特に効果的です。

Compaq Insight Manager についての詳細は、`insight_manager(5)` および『システム管理ガイド』を参照してください。

1.2.3 その他のインタフェース

Tru64 UNIX オペレーティング・システムには、その他にも複数のシステム管理アプリケーションが含まれています。一部のアプリケーションはグラフィック機能を必要としますが、コマンド行からシステムを構成できるアプリケーションもあります。本書では、特定の構成作業で利用可能な場合、これらのユーティリティについて説明します。

利用可能なユーティリティの一覧は、『システム管理ガイド』の第 2 章を参照してください。各ユーティリティについての詳細は、リファレンス・ページとオンライン・ヘルプを参照してください。

1.2.4 構成ファイルの手動による編集

本書のいくつかの節では、管理作業を実行した場合に更新または修正されるシステム・ファイルについて説明しています。十分な経験のある UNIX 管理者の場合には、本書で説明しているユーティリティを起動するよりも、これらのファイルを手動で編集することによって、システムを管理する方法が好ましいかもしれません。ただし、システム・ファイルを更新する場合は、これらのファイルの構造が保持されるように、適切なユーティリティを使用することを推奨します。

重要な注意事項は、次のとおりです。

- コンテキスト依存のシンボリック・リンク (CDSL)

多くのシステム・ファイルは、TruCluster Server クラスタを使いやすくするために作成された、特別なシンボリック・リンクとして存在しています。このようなシンボリック・リンクは、ほとんどのユーザには透過的ですが、これらのリンクが壊れた場合は、再作成しない限り、システムがクラスタを結合することができなくなります。本書では、特に手動で作成しなければならない、ごく一部の CDSL について説明しています。ファイル・システムにある CDSL の完全なリストについては、リ

ファレンス・ページの `hier(5)` を参照してください。詳細については、『システム管理ガイド』を参照してください。

- バイナリ・データベースおよび構成定義

多くのシステム構成要素は、テキスト・ファイルおよびバイナリ・ファイルの両方にデータを書き込みますが、そのような構成要素の管理ユーティリティは、バイナリ・ファイルの方をたびたび再作成します。その他のシステム情報はたびたび保存され、システムを更新した場合に復元して再使用することにより、時間および労力を節約できるようにします。

- クラスタの内部的なサポート

個々のシステムは、TruCluster Server クラスタを結合することができ、多くのシステム・ファイルは、クラスタを内部的にサポートするように修正されました。たとえば、`rc.config` ファイルには、2 つの関連付けられたファイル、`rc.config.common` および `rc.config.site` ができたため、実行時構成変数を格納することができるようになりました。`rcmgr` ユーティリティを使用してこれらのファイルを変更することにより、これらのファイルの完全性および一貫性を保証します。

- アップデート・インストール

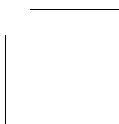
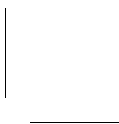
アップデート・インストールの実行時に、変更された情報は既存のシステム・ファイル内にマージされます。この処理では、`.new.*` および `.proto.*` ファイルが重要です。詳細については、『インストール・ガイド』を参照してください。

多くの場合、システム・ファイルを手動で編集するよりも、SysMan Menu ユーティリティを使用する方が最善の方法です。このため、本書ではこのユーティリティについて多くのことを説明しています。

1.2.5 インストールと構成のクローニング

Tru64 UNIX オペレーティング・システムには、インストール・クローニングと構成クローニングという 2 つのクローニング機能があります。これらのクローニング機能を使用すれば、システムのインストールと構成に伴う手間を最小限に抑えることができます。これらの機能は、同一構成のシステムを同じ方法でいくつもセットアップする場合に、特に効果的です。これは、すでに稼働しているシステムの構成を構成記述ファイル (CDF ファイル) に取り込み、このファイルを使用して残りのシステムのインストールと構成を行うことができるためです。

詳細については、『インストレーション・ガイド — 上級ユーザ編』を参照してください。



2

基本的なネットワーク接続

この章では、次の各トピックについて説明します。

- Tru64 UNIX の基本的なネットワーク環境 (2.1 節)
- ネットワーク構成の準備 (2.2 節)
- ネットワーク・コンポーネントの構成方法 (2.3 節)
- 多重ネットワーク・インタフェースの管理方法 (2.4 節)
- ネットワーク・インタフェースのアクセス・フィルタを有効化する方法 (2.5 節)
- FDDI のパラメータを表示および変更する方法 (2.6 節)
- トークン・リングのソース・ルーティングの管理方法 (2.7 節)
- トークン・リングの IP MTU のサイズを表示および変更する方法 (2.8 節)
- ネットワークのサービス品質 (QoS) の管理方法 (2.9 節)

注意

この章では、IPv4 (Internet Protocol Version 4) 環境でのネットワーク・インタフェースの構成について説明しています。このため、この章に出てくる IP (Internet Protocol) および TCP/IP (Transmission Control Protocol/Internet Protocol) は、すべて IPv4 を想定しています。IPv6 のネットワーク環境での構成についての詳細は、第 3 章を参照してください。

ATM の詳細については第 6 章を、ポイント・ツー・ポイント接続 (2 地点間接続) についての詳細は第 8 章を参照してください。

トラブルシューティング情報については 10.3 節を参照してください。

2.1 ネットワーク環境

システムをネットワークに接続するには、ネットワーク・インタフェース・カード (NIC) の設定方法と、他のシステムにメッセージをルーティングする方法を知っている必要があります。この節では、これらの方法の把握に役立つ情報を紹介します。

2.1.1 ネットワーク・インタフェース

コンピュータ・システムは NIC を介してネットワークに接続されます。(NIC は「ネットワーク・インタフェース」、あるいは「ネットワーク・アダプタ」とも呼ばれます。) エンド・システムやホストのネットワーク・インタフェースは、次の 4 通りの構成で実装できます。

- サブネットとのシングル・インタフェース接続
- サブネットとの多重インタフェース接続
- 自動フェイルオーバー機能を備えた多重インタフェース接続 (NetRAIN)
- 集約された多重インタフェース接続 (リンク・アグリゲーション)

ルータは通常、複数のインタフェースを備えており、各インタフェースはそれぞれ異なるサブネットに接続されます。図 2-1 のネットワークでは、ホスト A、ホスト B という 2 台のホストが、それぞれ 1 つのインタフェースを介してサブネットに接続されています。

図 2-1: シングル・インタフェース構成の例

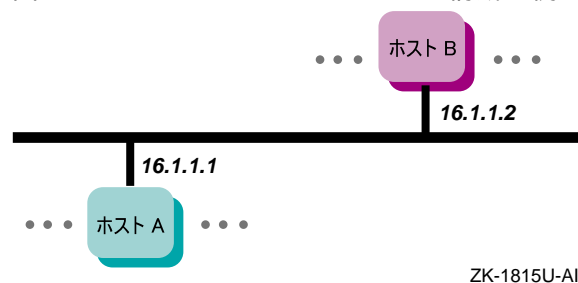


表 2-1 は、多重ネットワーク・インタフェースを使用する各構成の特徴を示しています。多重インタフェースを使用する場合には、この表を参考にして適切な構成を選択できます。

2-2 基本的なネットワーク接続

表 2-1: 多重インタフェース構成の比較

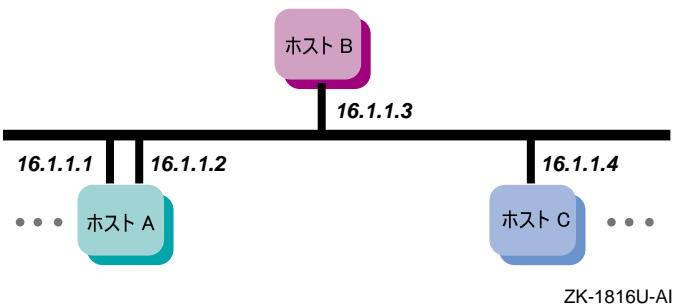
構成	特徴
サブネットとの多重インタフェース接続	高いスループットと，コネクション単位でのインタフェース間の負荷分散 (発信トラフィックのみ)
NetRAIN	信頼性と可用性
リンク・アグリゲーション (トランキング)	高いスループット，インタフェース間の負荷分散 (発信/着信トラフィック)，および可用性

以下の項では，これらの各構成について詳しく説明します。

2.1.1.1 サブネットとの多重インタフェース接続

1 つのシステムに，アクティブなネットワーク・インタフェースを複数設定することが可能であり，しかもそれぞれのネットワーク・インタフェースを同じサブネットに接続できます。図 2-2 のホスト A は，そのような構成の例です。このホストでは，インタフェース `tu0` に `16.1.1.1`，`tu1` に `16.1.1.2` をそれぞれ割り当て，双方で同じネットマスクを使用しています。

図 2-2: 1 つのサブネット内での多重インタフェースの使用例



コネクションの確立時には，カーネルによってコネクション数が最も少ないインタフェースが使用されます。その結果，各インタフェースのコネクション数が均等化されるため，1 つのネットワーク・アダプタでサブネットに接続しているシステムに比べ，より高いスループットが得られます。

この構成では NetRAIN のように信頼性が向上したり，フェイルオーバ機能が得られるわけではありません。あくまで，ネットワークにアクセスする経路が複数確保されるだけです。

システムとサブネット間のインタフェースを多重化する状況としては，次に挙げるような場合があります。

- 単独のサブネットで構成されるネットワークで、一部のシステムにより多くの帯域幅が必要になった場合。
- ネットワークのスループットを高める方法として、ネットワーク・インフラストラクチャを新しい高速技術 (ギガビット・イーサネットなど) にアップグレードする手段が採れない場合。
- 特定システムのネットワーク接続がスループットのボトルネックになっており、その一方で接続先スイッチの稼働率と、利用可能なポートおよび帯域幅に余裕がある場合。当該システムにネットワーク・インタフェースを増設すれば、リソースの競合が減少します。
- 使用できる IP サブネットが 1 つしかない環境で、1 つのネットワーク・インタフェースで可能な帯域幅以上の帯域幅が必要になった場合。

サブネットとのインタフェースを多重化したシステムを正しく動作させるためには、次に挙げるすべての条件を充足する必要があります。

- 次に挙げるいずれかの物理ネットワークであること。
 - イーサネット・スイッチ (10/100/ギガビット)
 - FDDI スイッチ
 - ATM CLIP (Classical IP)
 - ATM LANE (LAN Emulation)
 - PPP (Point-to-Point)
- ルーティング・デーモン (gated や routed) が動作していないこと。
- 同じサブネットに接続する各インタフェースを介して、すべてのリモート・システムにアクセスできること。たとえば、該当する各ネットワーク・インタフェースが単独で構成されていたとしても、同じリモート・システム宛てに ping コマンドを送信して、すべてのネットワーク・インタフェースで応答が得られる必要があります。したがって、各インタフェースは、いずれも同じ物理ネットワーク・スイッチに接続されている必要があります。

この構成は、コネクションが常に同じネットワーク・インタフェース上で維持されることを前提としたネットワーク・ソフトウェアやコマンドに影響を与える可能性があります。具体的な例を次に示します。

- マルチキャスト送信が正しく機能しない可能性がある。

- 使用されるネットワーク・インタフェースがパケットごとに切り替わることがあるため、`traceroute` などのユーティリティでは整合性のある結果が得られない可能性がある。

この機能には、特別な設定は必要ありません。2.3.1 項の説明に従って各ネットワーク・インタフェースを構成し、それぞれのインタフェースに同じサブネットの IP アドレスを割り当てます。

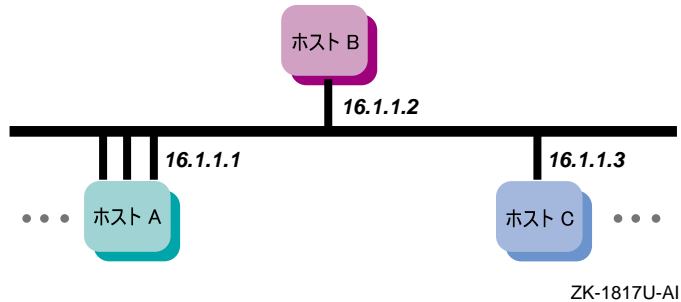
ネットワーク・インタフェースを構成すると、特に指定しなくても、インタフェース経路が自動的にルーティング・テーブルに追加されます。`route` コマンドや `/etc/routes` ファイルを使用して経路を明示的に追加する場合には、多重インタフェースの経路を追加する方法について、`route(8)` の説明を参照してください。明示的に経路を追加する場合としては、たとえば多重インタフェースのデフォルト経路を追加する場合などが考えられます。カーネルのルーティング・テーブルを表示する方法については、`netstat(1)` を参照してください。

2.1.1.2 NetRAIN

NetRAIN (Redundant Array of Independent Network Adapters) インタフェースは、さまざまな種類の障害からネットワーク接続を保護するメカニズムです。

NetRAIN は、同じ LAN (ローカル・エリア・ネットワーク) セグメントに接続された複数のネットワーク・インタフェースを、NetRAIN セットと呼ばれる 1 つの仮想インタフェースとして統合します。この仮想インタフェース内では、いずれか 1 つのネットワーク・インタフェースが常にアクティブになっており、残りのインタフェースは休止しています。アクティブなインタフェースで障害が発生すると、フェイルオーバー時間と呼ばれる時間間隔内に、休止していたいずれか 1 つのインタフェースが同じ IP アドレスを引き継いでアクティブになります。フェイルオーバー時間は調整可能です。図 2-3 のホスト A は、NetRAIN セットとして構成された 3 つのインタフェースを備えています。この NetRAIN 仮想インタフェースには、IP アドレス 16.1.1.1 が割り当てられています。

図 2-3: NetRAIN 構成の例



NetRAIN 構成の詳細については、2.4.1 項を参照してください。

NetRAIN は、発生した障害を検出して報告する NIFF (Network Interface Failure Finder) を使ってネットワーク・インタフェースの状態を監視します。NIFF は NetRAIN とは独立に使用することも可能です。NIFF の詳細については、`niff(7)` を参照してください。

MAC アドレスに基づくライセンス認証と NetRAIN

ネットワーク・アダプタの MAC (Media Access Control) アドレスを使ってマシンを識別するライセンス認証方式は、NetRAIN による MAC アドレスの切り替えの影響を受ける可能性があります。

すべてのネットワーク・ドライバは、インタフェースの MAC アドレスを取得する `SIOCRPHYSADDR ioctl` をサポートしています。この `ioctl` は次の 2 つのアドレスを含む配列を返します。

- ハードウェアのデフォルト・アドレス
LAN アダプタの内蔵 PROM から取り出した固定的なアドレス
- 現在の物理アドレス
ネットワーク上の通信に使われるアドレス

MAC アドレスに基づくライセンス方式では、`SIOCRPHYSADDR ioctl` が返すハードウェアのデフォルト・アドレスを使用する必要があります。現在の物理アドレスは NetRAIN が必要に応じて変更するため、使用しないでください。`SIOCRPHYSADDR ioctl` を使用したサンプル・プログラムについては、使用しているネットワーク・アダプタのリファレンス・ページ (`ln(7)` や `tu(7)` など) を参照してください。

2.1.1.3 リンク・アグリゲーション

リンク・アグリゲーション (トランキング) とは、1 枚以上の物理イーサネット NIC をまとめ、1 つの論理リンクを形成する技術です。(上位層で動作するソフトウェアは、このリンク・アグリゲーション・グループを 1 つの論理インタフェースとして認識します。) 論理リンク上のトラフィックはリンク・アグリゲーション・グループを構成する各物理ポートに分散されるため、単独のインタフェースに比べ、より高速に伝送されます。

リンク・アグリゲーションには次に挙げる利点があります。

- ネットワーク帯域幅の拡張
リンク・アグリゲーション・グループを構成するポート (NIC) の数と、各ポートの速度に比例して帯域幅が拡張されます。
- フォールト・トレランス
リンク・アグリゲーション・グループに含まれるいずれかのポートで障害が発生すると、ソフトウェアによって障害が検出され、他の利用可能なポートにトラフィック経路が変更されます。この機能は、DEGPA (alt) デバイス、DEGXA (bcm) デバイス、DE60x (ee) デバイスでのみ使用できます。
- 負荷の均等化
リンク・アグリゲーション・グループを構成する各ポート間では、着信トラフィックと発信トラフィックの負荷がともに均等化されます。パケットの送信時に、システムが負荷分散アルゴリズムを使って送信ポートを決定します。次に挙げる負荷分散アルゴリズムがサポートされています。

宛先 IP アドレス

IP パケットの場合は宛先 IP アドレスのハッシュ、IP 以外のパケットの場合は宛先 MAC アドレスのハッシュを基に、使用するポートが決定されます。特定のアドレス宛てに送信されるトラフィックでは、すべてリンク・アグリゲーション・グループ内の同じポートで伝送されるため、宛先には正しい順序でパケットが届きます。

宛先 MAC アドレス

宛先 MAC アドレスのハッシュに基づいてポートが選択されます。特定の MAC アドレス宛てに送信されるトラフィックではす

べて、リンク・アグリゲーション・グループ内の同じポートが使用されます。

トランスポート・ポート番号

システムから送信される TCP や UDP のパケットの場合、送信元および宛先の TCP または UDP ポート番号のハッシュに基づいてポートが選択されます。他のパケット (システムによって転送された TCP および UDP パケットなど) の場合は、宛先 IP アドレス (dstip) アルゴリズムが使用されます。特定の送信元 + 宛先ポートのペアに対するトラフィックではすべて、リンク・アグリゲーション・グループ内の同じポートが使用されます。

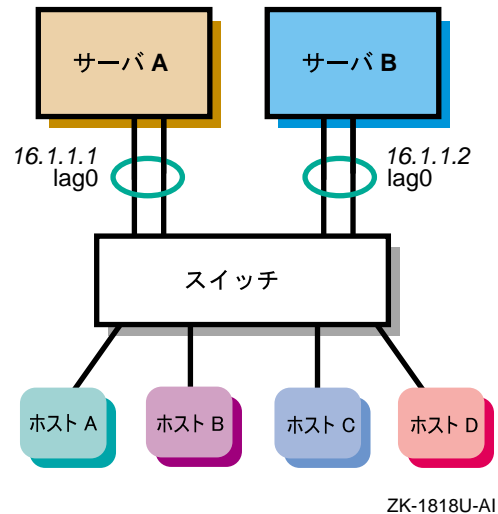
ラウンド・ロビン

ポートはサイクリックに選択されます。

各アルゴリズムとその使用方法、帯域幅の利用については、lag(7) を参照してください。

リンク・アグリゲーション・グループによる仮想インタフェースは、サーバ間およびサーバ/スイッチ間のポイント・ツー・ポイント接続に使用できます。図 2-4 はリンク・アグリゲーション構成の例を示しています。図中のサーバ A、サーバ B は、どちらも 2 つのインタフェースで構成されるリンク・アグリゲーション・グループを介して 1 つのスイッチに接続されており、各リンク・アグリゲーション仮想インタフェースには IP アドレスが 1 つずつ割り当てられています。

図 2-4: リンク・アグリゲーション構成の例



リンク・アグリゲーションの構成方法については、2.4.3 項を参照してください。

2.1.2 ルーティング

ネットワークに接続されているすべてのシステム（ホストおよびルータ）は、他のネットワーク上のシステムとの通信を可能にするためには、ネットワーク・ルーティングをサポートするように構成する必要があります。ルーティングとは、ネットワーク上の 1 つのシステムから他のシステムに送信されるパケットの伝送経路を指定することです。他のネットワーク上のシステムとの通信も、ルーティングによって可能になります。ルーティングで使用する経路は、各システムのルーティング・テーブルまたはルーティング・データベースに登録されます。これらのテーブルやデータベース内の経路エントリは、次に挙げるデータから構成されています。

- 宛先アドレス（ネットワークまたはホスト）
- そのシステムから宛先システムまでの間で次に位置するホップのアドレス
- そのシステムのネットワーク・アドレス（経路がインタフェースを介する場合）
- ネットワーク・インタフェース（tu0, fta0 など）
- 路離（ホップ数, MTU など）

システムを構成すると、ループバック・インタフェース (lo0) の経路が自動的に設定されます。さらに、システム構成に追加した各インタフェースの経路は、SysMan のインタフェース設定アプリケーションで設定できます。また、次のいずれかの方法を使用すれば、その他の経路を追加できます。

- ネットワーク・マップを基に手作業で経路を登録する方法。この方法で登録した経路は静的経路と呼ばれます。ネットワークの物理構成を変更した場合、ノードのアドレスやサブネットに変更があれば、それを各システム上のルーティング・テーブルに反映する必要があります。
- gated デモンまたは routed デモンを実行し、経路を動的に生成、保守、および更新する方法。このような経路は動的経路と呼ばれます。ネットワークの物理構成を変更すると、これらのデモンが他のノードやルータからのメッセージを受信して、ルーティング・テーブルのエントリを自動的に変更します。

上記の方法のほか、ICMP (Internet Control Message Protocol) のリダイレクト・メッセージを基に、ルーティング・テーブルに経路が追加される場合もあります。このメッセージはルータからホストに送信され、ローカル・ネットワーク上の他のルータにトラフィックを転送するように要求します。2.2 節 には、ルーティング方法の種類と、適切な方法を選択するうえで役立つ情報が示されています。

2.2 構成の準備

ネットワーク設定アプリケーションを使用して、ネットワーク構成要素を構成します。この後の項には、ネットワーク構成要素の構成に必要な情報を記録するためのワークシートが含まれています。

2.2.1 インタフェースとデーモンのための情報

図 2-5 に、インタフェースおよびデーモンのワークシートを示します。以降の各項目では、このワークシートに記録する際に必要な情報について説明します。本書をオンラインで参照している場合には、プリント機能を使用して、このワークシートをプリントできます。

図 2-5: インタフェースおよびデーモン・ワークシート

インタフェースおよびデーモン・ワークシート	
すべてのネットワーク・インタフェース	
アダプタ名:	_____
ホスト名:	_____
インターネット・アドレス・ソース:	DHCP サーバ <input type="checkbox"/> ユーザ指定 <input type="checkbox"/>
インターネット・アドレス:	_____
ネットワーク・マスク:	_____
Token Ring インタフェース	
アダプタ・スピード:	_____
NetRAIN インタフェース	
セット・メンバ:	_____
Link Aggregation インタフェース	
ポート:	_____
rwhod デーモン	
rwhod:	Yes <input type="checkbox"/> No <input type="checkbox"/>
フラグ:	ブロードキャストのみ <input type="checkbox"/> Listen のみ <input type="checkbox"/> 両方 <input type="checkbox"/>
routed デーモン	
routed:	Yes <input type="checkbox"/> No <input type="checkbox"/>
フラグ:	<input type="checkbox"/> ゲートウェイ・ホストで routed を実行 <input type="checkbox"/> すべてのパケットを標準出力へ出力 <input type="checkbox"/> デバッグ情報を記録
RIP データ:	供給 <input type="checkbox"/> 供給しない <input type="checkbox"/>
gateways ファイル	
デスティネーションのタイプ:	ネット <input type="checkbox"/> ホスト <input type="checkbox"/>
デスティネーション:	_____
ゲートウェイ:	_____
ホップ・カウント:	_____
ルート・タイプ:	外部 <input type="checkbox"/> Passive <input type="checkbox"/> Active <input type="checkbox"/>
gated デーモン	
gated:	Yes <input type="checkbox"/> No <input type="checkbox"/>
構成ファイル:	_____
IP ルータ	
IP ルータ:	Yes <input type="checkbox"/> No <input type="checkbox"/>

2.2.1.1 ネットワーク・インタフェース

アダプタ名

ネットワーク・インタフェースのデバイス名です。オペレーティング・システムでサポートされているネットワーク・インタフェースのいくつかを以下に示します。

インタフェース	デバイス名
イーサネット	ee
	le
	ln
	tu
	xna
FDDI (Fiber Distributed Data Interface)	faa
	fta
	fza
ギガビット・イーサネット	alt
トークン・リング	tra

2.4.1 項に示すように NetRAIN インタフェースを構成している場合、アダプタ名は NetRAIN セットの仮想デバイス名 (nr) です。一方、リンク・アグリゲーション・グループを構成している場合には、2.4.3 項で説明するように、アダプタ名はグループの仮想デバイス名 (lag) になります。

ホスト名

使用しているシステムに割り当てられている完全修飾ホスト名。完全修飾ホスト名は、ホスト名とドメイン名からなります。ホスト名と各レベルのドメイン名は、ピリオド (.) で区切ります。ホスト名については、ネットワーク管理者にお問い合わせください。

インターネット・アドレス・ソース

イーサネット、FDDI、NetRAIN インタフェースに関する、システムのネットワーク・アドレスのソース。DHCP (Dynamic Host Configuration Protocol) サーバを使用してブート時に各システムに IP アドレスを割り当てている場合は、「DHCP サーバ」をチェックします。システム構成の一部として IP アドレスやネットワーク・マスクを割り当てる場合は、「ユーザ指定」をチェックします。

インターネット・アドレス

使用しているシステムのインターネット・プロトコル (IP) アドレス。IP アドレスをあてがう場合は、このスペースに記入します。一時的

に IP アドレスを割り当てるのに DHCP を使用する場合は、このスペースは空欄のままにします。

ネットワークに指定 IP アドレスがない場合は、以下のサービスから取得する必要があります。ネットワーク・アドレスを取得したら、固有の IP アドレスとホスト名をネットワーク上の各システムに割り当ててください。

ネットワークのインターネット・アドレスの取得については、下記にお問い合わせください。

American Registry for Internet Numbers
4506 Daly Drive, Suite 200
Chantilly, VA 20151

Voice: (703) 227-0660
FAX: (703) 227-0676
Email: reg-services@arin.net (一般的なお問い合わせ)
hostmaster@arin.net (IP アドレスの登録)
WWW: <http://www.arin.net>

ヨーロッパでは、下記にお問い合わせください。

RIPE Network Coordination Center
Singel 258
1016 AB Amsterdam
The Netherlands

Voice: +31 20 535 4444
FAX: +31 20 535 4445
E-mail: ncc@ripe.net (一般的なお問い合わせ)
hostmaster@ripe.net (IP アドレスの登録)
WWW: <http://www.ripe.net>

アジアおよび太平洋地域では、下記にお問い合わせください。

Asia Pacific Network Information Center
Level 1, 33 Park Road
P.O. Box 2131
Milton, QLD 4064
Australia

Voice: +61 7 3367 0490
FAX: +61 7 3367 0482
E-mail: info@apnic.net (一般的なお問い合わせ)
hostmaster@apnic.net (IP アドレスの登録)

WWW: <http://www.apnic.net>

注意

インターネット・ネットワークに接続する予定がない場合でも、NIC にネットワークを登録してください。登録しておく、後からインターネット・ネットワークへの接続を決めた場合でも、ネットワークのホスト・アドレスのすべてを変更する必要がなくなります。

ネットワーク・マスク

ネットワークのサブネット・マスク。サブネットワークを使用すると、LAN に接続されている各システムを、1 つのアドレスによってインターネット・ネットワークに認識させることができます。一方、ローカルではそれらのシステムを、一連のアドレスによって認識させることができます。サブネットワークはホスト、つまり異なる物理ネットワークを論理的にグループ化したものとして表すことができます。ネットワークでサブネットワーク・ルーティングを使用する場合は、ネットワーク上の各システムで同じサブネット・マスクが定義されている必要があります。

次の表を利用して、使用しているサブネット・マスクを確認してください。サブネットワークを使用しない場合は、 n はゼロ (0) です。それ以外の場合、 n は 1 ~ 255 です。

クラス	IP アドレスの範囲	サブネット・マスク
A	0.0.0.0 ~ 127.0.0.0	255. n . n . n
B	128.0.0.0 ~ 191.0.0.0	255.255. n . n
C	192.0.0.0 ~ 223.0.0.0	255.255.255. n

サブネットワーク・ルーティングを使用している既存のネットワークに自分のシステムを接続する場合は、ネットワーク管理者に正確なサブネット・マスクをお問い合わせください。

2.2.1.2 Token Ring インタフェース

アダプタ・スピード

ご使用のシステムが Token Ring をサポートしている場合、システムの Token Ring アダプタの速度を指定します。4Mb/s と 16Mb/s の 2 つの速度をサポートしています。省略時の速度は、16Mb/s です。

2.2.1.3 NetRAIN インタフェース

NetRAIN インタフェースは、複数のネットワーク・アダプタを備えたシステムの可用性を向上させます。詳細については、2.1.1.2 項を参照してください。

セット・メンバ

NetRAIN セットの一部であるネットワーク・インタフェースのデバイス名です。NetRAIN セット内のいずれかのインタフェースが機能を停止した場合、NetRAIN はこのリストにある他のインタフェースにフェイルオーバーします。

2.2.1.4 LAG インタフェース

リンク・アグリゲーション・インタフェースは、複数のネットワーク・アダプタを備えたシステムに、より高い可用性とフォールト・トレランス、および負荷分散をもたらします。詳細については、2.1.1.3 項を参照してください。

ポート

リンク・アグリゲーション・グループ内のポートとして使用しているネットワーク・インタフェースのデバイス名。グループ内のいずれかのインタフェースで障害が発生すると、そのインタフェースを経由していたトラフィックは、他の利用可能な 1 つ以上のポートに移されます。

2.2.1.5 rwhod デーモン

rwhod は、rwho プログラムおよび ruptime プログラムで使用されるデータベースの保守を行うデーモンです。これらのプログラムは、システムとシステムの現在のユーザに関する情報を、リモート・システムのユーザに提供します。

rwhod

rwhod デーモンを実行する場合は、Yes をチェックします。それ以外の場合は、No をチェックします。

rwhod デーモンを実行すると、rwho および ruptime コマンドが使用できます。

フラグ

rwhod デーモンに rwho パケットを送信させ着信パケットを無視させる場合は、「ブロードキャストのみ」をチェックします。rwhod デーモンにブロードキャスト rwho パケット以外の着信パケットを収集させる場合は、「Listen のみ」をチェックします。rwhod デーモンに両方の動作を行わせる場合は、「両方」をチェックします。

詳細については、rwhod(8) を参照してください。

2.2.1.6 routed デーモン

routed デーモンを使用すれば、ルーティング情報プロトコル (RIP) の内部ルーティング・テーブルの更新を自動化できます。

routed

routed デーモンを実行する場合は、Yes をチェックします。それ以外の場合は、No をチェックします。routed デーモンによる経路の動的管理は、使用しているネットワークとシステムが次の条件を満たしている場合のみ利用してください。

基準	種類または値
ネットワークの規模	複数のサブネットを含む中規模以上の LAN または WAN
ネットワーク・トポロジ	可変
必要な経路数	ループバック、ネットワーク・インタフェースの経路など多数
経路を通知するルータ	あり
構成の複雑さ	低
システムのオーバーヘッド	低

routed デーモンまたは gated デーモンの実行を選択できますが、両方を実行することはできません。これらのデーモンおよび静的ルーティングについての詳細は、次の URL の Tru64 UNIX のドキュメントのホーム・ページにある『*Best Practice for Network Routing*』を参照してください。

<http://tru64unix.compaq.co.jp/document/>

フラグ

routed デーモンをどのように実行するかを指定します。ゲートウェイ・ホストで routed デーモンを実行するか、すべてのパケットを標準出力へ出力するか、デバッグ情報を記録するかを選択できます。使用するオプションをチェックしてください。詳細については、`routed(8)` を参照してください。

RIP データ

routed が RIP 情報を供給する場合は、「供給」をチェックしてください。それ以外の場合は「供給しない」をチェックしてください。

2.2.1.7 gateways ファイル

gateways ファイルは、routed デーモンが使用するインターネット・ルーティング情報を保持します。このファイルには、次のパラメータを指定します。

デスティネーションのタイプ

ルートがネットワークの場合は「ネット」をチェックします。ルートが特定のホストの場合は「ホスト」をチェックします。

デスティネーション

デスティネーション名あるいは IP アドレス (ドット・フォーマット)。

ゲートウェイ

メッセージを転送するゲートウェイ・ホストの名前あるいは IP アドレス。

ホップ・カウント

ローカル・ネットワークからデスティネーション・ネットワークまでのホップ・カウントあるいはゲートウェイ数。

ルート・タイプ

ゲートウェイが RIP ルーティング情報を変換することを期待する場合は「Active」をチェックします。ゲートウェイが RIP ルーティング情報を変換することを期待しない場合は「Passive」をチェックします。他のルーティング・プロセスがルートをインストールすることをゲートウェイが routed に知らせるようにする場合は、「外部」をチェックします。

詳細については、gateways(4) を参照してください。

2.2.1.8 gated デーモン

gated デーモンを使用すれば、さまざまなルーティング・プロトコル用の、システムの内部ルーティング・テーブルを自動的に更新できます。

gated

gated デーモンを実行する場合は、Yes をチェックします。それ以外の場合は、No をチェックします。gated デーモンによる経路の動的管理は、使用しているネットワークとシステムが次の条件を満たしている場合のみ利用してください。

基準	種類または値
ネットワークの規模	複数のサブネットを含む中規模以上のネットワーク
ネットワーク・トポロジ	可変
必要な経路数	ループバック、ネットワーク・インタフェースの経路など多数
経路を通知するルータ	あり
構成の複雑さ	中～高
システムのオーバーヘッド	低
システムの役割	ホスト、ルータ、またはクラスタ・メンバ

routed デーモンまたは gated デーモンの実行を選択できますが、両方を実行することはできません。これらのデーモンおよび静的ルーティングについての詳細は、次の URL の Tru64 UNIX のドキュメントのホーム・ページにある『*Best Practice for Network Routing*』を参照してください。

<http://tru64unix.compaq.co.jp/document/>

構成ファイル

代わりの構成ファイル名。省略時の設定では、gated デーモンは /etc/gated.conf ファイルを使用します。

2.2.1.9 IP ルータ

IP ルータとは、複数の TCP/IP ネットワークに接続され、これらのネットワーク間でパケットの受信と転送を行うゲートウェイ・ホストのことです。

複数のネットワーク・インタフェースがインストールされ、構成されている場合は、システムを IP ルータとして構成することができます。routed デーモンあるいは gated デーモンのどちらかを構成しておく必要があります。

IP ルータ

システムを IP ルータとして実行したい場合は Yes をチェックします。
そうでない場合は No をチェックします。

2.2.2 ネットワーク・ファイルのための情報

図 2-6 にネットワーク・ファイル・ワークシートを示します。この後の項で、このワークシートに記録する情報について説明します。本書をオンラインで参照している場合には、プリント機能を使用してワークシートをプリントできます。

図 2-6: ネットワーク・ファイル・ワークシート

IPv6 構成ワークシート 1

スタティック・ルート・ファイル (/etc/routes)

デスティネーション・タイプ: 省略時のゲートウェイ ☐ ホスト ☐ ネットワーク ☐

デスティネーション: _____

経由ルート: ゲートウェイ ☐ インタフェース ☐

ゲートウェイ: _____

ホスト・ファイル (/etc/hosts)

ホスト名: _____

インターネット・アドレス: _____

別 名: _____

ホスト等価ファイル (/etc/hosts.equiv)

ホスト名: _____

ユーザ名: _____

Networks ファイル (/etc/networks)

ネットワーク名: _____

ネットワーク・アドレス: _____

別 名: _____

2.2.2.1 スタティック・ルート・ファイル (/etc/routes)

routes ファイルは、システムのブート時に内部ルーティング・テーブルに追加される静的経路を指定します。

静的経路は、ネットワークとシステムが次の条件を満たしている場合のみ使用してください。

基準	種類または値
ネットワークの規模	小規模な LAN (複数のホストと 1 台のゲートウェイまたはルータ)
ネットワーク・トポロジ	固定
必要な経路数	ループバック、ネットワーク・インタフェースの経路など少数
経路を通知するルータ	なし
構成の複雑さ	低
システムのオーバーヘッド	なし

静的ルーティング，`gated` デモン，および `routed` デモンについての詳細は，次の URL の Tru64 UNIX のドキュメントのホーム・ページにある『*Best Practice for Network Routing*』を参照してください。

<http://tru64unix.compaq.co.jp/document/>

静的経路を使用する場合には，次のパラメータを `routes` ファイルに指定します。

デスティネーション・タイプ

システムから，`/etc/routes` に格納されている別のホストまたはネットワークへの特定のパスです。静的経路は，ネットワーク・ソフトウェアによって更新されることはありません。省略時のゲートウェイにする場合は，「省略時のゲートウェイ」をチェックします。ホストにする場合は，「ホスト」をチェックします。ネットワークにする場合は，「ネットワーク」をチェックします。

デスティネーション

ルート・デスティネーションの名前または IP アドレス。省略時のゲートウェイの場合，省略時のデスティネーションは `default` です。

経由ルート

ゲートウェイを介してルーティングしている場合は，「ゲートウェイ」をチェックします。インタフェースを介してルーティングしている場合は，「インタフェース」をチェックします。

ゲートウェイ

ゲートウェイまたはインタフェースの名前，あるいはその IP アドレス。

詳細については，`routes(4)` を参照してください。

2.2.2.2 ホスト・ファイル (`/etc/hosts`)

`hosts` ファイルは，ネットワーク上の既知のホストについての重要なアドレス情報を保持します。このファイルには，次のパラメータを指定します。

ホスト名

`/etc/hosts` ファイルに追加する，ネットワーク上の他のホスト名。

ネットワークが分散データベース・ルックアップ・サービス (DNS/BIND または NIS) を実行している場合は、`/etc/hosts` ファイルにネットワークの各ホストをリストする必要はありません。ただし、`/etc/hosts` ファイルに、DNS/BIND または NIS サーバとして指定されたネットワーク上のシステムを 4 つか 5 つリストしておいてください。

インターネット・アドレス

`/etc/hosts` ファイルに追加する、ネットワーク上の他のホストの IP アドレス。

別名

`/etc/hosts` ファイルに追加する、ネットワーク上の他のホストの別名 (もしあれば)。

詳細については、`hosts(4)` を参照してください。

2.2.2.3 ホスト等価ファイル (`/etc/hosts.equiv`)

`hosts.equiv` ファイルは、ローカル・システム上でコマンドを実行できるリモート・システムとユーザの名前を保持します。このファイルには、次のパラメータを指定します。

ホスト名

`/etc/hosts.equiv` ファイルに記述するトラステッド・ホスト名。
`/etc/hosts.equiv` ファイルにリストされている各システムは、論理的にローカル・システムと同じであるため、ローカル・システムと全く同じものとして扱われます。

`/etc/hosts.equiv` ファイルの設定は任意ですが、システムでこのファイルを用意する場合はこのファイルを作成し、すべてのトラステッド・ホスト名を追加する必要があります。

ユーザ名

トラステッド・ホストのユーザ名。

詳細については、`hosts.equiv(4)` を参照してください。

2.2.2.4 networks ファイル (/etc/networks)

networks ファイルは、システムからアクセスする必要がある既知のネットワークに関する情報を保持します。このファイルには、次のパラメータを指定します。

ネットワーク名

ネットワークの正式なインターネット名。

ネットワーク・アドレス

ネットワークの IP アドレス。

別名

/etc/networks ファイルに追加されている非公式のネットワーク名。

詳細については、networks(4) を参照してください。

2.3 ネットワーク構成要素の構成

Common Desktop Environment (CDE) のアプリケーション・マネージャの SysMan Menu アプリケーションを使用すると、システムに次のネットワーク構成要素を構成することができます。

- ネットワーク・インタフェース (イーサネット, FDDI, およびトークン・リング)
- リモート who サービス (rwhod デモン)
- ルーティング・サービス (routed デモン, gated デモン, IP ルータ)
- スタティック・ルート・ファイル (/etc/routes)
- ホスト・ファイル (/etc/hosts)
- ホスト同値ファイル (/etc/hosts.equiv)
- ネットワーク・ファイル (/etc/networks)

SysMan Menu アプリケーションを起動するには、1.2.1 項の手順に従ってください。構成作業の手間を軽減するための代替手段についても、この項を参照してください。

2.3.1 ネットワーク・インタフェースの構成

イーサネット、FDDI、またはトークン・リングのネットワーク・インタフェースを構成するには、次の手順に従ってください。NetRAIN の構成方法については 2.4.1 項、リンク・アグリゲーション・グループの構成方法については 2.4.3 項をそれぞれ参照してください。

注意

現在の環境で初めてのシステムを構成する場合には、作業を進める前にネットワーク・アダプタ・モードがコンソール・レベルに正しく設定されていることを確認してください。たとえば、ネットワークが 10base2 イーサネットであり、システムが 10 baseT イーサネットを使用するように構成されていると、コンソールの変数を正しく設定しない限り、システムはこのネットワークを認識できません。フル・インストールの前提条件となるタスクについての詳細は、『インストール・ガイド』を参照してください。

1. SysMan Menu から [ネットワーク] [基本ネットワーク・サービス] [ネットワーク・カードの設定] を選択し、「Network Interface Card (NIC) の設定」ダイアログ・ボックスを表示します。
代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman interface
```


システムに取り付けられているすべてのネットワーク・アダプタが、ダイアログ・ボックスにリストされます。
2. 構成するネットワーク・アダプタを選択します。選択したインタフェースのダイアログ・ボックスが表示されます。
3. 「ホスト名」フィールドにインタフェースの名前を入力します。
4. イーサネット・インタフェースを構成するには、次の手順に従ってください。
 - a. DHCP サーバから IP アドレス・データを取得する場合は、「DHCP を使用」ラジオ・ボタンを選択します。それ以外の場合は、「ユー

ザが提供する値」ラジオ・ボタンを選択して、該当するフィールドに IP アドレスとネットワーク・マスク・データを入力します。

- b. [追加フラグ] ボタンを選択して、「追加フラグの設定」ダイアログ・ボックスを表示します。選択したインタフェースの詳細な構成パラメータが表示されます。
- c. 使用可能にしたい、その他のインタフェース・オプションのチェック・ボックスおよびラジオ・ボタンを選択し、オプションの `ifconfig` 引数に必要な値があれば入力します。
- d. 手順 7 に進みます。

5. FDDI インタフェースを構成するには、次の手順に従ってください。

- a. DHCP サーバから IP アドレス・データを取得する場合は、「DHCP を使用」ラジオ・ボタンを選択します。それ以外の場合は、「ユーザが提供する値」ラジオ・ボタンを選択して、該当するフィールドに IP アドレスとネットワーク・マスク・データを入力します。
- b. [追加フラグ] ボタンを選択して、「追加フラグの設定」ダイアログ・ボックスを表示します。選択したインタフェースの詳細な構成パラメータが表示されます。
- c. 使用可能にしたい、その他のインタフェース・オプションのチェック・ボックスおよびラジオ・ボタンを選択し、オプションの `ifconfig` 引数に必要な値があれば入力します。
- d. 手順 7 に進みます。

6. トークン・リング・インタフェースを構成するには、次の手順に従ってください。

- a. 「IP アドレス」フィールドに、ホスト・デバイスの IP アドレスを入力します。
- b. 「ネットワーク・マスク」フィールドにインタフェースのマスク変数を入力します。
- c. [追加フラグ] ボタンを選択して、「追加フラグの設定」ダイアログ・ボックスを表示します。選択したインタフェースの詳細な構成パラメータが表示されます。

- d. 使用可能にしたい、その他のインタフェース・オプションのチェック・ボックスおよびラジオ・ボタンを選択し、オプションの `ifconfig` 引数に必要な値があれば入力します。4 または 6 のうちいずれか正しいアダプタ・スピードを選択します。
 - e. 手順 7 に進みます。
- 7. [了解] を選択して、入力したパラメータを確認し、「追加フラグの設定」ダイアログ・ボックスを閉じます。構成しているアダプタのダイアログ・ボックスが表示されます。
 - 8. [了解] を選択してネットワーク・インタフェースの構成を確認し、アダプタのダイアログ・ボックスを閉じます。「NIC」ダイアログ・ボックスが表示されます。
 - 9. 必要であれば手順 2 ~ 8 を繰り返し、他のアダプタを構成します。他のアダプタを構成しない場合は、新しい構成でネットワーク・サービスを開始し、変更をすぐに適用するために、[了解] を選択します。システムは変更を適用し、「NIC」ダイアログ・ボックスを閉じます。

「NIC」ダイアログ・ボックスを使用して、ネットワーク・インタフェースを変更したり構成解除することもできます。詳細は、アプリケーションのオンライン・ヘルプを参照してください。

注意

ネットワークを使用するようにシステムをいったん構成すると、CDE はネットワークに依存するようになります。そして、ネットワーク・サービスが利用できない場合には、CDE の機能の一貫性が損なわれることがあります。このため、ネットワーク・インタフェースを 1 つしか持たないシステムで、そのインタフェースを変更したり構成解除すると、予期できない状態にシステムが陥ることがあります。この問題を回避するために、ネットワーク・インタフェースに変更を加えたときには、直ちにシステムをリブートしてください。さらに、ネットワーク・インタフェースを構成解除した場合には、代わりとなる新しいネットワーク・インタフェースを構成してからリブートしてください。

構成したネットワーク・インタフェースの接続状態の監視とテストについては、第 11 章を参照してください。

2.3.2 rwhod デーモンの構成

rwhod デーモンを構成するには、次の手順に従ってください。

1. SysMan Menu で [ネットワーク] [基本ネットワーク・サービス] [リモート who サービスの設定 (rwhod)] を選択し、「リモート who サービス (rwhod) の設定」ダイアログ・ボックスを表示します。

代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman rwhod
```

ユーティリティから、リモート who サービスをシステムで実行するかどうか確認されます。

2. 「はい」ラジオ・ボタンを選択し、リモート who サービスを使用可能にします。
3. 該当する rwhod フラグ・ラジオ・ボタンを選択します。
4. [了解] を選択し、変更を保存します。ユーティリティから、変更が保存されたことが通知され、直ちにその変更を適用するかどうか確認されます。
5. [はい] を選択して直ちに変更を適用するか、[いいえ] を選択して「rwhod サービスの設定」ダイアログ・ボックスを閉じ、次にシステムをリブートするときに変更を適用します。
6. [了解] を選択して情報メッセージを消去し、「リモート who サービス (rwhod) の設定」ダイアログ・ボックスを閉じます。

「リモート who サービス (rwhod) の設定」ダイアログ・ボックスを使用して、rwhod デーモンを使用不能にすることもできます。詳細については、オンライン・ヘルプを参照してください。

2.3.3 routed デーモンの構成

routed デーモンを構成するには、次の手順に従ってください。

1. SysMan Menu で [ネットワーク] [基本ネットワーク・サービス] [ルーティング・サービスの設定 (gated, routed, IP ルータ)] を選択し、「ルーティング・サービスの設定」ダイアログ・ボックスを表示します。

代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman routing
```

ユーティリティは、`gated` および `routed` デーモンを構成し、システムを IP ルータとして設定するために使用できるオプションのリストを表示します。

2. 「Routed」ラジオ・ボタンを選択すると、`routed` デーモンが使用可能になります。
3. システムを IP ルータとして稼働させるには、該当するチェック・ボックスを選択します。
4. `routed` デーモンをゲートウェイで実行するには、該当するチェック・ボックスを選択します。
5. `routed` デーモンをゲートウェイ・ホストで実行し、RIP (Routing Information Protocol) データを提供するには、「RIP データの提供」ラジオ・ボタンを選択します。`routed` デーモンが RIP 情報を提供しないようにするには、「静的実行」ラジオ・ボタンを選択します。
6. [ゲートウェイの設定] ボタンを選択すると、「ゲートウェイの設定」ダイアログ・ボックスが表示されます。次の手順に従ってください。
 - a. 新しいゲートウェイを追加するには、[追加] を選択します。「追加/修正」ダイアログ・ボックスが表示されます。
 - b. デスティネーションがネットワークの場合には、「送付先タイプ」フィールドで「ネットワーク」ラジオ・ボタンを選択します。デスティネーションがホストの場合には、「特定のホスト」ラジオ・ボタンを選択します。
 - c. デスティネーション名、IP アドレス、または `default` を、「送付先」フィールドに入力します。
 - d. ゲートウェイ・ホストの IP アドレスの名前を、「ゲートウェイ」フィールドに入力します。
 - e. ホップ・カウントを「ホップ数」フィールドに入力します。
 - f. 「ゲートウェイ・タイプ」ラジオ・ボタンのいずれか 1 つを選択します。

- g. [了解] を選択して入力した情報を確認し、「追加/修正」ダイアログ・ボックスを閉じます。a から g までの手順を、他のゲートウェイについても繰り返します。
- h. [了解] を選択して変更を保存し、「ゲートウェイの設定」ダイアログ・ボックスを閉じます。

- 7. 「ルーティング・サービスの設定」ダイアログ・ボックスの [了解] を選択して、変更を保存します。ユーティリティが、変更を確認し、デーモンを直ちに起動するかどうかを確認するためのダイアログ・ボックスを表示します。
- 8. [はい] を選択して直ちにデーモンを起動し、変更を適用するか、[いいえ] を選択して「ルーティング・サービスの設定」ダイアログ・ボックスを閉じ、次にシステムをリブートするときに変更を適用します。
[はい] を選択すると、デーモンが実行されるというメッセージが表示されます。[了解] を選択して、このメッセージを消去し、「ルーティング・サービスの設定」ダイアログ・ボックスを閉じます。

「ルーティング・サービスの設定」ダイアログ・ボックスを使用して、`routed` デーモンを使用不可にすることもできます。詳細については、オンライン・ヘルプを参照してください。

`routed` デーモンと `gateways` ファイルについての詳細は、`routed(8)` および `gateways(4)` を参照してください。

2.3.4 gated デーモンの構成

`gated` デーモンを構成するには、次の手順に従ってください。

- 1. SysMan Menu で [ネットワーク] [基本ネットワーク・サービス] [ルーティング・サービスの設定 (`gated`, `routed`, IP ルータ)] を選択し、「ルーティング・サービスの設定」ダイアログ・ボックスを表示します。
代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman routing
```

ユーティリティは、`gated` および `routed` デーモンを構成し、システムを IP ルータとして設定するために使用できるオプションのリストを表示します。

2. 「Gated」ラジオ・ボタンを選択すると、gated デーモンが使用可能になります。
3. システムを IP ルータとして実行するには、該当するチェック・ボックスを選択します。
4. 「設定ファイル」フィールドに gated 構成ファイルのファイル名を入力します。

注意

gated デーモンを構成するには、`/etc/gated.conf` ファイルを `gated.conf(4)` で指定された形式で設定しなければなりません。省略時の `/etc/gated.conf` ファイルは、本ソフトウェアをインストールしたときに提供されます。

5. 「ルーティング・サービスの設定」ダイアログ・ボックスの[了解]を選択して、変更を保存します。変更を確認し、デーモンを直ちに起動するかどうかを確認するダイアログ・ボックスが表示されます。
6. [はい]を選択して直ちにデーモンを起動し、変更を適用するか、[いいえ]を選択して「ルーティング・サービスの設定」ダイアログ・ボックスを閉じ、次にシステムをリブートするときに変更を適用します。

[はい]を選択すると、デーモンが実行されるというメッセージが表示されます。[了解]を選択して、このメッセージを消去し、「ルーティング・サービスの設定」ダイアログ・ボックスを閉じます。

「ルーティング・サービスの設定」ダイアログ・ボックスを使用して、gated デーモンを使用不可にすることもできます。詳細については、オンライン・ヘルプを参照してください。

gated デーモンと `gated.conf` ファイルについての詳細は、`gated(8)` および `gated.conf(4)` を参照してください。

2.3.5 IP ルータとしてのシステムの構成

システムが IP ルータとして機能するには、システムに 2 つのネットワーク・インタフェースがインストールされ構成されていなければならない、さらに

routed または gated デーモンが構成されていなければなりません。システムを IP ルータとして構成する手順は次のとおりです。

1. SysMan Menu で [ネットワーク] [基本ネットワーク・サービス] [ルーティング・サービスの設定 (gated, routed, IP ルータ)] を選択し、「ルーティング・サービスの設定」ダイアログ・ボックスを表示します。

代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman routing
```

ユーティリティは、gated および routed デーモンを構成し、システムを IP ルータとして設定するために使用できるオプションのリストを表示します。

2. システムを IP ルータとして実行するためには、該当するチェック・ボックスを選択します。
3. [了解] を選択して、変更を保存します。変更を確認し、routed または gated デーモンを起動または再起動するかどうかを確認するダイアログ・ボックスが表示されます。

4. [はい] を選択して直ちにデーモンを起動し、変更を適用するか、[いいえ] を選択して「ルーティング・サービスの設定」ダイアログ・ボックスを閉じ、次にシステムをリブートするときに変更を適用します。

[はい] を選択すると、デーモンが実行されるというメッセージが表示されます。[了解] を選択して、このメッセージを消去し、「ルーティング・サービスの設定」ダイアログ・ボックスを閉じます。

「ルーティング・サービスの設定」ダイアログ・ボックスを使用して、IP ルータとしてのシステムを構成解除することもできます。詳細については、オンライン・ヘルプを参照してください。

2.3.6 スタティック・ルート・ファイルの構成

routes ファイルを構成するには、routes ファイルにエントリ (スタティック・ルート) を追加します。次の手順に従ってください。

1. SysMan Menu で [ネットワーク] [基本ネットワーク・サービス] [スタティック・ルートの設定 (/etc/routes)] を選択し、「スタティック・ルートの設定」ダイアログ・ボックスを表示します。

代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman route
```

2. スタティック・ルートを追加するには、[追加] を選択します。「追加/修正」ダイアログ・ボックスが表示されます。
3. 「送付先タイプ」ラジオ・ボタンのいずれか 1 つを選択します。
4. ホストおよびネットワーク・デスティネーションについては、次の手順に従ってください。
 - a. デスティネーション・ネットワークまたはホストの完全な名前または IP アドレスを「送付先」フィールドに入力します。
 - b. 「ルート経由」ラジオ・ボタンのいずれか 1 つを選択します。ルートがゲートウェイを経由する場合には、[ゲートウェイ] ボタンを選択します。ルートがインタフェースを経由する場合には、[インタフェース] ボタンを選択し、手順 6 に進みます。
5. ゲートウェイの場合には、メッセージの転送先となるゲートウェイ・ホストの完全な名前、または IP アドレスを「ゲートウェイ」フィールドに入力します。
6. [了解] を選択してエントリを確認し、リストに追加します。2 から 6 までの手順を、他のスタティック・ルートについても繰り返します。
7. [了解] を選択して、変更を保存します。変更を確認し、スタティック・ルート・サービスを起動するかどうか確認するダイアログ・ボックスが表示されます。
8. [はい] を選択して直ちにサービスを起動し、変更を適用するか、[いいえ] を選択して「スタティック・ルートの設定」ダイアログ・ボックスを閉じ、次にシステムをリブートするときに変更を適用します。

[はい] を選択した場合には、[了解] を選択して「スタティック・ルートの設定」ダイアログ・ボックスを閉じます。

「スタティック・ルートの設定」ダイアログ・ボックスを使用して routes ファイルのエントリを変更、または削除することもできます。詳細については、オンライン・ヘルプを参照してください。

routes ファイルについての詳細は、routes(4) を参照してください。

2.3.7 hosts ファイルの構成

hosts ファイルを構成するには、次の手順に従ってください。

1. SysMan Menu で [ネットワーク] [基本ネットワーク・サービス]
[ホスト・ファイルの設定 (/etc/hosts)] を選択し、[ホスト・ファイルの
設定] ダイアログ・ボックスを表示します。
代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman host
```
2. ホストを追加するには、[追加] を選択します。「追加/修正」ダイア
ログ・ボックスが表示されます。
3. 正式なホスト名を「ホスト名」フィールドに入力します。
4. 新しいホストの IP アドレスを「ホスト・アドレス」フィールドに入
力します。
5. オプションとして、このホストの正式ではない、1 つまたは複数の名前
を「エイリアス」フィールドに入力することもできます。さらに、「コ
メント」フィールドには、ホストの位置など関連情報を入力します。
6. [了解] を選択してエントリを確認し、リストに追加します。2 から 6 ま
での手順を、他のホストについても繰り返します。
7. [了解] を選択して /etc/hosts ファイルを更新し、「ホスト・ファイル
の設定」ダイアログ・ボックスを閉じます。

「ホスト・ファイルの設定」ダイアログ・ボックスを使用して hosts ファイ
ルのエントリを変更、または削除することもできます。詳細については、オ
ンライン・ヘルプを参照してください。

hosts ファイルについての詳細は、hosts(4) を参照してください。

2.3.8 hosts.equiv ファイルの構成

hosts.equiv ファイルを構成するには、次の手順に従ってください。

1. SysMan Menu で [ネットワーク] [基本ネットワーク・サービス]
[等価ホスト・ファイルの設定 (/etc/hosts.equiv)] を選択し、「等価ホ
スト・ファイルの設定」ダイアログ・ボックスを表示します。
代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman hosteq
```

2. ホストを追加するには、[追加] を選択します。「追加/修正」ダイアログ・ボックスが表示されます。
3. 「ホスト名」フィールドにリモート・ホスト名を入力します。

注意

ネットワーク上にないホストを追加することはできません。

4. リモート・ホストのユーザ名を「ユーザ名」フィールドに入力します。
5. [了解] を選択してエントリを確認し、リストに追加します。2 から 5 までの手順を、他のリモート・ホストについても繰り返します。
6. [了解] を選択して `/etc/hosts.equiv` ファイルを更新し、「等価ホスト・ファイルの設定」ダイアログ・ボックスを閉じます。

「等価ホスト・ファイルの設定」ダイアログ・ボックスを使用して `hosts.equiv` ファイルのエントリを変更、または削除することもできます。詳細については、オンライン・ヘルプを参照してください。

`hosts.equiv` ファイルについての詳細は、`hosts.equiv(4)` を参照してください。

2.3.9 networks ファイルの構成

`networks` ファイルを構成するには、次の手順に従ってください。

1. SysMan Menu で [ネットワーク] [基本ネットワーク・サービス] [ネットワーク・ファイルの設定 (/etc/networks)] を選択し、「ネットワーク・ファイルの設定」ダイアログ・ボックスを表示します。

代わりに、次のコマンドをコマンド行に入力することもできます。

```
# /usr/bin/sysman networks
```

2. ネットワークを追加するには、[追加] を選択します。「追加/修正」ダイアログ・ボックスが表示されます。
3. 正式なネットワーク名を「ネットワーク名」フィールドに入力します。
4. ネットワークの IP アドレスを「ネットワーク・アドレス」フィールドに入力します。

5. ネットワークに正式ではない名前 (別名) が割り当てられている場合には、別名を「エイリアス」フィールドに入力します。
6. [了解] を選択してエントリを確認し、リストに追加します。2 から 6 までの手順を、他のネットワークについても繰り返します。
7. [了解] を選択して `/etc/networks` ファイルを更新し、「ネットワーク・ファイルの設定」ダイアログ・ボックスを閉じます。

「ネットワーク・ファイルの設定」ダイアログ・ボックスを使用して `networks` ファイルのエントリを変更、または削除することもできます。詳細については、オンライン・ヘルプを参照してください。

`networks` ファイルについての詳細は、`networks(4)` を参照してください。

2.3.10 IP 別名の構成

IP 別名とは、インタフェースの別のネットワーク・アドレスです。IP 別名は、通常、そのインタフェースの 1 次 IP アドレスと同じサブネット内のアドレスになります。

IP 別名を構成するには、次の情報が必要です。

- IP 別名アドレス
- IP 別名アドレスに関連付けられるネットマスクの値
- IP 別名アドレスに関連付けられるホスト名

IP 別名を構成するには、次の手順に従ってください。

1. IP アドレスおよびホスト名を `/etc/hosts` ファイルに追加します (2.3.7 項を参照してください)。
2. `/etc/inet.local` ファイルを編集し、別名を構成するコマンドを追加します。次の構文を使用します。

```
ifconfig interface alias IP_alias_address netmask IP_alias_netmask
```

たとえば、次のようになります。

```
ifconfig tu0 alias 18.54.76.129 netmask 255.255.255.0
```

`ifconfig` のパラメータについての詳細は、`ifconfig(8)` を参照してください。

3. 次のコマンドを入力して、ネットワーク・サービスを再起動します。

```
# rcinet restart
```

2.4 多重ネットワーク・インタフェースの管理

この節では、複数のネットワーク・インタフェースを備えたシステムで、次の各作業を実行する方法について説明します。

- NetRAIN の構成
- NetRAIN の監視
- リンク・アグリゲーション・グループの構成

2.4.1 NetRAIN の構成

NetRAIN 仮想インタフェースを設定する前に、以下のハードウェア制限と構成上の注意事項を確認してください。

- 現在アイドル状態のインタフェースから、NetRAIN セットを構築する必要があります。つまりインタフェースは、SysMan Menu の「Network Interface Card (NIC) の設定」ダイアログ・ボックス内で "up" と表示されず、割り当てられた IP アドレスを持つことができません。
- 単一の LAN セグメントで使用されている 2 つ以上の同一タイプのネットワーク・インタフェース (FDDI, ATM LAN エミュレーション, あるいはイーサネット) を使用する必要があります。イーサネット・アダプタを使用する場合は、それらはすべて同じスピードでなければなりません。
- NetRAIN 仮想インタフェース (nr) または NetRAIN セットを構成するインタフェースを越えて LAT を実行することはできません。
- リンク・アグリゲーション・グループ (lag) を NetRAIN セットに含めることはできません。
- ネットワークへの物理的に冗長なパスを持たせるために、各ネットワーク・インタフェースから、対応するハブまたはコンセントレータへは、別のケーブルを使用してください。これにより、ケーブルが差し込まれていないためにネットワーク障害が発生するのを抑えることができます。
- NetRAIN がネットワークの障害を正しく検知し応答するように、タイムアウト値は必要に応じて調整できます。これらのパラメータは、sysconfig コマンド、ifconfig コマンド、および ioctl システム・コールで調整することができます。詳細については、

nr(7), ifconfig(8), sysconfig(8), dxkernel tuner(8), および sys_attrs_netrain(5) を参照してください。

省略時の設定では、これらのパラメータはイーサネット経由のオペレーション用に調整されますが、ご使用の環境で省略時の値およびその他のタイムアウト値が機能しないようにすることも可能です。たとえばスイッチに接続している場合、フェイルオーバー時間はそのスイッチと構成状況に依存します。

- LANE 上で NetRAIN を実行して、ギガスイッチを含むいくつかの ATM スイッチで許容可能なフェイルオーバー時間を確保するためには、UNI Version 3.1 を使用する必要があります。UNI Version 3.0 を使用すると、いくつかのスイッチでは省略時の設定で T309 タイマーの値が 90 秒に設定されているため、フェイルオーバー時間が長くなる可能性があります。スイッチで T309 タイマーが変更可能な場合は、UNI Version 3.1 の値と同じように T309 タイマーの値を 10 秒に設定することにより、フェイルオーバー時間を短縮することができます。

NetRAIN 構成パラメータは、他のネットワーク・インタフェースのパラメータとともに /etc/rc.config ファイルに格納されています。これらの変数の値を変更するには、rcmgr ユーティリティを使用します。rcmgr ユーティリティについての詳細は、rcmgr(8) を参照してください。

注意

以下の手順で使用している NetRAIN パラメータは、大文字と小文字が区別されます。必ず表記どおりに大文字で入力してください。

NetRAIN を構成するには、次の手順に従ってください。

1. root でログインします。
2. 1 つまたは複数の NetRAIN セットを、次のように構成します。

- a. NetRAIN インタフェースの名前を設定します。

```
# rcmgr set NRDEV_n netrain-interface-id
```

netrain-interface-id には、NetRAIN インタフェースの名前を nrn の形式で指定します。

NRDEV_*n* 変数の *n* と *nrn* インタフェースの *n* には同じ値を指定してください。たとえば、NetRAIN インタフェースが構成されていないシステムでは、NRDEV_0, nr0 と指定します。

- b. どのネットワーク・インタフェースが NetRAIN のセットの一部であるかを示し、必要な場合には、フェイルオーバ・タイムアウト値を入力します。

```
# rcmgr set NRCONFIG_n interface-id,interface-id [nrtimers integer,integer]
```

注意

インタフェースを指定する際には、*interface-id* パラメータとコンマ (,) の間に空白文字を入れないでください。たとえば、イーサネット・インタフェースを 2 つ指定する場合には、tu0, tu1 ではなく tu0,tu1 と指定します。

nrtimers の値は、システムがインタフェースを切り替えるまでの時間を示します。*nrtimers* の値についての詳細は、*ifconfig*(8) を参照してください。

- c. NetRAIN セットの構成が完了したことを、システムに通知します。

```
# rcmgr set NR_DEVICES integer
```

integer の値を、作成した NetRAIN セットの数で増分します。たとえば、NetRAIN セットを 1 つ作成した場合には、*integer* は 1 です。

3. 作成した 1 つまたは複数の NetRAIN セットのネットワーク・パラメータを、次のように構成します。

- a. インタフェース名を設定します。

```
# rcmgr set NETDEV_n netrain-interface-id
```

netrain-interface-id には、手順 2a で指定したのと同じ *nrn* ID を指定します。

rc.config ファイルに、他のネットワーク・インタフェースが構成されている場合には、次に利用可能な NETDEV_*n* 変数を探して使用する必要があります。たとえば、NETDEV_0 を使用して NetRAIN セットの一部ではないイーサネット・カードを構成した場合は、次に利用可能な変数は、NETDEV_1 です。

- b. NetRAIN インタフェースを初期化するために使用する `ifconfig` パラメータを設定します。

```
# rcmgr set IFCONFIG_n IP-address netmask network-mask
```

手順 3a で説明したように、`rc.config` ファイルで他のネットワーク・インタフェースを構成した場合には、次に利用可能な `IFCONFIG_n` 変数を使用する必要があります。

- c. 新たにネットワーク・インタフェースを追加して構成したことを、システムに通知します。

```
# rcmgr set NUM_NETCONFIG integer
```

integer の値を、作成した NetRAIN セットの数で増分します。
`rc.config` ファイルで別のネットワーク・インタフェースを構成している場合には、そのファイル内の `NUM_NETCONFIG` の値に NetRAIN インタフェースの数を加算する必要があります。

4. ネットワーク・サービスを再起動して、変更を適用します。

NetRAIN セットをいったん構成すれば、システムを再起動するたびに、その NetRAIN インタフェースが利用可能になります。

オプションとして、`ifconfig` コマンドを使用して、NetRAIN インタフェースをコマンド行から構成することもできますが、リブートするときに変更は保持されません。詳細については、`ifconfig(8)` を参照してください。

例 2-1 と例 2-2 は、異なる NetRAIN 構成を作成する場合のコマンド入力例を示しています。

他のネットワーク・インタフェースが構成されていないシステムで、2 つのイーサネット・インタフェース (`tu0` および `tu1`) を持つ NetRAIN セットを 1 つ作成する場合には、例 2-1 に示すようなコマンド群を入力します。

例 2-1: 単独の NetRAIN セットの作成

```
# rcmgr set NRDEV_0 nr0[1]
# rcmgr set NRCONFIG_0 tu0,tu1[2]
# rcmgr set NR_DEVICES 1[3]
# rcmgr set NETDEV_0 nr0[4]
# rcmgr set IFCONFIG_0 18.240.32.40 netmask 255.255.255.0[5]
# rcmgr set NUM_NETCONFIG 1[6]
```

- [1] NetRAIN セットを `nr0` という名前で作成します。

- ② nr0 セットが tu0 および tu1 インタフェースから成っていることを示します。このコマンドが実行されるまで、どちらのインタフェースも休止状態 (down) でなければなりません。
- ③ NetRAIN セットが 1 つあることをシステムに通知します。
- ④ NetRAIN 仮想インタフェースに対応するネットワーク・インタフェースを、nr0 という名前で作成します。
- ⑤ NetRAIN 仮想インタフェースの IP アドレスとネットワーク・マスクを定義します。
- ⑥ ネットワーク・インタフェースが 1 つあることをシステムに通知します。

2 つの FDDI インタフェース (fta0 および fta1) を持つ NetRAIN セットと、2 つの ATM LANE インタフェース (elan0 および elan1) を持つ NetRAIN セットを 1 つずつ、別のネットワーク・インタフェースが 1 つ構成されているシステム (NETDEV_0 が tu0) に作成するには、例 2-2 に示すようなコマンド群を入力します。

例 2-2: 2 つの NetRAIN セットの作成

```
# rcmgr set NRDEV_0 nr0 ①
# rcmgr set NRDEV_1 nr1
# rcmgr set NRCONFIG_0 fta0,fta1 ②
# rcmgr set NRCONFIG_1 elan0,elan1 nrtimers 4,16 ③
# rcmgr set NR_DEVICES 2 ④
# rcmgr set NETDEV_1 nr1 ⑤
# rcmgr set NETDEV_2 nr2
# rcmgr set IFCONFIG_1 18.240.31.40 netmask 255.255.255.0 ⑥
# rcmgr set IFCONFIG_2 18.240.31.42 netmask 255.255.255.0
# rcmgr set NUM_NETCONFIG 3 ⑦
```

- ① nr0 という NetRAIN セットと nr1 という NetRAIN セットを作成します。
- ② nr0 セットが fta0 および fta1 インタフェースから成っていることを示します。このコマンドが実行されるまで、どちらのインタフェースも休止状態 (down) でなければなりません。
- ③ nr1 セットが elan0 および elan1 インタフェースから成っていることを示します。どちらのインタフェースも、現在はアイドル状態です。さらに、このセットのフェイルオーバー値 nrtimers を設定します。この例の値は ATM LANE インタフェースで推奨される初期値であり、この項の冒頭で説明したように、構成によっては変更しないと動作しない

場合があります。 `nrtimers` の値についての詳細は、`ifconfig(8)` を参照してください。

- ❷ 2 つの NetRAIN セットがあることをシステムに通知します。
- ❸ 2 つの NetRAIN 仮想インタフェースに対応するネットワーク・インタフェースを、`nr0` という名前と、`nr1` という名前で作成します。
- ❹ 各 NetRAIN 仮想インタフェースの IP アドレスとネットワーク・マスクを定義します。
- ❺ ネットワーク・インタフェースが 3 つ (NetRAIN 仮想インタフェースが 2 つと、既存のイーサネット・インタフェース) あることをシステムに通知します。

2.4.2 NetRAIN の動作状況の監視

NetRAIN セットのどのメンバがアクティブなインタフェースであるか確認するためには、`ifconfig` コマンドを使用します。次に例を示します。

```
# ifconfig nr0
nr0: flags=8c63<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,SIMPLEX>
    NetRAIN Attached Interfaces: ( fta0 fta1 ) Active Interface: ( fta0 )
    inet 18.240.32.40 netmask ffffffff00 broadcast 18.240.32.255 ipmtu 4352
```

この例では次のことを示しています。

- 仮想インタフェース `nr0` が実行中で、その IP アドレスは `18.240.32.40` です。
- NetRAIN セットは 2 つの物理インタフェース `fta0` および `fta1` で構成されています。
- NetRAIN は、`fta0` を使用して通信しています。NetRAIN が、`fta0` がアクティブでないことを検知すると、セット内の次のインタフェース `fta1` に切り替えられます。

NetRAIN インタフェースが実行されている間にすべてのセット・メンバの状態を見るには、`niffconfig` コマンドを使用します。次に例を示します。

```
# niffconfig -v
Interface:  tu1, state: DEAD, t1: 4, dt: 2, t2: 10, time to dead: 0,
current_interval: 2, next time: 2
Interface:  nr0, state: GREEN, t1: 4, dt: 2, t2: 10, time to dead: 0,
current_interval: 4, next time: 4
Interface:  tu0, state: GREEN, t1: 4, dt: 2, t2: 10, time to dead: 0,
current_interval: 4, next time: 4
```

この例では、仮想インタフェース `nr0` が実行され、NetRAIN が通信に `tu0` を使用しているのが見られます。この例ではまた、セットの各メンバの `nrtimers` 値を示しています。これらの値についての詳細は、`ifconfig(8)` を参照してください。

ネットワーク・インタフェースの接続状態を監視する方法についての詳細は、11.2 節を参照してください。

2.4.3 リンク・アグリゲーション・グループの構成

リンク・アグリゲーション・グループを構成する前に、リンク・アグリゲーション・カーネル・サブシステム (`lag.mod`) がカーネルに組み込まれていることを、次のコマンドを実行して確認してください。

```
# sysconfig -q lag
```

`lag`: サブシステムの属性が表示されない場合には、次の手順でサブシステムを組み込みます。

1. システム構成ファイルを編集し、次のエントリを追加します。

```
options LAG
```

省略時の構成ファイルは `/sys/conf/SYSTEM_NAME` です。

`SYSTEM_NAME` の部分には、使用しているホストのプロセッサ名 (大文字) が入ります。

2. `doconfig -c` コマンドを実行してカーネルを再構築します。カーネルの再構築に不慣れな場合は、『システム管理ガイド』を参照してください。
3. システムをリブートします。システムに他のユーザがログインしていないことを確認した後、次のようなコマンドを実行します。

```
# shutdown -r +5 "Adding Link Aggregation software option ..."
```

リンク・アグリゲーション・カーネル・サブシステムをカーネルに組み込むと、リンク・アグリゲーション・グループの構成を開始できます。ただし、リンク・アグリゲーション仮想インタフェースをセットアップする前に、次に挙げるハードウェアの制約と構成上の注意事項に目を通してください。

- リンク・アグリゲーション・グループの作成には、アイドル状態にあるインタフェース群を使用する必要があります。言い換えれば、SysMan Menu の「Network Interface Card (NIC) の設定」ダイアログ・ボックスで「up」と表示されておらず、かつ IP アドレスが割り当てられてないインタフェースが対象になります。

- 同じサーバまたはスイッチに接続されたイーサネット・ネットワーク・インタフェースを2つ以上使用してください。これらのインタフェースは同じ種類、同じ通信速度で、いずれも全二重モードで動作することが条件です。FDDI インタフェース (faa, fta, fza, mfa) または NetRAIN インタフェース (nr) をリンク・アグリゲーション・グループに含めることはできません。
- 接続先のサーバやスイッチも、リンク・アグリゲーション用に構成する必要があります。
- リンク・アグリゲーション仮想インタフェース (lag) や、リンク・アグリゲーション・グループを構成するインタフェース上では、LAT は実行できません。
- フェイルオーバーがサポートされるのは、DEGPA (alt) デバイス、DEGXA (bcm) デバイスおよびDE60x (ee) デバイスのみです。また、フェイルオーバー時間は変更できません。

リンク・アグリゲーション・グループを構成する手順は次のとおりです。

1. root としてログインします。
2. /etc/inet.local ファイルを編集します。
3. リンク・アグリゲーション・グループを作成する lagconfig -c ステートメントを追加します。
4. 1つのポート (物理インタフェース) のリンク・アグリゲーションを有効化する lagconfig -p ステートメントを追加します。さらに、リンク・アグリゲーションを有効化する残りのポートに対応する lagconfig -p ステートメントを追加します。
5. ifconfig ステートメントを追加します。このステートメントによってリンク・アグリゲーション・グループの仮想インタフェースに IP アドレスが割り当てられ、仮想インタフェースが有効化されます。
6. 変更を保存してファイルを閉じます。
7. 次のコマンドを実行してネットワーク・サービスを再起動します。

```
# rcinet restart
```

いったん構成したリンク・アグリゲーション・グループは、システムを再起動するたびに有効になります。

リンク・アグリゲーション・グループは、lagconfig コマンドと ifconfig コマンドを使ってコマンド行から構成することも可能です。ただし、この方法による変更はシステムをリブートすると失われてしまいます。詳細については、lagconfig(8) と ifconfig(8) を参照してください。

例 2-3 は、3 つのポート (インタフェース) から構成されるリンク・アグリゲーション・グループを作成する際に /etc/inet.local ファイルに追加する行の例を示しています。

例 2-3: リンク・アグリゲーション・ステートメントの例

```
# lagconfig -c 1
# lagconfig -p ee0 key=1 2
# lagconfig -p ee1 key=1 3
# lagconfig -p ee2 key=1 4
# ifconfig lag0 16.1.2.3 netmask 255.255.255.0 up 5
```

- ❶ 省略時のキー値と次に利用可能なインタフェース番号でリンク・アグリゲーション・グループを作成します。このシステムにはリンク・アグリゲーション・グループは構成されていないため、作成するアグリゲーション・グループのキー値は 1、インタフェース番号は 0 (lag0) になります。
- ❷ インタフェース ee0 のリンク・アグリゲーションを有効化します。このコマンドが実行されるまで、ee0 は休止状態 (down) でなければなりません。
- ❸ インタフェース ee1 のリンク・アグリゲーションを有効化します。このコマンドが実行されるまで、ee1 は休止状態 (down) でなければなりません。
- ❹ インタフェース ee2 のリンク・アグリゲーションを有効化します。このコマンドが実行されるまで、ee2 は休止状態 (down) でなければなりません。
- ❺ リンク・アグリゲーション仮想インタフェースの IP アドレスを 16.1.2.3 に設定します。この結果、有効化された各ポートは、同じキーが割り当てられたリンク・アグリゲーション・グループに追加され、これらのポートを介したトラフィック伝送が可能になります。

2.5 インタフェースでのアクセス・フィルタリングの設定

インタフェース・アクセス・フィルタリングは、IP スプーフィング・アタックを検出および防止するために役立ちます。インタフェース・アクセス・フィルタリングの設定方法は以下のとおりです。

1. `/etc/ifaccess.conf` ファイルを作成し、入力パケットのソース・アドレスをチェックするものに対してエントリを追加します。
2. `ifconfig` コマンドに `+filter` パラメータを指定して実行し、ネットワーク・インタフェースでのアクセス・フィルタリングを可能にします。

詳細については、`ifaccess.conf(4)` および `ifconfig(8)` を参照してください。

2.6 FDDI パラメータの表示と変更

FDDI アダプタのパラメータを表示または変更するには、`fddi_config` コマンドを使用します。

FDDI アダプタのパラメータを表示するには、次の構文で `fddi_config` コマンドを使用します。

fddi_config `-i interface_name -d`

FDDI アダプタのパラメータを変更するには、`root` でログインし、表 2-2 に示すオプションを 1 つ以上指定して `fddi_config` を実行します。

表 2-2: `fddi_config` コマンドのオプション

オプション	機能
<code>-i interface_name</code>	<code>interface_name</code> の FDDI 特性を変更したり表示したりします。インタフェース名を指定する必要があります。
<code>-c counter_update_interval</code>	ドライバ・カウンタが DEFTA アダプタによって更新される時間間隔を決定します。省略時の値は 1 秒です。時間間隔をゼロ (0) に設定すると、カウンタは更新されません (DEFTA (fta) FDDI インタフェースの場合だけ)。
<code>-d</code>	設定できる FDDI インタフェース・パラメータを表示します。

表 2-2: fddi_config コマンドのオプション (続き)

オプション	機能
-l lem_threshold	Link Error Monitor (LEM のエラー・レートのしきい値を設定します。LEM のエラー・レートのしきい値は、 1×10^{-n} です。n の範囲は -5 ~ -8 です。省略時の LEM のしきい値は、 1×10^{-8} です。
-p [1 0]	指定された FDDI インタフェースのリング・パージャの状態を設定します。値 1 ではリング・パージャの機能が有効になり、値 0 では無効になります。
-r restricted_token_timeout	Restricted Token Timeout パラメータを設定します。つまり、終了するまで、単一の限定されたモード・ダイアログを持続できる時間を定義します。このパラメータの範囲は、0 ~ 10000 ミリ秒です。省略時の値は、1000 ミリ秒です。
-t token_request_time	要求トークンのローテーション時間 (T_req) を interface_name に対してに設定します。T_req は、リングの初期化プロセスの間に、リングの TTRT (Target Token Rotation Time) を折衝する目的に使用します。このパラメータの範囲は、4.0 ~ 167.77208 ミリ秒です。省略時の値は、8.0 ミリ秒です。
-v valid_transmit_time	ある特定の FDDI インタフェースの Valid Transmission Time (TVX) タイマを設定します。TVX タイマの範囲は、2.35 ~ 5.2224 ミリ秒です。省略時の値は、2.6214 ミリ秒です。
-x [1 0]	インタフェースの全二重の動作を有効 (1) または無効 (0) にします。全二重の動作が有効な場合、インタフェースは、Idle, Request, Confirm, または Operational のいずれかの状態にあります (DEFTA (fta) FDDI インタフェースの場合だけ)。

このコマンドについての詳細は、fddi_config(8) を参照してください。

次の例は、設定できる FDDI インタフェース・パラメータを表示する方法を示します。

```
% /usr/sbin/fddi_config -i fza0 -d
fza0 ANSI FDDI settable parameters

Token Request Time:          0.0000 ms
Valid Transmission Time:     0.0000 ms
```

```
LEM Threshold: 0
Restricted Token Timeout: 15.8314 ms
Ring Purger State: (null)
```

```
fza0 Full Duplex Mode: Disabled
```

```
fza0 Counter Update Interval: 10 sec
```

次の例は、fza0 インタフェースの TRT (Token Request Time) の値を 10.2 に変更する方法を示しています。

```
# fddi_config -t10.2 -i fza0
```

次の例は、リング・パージャをオフにする方法を示しています。

```
# fddi_config -p 0 -i mfa0
```

2.7 トークン・リングのソース・ルーティングの管理

ソース・ルーティングとは、トークン・リング LAN 上のシステムが、相互接続された別のトークン・リング LAN 上のシステムにメッセージを送信するために使用するブリッジ機構です。この機構のもとで、メッセージのソースであるシステムは、経路発見プロセスを使用して、トークン・リング LAN 上の最適な経路を決定し、デスティネーション・システムにブリッジします。ソース・システムは、ソース・システムのソース・ルーティング・テーブルに、最適な経路を格納します。

DETRA アダプタを取り付けて構成したシステムをブートすると、省略時の設定によって、トークン・リングのソース・ルーティングが初期化されます。トークン・リングのソース・ルーティングを管理するには、srconfig コマンドを使用します。

表 2-3 に、srconfig コマンドのオプションを示します。srconfig コマンドのオプションはすべて、大文字小文字を識別しません。つまり、コマンドの各オプションは、大文字でも、小文字でも、両者を混在させても入力できます。各フラグの短縮形は、大文字の英字で示します。

表 2-3: srconfig コマンドのオプション

オプション	機能
<code>-DElEntry mac_address^a</code>	ソース・ルーティング・テーブルのエントリを削除します。
<code>-DISEntry mac_address^a</code>	ソース・ルーティング・テーブルのエントリを無効にします。これによって、エントリが Stale とマーク付けされます。
<code>-RAttr</code>	ソース・ルーティングの属性を表示します。
<code>-RCounter</code>	ソース・ルーティングのカウンタを表示します。
<code>-REntry mac_address</code>	特定のソース・ルーティング・テーブルのエントリを表示します。
<code>-RTable</code>	ソース・ルーティング・テーブルを表示します。
<code>-SETAgetimer timer^a</code>	Source Routing Aging Timer の値を設定します。この値によって、ソース・ルーティング・テーブルのエントリが無効または Stale とマーク付けされるまで有効であり続ける時間の長さを指定します。この値を設定しない場合、システムの省略時の値は 120 秒です。
<code>-SETDsctimer timer^a</code>	Source Routing Discovery Timer を設定します。この値によって、経路発見プロセスが終了するまでに使用できる時間の長さを指定します。この値を設定しない場合、システムの省略時の値は 5 秒です。
<code>-SETMaxentry value^a</code>	ソース・ルーティング・テーブルに許されているエントリの最大数を設定します。このエントリの範囲は 256 の倍数で、1024 ~ 2048 の数です。このパラメータは、増やすことはできますが、減らすことはできません。この値を設定しない場合、システムの省略時の値は 1024 です。
<code>-u</code>	MAC のアドレスが標準以外の形式であることを指定します。このオプションは、 <code>-DElEntry mac_address</code> 、 <code>-DISEntry mac_address</code> 、および <code>-RTable</code> オプションと一緒にの場合にだけ使用できます
<code>-Zcounter</code>	ソース・ルーティングのカウンタをゼロに設定します。

^aスーパーユーザの特権が必要です。

このコマンドとオプションについての詳細は、`srconfig(8)` を参照してください。

次の例では、`-SetMaxEntry` オプションの短縮形を使用して、ルーティング・テーブルのエントリの数を 1024 から 1280 に増加させます。

```
# srconfig -setm 1280
Current SR Table size is : 1024
New SR Table size is : 1280
```

次の例では、`-RAattr` オプションの短縮形を使用して、ソース・ルーティングの属性の使用状況について表示します。

```
# srconfig -ra
Source Routing is enabled
Current SR Aging Timer      : 120
Current SR Discovery Timer  : 10
Current SR Table size is    : 1024
```

次の例では、`-RCounter` オプションの短縮形を使用して、ソース・ルーティングの各カウンタを表示します。

```
# srconfig -rc
ARE Frames Sent              : 000000001
ARE Frames received          : 000000000
Route Discovery Failures     : 000000001
```

次の例では、`-RTable` オプションの短縮形を使用して、標準形式の MAC のアドレスと、ソース・ルーティング・テーブルのエントリをすべて表示します。なお、バックスラッシュ文字 (\) は本書のレイアウトとの関係で、便宜上改行されている部分を示します。この文字は実際の出力には表示されず、当該行がそのまま継続されます。

```
# srconfig -rt
Target Node MAC Address 00-00-0C-01-08-E9 (ip = 130.180.4.3) \
Have Route [1]
Routing Information: SRF, length 8, direction 0, largest frame \
4472 octets [2]
Route Descriptors: 021C 7FFC 0220 0000 0000 0000 0000 0000 [3]

Target Node MAC Address 00-00-C9-10-1B-F5 On Ring [4]

Target Node MAC Address 08-00-2B-2C-F1-F9 (ip = 130.180.4.2) \
Stale (Have Route) [5]
Routing Information: SRF, length 8, direction 0, largest frame 4472 octets
Route Descriptors: 021C 7FFC 0220 0000 0000 0000 0000 0000

Target Node MAC Address 00-00-C9-0B-33-80 Stale (On Ring)
```

- [1] Have Route は、ソース・システムがデスティネーション・システムへの有効なパスを持っていることを示します。

- ② 経路発見プロセスへの応答として、デスティネーション・システムによって返された情報。
- ③ デスティネーション・システムへのパスを構成する LAN セグメントとブリッジ。
- ④ On Ring は、デスティネーション・システムがソース・システムと同じリング上にあり、ソース・ルーティングを必要としないことを示します。
- ⑤ Stale は、エントリが無効で、経路発見プロセスによって更新される必要があることを示します。

次の例では、`-RTable` の短縮形を使用して、非標準の形式の MAC のアドレスとともにソース・ルーティング・テーブルのエントリをすべて表示しています。なお、バックスラッシュ文字 (`\`) は本書のレイアウトとの関係で、便宜上改行されている部分を示します。この文字は実際の出力には表示されず、当該行がそのまま継続されます。

```
# srconfig -rt -u
Target Node MAC Address 00:00:30:80:10:97 (ip = 130.180.4.3) Have Route
Routing Information: SRF, length 8, direction 0,largest frame 4472 octets
Route Descriptors: 021C 7FFC 0220 0000 0000 0000 0000 0000

Target Node MAC Address 00:00:93:08:D8:AF On Ring

Target Node MAC Address 10:00:D4:34:8F:9F (ip = 130.180.4.2) Stale \
(Have Route)
Routing Information: SRF, length 8, direction 0,largest frame 4472 octets
Route Descriptors: 021C 7FFC 0220 0000 0000 0000 0000 0000

Target Node MAC Address 00:00:93:D0:CC:01 Stale (On Ring)
```

2.8 トークン・リング IP MTU のサイズの表示と変更

省略時の設定では、DETRA アダプタは、4092 バイトの IP 最大転送ユニット (MTU) サイズを使用します。さまざまな IP MTU サイズを使用する各種のアダプタが存在するマルチベンダ環境では、種々のネットワークを接続するブリッジは、より小さなパケット・サイズを転送するように設定することになります。その結果、ブリッジがパケットを抜かしたり、リモート・ホストがパケットをリジェクトしたりする可能性があります。ネットワークでいずれかの状況が発生した場合は、ネットワーク上のホストすべての IP MTU サイズを減らし、すべてのホストが必ず同じパケット・サイズを使用するようにしてください。

次のコマンドは、DETRA インタフェースの IP MTU のサイズを 4092 バイトとして表示します。


```
% ifconfig tra0
tra0: flags=9863<UP,BROADCAST,NOTRAILERS,RUNNING>
    inet 16.141.208.3 netmask ffffffff00 broadcast 16.141.208.255 ipmtu 4092
```

次の例は、DETRA インタフェースの IP MTU のサイズに 2044 バイトを設定します。

```
% ifconfig tra0 ipmtu 2044
```

2.9 ネットワークのサービス品質の管理

インターネット・ネットワークにおけるアプリケーションの帯域幅に関する需要が高まっているため、ネットワーク帯域幅の拡張は、ほんの一時的な解決方法に過ぎません。最近のリアルタイム・アプリケーションでは、より広い帯域幅と少ない待ち時間の両方が求められています。明らかに、帯域幅の管理の重要性は増しています。

ベスト・エフォート配信サービスが提供される IP ネットワークでは、受動的な帯域幅管理の形式を採用しています。出力キューに空きがない、つまり、激しいネットワーク・トラフィックおよび混雑が明らかな場合には、パケットはそのまま廃棄されます。上位レベルのプロトコルには、データが損失されたことを検出できるものもありますが、そうでないものもあります。

サービス品質 (QoS) は、通常は、ネットワーク帯域幅を積極的に管理するという概念に結びつけられます。このシナリオでは、すべてのネットワーク要素 (ホスト、アプリケーション、ルータなど)、およびすべてのネットワーク・プロトコル・レイヤは相互に動作し、一定したトラフィックおよびサービスをネットワークのエンド・ツー・エンドで保証します。リアルタイム・アプリケーションのネットワーク帯域幅は予約されていますが、十分な帯域幅が、ベスト・エフォートのトラフィックのために残されています。

本オペレーティング・システムの主なネットワーク QoS の構成要素は、次のとおりです。

- トラフィック制御サブシステム

ロードされていないネットワーク・インタフェースを経由するベスト・エフォート配信を見積る QoS を、アプリケーション・データ・フローに提供します。

トラフィック制御は、イーサネットおよび FDDI インタフェースでサポートされています。

- リソース予約プロトコル (RSVP)

ローカルシステム上およびネットワークを経由して帯域幅を予約するメカニズムを提供します。本オペレーティング・システムでは、RSVP は `rsvdpd` デーモンの形式で実装されています。`rsvdpd` デーモンは、トラフィック制御サブシステムを使用して、特定のネットワーク・インタフェースに、フローおよびフィルタをインストールおよび変更します。

- **RSVP アプリケーション・プログラミング・インタフェース (RAPI)**

`rsvdpd` デーモンと通信するために、機能強化された QoS を必要とするローカル・アプリケーションを使用可能にします。RAPI ルーチンを使用すると、アプリケーションは、リソース (この場合は帯域幅) の予約をローカル・システム上で実行するか、ネットワーク上の他のノードにサービスについてアダプタイズするか、あるいはその両方を実行することができます。RAPI ルーチンについての詳細は、『ネットワーク・プログラミング・ガイド』を参照してください。

2.9.1 トラフィック制御サブシステムの管理

トラフィック制御サブシステムは、次のタスクを実行します。

- デバイスのピーク出力速度、予約できる帯域幅の割合、並行フローの最大数などのインタフェース・パラメータを保守する、アドミッション制御メカニズムを実装します。
- アプリケーションが、許可されている以上の速度でデータを処理しないよう保証します。
- フローおよびフィルタをインストールしたり、削除したりするために、`rsvdpd` デーモンと `ifftcntl` コマンドのインタフェースをとります。
- すべての出力パケット・ヘッダを、既存のフィルタ仕様と照合し、どの出力キューにパケットを配置するかを決定します。

詳細については、`ifftcntl(8)` を参照してください

`rsvdpd` デーモンが、特定のネットワーク・インタフェースのフローおよびフィルタをインストールしたり、変更したりするには、トラフィック制御がローカル・システムで使用可能になっていることが必要です。トラフィック制御をローカル・システムで使用可能にするには、`ether_cl_scheduler` システム属性が使用可能になって (1 に設定されて) いることを確認してください。このシステム属性が使用可能になっていない場合には、`sysconfig`

コマンドまたは `dxkerneltuner` を使用して使用可能にします。その後、システムをリブートします。

2.9.2 RSVP の管理

RSVP は、QoS を、ポイント・ツー・マルチポイントまたはポイント・ツー・ポイントの、特定の IP データ・フローまたはセッションに割り当てます。特定のマルチキャスト・セッションのデータ・パケットを受信するためには、ホストが、対応する IP マルチキャスト・グループに属していなければなりません。1 つのセッションに複数の送信者がある場合もあり、デスティネーションがマルチキャスト・アドレスであれば、複数の受信者がある場合もあります。

`rsvpd` デーモンには、次のような機能があります。

- 受信される RSVP メッセージを待つ。
- ローカル・ホスト上の RSVP 対応のアプリケーションと、RAPI 経由での通信。
- オペレーティング・システムのトラフィック制御サブシステムとのインタフェース。

詳細については、`rsvpd(8)` を参照してください。

2.9.2.1 `rsvpd` の起動および終了

`rsvpd` デーモンを起動するには、次のコマンドを入力します。

```
# /usr/sbin/rsvpd
```

システムのブート時にこのデーモンを自動的に起動するには、このコマンドを `/etc/inet.local` ファイルに取り込みます。デーモンおよびそのオプションについての詳細は、`rsvpd(8)` を参照してください。

`rsvpd` デーモンを終了するには、次のコマンドを入力します。

```
# kill -9 `cat /var/run/rsvpd.pid`
```

`rsvpd` デーモンが、スタートアップまたはシャットダウン・プロシージャ中にアプリケーションを起動したり、終了したりすることはありません。さらに、このデーモンでは、アプリケーションに関するオンディスク構成情報が保守されません。`rsvpd` デーモンが起動されるときは常に、以前の予約に関する情報は残っていません。

通常、オペレーティング・システム上のすべてのデーモンは、システムが実行レベルを変更すると、同時に起動または終了されます。一方で、アプリケーションは、rsvpd デーモンを起動する前の状況、または rsvpd が再起動されるときに実行している状況を正しく処理しなければなりません。このような場合には、ローカル・アプリケーションは、rsvpd デーモンとの通信を再開する必要があります。

2.9.2.2 ネットワーク・インタフェースの追加および削除

システムのネットワーク・インタフェースを追加または削除するときには、利用可能なインタフェースのテーブルをアップデートするために、rsvpd デーモンを終了し、再起動する必要があります。次のコマンドを入力してください。

```
# kill -9 `cat /var/run/rsvpd.pid`  
# /usr/sbin/rsvpd
```

2.9.2.3 RSVP セッション情報の表示

ルーティング・システムまたはエンド・システムに関する RSVP セッション情報を表示して、RSVP がシステムで正常に動作しているかどうか判断することができます。RSVP セッション情報により、接続が設定されているかどうか、および予約が実行されているかがわかります。

ローカル・システムでのアクティブな RSVP セッションを監視するには、次のコマンドを入力します。

```
# /usr/sbin/rsvpstat
```

省略時の設定では、rsvpstat コマンドにより、現在のシステムでアクティブなすべての RSVP セッション、送信者、および受信者のリストが表示されます。RSVP セッション情報には、セッション番号、デスティネーション・アドレス、IP プロトコル、ポート番号、およびそのセッションの PATH および RESV も含まれます。

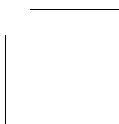
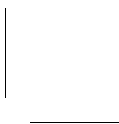
送信者からの実際の PATH メッセージの内容などの送信者情報を表示するには、次のコマンドを入力します。

```
# /usr/sbin/rsvpstat -Sv
```

受信者からの実際の RESV メッセージの内容などの受信者情報を表示するには、次のコマンドを入力します。

```
# /usr/sbin/rsvpstat -Rv
```

詳細については、`rsvpstat(8)` を参照してください。



IPv6 (Internet Protocol Version 6)

IPv6 (Internet Protocol Version 6) は全く新しいネットワーク層プロトコルであり、インターネット・アーキテクチャの大きな改訂でもあります。このため、IPv6 には、IPv4 での経験が取り入れられています。この章では、次のトピックについて説明します。

- IPv6 の歴史的背景と目的 (3.1 節)
- 用語 (3.2 節)
- IPv6 のアドレッシング (3.3 節)
- トンネルを用いた IPv6 の展開 (3.4 節)
- IPv6 の環境 (3.5 節)
- IPv6 構成の準備 (3.6 節)
- IPv6 アドレッシングをサポートするシステムの構成方法 (3.7 節)
- 構成後の作業の実施方法 (3.8 節)
- IPv6 動作のログを記録する方法 (3.9 節)

トラブルシューティング情報については、10.4 節を参照してください。

3.1 IPv6 の歴史的背景

1990 年代の初めには、現在の TCP/IP アーキテクチャのアドレス空間および一部の側面が、インターネットの爆発的な成長に対応できなくなるとインターネット関係者の間で指摘されていました。具体的な問題としては、インターネット・アドレス空間の不足、ルーティング・テーブルのサイズ不足、および新しい技術や機能を実現するための条件の高度化などがあります。

IETF (Internet Engineering Task Force) では、32 ビットのインターネット・プロトコル (IPv4) アドレスの使用方法について、いくつかの研究や改善が試みられました。さらに、より長期的な目標として、インターネットの成長を妨げる可能性のあるプロトコルとサービスを特定し、他のプロトコルやサービスで置き換えるための活動も実施されました。

これらの試みの結果，ルータのオーバーヘッドやネットワーク管理の観点から，IPv4 の 32 ビット・アドレス・アーキテクチャが最大の問題であることが分かりました。しかも，IPv4 アドレスの割り当てはブロックが大きすぎたり小さすぎるなど不均等になる場合が多く，既存のネットワーク内で変更することは困難です。

1994 年 7 月，IPng (Internet Protocol Next Generation) は新しいネットワーク層プロトコルとして IPv6 (Internet Protocol Version 6) を発表し，IETF のワーキング・グループが仕様の作成を開始しました。IPv6 プロトコルが選択されるまでの過程についての詳細は，RFC 1752 (“The Recommendation for the IP Next Generation Protocol”) を参照してください。

3.2 用語

この章では，次の用語を使用しています。

ノード

通信に IPv6 プロトコルを使用するあらゆるシステム。

ルータ

他のノード宛の IPv6 パケットを転送するノード。通常，このようなシステムには複数のネットワーク・インタフェース・カード (NIC) が装備，構成されています。

ホスト

ルータ以外のノード。

リンク

リンク層でのノード間通信に使用される媒体または設備。イーサネット，FDDI，PPP リンク，インターネット層トンネリングなどがあります。

インタフェース

ノードをリンクに接続する部分。この部分には通常，IPv6 のアドレスが割り当てられます。物理 NIC (tu0，ee0 など) や，仮想ネットワーク・インタフェース (3.6.2.3 項で説明する ipt0 など) があります。

トンネル

プロトコルを他のプロトコルのパケット内にカプセル化したパケットによるリンク。この方式では，一方のプロトコルのパケットは他方のプロトコルのインフラストラクチャ上で伝送することができます。このような処理

をトンネリングといいます。使用できるトンネルのタイプについては、3.4 節を参照してください。

3.3 IPv6 のアドレッシング

この節では、管理者を対象として、IPv6 のアドレッシングの概要について説明します。すでにこの情報をご存知の方は、3.5 節に進んでください。

IPv6 の最も大きな特徴は、IPv6 アドレス自体にあります。IPv6 では、アドレスが従来の 32 ビットから 128 ビットに拡張されました。この節では、次のトピックについて説明します。

- アドレスのテキスト表記
- アドレスの自動構成
- アドレス解決
- アドレス割り当て

3.3.1 アドレスのテキスト表記

次の構文を使用すると、IPv6 アドレスをテキスト文字列で表記できます。

x:x:x:x:x:x

x は、アドレス内の 1 つの 16 ビット値を表す 16 進数です。たとえば、次のアドレスは IPv6 アドレスです。

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1070:0:0:0:0:800:200C:417B

IPv6 アドレスには、ゼロ (0) のビットがいくつも連続して含まれる場合があります。そのようなアドレスを表記する場合には、アドレス内に 1 回だけ 2 つのコロン文字 (:) を使用し、1 個以上の、ゼロの 16 ビット・グループを表すことができます。たとえば、上記の 2 番目の IPv6 アドレスの例は、次のように圧縮できます。

1070::800:200C:417B

IPv4 ノードと IPv6 ノードが混在する環境では、IPv6 アドレスを次の構文で表記することもできます。

x:x:x:x:d.d.d.d

この場合、 x はアドレスの上位 6 つの 16 ビット値を表す 16 進数、 d はアドレスの下位 4 つの 8 ビット値を表す 10 進数 (標準の IPv4 ドット表記) です。たとえば、次のアドレスは IPv6 アドレスです。

```
0:0:0:0:0:0:13.1.68.3
```

```
0:0:0:0:0:FFFF:129.144.52.38
```

この 2 つのアドレスは、次のように圧縮できます。

```
::13.1.68.3
```

```
::FFFF:129.144.52.38
```

IPv4 アドレス・プレフィックスと同様、IPv6 アドレス・プレフィックスも CIDR (Classless Inter-Domain Routing) 記法で表されます。この記法のフォーマットは、次のとおりです。

ipv6-address/prefix-length

たとえば、60 ビットの 16 進プレフィックス 12AB00000000CD3 は、次のいずれかのように表記できます。

```
12AB:0000:0000:CD30:0000:0000:0000:0000/60
```

```
12AB::CD30:0:0:0:0/60
```

```
12AB:0:0:CD30::/60
```

3.3.2 アドレスの種類

IPv6 アドレスには、次の 3 種類があります。

- ユニキャスト
- エニーキャスト
- マルチキャスト

注意

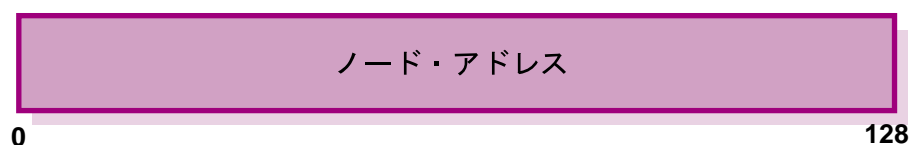
IPv4 とは異なり、IPv6 ではブロードキャスト・アドレスは定義されていません。ブロードキャスト・アドレスの機能を使用するには、リンク・ローカル・スコープのマルチキャスト・アドレスを使用します (3.3.2.3 項を参照)。

以降の項では、ユニキャスト・アドレスとマルチキャスト・アドレスのみを取り上げ、それぞれの例を紹介します。

3.3.2.1 ユニキャスト・アドレス

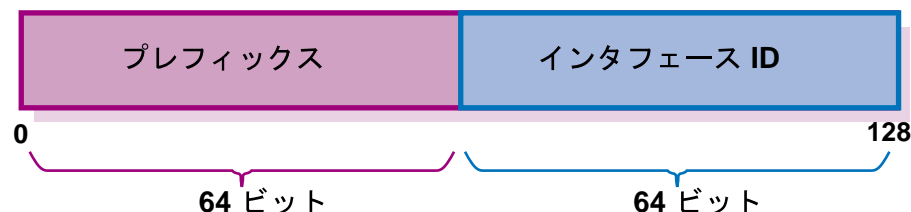
ユニキャスト・アドレスは、物理ネットワーク・インタフェースの識別子です。1つのユニキャスト・アドレスへ送信されたパケットは、そのアドレスで識別されるインタフェースを持つノードに配信されます。

ユニキャスト・アドレスは通常、次のフォーマットで表現されます。



ZK-1291U-AI

このアドレスは、次に示すように、通常は64ビットのプレフィックスと、それに続く64ビットのインタフェースIDからなります。

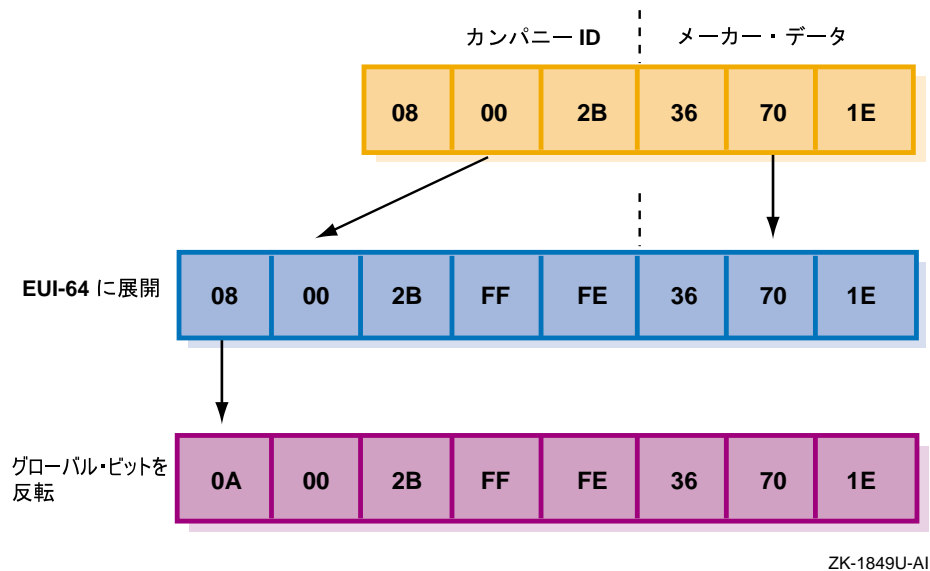


ZK-1292U-AI

インタフェースIDは、1つのリンク上の特定インタフェースを示します。同じリンク上に存在する各インタフェースは、それぞれ異なるインタフェースIDを持つ必要があります。ただし、より広いスコープでインタフェースIDが一意になることもあります。多くの場合、インタフェースのIDには、そのリンク層アドレスが利用されます。1つのノードの複数のインタフェースに、同じインタフェースIDが使用されることもあります。

RFC 2373によれば、大部分のプレフィックスには64ビットのインタフェースIDが必要です。48ビットのMACアドレスからインタフェースIDを作成するには、アドレスの中間位置に2つの16進数(0xFFと0xFE)を挿入して64ビット化した後、7ビット目のユニバーサル/ローカル・ビットを反転します。図3-1は、この処理を図示しています。

図 3-1: MAC アドレスに基づくインタフェース ID の作成



一般的なユニキャスト・アドレスと、その値を次に示します。

未指定アドレス

未指定アドレスはアドレスがないことを示し、インタフェースに割り当てられることはありません。未指定アドレスの値は `0:0:0:0:0:0:0:0` (圧縮フォームでは `::`) です。

ループバック・アドレス

IP データグラムを自分へ送信するためにノードが使用するアドレス。通常はループバック・インタフェースに割り当てられます。IPv6 のループバック・アドレスの値は、`0:0:0:0:0:0:0:1` (圧縮フォームでは `::1`) です。

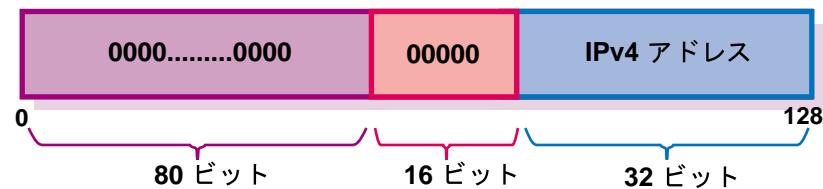
IPv4 アドレスが埋め込まれた IPv6 アドレス

IPv4 と IPv6 が混在している環境で使用されるアドレス。次のアドレスのいずれかです。

- IPv4 互換 IPv6 アドレス

IPv4 のルーティング・インフラストラクチャを通して IPv6 パケットをトンネリングするために、IPv6 ノードが使用するアドレス。

IPv4 のアドレスは、下位 32 ビットで運ばれます。このアドレスのフォーマットは、次のとおりです。



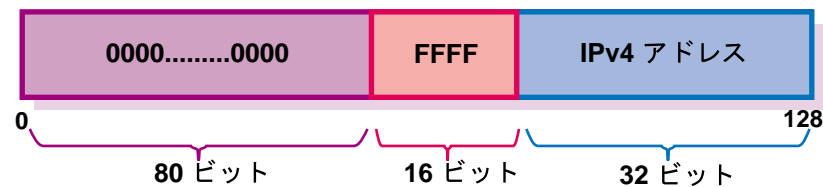
ZK-1293U-AI

注意

IPv4 互換 IPv6 アドレスは、DNS (Domain Name System) や、ローカルの `/etc/ipnodes` ファイルでは使用しないでください。

- IPv4 射影 IPv6 アドレス

IPv4 アドレスを表現し、IPv6 をサポートしていないノード (IPv4 のみのノード) を識別するために使用されるアドレス。このアドレスは IPv6 パケットでは使用されません。このアドレスのフォーマットは、次のとおりです。



ZK-1294U-AI

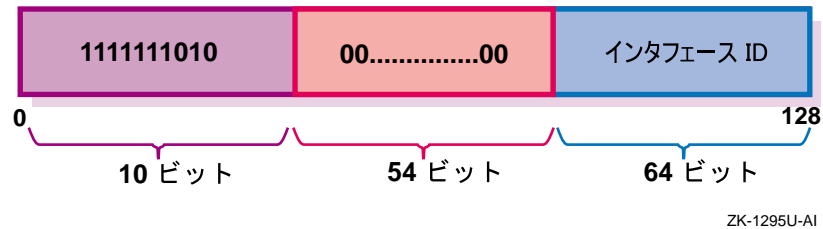
ローカル使用 IPv6 ユニキャスト・アドレス

次のいずれかのアドレスです。

- リンク・ローカル・アドレス

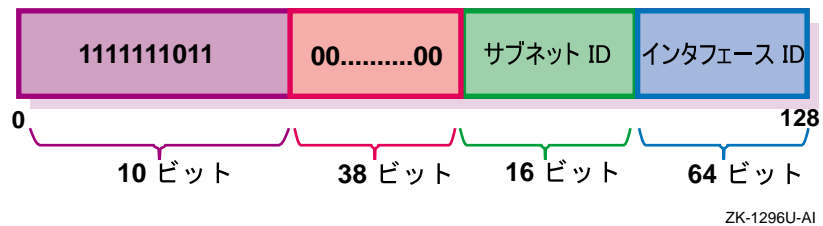
アドレスの自動構成や、近隣ノード検出を実行する場合、またはルータが存在しない場合に、単一リンク上のアドレッシングに使用されるアドレス。このアドレスは、該当するインタフェースが接

続されているリンク上のみで一意であるものと見なされます。このアドレスのフォーマットは、次のとおりです。



- サイト・ローカル・アドレス

グローバルなインターネットに接続されていないサイトや組織で使用するアドレス。このアドレスは、該当するインタフェースが接続されるサイト内のみで一意であるものと見なされます。このアドレスのフォーマットは、次のとおりです。



サイト・ローカル・アドレスを使用する場合には、次の点に留意してください。

- 1つのノードを複数のサイトに接続しないでください。
- サイト・ローカル・アドレスをグローバル DNS で使用しないでください (サイト・ローカル・アドレスは、サイト外部からは見えないようにしてください)。
- サイト・ローカル・アドレスの動的 DNS 更新はサポートされません。
- サイト・ローカル・プレフィックスを含む経路をサイト外に通知したり、送信しないでください。

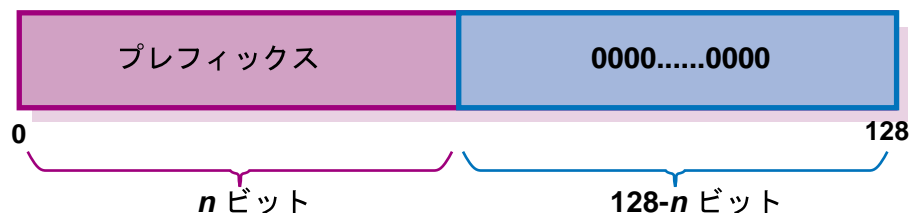
インタフェースは通常、複数の IPv6 アドレスを持ちます。IPv6 を構成してシステムをブートすると、LAN、PPP、および構成したトンネル・インタ

フェースに、リンク・ローカル・アドレスが自動的に割り当てられます。さらに、リンク上にルータが存在する場合には、グローバル・ユニキャスト・アドレスがインタフェースに自動設定されます。

3.3.2.2 エニーキャスト・アドレス

エニーキャスト・アドレスはノードのグループに対する識別子であり、IPv4のエニーキャスト・アドレスと類似しています。エニーキャスト・アドレスに送られたパケットは、そのアドレスで識別されるインタフェースを備えた1つのノードに配信されます。通常は、ルーティング・プロトコルでの距離計測で最も近いノードになります。

エニーキャスト・アドレスはユニキャスト・アドレス空間から割り当てられ、ユニキャスト・アドレスと区別することはできません。サブネット・ルータ・エニーキャスト・アドレスと RFC 2526 で定義されたアドレスだけが、簡単に識別できます。サブネット・ルータ・エニーキャスト・アドレスに送られたパケットは、発信したホストに最も近いルータにのみ配信されます。エニーキャスト・アドレスのフォーマットは、次のとおりです。

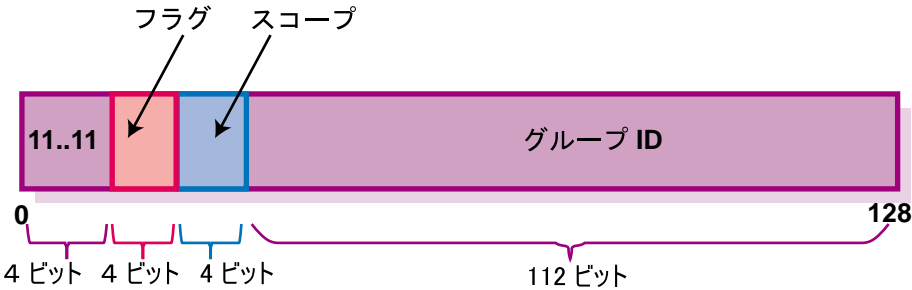


ZK-1881U-AI

上記のフォーマットでは、サブネットのプレフィックスは特定のリンクを識別するプレフィックスになっています。エニーキャスト・アドレスは、インタフェースの識別子がゼロに設定されている点以外は、インタフェースのユニキャスト・アドレスと同じです。

3.3.2.3 マルチキャスト・アドレス

IPv4 マルチキャスト・アドレスと同様、マルチキャスト・アドレス是一群のノードを示す識別子です。マルチキャスト・アドレスのフォーマットを次に示します。



ZK-1303U-AI

上記のアドレス・フォーマット内の各フィールドについて、次に説明します。

11111111 アドレスがマルチキャスト・アドレスであることを示します。

フラグ 0000 または 0001 です。前者は恒久割り当ての (周知の) マルチキャスト・アドレスで、後者は非恒久割り当ての (一時的な) マルチキャスト・アドレスを示します。

スコープ マルチキャスト・グループのスコープを示します。Scope の値を、次の表に示します。

値 (16 進)	スコープ
1	ノード・ローカル
2	リンク・ローカル
5	サイト・ローカル
8	組織ローカル
E	グローバル

グループ ID 指定されたスコープ内のマルチキャスト・グループを識別します。

表 3-1は、周知のマルチキャスト・アドレスの例を示しています。

表 3-1: 周知のマルチキャスト・アドレス

マルチキャスト・アドレス	意味
FF02::1	全ノード (リンク・ローカル)
FF02::2	全ルータ (リンク・ローカル)
FF02::9	全 RIPng ルータ (リンク・ローカル)

3.3.3 アドレス・プレフィックス

各 IPv6 アドレスには、アドレス・タイプを示す固有のビット・パターンが先頭に付けられます。このビット・パターンは、フォーマット・プレフィックス (または単に「プレフィックス」) と呼ばれます。表 3-2 は、IPv6 アドレス・タイプをいくつかリストし、対応するプレフィックスを示しています。

表 3-2: IPv6 アドレス・タイプとプレフィックス

アドレス・タイプ	プレフィックス
集約可能グローバル・ユニキャスト	2000::/3
リンク・ローカル	FE80::/10
サイト・ローカル	FEC0::/10
マルチキャスト	FF00::/8

3.3.4 アドレスの自動構成

IPv6 アドレスでの変更により、次のアドレス構成が定義されました。

- ステートレス・アドレスの自動構成
- ステートフル・アドレスの自動構成である、DHCPv6 (Dynamic Host Configuration Protocol Version 6)

ステートレス・モデルでは、ノードはルータ通知パケットをリッスンすることによって、アドレス・プレフィックスを得ます。このプレフィックスと、データリンク固有のインタフェース識別子を結合して、アドレスが形成されます。このインタフェース識別子は通常、インタフェースのデータリンク・アドレスから抽出されます。このモデルは、アドレスの構成を厳密に制御する必要がない場合に適しています。詳細については、RFC 2462 を参照してください。

DHCPv6 では、ホストは専用の構成サーバにアドレス、構成情報、およびサービスを要求することができます。このモデルは、クライアント/サーバ・モデルでアドレスを割り当てる場合に適しています。DHCPv6 Internet Draft は現在、改訂作業が進められています。詳細については、<http://www.ietf.org/html.charter/dhc-charters.html> にある「Dynamic Host Configuration」Web ページを参照してください。

注意

現バージョンの Tru64 UNIX は DHCPv6 をサポートしていません。

どちらの方法でも、構成される各アドレスには存続期間が対応付けられています。このためシステムは、期限の切れたアドレスを解放し、新しいアドレスを取得しなければなりません。これらの自動構成に、更新後のアドレス情報を DNS (Domain Name System) サーバに登録する機能を付け加えれば、ネットワークの番号再割り当てが可能となり、ネットワーク上の各ホストに手作業で介入することなくネットワーク・アドレスの制御を行うことができます。

3.3.5 アドレス解決

DNS (Domain Name System) は、名前を IP アドレスにマッピングしたり、逆に IP アドレスに対応する名前にマッピングするサービスを提供します。IPv6 でアドレスのサイズが大きくなったため、DNS には次の新しい機能が追加されました。

- AAAA タイプのリソース・レコード
ネットワークのバイト順に符号化された IPv6 アドレスを保持します。オペレーティング・システムに付属しているバージョンの BIND は、AAAA レコードをサポートしています (BIND は、Tru64 UNIX で実装されている DNS です)。
- AAAA 照会
インターネット・クラス内の特定のドメイン名の照会を行うと、その応答として、関連する全 AAAA リソース・レコードが戻されます。
- IP6.INT ドメイン
指定アドレスに対応する名前の検索 (アドレスから名前へのマッピング) を行うためのドメインです。IPv6 アドレスは、ドット記号 (.) で区切ら

れた 4 ビット値の末尾に .IP6.INT が付加されたシーケンスとして、逆順で表されます。たとえば、4321:0:1:2:3:4:567:89ab という IPv6 アドレスの逆引きルックアップ・ドメイン名は、次のとおりです。

```
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.1.2.3.4.IP6.INT
```

IPv6 環境で BIND を構成する際のガイドラインについては、『ネットワーク管理ガイド：サービス編』を参照してください。

3.3.6 アドレス割り当て

IPv6 アドレスは、世界各地の登録局で登録が受け付けられています。IPv6 がすでに構成されているネットワークにシステムを接続すると、そのシステムには必要な IPv6 アドレスが自動的に設定されます。

運営するサイトで利用可能な IPv6 アドレスの範囲については、利用しているインターネット・サービス・プロバイダ (ISP) に問い合わせてください。地域別の登録局とアドレスの割り当てについての詳細は、IANA の Web ページ (<http://www.iana.org/ipaddress/ip-addresses.htm>) を参照してください。

IPv6 RFC のさまざまな実装をテストするため、IETF は一時的な IPv6 アドレスの割り当てスキームを定義しました。このスキームに従うと、6bone 上で IPv6 をテストするためのアドレスを、ホストやルータに割り当てることができます。6bone によるアドレス割り当てについての詳細は、次の 6bone のホーム・ページを参照してください。

<http://www.6bone.net>

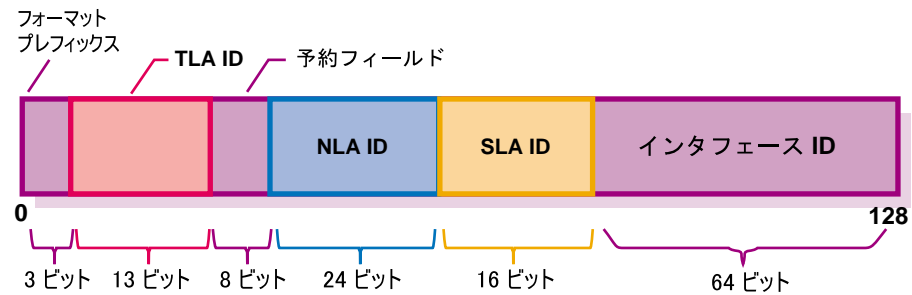
現在、6bone のテスト・アドレスは、集約可能グローバル・ユニキャスト・アドレスです。6bone のアドレス割り当てについては、6bone サービス・プロバイダ (gw-6bone@pa.dec.com など) にお問い合わせください。

以降の項では、集約可能グローバル・ユニキャスト・アドレスと集約可能テスト・アドレスについて説明します。

3.3.6.1 集約可能グローバル・ユニキャスト・アドレス・フォーマット

IPv6 の集約可能グローバル・ユニキャスト・アドレス・フォーマットは、プロバイダ・ベースの現行の集約方式と、相互接続点ベースの新しい集約方式をサポートするように設計されています。サイトがプロバイダと相互接続点のどちらに接続する場合でも、このアドレス・フォーマットによって、効率的な経路集約が可能です。集約可能グローバル・ユニキャスト・ア

ドレスのフォーマットを、次に示します。詳細については、RFC 2374 を参照してください。



ZK-1301U-AI

上記のアドレス・フォーマット内の各フィールドについて、次に説明します。
フォーマット・プレフィックス

フォーマット・プレフィックス。集約可能グローバル・ユニキャスト・アドレスの場合、このフィールドの値は 001 です。

TLA ID

トップレベル集約識別子。

予約フィールド

将来使用するために予約されています。現在は、すべてゼロ (0) が設定されます。

NLA ID

次レベル集約識別子。TLA ID の管理者によって、アドレッシング階層の構築と、エンド・ユーザのサイトの識別のために割り当てられます。TLA ID を割り当てられた各組織には、24 ビットの NLA ID 空間も割り当てられます。この空間のレイアウトと使い方は、該当する組織が決めます。

SLA ID

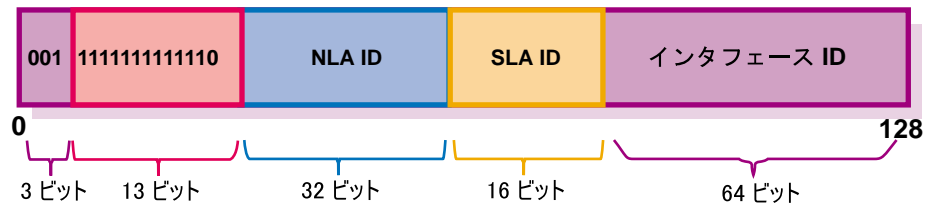
サイト・レベル集約識別子。エンド・ユーザのサイトで、独自のローカル・アドレッシング階層の構築とサブネットの識別のために使用されます。

インタフェース ID

リンクに接続されているインタフェースを識別する 64 ビットのインタフェース識別子。

3.3.6.2 集約可能テスト・アドレス・フォーマット

IPv6 のテスト用の集約可能グローバル・ユニキャスト・アドレスのフォーマットを、次に示します。提案されているテスト用アドレス割り当て計画についての詳細は、RFC 2471 を参照してください。



ZK-1341U-AI

上記のアドレス・フォーマット内の各フィールドについて、次に説明します。

001

集約可能グローバル・ユニキャスト・アドレスのフォーマット・プレフィックス。

11111111111110

6bone のトップレベル集約 (TLA: Top-Level Aggregation) 識別子 (0x1FFE)。この識別子は IANA (Internet Assigned Numbers Naming Authority) によって予約されており、IPv6 のテスト用として一時的に使用されています。

NLA ID

次レベル集約識別子 (Next-Level Aggregation Identifier)。6bone ネットワーク上にアドレッシング階層を構築し、エンド・ユーザのサイトを識別するために、TLA ID の管理者によって割り当てられる ID。

SLA ID

サイト・レベル集約識別子 (Site-Level Aggregation Identifier)。独自のローカル・アドレッシング階層を構築し、サブネットを識別するために、エンド・ユーザのサイトによって割り当てられる ID。

インタフェース ID

リンクに接続されているインタフェースを識別する 64 ビットのインタフェース識別子。

TLA および NLA の割り当てに関する最新情報は、次の 6bone ホーム・ページを参照してください。

<http://www.6bone.net>

3.4 トンネルを用いた IPv6 の展開

インターネットと一般のネットワークは IPv4 の上に構築されているので、IPv6 のルーティング構造を徐々に構築する際には、IPv4 のルーティング構造を使用して IPv6 のトラフィックを運ぶ方法を知っておく必要があります。IPv4 ルーティング構造を通して IPv6 トラフィックのルーティングを行う場合の最適なメカニズムは、トンネリングです。サポートされているトンネルのタイプは次のとおりです。

- 自動
- 6to4
- 構成済み

次に、各トンネルとその長所と短所について説明します。トンネルが強力であるほど、構成と管理の作業量が増えます。トンネルについての追加情報は、次の場所にある『ネットワークへの IPv6 の導入』Best Practice にも記載されています。

http://tru64unix.compaq.co.jp/document/bp/network_bp.html

3.4.1 自動トンネル

IPv6 自動トンネルは、構成と実施が最も簡単なトンネルです。このメカニズムにより、グローバル IPv4 アドレスを持つホストは、自動的に IPv4 ネットワーク上にトンネルを作成できるようになります。トンネルは仮想インタフェース (tun0) として作成され、IPv4 アドレスから生成された IPv4 互換 IPv6 アドレスによって構成されます。パケットの宛先アドレスはトンネルの終端の宛先を指定します。IPv4 互換 IPv6 アドレスについては、3.3.2.1 項を参照してください。

このメカニズムは、ホストを IPv6 に移行する際に適した方法です。アプリケーションの移植、テスト、実験を IPv6 プロトコルで行えるためです。ただし、自動トンネルには次のような制限があります。

- グローバル (プライベートでない) IPv4 アドレスが必要です。
- ルータよりホストに適しています。自動トンネル上で RIPng プロトコルを使用したり、トンネルを通してパケットを転送したりすることはできません。
- 通信相手のノードは、IPv4 互換 IPv6 アドレスで構成されているノードのみになります。ネイティブの IPv6 アドレスのみで構成されたノードとは通信できません。
- IPv6 コミュニティによって廃止されるおそれがあります。生産環境では採用しないようにしてください。

3.4.2 6to4 トンネル

6to4 トンネルは自動トンネルの一種ですが、接続性が高くなっています。このメカニズムを使用すると、6to4 サイトと呼ばれる特別な IPv6 サイトが、グローバル IPv4 アドレスを 1 つ使用して、IPv4 ネットワークを通してトンネルを作成して他の 6to4 サイトと通信できるようになります。トンネルは、IPv4 ネットワーク接続ポイントのノード上の仮想インタフェース (tun1) として作成されます。このノードは個別のホストでも、Border Router と呼ばれるルータでもかまいません。このトンネルは、IPv4 アドレスから生成された特別な 6to4 アドレスで構成されます。パケットの宛先アドレスはトンネルの終端の宛先を指定します。

6to4 サイトの内部では、Border Router はグローバル IPv4 アドレスから 6to4 サイト・プレフィックスを作成し、そのプレフィックスを 6to4 サイト内の全ノードに公開します。各ノードは 6to4 プレフィックスに基づいて自動的に 6to4 アドレスを構成します。特別な構成は不要です。6to4 サイト内のノードは、ネイティブの IPv6 を用いてお互いに通信します。サイトの外に向けられたトラフィックはすべて、Border Router に転送されます。

このメカニズムは構成が簡単で、生産環境に採用できます。ただし、6to4 トンネルには次のような制限があります。

- 通信できるノードが、6to4 アドレスで構成されたノードに限られます。ただし、サードパーティの 6to4 Relay Router サービスまたはインター

ネット上の 6to4 リレー・サービスを使用すると、ネイティブの IPv6 アドレスのみで構成されたノードとも通信できます。

- 基礎を成す IPv4 ネットワーク・ルーティング構造に依存しています。そのため、ルーティングはネイティブの IPv6 接続や構成済みトンネルほど効率的ではありません。

3.4.3 構成済みトンネル

構成済みトンネルは、構成と実施が最も複雑なトンネルです。構成済みトンネルには次の 2 種類があります。

- IPv4 構成済みトンネル — IPv4 または IPv6 パケットを IPv4 パケットにカプセル化し、そのパケットを IPv4 ネットワーク構造を通して伝送します。IPv6 over IPv4 構成済みトンネルでは、IPv6 のサイトとホストを、IPv4 ネットワークを通して他の IPv6 ノードと通信させることができます。
- IPv6 構成済みトンネル — IPv4 または IPv6 パケットを IPv6 パケットにカプセル化し、そのパケットを IPv6 ネットワーク構造を通して伝送します。IPv6 over IPv6 構成済みトンネルは、Mobile IPv6 に対応させるための技術であり、トラフィック・エンジニアリングにも使用できます（たとえば、IPv6 マルチホーミングのサポートなど）。

構成済みトンネルは仮想インタフェース (iptx) として作成され、IPv4 アドレス (IPv4 構成済みトンネルの場合) または IPv6 (IPv6 構成済みトンネルの場合) を、終端の送信元および宛先として使用します。いずれかの構成済みトンネルを通して IPv6 トラフィックを伝送する場合、IPv6 アドレスをトンネル・インタフェース上に構成します。いずれかの構成済みトンネルを通して IPv4 トラフィックを伝送する場合、IPv4 アドレスをトンネル・インタフェース上に構成します。

このメカニズムは最も強力なトンネリングですが、次のような制限があります。

- 各トンネルの終端を組織的に構成しておく必要があります。
- トラフィックを効率的にルーティングするためには、管理者が熟練していなければなりません。終端の構成に誤りがあると、ルーティングの効率低下、ルーティングのループ、またはその両方が発生するおそれがあります。

3.5 IPv6 の環境

この節では、IPv6 のいくつかの構成例を紹介します。IPv6 を構成しようとしているシステムの環境に最も近い構成を選んでください。これらの構成例は、3.6 節でも、選択されたシステムを各構成に従って設定する方法を説明する際に使用します。構成例に含まれる IPv6 のグローバル・アドレスやアドレス・プレフィックスには、3.3.6.2 項で説明したフォーマットを使用しています。

IPv6 は LAN と PPP ネットワークのインタフェースでサポートされます。IPv6 環境でサポートされているコマンドとデーモンについては、『*Tru64 UNIX 概要*』のリストを参照してください。

図 3-2 は、ホスト A とホスト B が IPv6 で通信を行うシンプルな LAN 構成を示しています。

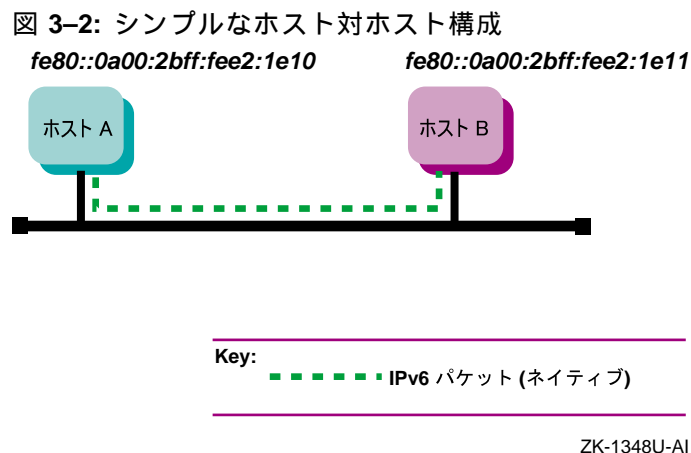


図 3-3 は、ホスト A、ホスト B、およびルータ A が IPv6 で通信を行うシンプルな LAN 構成を示しています。ホスト A とホスト B は、ルータ A からグローバル・アドレスを取得します。

図 3-3: ホスト対ホスト構成 (ルータあり)

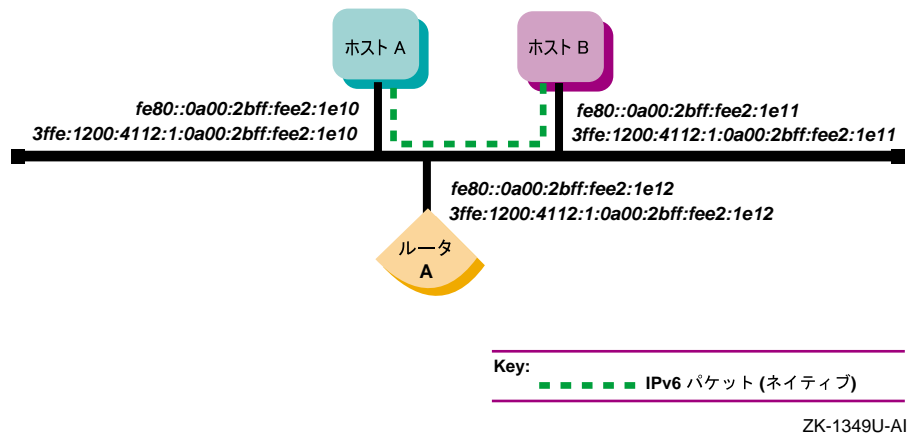


図 3-4 は、2 つの IPv6 ネットワークを 1 台の IPv6 ルータ (ルータ A) を通して接続した構成を示しています。

図 3-4: IPv6 ネットワーク対 IPv6 ネットワーク構成 (ルータあり)

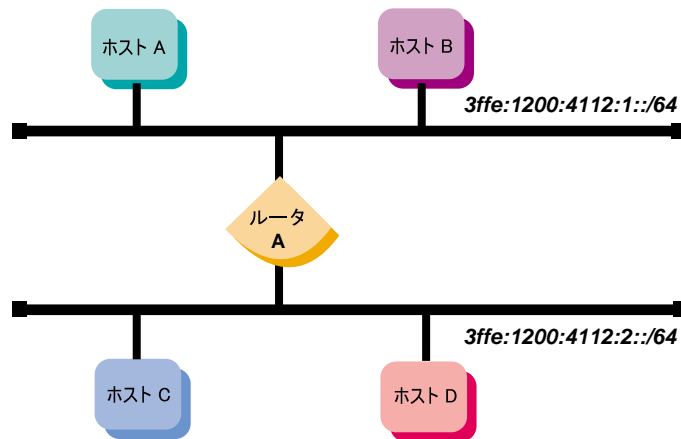
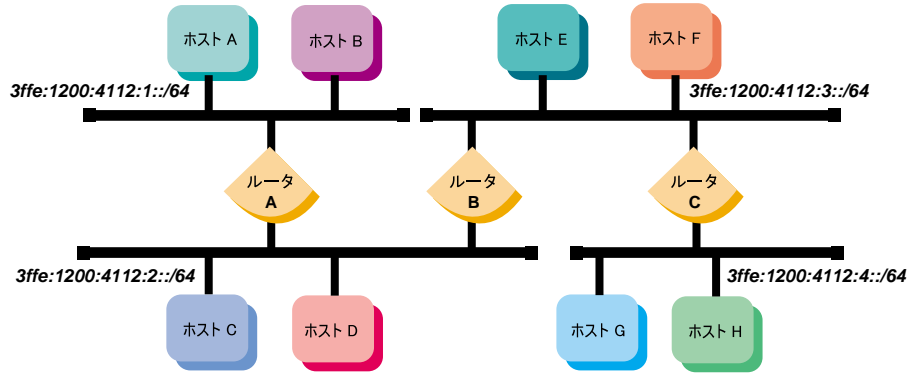


図 3-5 は、4 つの IPv6 ネットワークを 3 台のルータで接続した構成を示しています。3 台のルータは、RIPng プロトコルを使用して、ルーティング情報を交換します。

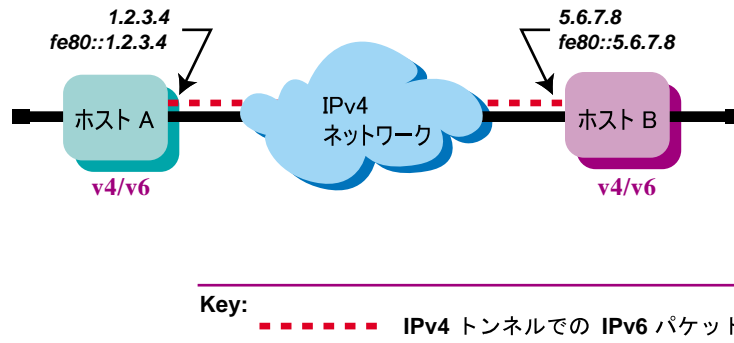
図 3-5: 複数の IPv6 ネットワークと複数のルータがある構成



ZK-1351U-AI

図 3-6 は、1 つの IPv4 ネットワークに接続されたホスト A とホスト B が、IPv4 の構成済みトンネルを通して IPv6 で通信する構成を示しています。

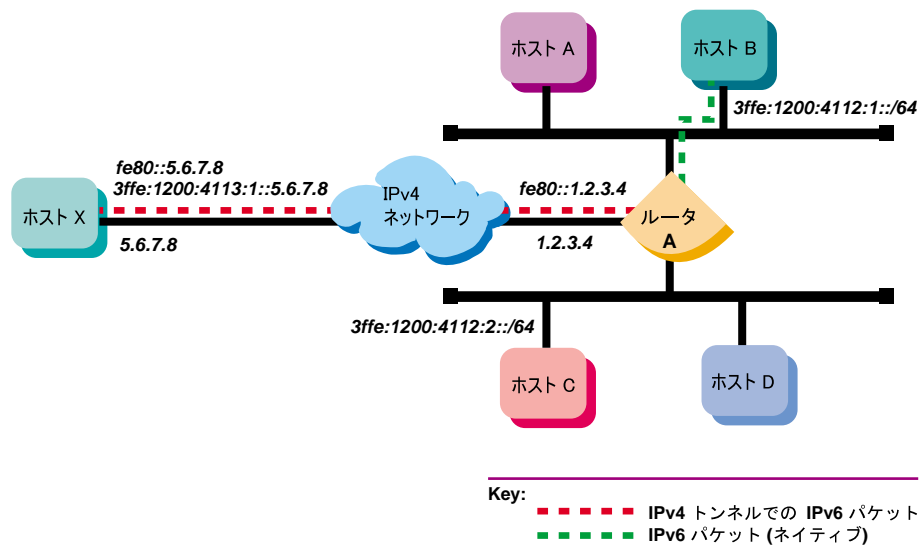
図 3-6: ホスト対ホスト構成 (構成済みトンネルあり)



ZK-1298U-AI

図 3-7 は、ホスト X が IPv4 ネットワークに接続されており、1 台の IPv6 ルータ (ルータ A) が同じ IPv4 ネットワークと 2 つの IPv6 ネットワークに接続されている構成を示しています。ホスト X は、ホスト X とルータ A との間の IPv4 構成済みトンネルを通して、IPv6 でホスト B と通信します。

図 3-7: ホスト対ルータ構成 (トンネリングあり)



ZK-1347U-AI

図 3-8 は、4 つの IPv6 ネットワークが 2 台のルータと IPv4 ネットワークを介して接続されている構成を示しています。ホスト A は、ルータ A とルータ B との間の IPv4 構成済みトンネルを通してホスト F と通信します。

図 3-8: IPv6 ネットワーク対 IPv6 ネットワーク構成 (構成済みトンネルあり)

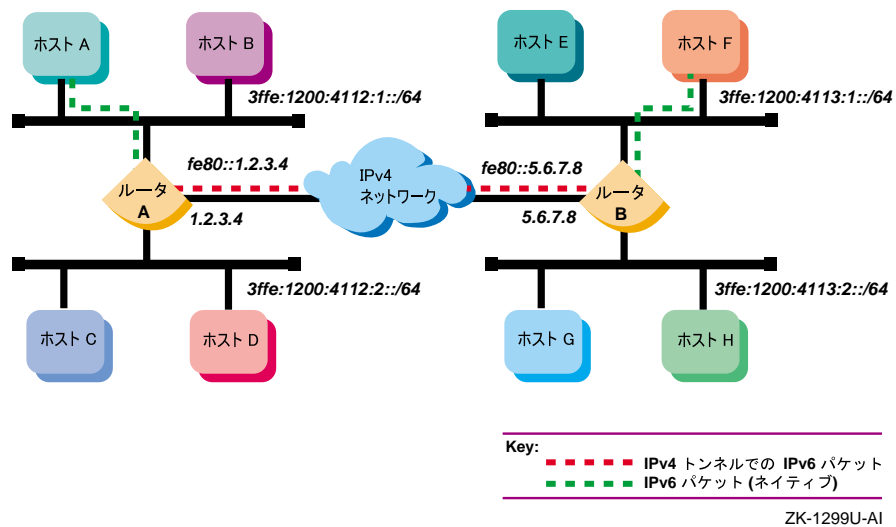
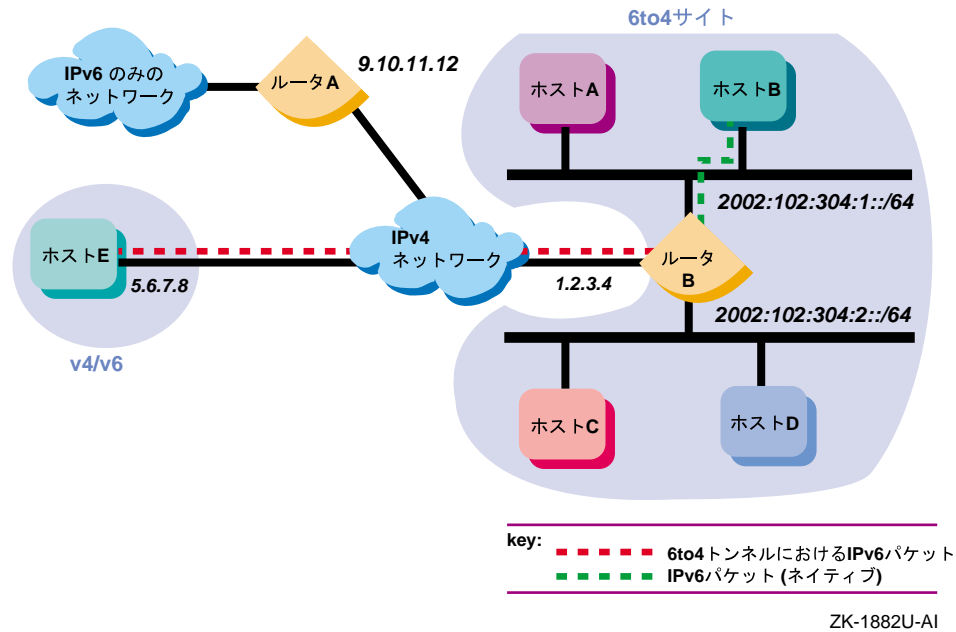


図 3-9 は、ホスト E が IPv4 ネットワークに接続され、ルータ B (IPv6 ルータ) が同じ IPv4 ネットワークに接続され、また同時に 2 つの IPv6 ネットワークにも接続されている構成を示しています。ホスト E は、ホスト E とルータ B の間の 6to4 トンネルを通してホスト B と通信します。

図 3-9: 6to4 構成



3.6 IPv6 のプランニング

IPv6 はどのようなノードにも構成できます。クラスタ構成では、クラスタ内の各メンバに個別に IPv6 を構成することが可能です。

注意

IPv6 はクラスタ全体の通信ではサポートされていないため、IPv6 のアドレスをクラスタ別名に使用することはできません。クラスタの構成については、『クラスタ管理ガイド』を参照してください。

この節では、IPv6 を構成する前に行う必要がある作業について説明します。

3.6.1 カーネル内の IPv6 サポートの確認

IPv6 (IPV6) と IP-in-IP トンネリング (IPTUNNEL) のサポートがカーネル内にあることを、次のコマンドを実行して確認します。

```
# sysconfig -q ipv6  
# sysconfig -q iptunnel
```

サブシステム属性の `ipv6:` または `iptunnel:` が表示されない場合には、次の手順を実行します。

1. 次のコマンドで新しいカーネルを構築します。

```
# doconfig -c SYSTEM_NAME
```

IPv6 オプションと IPTUNNEL オプション、およびその他の必要なオプションを選択します。

2. 元のカーネルを保存し、新しいカーネルを `root` ディレクトリに移動します。

```
# mv /vmunix /vmunix.save  
# mv /sys/SYSTEM_NAME/vmunix /vmunix
```

3. システムをリブートします。リブートする際には、システムに他のユーザがないことを確認してください。次のようなコマンドを使用します。

```
# shutdown -r +5 "Adding IPv6 and IPTUNNEL kernel options ..."
```

以上の手順が完了すると、IPv6 ネットワーク環境で通信できるようにシステムを構成する準備が整います。

3.6.2 構成の準備

IPv6 がカーネルでサポートされていることを確認した後、IPv6 構成ユーティリティ (`ip6_setup`) を実行して、システムを IPv6 ネットワーク環境で通信できるように構成します。`ip6_setup` ユーティリティでは、次のシステムを構成できます。

- IPv6 ホスト
- IPv6 ルータ

`ip6_setup` 構成ユーティリティは、起動後にシステムの情報を収集し、その他の構成情報の入力を求めます。

IPv6 ネットワーク・ソフトウェアの構成を行う前に、システムおよびネットワーク環境の情報を収集しておかなければなりません。IPv6 構成のワークシートを、図 3-10 および 図 3-11 に示します。以降の項では、このワークシートに記録する必要のある情報について説明します。本書をオンラインで参照している場合は、印刷機能を使用するとワークシートのコピーを印刷できます。

図 3-10: IPv6 構成ワークシート 1

IPv6 構成ワークシート 1	
IPv6 ルータ:	<input type="checkbox"/> Yes <input type="checkbox"/> No
DNS/BIND 自動更新 (ホストのみ):	<input type="checkbox"/> Yes <input type="checkbox"/> No
IPv6 インタフェース:	_____
PPP上のIPv6ルーティング (ルータのみ):	<input type="checkbox"/> Yes <input type="checkbox"/> No
6to4 トンネル:	<input type="checkbox"/> Yes <input type="checkbox"/> No
構成済みトンネル:	<input type="checkbox"/> Yes <input type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input type="checkbox"/> No
IPv6の開始:	<input type="checkbox"/> Yes <input type="checkbox"/> No
DNS/BIND	
ドメイン名:	_____
6to4 トンネル	
ホスト・アドレス:	_____
サイト・プレフィックス:	_____
アドレス・プレフィックス (ホストのみ):	_____
リレー・ルータ・アドレス:	_____
Configured トンネル	
タイプ:	<input type="checkbox"/> IPv4 <input type="checkbox"/> IPv6
インタフェース:	_____
宛先アドレス:	_____
発信元アドレス:	_____
RIPng:	<input type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレフィックス:	_____

図 3-11: IPv6 構成ワークシート 2

IPv6 構成ワークシート 2	
ルータ	
インターフェース:	_____
RIPng:	<input type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレフィックス:	_____
_____	_____
インターフェース:	_____
RIPng:	<input type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレプレフィックス:	_____
_____	_____
手動経路	
宛先プレフィックス:	_____
インターフェース:	_____
次のホップ・アドレス:	_____
宛先プレフィックス:	_____
インターフェース:	_____
次のホップ・アドレス:	_____

IPv6 ルータ

システムを IPv6 ルータとして構成する場合は Yes をチェックします。ルータとしない場合は、No をチェックします。No をチェックすると、システムは IPv6 ホストとして構成されます。

IPv6 ルータは、LAN や構成済みのトンネルなど、接続されているリンク上の全ホストにアドレス・プレフィックスを通知し、パケットを宛先に転送できます。パケットはリンク上で直接転送することも、IPv4 トンネルを通して転送することも可能です。

DNS/BIND 自動更新 (ホストのみ)

システムのアドレスを DNS/BIND データベースに自動的に記録する場合には Yes、自動記録が不要であれば No をチェックします。Yes をチェックした場合には、システムを DNS/BIND クライアントとして構成しなければならず、DNS/BIND サーバは DNS データベースの動的更新をサポートしていなければなりません。DNS/BIND サーバの

構成方法については、『ネットワーク管理ガイド：サービス編』を参照してください。

IPv6 インタフェース

IPv6 ネットワークへのネットワーク・インタフェースとして使用するデバイスの名前 (le0 や fta0 など) を入力します。構成済みトンネルをシステムに作成するだけの場合は、none と入力します。

PPP 上の IPv6 ルーティング (ルータのみ)

PPP インタフェース上で IPv6 ルーティングを使用する場合には Yes，使用しない場合は No をチェックします。PPP インタフェースの構成については、ppp_manual_setup(7) を参照してください。

6to4 トンネル

6to4 トンネル上で IPv6 を使用する場合には Yes，使用しない場合は No をチェックします。1 本の 6to4 トンネルは、IPv4 ネットワーク内に送信元を 1 箇所と宛先を 1 箇所持ちます。

構成済みトンネル

構成済みの IPv4 トンネル上で IPv6 を使用する場合には Yes，使用しない場合は No をチェックします。1 本の構成済みの IPv4 トンネルは、IPv4 ネットワーク内に送信元を 1 箇所と宛先を 1 箇所持ちます。自動トンネルではなく構成済みトンネルを使用してください。構成済みトンネルを複数定義することもできます。

自動トンネル

IPv4 自動トンネル上で IPv6 を使用する場合には Yes，使用しない場合は No をチェックします。

注意

自動トンネルは、今後廃止される可能性があるので、使用しないでください。

手動経路

他のシステムへの経路を手動構成する場合は Yes , 手動構成しない場合は No をチェックします。

ルータ上では , 次の条件のいずれかが満たされる場合に静的経路を構成できます。

- 構成済みのトンネルを使用し , トンネル・リンクではアドレス・プレフィックスの通知を行わない。
- 構成済みのトンネルを使用し , トンネルの他端のルータは RIPng プロトコルを使用しない。
- システムは RIPng プロトコルを使用しない。

ホスト上では , ルータとの間で構成済みトンネルを使用し , そのルータが自分をトンネル・リンク上の省略時のルータとして通知しない場合に静的経路を構成できます。

IPv6 の開始

IPv6 を `ip6_setup` 構成ユーティリティから直接開始する場合には Yes , システムの次のブート時に開始する場合は No をチェックします。

3.6.2.1 DNS/BIND

ドメイン名

ノードの完全修飾ドメイン名。完全修飾ドメイン名は , ホスト名と DNS/BIND ドメイン名からなります (`host1.subdomain.example` など)。

3.6.2.2 6to4 トンネル

ホスト・アドレス

ノードの名前または IP アドレス (トンネルの終端)。

サイト・プレフィックス

`ip6_setup` ユーティリティは , 48 ビットの 6to4 サイト・プレフィックスを自動的に生成します。

アドレス・プレフィックス (ホストのみ)

システムが IPv6 ホストの場合は、6to4 トンネル・インタフェースに構成する、64 ビットの 6to4 プレフィックスを入力します。アドレス・プレフィックスの上位 48 ビットは、`ip6_setup` ユーティリティが生成するサイト・プレフィックスと同じでなければなりません。

リレー・ルータ・アドレス

IPv6 のみのネットワークで通信を行う場合は、リレー・ルータの 6to4 アドレスを入力します。

3.6.2.3 構成済みトンネル

タイプ

構成済みトンネルのタイプ。有効なタイプは IPv4 と IPv6 です。

インタフェース

構成済みトンネル・インタフェースの名前 (`ipt0` , `ipt1` など)。この値は、`ip6_setup` スクリプトが設定します。

宛先アドレス

リモート・ノードの IP アドレス (トンネルの相手側の端)。

発信元アドレス

ご使用のノードの IP アドレス (トンネルの自分側の端)。

RIPng

システムがルータであり、そのルータがトンネル・リンク上で RIPng プロトコルを使用して IPv6 ルーティング情報をトンネルのリモート側のルータと交換する場合は Yes、この条件に該当しない場合は No をチェックします。

アドレス・プレフィックス

システムがルータであり、トンネルのリモート側ノードにアドレス・プレフィックスを通知する場合は 64 ビットのプレフィックスを入力し、この通知を行わない場合は Done と入力します。

システムが IPv6 ホストであり、トンネルのリモート側ルータからアドレス・プレフィックスが通知されない場合には、このトンネル・インタフェース上に構成する 64 ビットのプレフィックスを入力します。

3.6.2.4 ルータ

インタフェース	RIPng プロトコルを使用したり、アドレス・プレフィックスを通知するインタフェース (LAN や PPP、構成済みトンネルなど) の名前。
RIPng	指定されたインタフェースでルータが RIPng プロトコルを使用し、リンク (LAN、PPP、構成済みトンネルなどの) 上で他のルータと IPv6 ルーティング情報を交換する場合は Yes、この条件に該当しない場合は No をチェックします。
アドレス・プレフィックス	<p>リンク上のすべてのホストにアドレス・プレフィックスを通知する場合は 64 ビットのプレフィックスを入力し、アドレス・プレフィックスを通知しない場合は Done と入力します。</p> <p>Done と入力すると、ルータによるアドレス・プレフィックスの通知が行われなため、各ホストは自分のプレフィックス情報を別のソースから取得する必要があります。</p> <p>IPv6 のプレフィックスはサブネットを定義します。このプレフィックスは通常、ネットワーク管理者によって、特定リンク用としてルータ上に構成されます。ルータは、構成されたプレフィックスを、そのリンクに接続されている全ノードに通知します。プレフィックスを通知する際には、プレフィックスの長さ、このプレフィックスがリンク上に存在するかどうか (近隣であるかどうか)、ステートレス・アドレス構成で利用できるかどうか、およびプレフィックスの有効時間もあわせて通知されます。</p>

3.6.2.5 手動経路

宛先プレフィックス	リモート IPv6 ネットワークのアドレス・プレフィックス。このアドレス・プレフィックスには、CIDR (Classless Inter-Domain Routing) スタイルのビット長情報が含まれています (例: 5F00::/8)。省略時の経路を使用する場合には、Default と入力します。
インタフェース	リモート IPv6 ネットワークへのトラフィック送信に使用するインタフェースの名前。
次のホップ・アドレス	宛先プレフィックスへのパス上に存在する最初のルータの IPv6 アドレス。そのルータのリンク・ローカル・アドレスを入力します。そのルータへのコネクションが IPv4 トンネル上にある場合には、トンネルのリモート側のリンク・ローカル IPv6 アドレスを入力します。

3.6.3 IPv6 構成例のシステムの構成

この項では、3.5 節で紹介した各構成例について説明し、それぞれの例でのシステムの構成方法を示します。また、特定の構成で利用可能な選択肢を紹介する場合もあります。

3.6.3.1 シンプルなホスト対ホスト構成

図 3-2 のホスト A とホスト B は、IPv6 リンク・ローカル・アドレスを使用します。特に指定しないかぎり、`ip6_setup` 構成ユーティリティは、システムのリンク・ローカル・アドレスを自動的に作成します。ホスト A の構成ワークシートの記入例を次に示します。

IPv6 構成ワークシート

IPv6 ルータ: ☐ Yes ☒ No
DNS/BIND 自動更新: ☐ Yes ☒ No
IPv6 インタフェース: tu0
構成済みトンネル: ☐ Yes ☒ No
自動トンネル: ☐ Yes ☒ No
手動経路: ☐ Yes ☒ No
IPv6 の開始: ☒ Yes ☐ No

ホスト A で IPv6 を構成した後, /etc/ipnodes ファイルを編集して, ホスト B のリンク・ローカル・アドレスをファイル内に記述します。ホスト B は, ホスト A とほぼ同じ手順で構成できます。

この構成では, グローバル・アドレス・プレフィックスは LAN 上で通知されません。グローバル・アドレス・プレフィックスの通知を行うには, ip6_setup ユーティリティでいずれかのノードをルータとして構成するか, LAN 構成に IPv6 ルータを追加します。IPv6 ルータは, リンク上でグローバル・アドレス・プレフィックスを通知します。

ローカル・ノードのリンク・ローカル・アドレスとグローバル・アドレスは, netstat -in コマンドを使用すれば参照できます。

ホスト A で telnet コマンドを使ってホスト B に接続するには, コマンドを次のように実行します。

```
# telnet fe80::0a00:2bff:fee2:1e11
```

リンク・ローカル・アドレスを指定する代わりに, アドレスとノード名を /etc/ipnodes ファイルに記述する方法もあります。この場合, telnet コマンドの引数には, ノード名を指定します。

3.6.3.2 ホスト対ホスト構成 (ルータあり)

図 3-3 では, ホスト A とホスト B がルータ A とともに LAN 上に配置されています。この場合, ルータ A が LAN 上でグローバル・アドレス・プレフィックス (3ffe:1200:4112:1::/64) を通知します。ホスト A とホスト B は, このアドレス・プレフィックスを使用して, グローバル IPv6 アドレスを作成します。テスト用のアドレスの取得方法については, 3.3.6 項を参照してください。ルータ A の構成ワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
DNS/BIND 自動更新:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	<u>tu0</u>
構成済みトンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
ルータ	
インタフェース:	<u>tu0</u>
RIPng:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アドレス・プレフィックス:	<u>3ffe:1200:4112:1::/64</u>
インタフェース:	_____
RIPng:	<input type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレフィックス:	_____

ルータ A で IPv6 を構成した後、`/etc/ipnodes` ファイルを編集して、他のノードのグローバル・アドレスをファイル内に追加します。この作業を、ホスト A とホスト B でも行います。代わりにグローバル・アドレスを使用して、ネットワーク内に DNS/BIND を確立することも可能です。

動的更新を使用可能にした DNS/BIND サーバをネットワークに追加した場合、ホスト A の構成ワークシートは次のようになります。

DNS/BIND 自動更新:	<input checked="" type="checkbox"/> yes <input type="checkbox"/> no
DNS/BIND	
ドメイン名:	<u>hosta.corp.example</u>

3.6.3.3 IPv6 ネットワーク対 IPv6 ネットワーク構成 (ルータあり)

図 3-4 では、ルータ A とその複数のインタフェースを介して、2 つの IPv6 ネットワークが相互に接続されています。ルータ A の構成ワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
DNS/BIND 自動更新:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	<u>tu0</u> <u>tu1</u> _____
構成済みトンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

ルータ	
インタフェース:	<u>tu0</u>
RIPng:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アドレス・プレフィックス:	<u>3ffe:1200:4112:1::/64</u>
インタフェース:	<u>tu1</u>
RIPng:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アドレス・プレフィックス:	<u>3ffe:1200:4112:2::/64</u>

3.6.3.4 複数の IPv6 ネットワークと複数のルータがある構成

図 3-5 では、4 つの IPv6 ネットワークが 3 台のルータを介して相互接続されています。この構成では、ネットワーク内の他のサブネットへのルートについての情報を得るため、ルータはルーティング情報を交換しなければなりません。この交換を行うには、各ルータで RIPng プロトコルを使用しなければなりません。ルータ A の構成ワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
DNS/BIND 自動更新:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	<u>tu0</u> <u>tu1</u> _____
構成済みトンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
ルータ	
インタフェース:	<u>tu0</u>
RIPng:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレフィックス:	<u>3ffe:1200:4112:1::/64</u>
インタフェース:	<u>tu1</u>
RIPng:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレフィックス:	<u>3ffe:1200:4112:2::/64</u>

他のルータの構成ワークシートもほぼ同じです。

3.6.3.5 ホスト対ホスト構成 (IPv4 構成済みトンネルあり)

図 3-6 では、2 つの IPv6 システムが構成済みトンネルを通じて、IPv4 ネットワーク越しに相互通信を行います。これらのシステムは IPv6 リンク・ローカル・アドレスを使用します。ホスト A の構成ワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
DNS/BIND 自動更新:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	<u>none</u>
構成済みトンネル:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
構成済みトンネル	
インタフェース:	<u>ipt0</u>
宛先 IPv4 アドレス:	<u>5.6.7.8</u>
発信元 IPv4 アドレス:	<u>1.2.3.4</u>
RIPng:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アドレス・プレフィックス:	<u> </u>
	<u> </u>

ホスト A で IPv6 を構成した後，`/etc/ipnodes` ファイルを編集して，ホスト B のリンク・ローカル・アドレスをファイル内に追加します。ホスト B は，ホスト A とほぼ同じ手順で構成できます。

この構成では，グローバル・アドレス・プレフィックスはトンネル上で通知されません。グローバル・アドレス・プレフィックスの通知を行うには，`ip6_setup` でいずれかのノードをルータとして構成します。IPv6 ルータは，リンク上でグローバル・アドレス・プレフィックスを通知します。

ローカル・ノードのリンク・ローカル・アドレスとグローバル・アドレスは，`netstat -in` コマンドを使用すれば参照できます。

ホスト A で `telnet` コマンドを使ってホスト B に接続するには，コマンドを次のように実行します。

```
# telnet fe80::5.6.7.8
```

リンク・ローカル・アドレスを指定する代わりに，アドレスとノード名を `/etc/ipnodes` ファイルに記述する方法もあります。この場合，`telnet` コマンドの引数には，ノード名を指定します。

3.6.3.6 ホスト対ルータ構成 (IPv4 構成済みトンネルあり)

図 3-7 では，ホスト X が構成済みトンネルを介して IPv4 ネットワーク越しにホスト B と通信を行います。どちらのノードも IPv6 アドレスを使用しま

す。この場合のトンネルは、ホスト X とルータ A との間に存在します。ルータ A が自分をトンネル・リンクの省略時のルータとして通知し、トンネル・リンク上でグローバル・アドレス・プレフィックスを通知する場合の、ホスト X の構成ワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
DNS/BIND 自動更新:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	<u>none</u>
構成済みトンネル:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
構成済みトンネル	
インタフェース:	<u>ipt0</u>
宛先 IPv4 アドレス:	<u>5.6.7.8</u>
発信元 IPv4 アドレス:	<u>1.2.3.4</u>
RIPng:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アドレス・プレフィックス:	<u></u>

ルータ A がトンネル・リンクでグローバル・アドレス・プレフィックスを通知しない場合、ホスト X の構成ワークシートの「構成済みトンネル」セクションにある「アドレス・プレフィックス」フィールドの値は `3ffe:1200:4113:1::/64` になります。また、ルータ A が自分をトンネル・リンクの省略時ルータとして通知しない場合、ホスト X の構成ワークシートに次の情報も記入します。

手動経路:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
手動経路	
宛先プレフィックス:	<u>default</u>
インタフェース:	<u>ipt0</u>
次のホップアドレス:	<u>fe80::1.2.3.4</u>

ルータ A がトンネル・リンク上でグローバル・アドレス・プレフィックスを通知する場合の、ルータ A の構成ワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
DNS/BIND 自動更新:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	<u>tu0</u> <u>tu1</u>
構成済みトンネル:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
構成済みトンネル	
インタフェース:	<u>ipt0</u>
宛先 IPv4 アドレス:	<u>5.6.7.8</u>
発信元 IPv4 アドレス:	<u>1.2.3.4</u>
RIPng:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アドレス・プレフィックス:	<u>3ffe:1200:4113:1::/64</u>

ルータ A がトンネル・リンク上でグローバル・プレフィックスを通知しない場合には、ルータ A の構成ワークシートの情報は次のようになります。ホスト X への「手動経路」に注意してください。宛先のネットワーク・プレフィックスを指定する代わりに、ホスト X へのホスト経路 (3ffe:1200:4113:1::5.6.7.8) を指定します。ホスト X のトンネル・インタフェースのリンク・ローカル IPv6 アドレス (fe80::5.6.7.8) が次のホップになります。

手動経路:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
手動経路	
宛先プレフィックス:	<u>3ffe:1200:4113:1::5.6.7.8</u>
インタフェース:	<u>ipt0</u>
次のホップ・アドレス:	<u>fe80::5.6.7.8</u>

3.6.3.7 IPv6 ネットワーク対 IPv6 ネットワーク構成 (IPv4 構成済みトンネルあり)

図 3-8 のホスト A は、1 本の構成済みトンネルを介して IPv4 ネットワーク越しにホスト F と通信します。ホスト構成は、3.6.3.1 項のホスト A に似ています。各ノードは、他のネットワーク上のノードとの通信で、自動

的に省略時のルータを使用します。ルータ A の構成ワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
DNS/BIND 自動更新:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	<u>tu0</u> <u>tu1</u> _____
構成済みトンネル:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
構成済みトンネル	
インタフェース:	<u>ipt0</u>
宛先 IPv4 アドレス:	<u>5.6.7.8</u>
発信元 IPv4 アドレス:	<u>1.2.3.4</u>
RIPng:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレフィックス:	_____
ルータ	
インタフェース:	<u>tu0</u>
RIPng:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アドレス・プレフィックス:	<u>3ffe:1200:4112:1::/64</u>
インタフェース:	<u>tu1</u>
RIPng:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アドレス・プレフィックス:	<u>3ffe:1200:4112:2::/64</u>

tu0 インタフェースと tu1 インタフェースにはルータが接続されていないため、これらのインタフェースで RIPng を使用する必要はありません。

ルータ B の構成も同様です。ただし、構成済みトンネルの送信元アドレスは 5.6.7.8、宛先アドレスは 1.2.3.4 になり、tu0 と tu1 上で通知されるアドレス・プレフィックスはそれぞれ 3ffe:1200:4113:1::/64 と 3ffe:1200:4113:2::/64 になります。

注意

トンネル・インタフェースで RIPng を使用するようにルータを構成していない場合には、各ルータ間の経路を手動で指定する必要があります。

3.6.3.8 6to4 トンネルの構成

図 3-9 では、6to4 サイト内のノードはホスト E のみです。このノードは、6to4 トンネルを用いて IPv4 ネットワークを通してホスト B と通信を行います。どちらのノードも IPv6 の 6to4 アドレスを使用します。この場合、トンネルはホスト E とルータ B の間にあります。ホスト E の物理インタフェースは IPv4 ネットワークに接続されているため、ホスト E の物理インタフェースには IPv6 は構成されていません。ただし、IPv6 は 6to4 トンネルに構成されています。ホスト E のワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
DNS/BIND 自動更新 (ホストのみ):	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	_____
PPP上のIPv6ルーティング (ルータのみ):	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
6to4 トンネル:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
構成済みトンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
6to4 トンネル	
ホスト・アドレス:	<u>5.6.7.8</u>
サイト・プレフィックス:	<u>2002:506:708::/48</u>
アドレス・プレフィックス (ホストのみ):	<u>2002:506:708::/64</u>
リレー・ルータ・アドレス:	<u>2002:90a:b0c:1::1</u>
構成済みトンネル	
インタフェース:	_____
宛先IPv4アドレス:	_____
ソースIPv4アドレス:	_____
アドレス・プレフィックス:	_____

ルータ B は他の 6to4 サイトに対する Border Router で、そのサイトの IPv6 ルータでもあります。ルータ B は各サブネットの 6to4 プレフィックスを公開しています。各 6to4 プレフィックスの上位 48 ビットは、6to4 サイト・プレフィックスと同じでなければなりません。ルータ B のワークシートの記入例を次に示します。

IPv6 構成ワークシート	
IPv6 ルータ:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
DNS/BIND自動更新 (ホストのみ):	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6 インタフェース:	<u>ee0</u> <u>ee1</u> <u>ee2</u>
PPP上のIPv6ルーティング (ルータのみ):	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
6to4 トンネル:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
構成済みトンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
自動トンネル:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
手動経路:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
IPv6の開始:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
6to4 トンネル	
ホスト・アドレス:	<u>1.2.3.4</u>
サイト・プレフィックス:	<u>2002:102:304::/48</u>
アドレス・プレフィックス (ホストのみ):	<u></u>
リレー・ルータアドレス:	<u>2002:90a:b0c:1::1</u>
ルータ	
インタフェース:	<u>ee1</u>
RIPng:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレフィックス:	<u>2002:102:304:1::/64</u>
インタフェース:	<u>ee2</u>
RIPng:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
アドレス・プレフィックス:	<u>2002:102:304:2::/64</u>

ホスト B のワークシートの記入例を次に示します。ルータ B は 6to4 アドレス・プレフィックスをサブネット上に公開しているので、ホスト B はサイトに参加する際に、自分の 6to4 アドレスを自動的に設定します。6to4 トンネルのインタフェースを構成する必要はありません。

IPv6 構成ワークシート

IPv6 ルータ: ☐ Yes ☒ No
 DNS/BIND 自動更新 (ホストのみ): ☐ Yes ☒ No

IPv6 インタフェース: _____

PPP上のIPv6ルーティング (ルータのみ): ☐ Yes ☒ No

6to4トンネル: ☐ Yes ☒ No

構成済みトンネル: ☐ Yes ☒ No

自動トンネル: ☐ Yes ☒ No

手動経路: ☐ Yes ☒ No

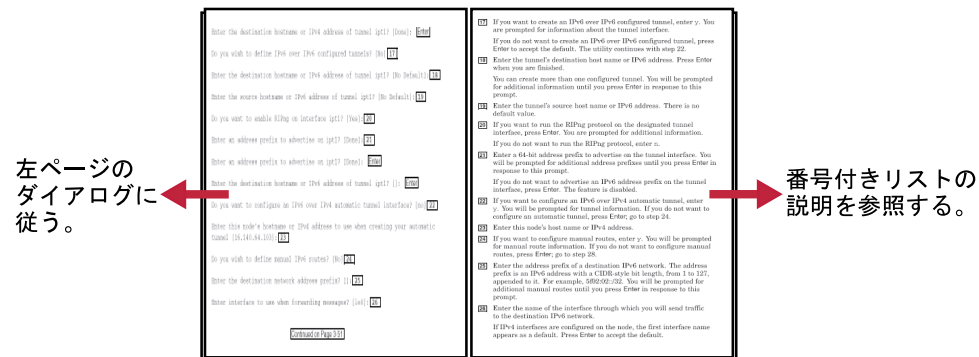
IPv6の開始: ☒ Yes ☐ No

3.7 システム上での IPv6 の構成

この節では、システムを IPv6 ホストまたは IPv6 ルータとして構成する方法を説明します。始める前に、構成ワークシートの記入が終わっていることを確認してください。

IPv6 は、`/usr/sbin/ip6_setup` ユーティリティを実行して構成します。このユーティリティは、IPv6 の通信に使用するインタフェースと接続のタイプを定義し、システム・ファイルを更新して IPv6 の動作ができるようにします。構成は、準備を除いて 10 分以内に終わります。

この項の説明の見方を、次に示します。



ZK-1884U-AI

この手順での省略時の応答は [] で囲まれています。Enter キーを押すと省略時の値が使用されます。

3.7.1 項 では、5 つのインタフェースを持つ IPv6 ホストの構成を説明します。インタフェースには、物理インタフェース (le0)、6to4 インタフェース (tun1)、IPv6 over IPv4 トンネル (ipt0)、IPv6 over IPv6 トンネル (ipt1)、自動トンネル (tun0) があります。le0 には手動経路が構成されています。

3.7.2 項 では、6 つのインタフェースを持つ IPv6 ルータの構成を説明します。インタフェースには、物理インタフェース (le0)、ポイント・ツー・ポイントのインタフェース (ppp0)、6to4 インタフェース (tun1)、IPv6 over IPv4 トンネル (ipt0)、IPv6 over IPv6 トンネル (ipt1)、自動トンネル (tun0) があります。le0 では、RIPng が起動され、手動経路が構成され、アドレス・プレフィックスが公開されています。ppp0 では、RIPng が起動され、アドレス・プレフィックスが公開されています。ipt0 および ipt1 では、RIPng が起動され、アドレス・プレフィックスが公開されています。

(このページは強制的に改ページしています。)

3.7.1 IPv6 ホストの構成

```
# /usr/sbin/ip6_setup   
  
This utility will gather some IPv4 information from your system  
then prompt you for IPv6 related information. You may enter a  
question mark (?) at any question for further explanation.  
  
Do you want to enable IPv6 in inetd services on this system? [Yes]:   
  
Do you want to configure this system as an IPv6 router? [No]:    
  
Do you want to enable dynamic updates of IPv6 addresses in the DNS/BIND namespace? [No]:   
  
Enter the fully qualified domain name for IPv6? [host1.corp.com]:    
  
Do you want to configure a 6to4 interface? [no]: y    
  
The 6to4 tunnel will be created as tun1  
  
Enter this node's hostname or IPv4 address to use when generating your site's  
6to4 prefix [16.140.64.103]:    
  
Your 6to4 site prefix is:  
2002:108c:4067::/48  
PLEASE SAVE THIS INFORMATION TO CONFIGURE YOUR 6TO4 SITE.  
  
Enter the address prefix to use on tun1 ? [2002:108c:4067::/64]:  
```

[ページ 3-48 に続く](#)

- ① IPv6 を初めて構成する場合、または以前にシステムを IPv6 のホストとして構成していた場合は、Enter を押して、ノードをルータではなく IPv6 ホストとして構成するように指示します。以前にシステムを IPv6 ルータとして構成していた場合は、y と入力します。

- ② DNS/BIND 名前データベース内の IPv6 アドレスを自動的に更新したい場合は y と入力します。ユーティリティは IPv6 の完全修飾ドメイン名の入力を促します。

Enter キーを押して省略時の値を指示したときには、手順 4 に進みます。

- ③ DNS/BIND 名前データベースに追加する IPv6 の完全修飾ドメイン名を入力します。

IPv4 がノード上に構成されている場合、現在の完全修飾ドメイン名が省略時の値として表示されます。Enter キーを押すと省略時の値が使用されます。

- ④ 6to4 インタフェースを構成する場合は、y と入力します。IPv4 のみのネットワークに接続された v4/v6 ホストで、他の 6to4 またはネイティブの IPv6 サイトと通信を行う場合には、6to4 インタフェースを構成します。この指定では、このホストのみを含む 6to4 サイトが作成されます。ユーティリティは、6to4 インタフェース情報の入力を促します。

6to4 サイトの内部にあるホストの場合は、6to4 アドレスが、標準の IPv6 メカニズムを用いて自動的に構成されるため、6to4 インタフェースを構成しないでください。このようなホスト、および他のすべてのホストの場合、Enter を押して省略時の値を使用し、手順 8 に進みます。

- ⑤ このホストのノード名または IPv4 アドレスを入力します。これは、6to4 サイト・プレフィックスを構成する際に使用されます。

IPv4 アドレスがノードに構成されている場合、そのアドレスが省略時の値として表示されます。Enter を押すと省略時の値が使用されます。

- ⑥ tun1 インタフェースで使用する、64 ビットのアドレス・プレフィックスを入力します。前の手順で作成した、6to4 サイトのアドレス・プレフィックスが省略時の値として表示されます。

Enter the hostname or 6to4 address of a 6to4 Relay Router? [2002:c058:6301::]: 7

6to4 interface configuration completed.

Enter the IPv6 LAN interfaces? [1e0]: 8

Do you wish to define IPv6 over IPv4 configured tunnels? [No] y 9

Enter the destination hostname or IPv4 address of tunnel ipt0? [No Default]: 16.140.64.142 10

Enter the source hostname or IPv4 address of tunnel ipt0? [16.140.64.103]: 11

Enter an address prefix to use on ipt0? [Done]: 12

Enter the destination hostname or IPv6 address of tunnel ipt1? [Done]:

Do you wish to define IPv6 over IPv6 configured tunnels? [No] y 13

- 7 このホストをネイティブの IPv6 サイト (IPv6 のみ) と通信させたいときには、6to4 Relay Router のホスト名または 6to4 ユニキャスト・アドレスを入力します。既知の 6to4 エニーキャスト・プレフィックスが省略時の値として表示されます。

Relay Router が不要の場合は、None と入力します。

これで、6to4 インタフェースの構成に必要な手順は終わりです。

- 8 IPv6 LAN インタフェースの名前を、空白文字で区切って入力します。

IPv4 インタフェースがノードに構成されている場合、そのインタフェース名が省略時の値として表示されます。Enter キーを押すと省略時の値が使用されます。構成済みトンネルのみを構成している場合は、none と入力します。

- 9 IPv6 over IPv4 構成済みトンネルを作成する場合は、y と入力します。トンネル・インタフェースの情報の入力が促されます。

Enter キーを押して省略時の値を指示したときには、手順 15 に進みます。

- 10 トンネルの宛先のホスト名または IPv4 アドレスを入力します。入力が終わったら Enter キーを押します。

構成済みトンネルは複数作成できます。プロンプトに対して Enter キーを押すまで、宛先を入力するプロンプトが繰り返し表示されます。

- 11 トンネルの送信元のホスト名または IPv4 アドレスを入力します。IPv4 アドレスがノードに構成されている場合、そのアドレスが省略時の値として表示されます。Enter キーを押すと、省略時の値が使用されます。

- 12 トンネル・インタフェースで使用するアドレス・プレフィックスを入力します。プロンプトに対して Enter キーを押すまで、アドレス・プレフィックスを入力するプロンプトが繰り返し表示されます。

ルータがトンネル・インタフェースのグローバル・アドレス・プレフィックスを公開していない場合は、アドレス・プレフィックスを入力します。プレフィックスの入力が終わったら Enter キーを押します。

ホストでトンネル・インタフェースの IPv6 アドレス・プレフィックスを使用したくないときには、Enter キーを押します。

- 13 IPv6 over IPv6 構成済みトンネルを作成する場合は、y と入力します。トンネル・インタフェースに関する情報の入力が促されます。

Enter キーを押して省略時の値を指示したときには、手順 17 に進みます。

Enter the destination hostname or IPv6 address of tunnel ipt1? [No Default]: 3ffe::2 **14**

Enter the source hostname or IPv6 address of tunnel ipt1? [No Default]: 3ffe::1 **15**

Enter an address prefix to use on ipt1? [Done]: **16**

Enter the destination hostname or IPv6 address of tunnel ipt2? [Done]:

Do you want to configure an IPv6 over IPv4 automatic tunnel interface? [no] y **17**

The automatic tunnel will be created as tun0

Enter this node's hostname or IPv4 address to use when creating your automatic tunnel [16.140.64.103]: y **18**

Do you wish to define manual IPv6 routes? [No] y **19**

Enter the destination network address prefix? []: 5f02:2::/32 **20**

Enter interface to use when forwarding messages? [le0]: y **21**

[ページ 3-52 に続く](#)

- 14 トンネルの宛先のホスト名または IPv6 アドレスを入力します。 入力が終わったら Enter を押します。

構成済みトンネルは複数作成できます。 プロンプトに対して Enter キーを押すまで、宛先を入力するプロンプトが繰り返し表示されます。

- 15 トンネルの送信元ホスト名または IPv6 アドレスを入力します。 省略時の値はありません。

- 16 トンネル・インタフェースで使用する 64 ビットのアドレス・プレフィックスを入力します。 プロンプトに対して Enter キーを押すまで、アドレス・プレフィックスを入力するプロンプトが繰り返し表示されます。

ルータがトンネル・インタフェースのグローバル・アドレス・プレフィックスを公開していない場合は、64 ビットのアドレス・プレフィックスを入力します。 プレフィックスの入力が終わったら、Enter キーを押します。

ホストでトンネル・インタフェースの IPv6 アドレス・プレフィックスを使用したくないときには、Enter キーを押します。

- 17 IPv6 over IPv4 自動トンネルを構成する場合は、y と入力します。 トンネル情報の入力が促されます。 自動トンネルを構成しない場合は Enter キーを押し、手順 19 に進みます。

- 18 このノードのホスト名または IPv4 アドレスを入力します。

- 19 手動経路を構成する場合は y と入力します。 手動経路情報の入力が促されます。 手動経路を構成しない場合は Enter キーを押して手順 23 に進みます。

- 20 宛先 IPv6 ネットワークのアドレス・プレフィックスを入力します。 アドレス・プレフィックスは、CIDR 形式のビット長 (1 ~ 127) を付加した IPv6 アドレスです。 たとえば、5f02:02::/32 のようになります。 プロンプトに対して Enter キーを押すまで、手動経路を入力するプロンプトが繰り返し表示されます。

- 21 宛先の IPv6 ネットワークにトラフィックを送信するために使用するインタフェースの名前を入力します。

IPv4 インタフェースがノードに構成されていない場合は、最初のインタフェースの名前が省略時の値として表示されます。 Enter キーを押すと省略時の値が使用されます。

Enter the next node's IPv6 address: [No Default]: 3ffe::5

Enter the destination network address prefix? [Done]:

You configured this node as a Host with the following

Interfaces:

```
tun1  6to4 Tunneling Enabled using 16.140.64.103
      Prefix 2002:108c:4067::/64
      Relay Router 2002:c058:6301::
le0    Dynamic Address Configuration Enabled
ipt0   Dynamic Address Configuration Enabled
      Tunnel Source 16.140.64.103
      Tunnel Destination 16.140.64.142
ipt1   Dynamic Address Configuration Enabled
      Tunnel Source 3ffe::1
      Tunnel Destination 3ffe::2
tun0   Automatic Tunneling Enabled using 16.140.64.103
```

Manual Routes:

```
5f02:2::/32                le0      3ffe::5 (G)
```

Do you wish to update the IPv6 startup procedures with this configuration? [No Default] y

Do you want to start IPv6? [Yes]:

- [22] 宛先ネットワークへのパスにある最初のルータの IPv6 アドレスを入力します。このアドレスと IPv6 アドレス・プレフィックスが、静的ルーティング・テーブルのエントリになります。

次のノードがこのノードと同じリンク上にあるか、または構成済みトンネルを通して到達可能である場合は、リンクにローカルなアドレスを入力します。次のノードが自動トンネルを通して到達可能であれば、IPv4 互換 IPv6 アドレスを入力します。その他の接続に対しては、IPv6 アドレスを入力します。

- [23] `ip6_setup` ユーティリティは構成情報を表示し、その構成情報で現在の起動手順を更新してよいか確認します。

その構成に不満がある場合は、`n` と入力します。ユーティリティはその場で終了し、現在の構成ファイルは変更されません。

その構成でよい場合は `y` と入力します。`ip6_setup` ユーティリティは、`/etc/inetd.conf`、`/etc/rc.config`、`/etc/routes` ファイルを IPv6 構成情報で更新します。`/etc/rc.config` ファイルには、システム起動スクリプトが IPv6 を起動するために使用する構成情報が含まれています。

- [24] IPv6 が現在システムで稼働していない場合は、IPv6 をその場で起動するかどうかを指定します。

IPv6 をその場で起動する場合は Enter キーを押します。`ip6_setup` ユーティリティが IPv6 を起動します。

その場で IPv6 を起動しない場合は `n` と入力します。IPv6 は次にシステムをブートした時に起動されます。

IPv6 が現在稼働中であれば、その場で再起動するかどうかを指定します。

3.7.2 IPv6 ルータの構成

```
# /usr/sbin/ip6_setup 

This utility will gather some IPv4 information from your system
then prompt you for IPv6 related information.  You may enter a
question mark (?) at any question for further explanation.

Do you want to enable IPv6 in inetd services on this system? [Yes]: 

Do you want to configure this system as an IPv6 router? [No]: y  

Do you want to configure a 6to4 interface? [no]: y  

The 6to4 tunnel will be created as tun1

Enter this node's hostname or IPv4 address to use when generating your site's
6to4 prefix [16.140.64.103]:  

Your 6to4 site prefix is:
      2002:108c:4067::/48
PLEASE SAVE THIS INFORMATION TO CONFIGURE YOUR 6TO4 SITE.

Enter the hostname or 6to4 address of a 6to4 Relay Router? [2002:c058:6301::]:  

6to4 interface configuration completed.

Enter the IPv6 LAN interfaces? [ le0 ]:  

Do you want to enable RIPng on interface le0? [Yes]:  
```

- ① IPv6 を初めて構成する場合、または以前にシステムを IPv6 のホストとして構成していた場合は、`y` と入力して、ノードをホストではなく IPv6 ルータとして構成するように指示します。以前にシステムを IPv6 ルータとして構成していた場合は、Enter キーを押します。

- ② 6to4 インタフェースを構成する場合は、`y` と入力します。6to4 Border Router の場合は、6to4 インタフェースを構成します。ユーティリティは、6to4 インタフェース情報の入力を促します。

その他のルータの場合は、Enter キーを押して省略時の値を使用し、手順 5 に進みます。

- ③ このルータのノード名または IPv4 アドレスを入力します。これは、IPv6 サイトに接続するインタフェース上でホストに公開可能な 6to4 サイト・プレフィックスを構成するために使用されます。このアドレスは、IPv4 ネットワークに接続されたルータのインタフェースに構成された、グローバルで有効な IPv4 アドレスでなければなりません。

IPv4 アドレスがノード上に構成されている場合、そのアドレスが省略時の値として表示されます。Enter キーを押すと省略時の値が使用されます。

- ④ この Border Router の 6to4 サイト内のホストを、ネイティブの IPv6 サイト (IPv6 のみ) と通信させる場合は、ホスト名を入力するか、または 6to4 Relay Router の 6to4 ユニキャスト・アドレスを入力します。既知の 6to4 エニキャスト・プレフィックスが省略時の値として表示されます。

Relay Router が不要の場合は `None` と入力します。

- ⑤ IPv6 LAN インタフェースの名前を、空白文字で区切って入力します。

IPv4 インタフェースがノードに構成されている場合、そのインタフェースの名前が省略時の値として表示されます。Enter キーを押すと省略時の値が使用されます。IPv4 または IPv6 の構成済みトンネルのみを構成している場合は、`none` と入力します。

- ⑥ このインタフェース上で RIPng プロトコルを使用するには、Enter キーを押します。その他の情報の入力が促されます。

RIPng プロトコルを使用しない場合は `n` と入力します。

Enter an address prefix to advertise on le0? [No Default]: 5f02:2::/64

Enter an address prefix to advertise on le0? [Done]:

Do you wish to configure IPv6 routing over any PPP links? [No] y

Enter a PPP interface name? [ppp0]:

Do you want to enable RIPng on interface ppp0? [Yes]:

Enter an address prefix to advertise on ppp0? [No Default]: 5f03:3::/64

Enter an address prefix to advertise on ppp0? [Done]:

Enter a PPP interface name? [Done]:

Do you wish to define IPv6 over IPv4 configured tunnels? [No]

- 7 このインタフェース上でルータが IPv6 アドレス・プレフィックスを公開するようにしたい場合は、64ビットのアドレス・プレフィックスを入力します。プロンプトに対して Enter キーを押すまで、アドレス・プレフィックスを入力するプロンプトが繰り返し表示されます。

6to4 Border Router の場合、64 ビットの 6to4 プレフィックスを、6to4 サイトに接続されたリンクに公開する必要があります。

このインタフェース上でルータが IPv6 アドレス・プレフィックスを公開しないようにする場合は、Done と入力します。アドレス・プレフィックスを入力しない場合、この機能は無効になります。

- 8 既存の PPP リンク上で IPv6 ルーティングを使用する場合は、y と入力します。PPP ルーティング情報の入力促されます。

IPv6 ルーティングを使用しない場合は、Enter キーを押して省略時の値を使用し、手順 12 に進みます。

- 9 IPv6 を使用する PPP インタフェースの名前を入力します。プロンプトに対して Enter キーを押すまで、PPP インタフェースを入力するプロンプトが繰り返し表示されます。

- 10 このインタフェースで RIPng プロトコルを使用する場合は、Enter キーを押します。その他の情報の入力促されます。

RIPng プロトコルを使用しない場合は n と入力します。

- 11 指定したインタフェース上で、ルータが IPv6 アドレス・プレフィックスを公開するようにしたい場合は、64 ビットのアドレス・プレフィックスを入力します。プロンプトに対して Enter キーを押すまで、アドレス・プレフィックスを入力するプロンプトが繰り返し表示されます。

指定したインタフェース上で、ルータが IPv6 アドレス・プレフィックスを公開しないようにする場合は Done と入力します。アドレス・プレフィックスを入力しない場合、この機能は無効になります。

- 12 IPv6 over IPv4 構成済みトンネルを作成する場合は y と入力します。トンネル・インタフェースに関する情報の入力促されます。

IPv6 over IPv4 構成済みトンネルを作成しない場合は、Enter キーを押して省略時の値を使用し、手順 17 に進みます。

Enter the destination hostname or IPv4 address of tunnel ipt0? [No Default]: 16.140.64.142

Enter the source hostname or IPv4 address of tunnel ipt0? [16.140.64.103]:

Do you want to enable RIPng on interface ipt0? [Yes]:

Enter an address prefix to advertise on ipt0? [Done]: aaa::/64

Enter an address prefix to advertise on ipt0? [Done]:

Enter the destination hostname or IPv4 address of tunnel ipt1? [Done]:

Do you wish to define IPv6 over IPv6 configured tunnels? [No] y

Enter the destination hostname or IPv6 address of tunnel ipt1? [No Default]: 3ffe::2

Enter the source hostname or IPv6 address of tunnel ipt1? [No Default]: 3ffe::1

Do you want to enable RIPng on interface ipt1? [Yes]:

- 13 トンネルの宛先ホスト名または IPv4 アドレスを入力します。入力が終わったら Enter キーを押します。

複数の構成済みトンネルを作成できます。プロンプトに対して Enter を押すまで、その他の情報を入力するプロンプトが繰り返し表示されます。

- 14 トンネルの送信元ホスト名または IPv4 アドレスを入力します。IPv4 アドレスがノードに構成されている場合、そのアドレスが省略時の値として表示されます。Enter キーを押すと省略時の値が使用されます。

- 15 指定したトンネル・インタフェースで RIPng プロトコルを使用するには、Enter キーを押します。その他の情報の入力が促されます。

RIPng プロトコルを使用しない場合は `n` と入力します。

- 16 指定したトンネル・インタフェース上で、ルータが IPv6 アドレス・プレフィックスを公開するようにしたい場合は、64 ビットのアドレス・プレフィックスを入力します。プロンプトに対して Enter キーを押すまで、アドレス・プレフィックスを入力するプロンプトが繰り返し表示されます。

指定したトンネル・インタフェース上で、ルータが IPv6 アドレス・プレフィックスを公開しないようにする場合は、`Done` と入力します。アドレス・プレフィックスを入力しない場合、この機能は無効になります。

- 17 IPv6 over IPv6 構成済みトンネルを作成する場合は、`y` と入力します。トンネル・インタフェースの情報の入力が促されます。

IPv6 over IPv6 構成済みトンネルを作成しない場合は、Enter を押して省略時の値を採用し、手順 22 に進みます。

- 18 トンネルの宛先のホスト名または IPv6 アドレスを入力します。入力が終わったら Enter キーを押します。

複数の構成済みトンネルを作成できます。プロンプトに対して Enter キーを押すまで、その他の情報を入力するプロンプトが繰り返し表示されます。

- 19 トンネルの送信元のホスト名または IPv6 アドレスを入力します。省略時の値はありません。

- 20 このトンネル・インタフェースで RIPng プロトコルを使用する場合は、Enter キーを押します。その他の情報の入力が促されます。

RIPng プロトコルを使用しない場合は `n` と入力します。

```

Enter an address prefix to advertise on ipt1? [Done]: bbbb::/64 Enter 21

Enter an address prefix to advertise on ipt1? [Done]: Enter

Enter the destination hostname or IPv6 address of tunnel ipt2? [Done]: Enter

Do you want to configure an IPv6 over IPv4 automatic tunnel interface? [no] Enter 22

Enter this node's hostname or IPv4 address to use when creating your automatic
tunnel [16.140.64.103]: Enter 23

Do you wish to define manual IPv6 routes? [No] y Enter 24

Enter the destination network address prefix? []: 5f02:2::/64 Enter 25

Enter interface to use when forwarding messages? [le0]: Enter 26

Enter the next node's IPv6 address: [No Default]: 3ffe::5 Enter 27

Enter the destination network address prefix? [Done]: Enter

You configured this node as a Router with the following 28

Interfaces:
  tunl  6to4 Tunneling Enabled using 16.140.64.103
        Prefix 2002:108c:4067::/64
        Relay Router 2002:c058:6301::
  le0    RIP Enabled
        Prefix 5f02:2::/64
  ppp0   RIP Enabled
        Prefix 5f03:3::/64
  ipt0   RIP Enabled
        Tunnel Source 16.140.64.103
        Tunnel Destination 16.140.64.142
        Prefix aaaa::/64
  ipt1   RIP Enabled
        Tunnel Source 3ffe::1
        Tunnel Destination 3ffe::2
        Prefix bbbb::/64
  tun0   Automatic Tunneling Enabled using 16.140.64.103

Manual Routes:
  5f02:2::/64          le0      3ffe::5 (G)

Do you wish to update the IPv6 startup procedures with this
configuration? [No Default] y Enter

Do you want to start IPv6? [Yes]: Enter 29

```

- [21] トンネル・インタフェース上で公開する 64 ビットのアドレス・プレフィックスを入力します。プロンプトに対して Enter キーを押すまで、アドレス・プレフィックスを入力するプロンプトが繰り返し表示されます。
- トンネル・インタフェース上で IPv6 アドレス・プレフィックスを公開しない場合は、Enter キーを押します。この機能は無効になります。
- [22] IPv6 over IPv4 自動トンネルを構成する場合は `y` と入力します。トンネル情報の入力促されます。自動トンネルを構成しない場合は Enter キーを押して手順 24 に進みます。
- [23] このノードのホスト名または IPv4 アドレスを入力します。
- [24] 手動経路を構成する場合は `y` と入力します。手動経路情報の入力促されます。手動経路を構成しない場合は Enter キーを押して手順 28 に進みます。
- [25] 宛先 IPv6 ネットワークのアドレス・プレフィックスを入力します。アドレス・プレフィックスは、CIDR 形式のビット長 (1 ~ 127) を付加した IPv6 アドレスです。たとえば、`5f02:02::/32` のようになります。プロンプトに対して Enter キーを押すまで、手動経路を入力するプロンプトが繰り返し表示されます。
- [26] 宛先の IPv6 ネットワークにトラフィックを送信するために使用するインタフェースの名前を入力します。
- IPv4 インタフェースがノードに構成されている場合は、最初のインタフェースの名前が省略時の値として表示されます。Enter キーを押すと省略時の値が使用されます。
- [27] 宛先ネットワークへのパスにある最初のルータの IPv6 アドレスを入力します。このアドレスと IPv6 アドレス・プレフィックスが、静的ルーティング・テーブルのエントリになります。
- 次のノードがこのノードと同じリンク上にあるか、または構成済みトンネルを通して到達可能である場合は、リンクにローカルなアドレスを入力します。次のノードが自動トンネルを通して到達可能であれば、IPv4 互換 IPv6 アドレスを入力します。その他の接続に対しては、IPv6 アドレスを入力します。
- [28] `ip6_setup` ユーティリティは構成情報を表示し、その構成情報で現在の起動手順を更新してよいか確認します。

その構成に不満がある場合は、`n` と入力します。ユーティリティはその場で終了し、現在の構成ファイルは変更されません。

その構成でよい場合は `y` と入力します。 `ip6_setup` ユーティリティは、`/etc/inetd.conf`、`/etc/rc.config`、`/etc/routes` ファイルを IPv6 構成情報で更新します。 `/etc/rc.config`、`/etc/routes`、`/etc/ip6rtrd.conf` ファイルには、システム起動スクリプトが IPv6 を起動するために使用する構成情報が含まれています。これらのファイルを編集すると構成を変更できます。

- [29]** IPv6 が現在システムで稼働していない場合は、IPv6 をその場で起動するかどうかを指定します。

IPv6 をその場で起動する場合は Enter キーを押します。 `ip6_setup` ユーティリティが IPv6 を起動します。

その場で IPv6 を起動しない場合は `n` と入力します。 IPv6 は次にシステムをブートした時に起動されます。

IPv6 が現在稼働中であれば、その場で再起動するかどうかを指定します。

3.8 構成後の作業

`ip6_setup` ユーティリティによる IPv6 の初期構成が完了したら、必要に応じて次の作業を実行します。

- 6bone ネットワークへの接続
- IPv6 用の新しいインタフェースの初期化
- インタフェースの IPv6 構成の解除
- 構成済みトンネルの作成
- インタフェースへのアドレスの追加またはアドレスの削除
- 省略時のルータの追加または削除
- オンリンク・プレフィックスへの経路の手動追加
- カーネルのルーティング・サポートの構成
- 実行時構成ファイル (`/etc/rc.config`) の編集
- ルータ構成ファイル (`/etc/ip6rtrd.conf`) の編集
- `ip6` および `iptunnel` カーネル・サブシステムのチューニング

以降の項では、これらの各作業について説明します。

3.8.1 6bone ネットワークへの接続

6bone ネットワークに接続するには、インターネット接続に通常使用している IPv4 パスに近い、適切な 6bone 接続ポイントを選択します。6bone の Web サイト (<http://www.6bone.net>) には、6bone ネットワークへの加入方法と接続ポイントのを見つけ方に関する情報が掲載されています。

たとえば、Compaq の Palo Alto サイト (米国カリフォルニア州) を経由して 6bone ネットワークに接続するには、ホストやルータ上の IPv6 の構成前または構成後に、次の手順を実行します。

1. ルータの IPv4 アドレスを次のアドレスに送信し、IPv4 トンネルを登録します。
`gw-6bone@pa.dec.com`
2. このトンネルのサポートが構成された旨を通知する HP からの返信を待ちます。ユーザのサイトで使用する IPv6 グローバル・アドレス・プレフィックスと、HP の Palo Alto のルータの IPv4 アドレスが HP から提供されます。
3. `ip6_setup` ユーティリティを実行してトンネルを構成します。ホストの構成については 3.7.1 項、ルータの構成については 3.7.2 項を参照してください。または、`iptunnel` コマンドを実行することもできます (3.8.4 項を参照)。
4. 次のいずれかの HP の IPv6 ノードに対して `ping` コマンドを実行し、トンネルが正しく機能しているかどうかを確認します。

```
altavista.ipv6.digital.com
ftp.ipv6.digital.com
www.ipv6.digital.com
```

3.8.2 IPv6 用の新しいインタフェースの初期化

システムに新しいインタフェース・カードを追加したり、他の種類のインタフェース・カードと交換した場合には、装着した新しいカードを IPv6 用に初期化しなければなりません。インタフェースを初期化するには、`ifconfig` コマンドを次の構文で使します。

```
ifconfig device ipv6 up
```

LAN インタフェースの場合、`ifconfig` コマンドはリンク・ローカル・アドレス (FE80::) を生成し、重複アドレスの検出処理を開始します。

たとえば、イーサネット・インタフェース `ee0` を IPv6 用に初期化するには、次のコマンドを実行します。

```
# ifconfig ee0 ipv6 up
```

ループバック・インタフェースを IPv6 用に初期化するには、次のコマンドを実行します。

```
# ifconfig lo0 ipv6 up
```

自動トンネル・インタフェースを初期化するには、次のコマンドを実行します。

```
# ifconfig tun0 ipv6 up
```

このコマンドを実行すると、システムのいずれかの IPv4 アドレスがトンネルの端点として選択されます。

新しいインタフェース・カードを継続して使用する場合には、`ip6_setup` ユーティリティを使用してください。

3.8.2.1 IPv6 インタフェース識別子の設定

インタフェースを初期化する際に `ifconfig` コマンドを `ip6interfaceid` パラメータ付きで使用すれば、IPv6 インタフェース ID も設定できます。たとえば、イーサネット・インタフェース `ee0` を IPv6 用に初期化し、インタフェース ID に 64 ビット値の `0x0123456789abcdef` を設定するには、次のコマンドを実行します。

```
# ifconfig ee0 ip6interfaceid ::0123:4567:89ab:cdef ipv6 up
```

インタフェース ID は標準の IPv6 アドレス・フォーマットで表現しますが、使用されるのは下位 64 ビットのみです。

3.8.3 インタフェースからの IPv6 の削除

インタフェースから IPv6 を削除すると、すべての IPv6 アドレスや、このインタフェースを経由する IPv6 経路など、このインタフェースに関連する IPv6 構成がすべて削除されます。インタフェースから IPv6 を削除するには、`ifconfig` コマンドを次の構文で使います。

```
ifconfig device -ipv6
```

たとえば、イーサネット・インタフェース `ee0` から IPv6 を削除するには、次のコマンドを実行します。

```
# ifconfig ee0 -ipv6
```

3.8.4 構成済みトンネルの作成

構成済みトンネル (手動トンネル) を作成するには、`/usr/sbin/iptunnel` コマンドを次の構文で使します。

```
iptunnel create remote-tunnel-endpoint [local-tunnel-endpoint]
```

たとえば、リモート・システム `16.20.136.47` へのトンネルを作成するには、次のコマンドを実行します。

```
# iptunnel create 16.20.136.47
```

作成したトンネルを IPv6 用に初期化するには、次のコマンドを実行します。

```
# ifconfig ipt0 ipv6 up
```

この変更を恒久的にするには、`ip6_setup` ユーティリティを使します。

3.8.5 インタフェースへのアドレスの追加

インタフェースへの IPv6 アドレスの追加または割り当てを行い、同時にインタフェース ID を自動的に追加するようにカーネルに指示するには、`ifconfig` コマンドを次の構文で使します。

```
ifconfig interface-name inet6 ip6prefix prefix
```

次のコマンドは、インタフェース `ln0` にプレフィックス `3ffe:1200:4112:2::/64` を割り当てます (インタフェース ID は `0a00:2bff:fe12:3456`)。このコマンドの結果、インタフェースのアドレスは `3ffe:1200:4112:2:0a00:2bff:fe12:3456` になります。

```
# ifconfig ln0 inet6 ip6prefix 3ffe:1200:4112:2::/64
```

`ip6prefix` パラメータが、インタフェース ID をアドレス・プレフィックスに自動的に追加するようにカーネルに指示します。

完全な IPv6 アドレスをインタフェースに手動で追加または割り当てるには、`ifconfig` コマンドを次の構文で使します。

```
ifconfig interface-name inet6 address
```

次のコマンドは、インタフェース `ee0` にアドレス `3ffe:1200:4112:2::1` を割り当てます。

```
# ifconfig ee0 inet6 3ffe:1200:4112:2::1
```

注意

IPv6 ホストでは、ルータから通知される情報を基に、`nd6hostd` デーモンによってインタフェース・プレフィックスが自動的に構成されます。

IPv6 ルータでは、`/etc/ip6rtrd.conf` ファイルの内容を基に、`ip6rtrd` デーモンによってインタフェース・プレフィックスが自動的に構成されます。

3.8.6 インタフェースからのアドレスの削除

インタフェースから IPv6 アドレスを手動で削除するには、`ifconfig` コマンドを次の構文で使します。

```
ifconfig interface-name inet6 delete address
```

次に例を示します。

```
# ifconfig ee0 inet6 delete 3ffe:1200:4112:2::1
```

3.8.7 省略時のルータの追加または削除

省略時のルータを追加するには、`route` ユーティリティを次の構文で使します。

```
route add -inet6 default router-address -dev interface
```

次に例を示します。

```
# route add -inet6 default fe80::0a00:2bff:fe12:3456 -dev ee0
```

省略時のルータを削除するには、`route` ユーティリティを次の構文で使します。

```
route delete -inet6 default router-address -dev interface
```

次に例を示します。

```
# route delete -inet6 default fe80::0a00:2bff:fe12:3456 -dev ee0
```

注意

IPv6 ホストの場合、ルータから通知される情報を基に、nd6hostd デーモンによってルータの追加および削除が自動的に行われます。

3.8.8 オンリンク・プレフィックス用の経路の手動追加

インタフェースにアドレスとプレフィックスを手動で追加すると、静的経路も追加できます。静的経路を追加すれば、プレフィックスが同じノードへのトラフィックは、ルータを経由せずに直接宛先に送信されます。たとえば、リンク・ローカル・アドレス `fe80::0a00:2bff:fe12:3456` で初期化したイーサネット・インタフェースにプレフィックス `3ffe:1200:4112:5::/64` を追加した場合、同じプレフィックスを持つ近隣ノードへの経路を追加するには、次のコマンドを使用します。

```
# route add -inet6 3ffe:1200:4112:5::/64 fe80::0a00:2bff:fe12:3456 -interface
```

このコマンドによって、プレフィックス `3ffe:1200:4112:5::/64` を持つ宛先が、アドレス `fe80::0a00:2bff:fe12:3456` のインタフェースからアクセスできるようになります。つまり、`3ffe:1200:4112:5::/64` がオンリンク・プレフィックスになります。

注意

IPv6 ホストでは、ルータから通知される情報を基に、nd6hostd デーモンが自動的にオンリンク・プレフィックスを追加します。

3.8.9 カーネルのルーティング・サポートの構成

ルータを構成するには、その前に `ipv6` カーネル・サブシステムの `ipv6forwarding` 属性と `ipv6router` 属性に 1 を設定して、転送を使用可能にする必要があります。これらの属性を設定するには、次に示す `sysconfig` コマンドを実行します。

```
# /sbin/sysconfig -r ipv6 ipv6forwarding=1
# /sbin/sysconfig -r ipv6 ipv6router=1
```

これらのコマンドは通常、IPv6 ルータとして構成したノードのシステム・スタートアップ・スクリプトで実行されます。

3.8.10 実行時構成ファイルの編集

システムを IPv6 ホストまたは IPv6 ルータとして構成すると、システムのスタートアップ手順で IPv6 の起動に使用される情報が、`/etc/rc.config` ファイルに格納されます。このファイルは、`rcmgr` コマンドを使用すると、必要に応じて編集できます。IPv6 は、次の変数を使用します。

`IPV6="yes|no"`

`yes` を設定すると、システムのスタートアップ時に IPv6 が起動されます。

`IP6DEV_n="dev"`

IPv6 のデバイス名を指定します。このデバイス名は、`rc.config` ファイル内に存在しなければなりません。`n` は整数で、0 から順に、デバイス 1 つごとに 1 ずつ増やします。

`IP6IFCONFIG_n_m="string"`

システムのスタートアップ時に `ifconfig` コマンド行で使用するオプションとパラメータを指定します。`n` は、`IP6DEV_n` 変数と同じ値の整数です。`m` は整数で、0 から順に、各デバイスの `ifconfig` 行 1 つごとに 1 ずつ増やします。

`NUM_IP6CONFIG="number"`

構成した IPv6 デバイスの数を指定します。

`IP6ROUTER="yes|no"`

`yes` を設定すると、ノードを IPv6 ルータとして構成します。`no` を設定すると、ノードを IPv6 ホストとして構成します。

`IP6RTRD="yes|no"`

`yes` を設定すると、IPv6 のスタートアップ時に IPv6 ルータ・デーモン (`ip6rtrd`) を起動します。

`IP6RTRD_FLAGS="string"`

`ip6rtrd` デーモンの起動時に使用するオプションとパラメータを含む文字列を指定します。

ND6HOSTD="yes|no"

yes を設定すると、IPv6 のスタートアップ時に IPv6 ホスト・デーモン (nd6hostd) を起動します。

ND6HOSTD_FLAGS="string"

nd6hostd デーモンの起動時に使用するオプションとパラメータを含む文字列を指定します。

IPTUNNEL_n="string"

システムのスタートアップ時に構成済みトンネルの作成に使用するオプションとパラメータを含む文字列を指定します。この変数を使用されるのは、IP6DEV_n 変数で指定したデバイスが構成済みトンネル (ipt0 など) である場合のみです。

例 3-1 に、/etc/rc.config ファイル内の IPv6 ホスト用変数の一例を示します。

例 3-1: IPv6 ホストの構成変数の例

```
IPV6="yes"
IP6DEV_0="tu0"
IP6IFCONFIG_0_0="ipv6 up"
IP6DEV_1="tun0"
IP6IFCONFIG_1_0="ipv6 up"
NUM_IP6CONFIG=2
IP6ROUTER="no"
IP6RTRD="no"
IP6RTRD_FLAGS=""
ND6HOSTD="yes"
ND6HOSTD_FLAGS=" -u -n host1.corp.com"
```

例 3-2 に、/etc/rc.config ファイル内の IPv6 ルータ用変数の一例を示します。

例 3-2: IPv6 ルータの構成変数の例

```
IPV6="yes"
IP6DEV_0="tu0"
IP6IFCONFIG_0_0="ipv6 up"
IP6DEV_1="tu1"
IP6IFCONFIG_1_0="ipv6 up"
```

例 3-2: IPv6 ルータの構成変数の例 (続き)

```
NUM_IP6CONFIG=2
IP6ROUTER="yes"
IP6RTRD="yes"
IP6RTRD_FLAGS="/etc/ip6rtrd.conf"
ND6HOSTD="no"
ND6HOSTD_FLAGS=""
```

3.8.11 ルータ構成ファイルの編集

システムを IPv6 ルータとして構成すると、ip6rtrd デーモンによって定期的にルータ通知メッセージが送信されます。このメッセージは、次の目的に使用されます。

- 自分自身を、IPv6 トラフィックの省略時ルータの候補として通知する
同じリンク上の IPv6 ノードは、この通知を近隣検出処理の一環として受信します。
- IPv6 アドレス・プレフィックスを通知する
この場合、同じリンク上の IPv6 ノードは、アドレスの自動構成を実行します。

/etc/ip6rtrd.conf ファイルには、ルータ通知メッセージの送信に必要な構成データが格納されています。このファイルは、システムがルータとして構成されている場合、ip6_setup の実行時に作成されます。リンク・インタフェースおよび通知されたプレフィックスが挿入され、その他の省略時の値が使用されます。このファイルは、複数のプレフィックス値を使用している場合など、ネットワーク環境上の必要に応じて編集できます。詳細については、ip6rtrd.conf(4) を参照してください。

例 3-3 に、ルータ構成ファイルの一例を示します。

例 3-3: ip6rtrd.conf ファイルの例

```
#
# Sample ip6rtrd configuration file
#
interface tu0 {
    MaxRtrAdvInterval 600
    MinRtrAdvInterval 200
```

例 3-3: ip6rtrd.conf ファイルの例 (続き)

```
AdvManagedFlag 0
AdvOtherConfigFlag 0
AdvLinkMTU 1500
AdvReachableTime 0
AdvRetransTimer 0
AdvCurHopLimit 64
AdvDefaultLifetime 1800
Prefix dec:1::/64 {
    AdvValidLifetime 1200
    AdvPreferredLifetime 600
    AdvOnLinkFlag 1
    AdvAutonomousFlag 1
}
}
```

3.8.12 カーネル・サブシステムのチューニング

IPv6 サブシステムは、sysconfig ユーティリティや dxkerneltuner ユーティリティを使用してチューニングできます。IPv6 サブシステムのチューニングについては sys_attrs_ipv6(5)、IP トンネル・サブシステムのチューニングについては sys_attrs_ip tunnel(5) を参照してください。

3.9 IPv6 デーモンのログ・ファイル

nd6hostd デーモンと ip6rtrd デーモンは、情報イベントや重大なイベントのログを、/var/adm/syslog.dated/date/daemon.log ファイルに取得します。このメッセージ・ファイルの内容は、SysMan Menu ユーティリティのイベント・ビューアで参照できます。イベント・ビューアについての詳細は、11.9 節を参照してください。

これらのデーモンは、省略時の設定ではデバッグ情報のログを取得しません。nd6hostd デーモンにデバッグ情報のログを取得させるには、次のコマンドを実行します。

```
# rcmgr set ND6HOSTD_FLAGS "-d -l /usr/tmp/nd6hostd.log"
# /usr/sbin/rcinet restart inet6
```

ip6rtrd デーモンにデバッグ情報のログを取得させるには、次のコマンドを実行します。

```
# rcmgr set IP6RTRD_FLAGS "-d -l /usr/tmp/ip6rtrd.log"
# /usr/sbin/rcinet restart inet6
```

IPsec (Internet Protocol Security) は、IPv4 (Internet Protocol Version 4) と IPv6 (Internet Protocol Version 6) 用に、相互運用可能で、高品質の暗号に基づくセキュリティを提供するセキュリティ・フレームワークです。このセキュリティは IP (Internet Protocol) の階層で実現され、IP とその上位層プロトコルの両方を保護します。

IP 層での全トラフィックに対してセキュリティが必要でない場合は、Secure Shell ソフトウェアや SSL (Secure Socket Layer) を使用する方法もあります。これらの技術についての詳細は、『セキュリティ管理ガイド』を参照してください。

この章では、次のような内容について説明します。

- IPsec 環境 (4.1 節)
- セキュア接続 (4.2 節)
- セキュリティ・アソシエーション (4.3 節)
- 鍵交換 (4.4 節)
- 証明書 (4.5 節)
- IPsec の計画 (4.6 節)
- IPsec の構成 (4.7 節)
- 構成後の作業 (4.8 節)

問題解決の情報については、10.5 節と付録 B を参照してください。

4.1 IPsec 環境

IPsec 環境では、IPsec プロトコルを使用するシステムには次のような役割があります。

- ホスト — 他のホストとのセキュア接続を確立して維持するシステム。

- セキュア・ゲートウェイ — 他のセキュア・ゲートウェイとのセキュア接続を確立して維持するファイアウォールまたはルータ。通常、他のホストのためにセキュア接続を確立します。

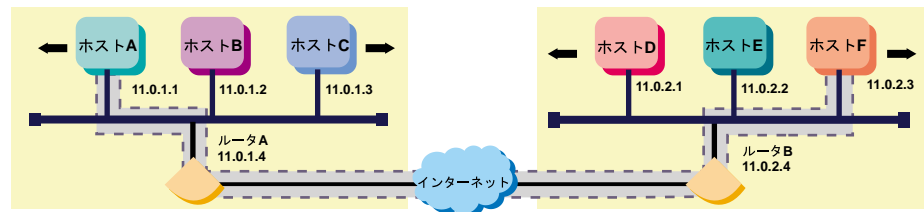
IPsec ホストは、セキュア・ゲートウェイとの間にセキュア接続を確立して維持することもできます。この場合、ホストは自分自身のためのセキュア・ゲートウェイとして動作します。

この節の後半には、IPsec 構成の例を示します。IPsec を構成しようとしているシステムの環境に最も近い構成を選択してください。これらの構成は、4.6.7 項で各構成でシステムを構成する方法を説明する際にも使用します。また、制限事項はすべて節の末尾に列挙しています。

4.1.1 ホスト対ホストの構成

図 4-1 は、ホスト A とホスト F が IPsec プロトコルを使用してセキュア接続を確立する単純な構成です。パケットは、トランスポート・モードで、エンド・ツー・エンドで保護されます。

図 4-1: ホスト対ホストの構成例

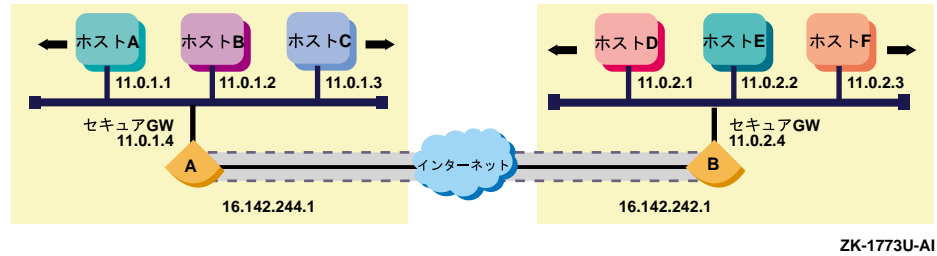


ZK-1780U-AI

4.1.2 セキュア・ゲートウェイ対セキュア・ゲートウェイの構成

図 4-2 は、2 つのセキュア・ゲートウェイが IPsec プロトコルを使用して、インターネットを通してセキュア接続を介して通信する構成です。この構成では、インターネットを通して VPN (Virtual Private Network) を作成します。

図 4-2: セキュア・ゲートウェイ対セキュア・ゲートウェイの構成例



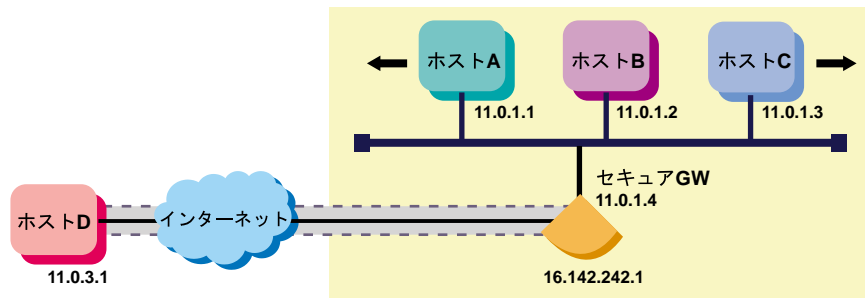
ZK-1773U-AI

Tru64 UNIX のホストが 2 つのサブネット間でセキュア・ゲートウェイとして動作している場合、このホストに対する受信と送信の両方の各パケットを処理しなければなりません。ゲートウェイのセキュア側つまりイントラネット側のパケットは、IPsec で保護されません (またはトランスポート・モードでエンド・ツー・エンドで保護されます)。ゲートウェイの非セキュア側つまりインターネット側のパケットは、リモート・セキュア・ゲートウェイへのトンネル・モードを用いて保護されます。

4.1.3 ホスト対セキュア・ゲートウェイの構成

図 4-3 は、リモート・ホストがインターネットを通してセキュア・ホストに接続されている構成です。ホストとセキュア・ゲートウェイの間のパケットは、トンネル・モードを用いて保護されています。

図 4-3: ホスト対セキュア・ゲートウェイの構成例



ZK-1772U-AI

リモート・ホストは、セキュア・ゲートウェイを管理するために、トランスポート・モードでセキュア・ゲートウェイとの間にセキュア接続を確立します。この場合、パケットはサブネットに転送されずにセキュア・ゲートウェイ上で終了します。

4.1.4 制限

IPsec のこの実装には次のような制限があります。

- 複数のノードへのセキュリティ・アソシエーションを必要とする単一の接続 (ポリシー) を指定することはできません。ホストは、自分自信のセキュア・ゲートウェイとして動作したり、リモート・セキュア・ゲートウェイの背後のホストとエンド・ツー・エンドの IPsec を行うことはできません。
- 証明書、CRL (Certificate Revocation List)、証明書の非公開鍵は、ローカル・ホストのファイルに保存しなければなりません。LDAP サーバを介したリモート・アクセスはサポートされていません。

4.2 セキュア接続

IPsec の動作は、システム上に定義されたセキュア接続によって決まります。各セキュア接続は、2 台のホスト間または 2 つのサブネット間の双方向接続を表します。セキュア接続の定義は、その接続の名前と規則を定義することで行います。それぞれの規則には次のようなものが含まれます。

セレクト	その規則に一致する受信または送信 IP パケットを識別します。セレクトでは、一致するパケットのローカル IP アドレス、リモート IP アドレス、上位層プロトコル、上位層ポートの値を指定します。すべての値でも特定の値のみでもかまいません。また、ローカルおよびリモートの値に、サブネットまたは IP アドレス・レンジを使用することもできます。
アクション	セレクトに一致する IP パケットの処理方法を記述します。パケットを破棄 (ドロップ) したり、IPsec 処理をバイパス (セキュリティ処理を通さずにパケットの出入りを許可する) したり、IPsec 処理を適用したりするアクションがあります。どの規則にも一致しないパケットは破棄されます。
プロポーザル	適用する IPsec プロトコルのセット、使用する認証および暗号化のアルゴリズム、関連するパラメータ (鍵) をリストします。手動鍵交換の場合、プロポー

ザルは 1 つ (プロトコルとアルゴリズムが 1 つ) に限られます。プロポーザルは、IPsec 処理のみを適用する規則に使用します。

SysMan IPsec ユーティリティは、IPsec 構成全体を形成するセキュア接続の定義に使用します。IPsec デーモン (ipsecd) は、起動されて規則をカーネルに取り込む際に、構成情報を読み取ります。

受信および送信パケットのそれぞれに対して、カーネルは SPD (Security Policy Database) をシーケンシャルにスキャンして、一致する規則を探します。そのため通常は、接続規則は最も限定的なものから最も一般的なものという順序に並べます。システムに出入りするトラフィックの処理方法を定義する接続を順番に並べたリストを、システムのセキュリティ・ポリシといいます。表 4-1 には、SysMan IPsec ユーティリティ内で事前に定義されている省略時の接続をリストしています。

表 4-1: SysMan の省略時の接続

接続	説明
allow-ike-io	IPsec 保護なしで、すべてのシステムとのポート 500 への IKE 入出力トラフィックを許可します。
allow-dns-io	IPsec 保護なしで、すべてのシステムとのポート 53 への DNS 入出力トラフィックを許可します。

また、SysMan IPsec ユーティリティを使用して、IPsec 処理を有効または無効にすることもできます。

注意

IPsec を有効にした場合、別のセキュア接続を定義していなければ、IKE と DNS を除く IP ネットワーク・トラフィックはすべて停止されます。

4.2.1 IPsec プロトコル

セキュア接続が定義されていないシステムでは、伝送される各パケットは保護されません。パケットの構造は、IPv4 では図 4-4、IPv6 では図 4-5 に示すようになっています。いったん送出すると、IP ヘッダとペイロードは横取

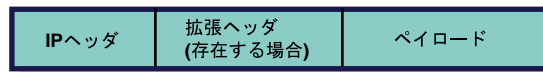
りされ、変更されて宛先に送られる可能性があります。宛先では、データが変更されたことは分かりません。

図 4-4: 一般的な IPv4 パケット (保護なし)



ZK-1774U-AI

図 4-5: 一般的な IPv6 パケット (保護なし)



ZK-1860U-AI

セキュア接続を定義したときには、パケットは次のようなトラフィック・セキュリティ・プロトコルで保護されます。

- 認証ヘッダ (AH)

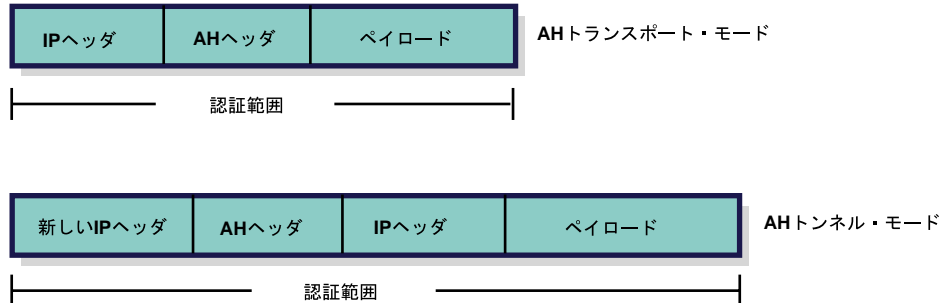
データ送信元の認証、コネクションレス完全性、再送攻撃保護サービスをデータグラムに対して行います。これにより、受信側は送信側の ID と、データが変更されていないことの両方を確認できます。

- ESP (Encapsulating Security Payload)

認証を使用する際に、AH プロトコルの保護をすべて行い、暗号化によってさらに秘匿性を高めています。

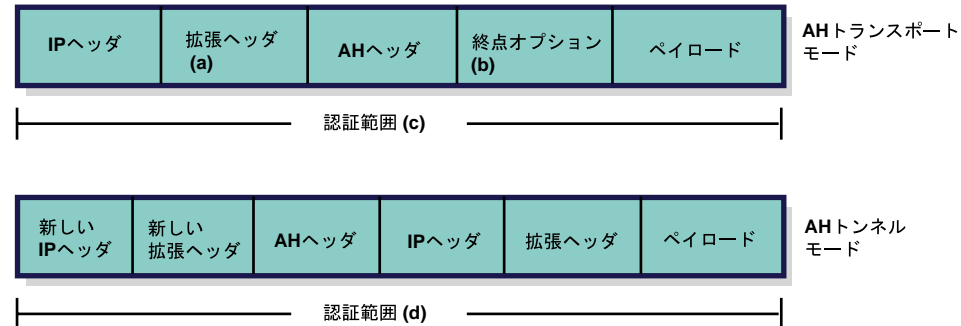
AH プロトコルは、トランスポート・モードまたはトンネル・モードのいずれかで動作します。図 4-6 では両方のモードで送出された IPv4 パケット、図 4-7 では両方のモードで送出された IPv6 パケットを示します。

図 4-6: AH トランスポート・モードと AH トンネル・モードのパケット (IPv4)



ZK-1775U-AI

図 4-7: AH トランスポート・モードと AH トンネル・モードのパケット (IPv6)



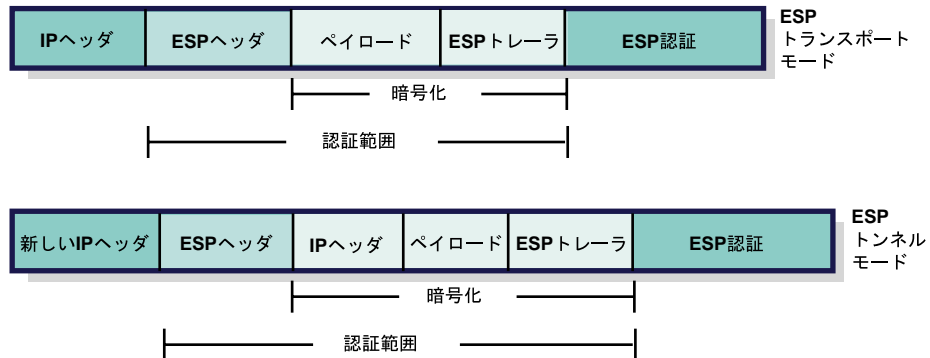
(a) 中継点、経路制御、および断片
(b) AHの前でも、後でも、両方でも可
(c) 変りやすいフィールドは認証されない
(d) 新しいIPヘッダの変りやすいフィールドは認証されない

ZK-1858U-AI

トランスポート・モードでは、オリジナルのパケットの IP ヘッダが、処理結果のパケットの IP ヘッダになります (AH ヘッダとペイロード)。これは、一般にホスト対ホストの通信で使用されます。トンネル・モードでは、パケットの前に新しい IP ヘッダ (トンネル・ヘッダ) と AH ヘッダが付加されます。内部の IP ヘッダには、オリジナルの送信元および宛先のアドレスが含まれ、外側のヘッダにはセキュア・ゲートウェイのアドレスが含まれています。一般に、これはセキュア・ゲートウェイと VPN 構成で使用されます。

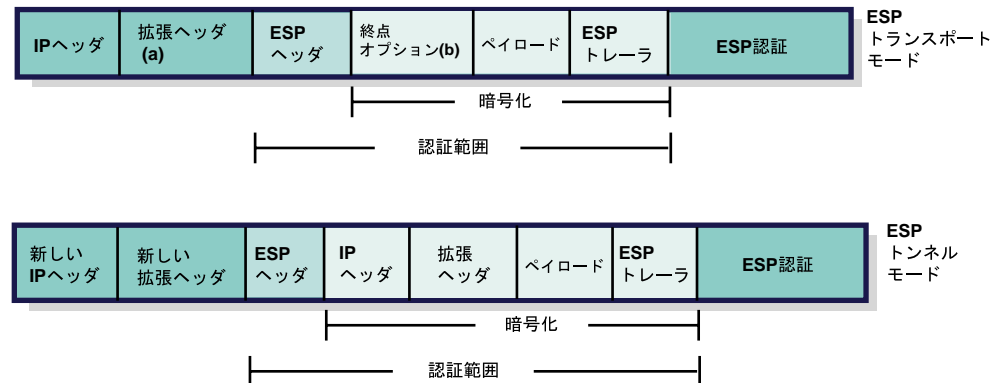
ESP プロトコルも、トランスポート・モードまたはトンネル・モードのいずれかで動作します。図 4-8 では両方のモードで送出された IPv4 パケット、図 4-9 では両方のモードで送出された IPv6 パケットを示します。

図 4-8: ESP トランスポート・モードと ESP トンネル・モードのパケット (IPv4)



ZK-1776U-AI

図 4-9: ESP トランスポート・モードと ESP トンネル・モードのパケット (IPv6)



(a) 中継点、経路制御、および断片
(b) ESPの前でも、後でも、両方でも可

ZK-1859U-AI

トランスポート・モードでは、パケットの IP ヘッダが、処理結果の暗号化パケットの IP ヘッダになります (ペイロードと ESP トレーラ)。これは、一般にホスト対ホストの通信で使用されます。トンネル・モードでは、暗号化されたパケット (オリジナルの IP ヘッダ、ペイロード、ESP トレーラ) の前に新しい IP ヘッダ (トンネル・ヘッダ) が付加されます。内部の IP ヘッダには、オリジナルの送信元および宛先のアドレスが含まれ、外側のヘッダには

セキュア・ゲートウェイのアドレスが含まれています。一般に、これはセキュア・ゲートウェイとVPN構成で使用されます。

AH および ESP プロトコルは、2 つの HMAC (Hashed Message Authentication Code)、すなわち Message Digest 5 (MD5-96) と Secure Hash Algorithm 1 (SHA1-96) の認証アルゴリズムをサポートします。ESP プロトコルは、DES (Data Encryption Standard)、3DES (triple-DES)、AES (Advanced Encryption Standard) の暗号化アルゴリズムをサポートします。

暗号化鍵管理手順およびプロトコルの使用とともに、これらのプロトコルは、どのような状況や方式でも採用できます。採用方法は、セキュリティおよびシステムに対して、ユーザ、アプリケーション、組織またはサイトが何を求めているかによって決まります。

4.3 セキュリティ・アソシエーション

セキュア接続を定義する際には、セキュリティ・アソシエーション (SA) と呼ばれるものを作成して確立するための情報を指定します。SA はセキュリティ・ポリシーの実例であり、次のような情報を含みます。

- SPI (Security Parameter Index)
- 認証アルゴリズム (AH または ESP)
- 暗号化アルゴリズム (ESP のみ)
- 暗号鍵と認証鍵
- 暗号化コンテキスト
- SA 存続期間
- 照合されるセレクタ

この情報は、保護対象パケットを照合して処理するために使用します。1 つの IPsec プロトコルを指定した単一のセキュア接続では、図 4-10 に示すように着信と発信両方の SA が作成されます。

図 4-10: 1 つのプロトコルに対して作成された SA



セキュア接続に AH と ESP プロトコルの両方を指定した場合，図 4-11 に示すように，プロトコルごとに着信と発信両方の SA が作成されます。

図 4-11: 2 つのプロトコルに対して作成された SA



netstat コマンドを使用すると SA を表示できます。

4.4 鍵交換

IPsec は認証および暗号化のための暗号鍵に依存しているので，通信する 2 つのシステムの間で鍵を交換し，それを定期的に変更するメカニズムが必要になります。Tru64 UNIX IPsec の実装には，鍵を交換する方法が 2 通りあります。

- 手動鍵交換
- IKE (Internet Key Exchange) プロトコルを使用した自動鍵交換

4.4.1 手動鍵交換

この鍵の管理および交換の方式は，ネットワーク内の各システムで鍵情報を手動で構成する 1 人の人物に依存しています。実際の鍵は，アルゴリズムに適した長さの 16 進文字列またはテキスト文字列です。

手動鍵交換は，小規模で変化の少ないテスト環境では使用できますが，多数のシステムが接続された大規模な実運用のネットワークでは，現実的ではありません。また，高品質の鍵を作成したり，セキュリティが危うくならないように十分な頻度で鍵を変更したり，その鍵を安全に交換することも困難です。

4.4.2 IKE

IKE プロトコルは、SA および鍵管理の望ましい方式です。この方式では、IPsec を実装した各システムは IKE を使用して SA を確立し、鍵情報を安全に交換します。IKE 交換はすべてポート 500 で送受信されます。省略時の設定では、この IPsec 実装は IPsec 接続を事前に定義してこのトラフィックを許可します。

IKE 交換は、開始システムと応答システムの 2 つのシステムの間で行われます。交換には次の 2 段階のフェーズがあります。

- フェーズ 1 — IKE 交換それ自体を保護する SA を設定します。
- フェーズ 2 — SA を設定し、2 つのシステム間の IP データグラムを保護する鍵を定義します。

フェーズ 1 交換は、フェーズ 2 交換より前に行う必要があります。

4.4.2.1 フェーズ 1 交換

IKE フェーズ 1 交換は、次のモードのいずれかを使用して行います。

- メイン・モード — 開始システムと応答システムの間で合計 6 つのメッセージを交換します。フェーズ 1 交換では、一般にこのモードが使用されます。
- アグレッシブ・モード — 開始システムと応答システムの間で合計 3 つのメッセージを交換します。

さらに、次のようなタイプの認証がサポートされています。すなわち、2 種類の電子署名、公開鍵暗号化、事前共有鍵です。高性能の鍵を生成してそれを安全に伝送できる場合以外は、電子署名と公開鍵暗号化の方が、事前共有鍵より望ましい方式です。

ここでは、フェーズ 1 交換でよく使用される、電子署名を使用したメイン・モード交換について説明します。このタイプのフェーズ 1 交換では、次のようなイベントが発生します。

1. 開始システムは、1 つまたは複数のプロポーザルのセットを、暗号化せずに他のシステムに送信します。他のシステム (応答システム) は、サポートするプロポーザルを応答します。

この交換の終わりには、認証方法、ハッシュ関数、暗号化アルゴリズムについて 2 つのシステムが合意しています。

2. 開始システムは、暗号化されていない Diffie-Hellman 公開値とランダム値 (**nonce** という) を送信します。応答システムは自分の Diffie-Hellman 公開値と nonce を送信します。

この交換の終わりには、2 つのシステムは、IKE 交換用に同じ認証鍵と暗号鍵を導き出し、フェーズ 2 交換を保護するための鍵を得るために使用する鍵データを導き出しています。

3. 開始システムは、暗号化された ID、電子署名、オプションの証明書を送信します。応答システムは自分の暗号化された ID、電子署名、オプションの証明書を送信します。一般に、ID は IP アドレスですが、IPsec の実装によって異なります。

この交換の終わりには、各システムはピアから認証された状態になっています。

どちらのピアも、フェーズ 1 存続期間を維持管理し、IKE SA に対する新しい鍵情報の交換と新しい鍵の生成を自動的に行います。

注意

各リモート IKE ピアに対して同時にサポートされるフェーズ 1 SA (セキュリティ・アソシエーション) は 1 つだけです。ピアに対して複数のフェーズ 1 SA の作成が必要となるポリシーを定義すると、IKE 接続の問題が発生するおそれがあります。

4.4.2.2 フェーズ 2 交換

IKE フェーズ 2 交換は、クイック・モードで行われます。このタイプの交換では、次のようなイベントが発生します。

1. 開始システムは、メッセージ・ペイロードの暗号化されたハッシュ、SA ペイロード、IP トラフィックを保護するための 1 つまたは複数のプロポーザルのセットを送信し、PFS (Perfect Forward Secrecy) を使用する場合は、Diffie-Hellman 公開値とグループ番号も送信します。応答システムは、メッセージ・ペイロードの暗号化されたハッシュ、SA ペイロード、IP トラフィックを保護するための 1 つまたは複数のプロポーザルのセットを送信し、PFS を使用する場合は、自分の Diffie-Hellman 公開値とグループ番号も送信します。

この交換の終わりには、2つのシステムが新しい nonce と Diffie-Hellman 公開値を交換し (PFS を使用する場合)、鍵を導き出しています。この鍵には、完全性チェック用の値を生成し、伝送されるデータグラムを暗号化する (選択されている場合) 鍵と、完全性チェック用の値を検証し、受信したデータグラムの暗号を解読する (選択されている場合) 鍵があります。

2. 開始システムは、フェーズ 1 認証鍵、メッセージ ID、両者の nonce の暗号化されたハッシュを送信します。

この交換の終わりには、両方のシステムは取り決めたセキュリティ・プロトコルの使用を開始して、ユーザの IP トラフィックを保護します。

どちらのピアも、フェーズ 2 存続期間を維持管理し、IPsec SA に対する新しい鍵情報の交換と新しい鍵の生成を自動的に行います。

4.5 証明書

IKE フェーズ 1 交換 (4.4.2 項を参照) では、事前共有鍵を使用した認証、または公開鍵暗号化を用いた認証を使用できます。次に示す公開鍵アルゴリズムがサポートされています。

- 電子署名標準 (DSS)
- RSA 署名
- RSA 暗号化

公開鍵方式ではすべて、証明書は不可欠です。

証明書は、システムの身元をそれに対応する公開鍵に結び付けるファイルです。証明書の情報は、CA (Certification Authority) と呼ばれる信頼のおける第三者に依存して確認します。この確認処理により、次に送信者を認証できるようになります。

電子署名と証明書を使用した処理は、次のとおりです。

1. システムの管理者は、公開鍵と非公開鍵のペアを生成し、公開鍵を証明書要求とともに CA に送信します。
2. CA は公開鍵をシステムの ID にバインド (署名) し、管理者への証明書を発行します。CA の署名を確認するために必要な公開鍵は、CA の証明書の中に格納されて配信されます。X.509 標準は証明書内の情報と、使用可能なデータ形式を定義します。

- 3. IKE フェーズ 1 交換の際に、システムは非公開鍵で署名された IKE データを他のシステムに送信します。通常は、対応する公開鍵を含む証明書も送信します。
- 4. 受信側システムは、証明書内の送信側システムの公開鍵を使用して、署名された IKE データの有効性を確認します。その前に、受信側システムは、CA の証明書を使用して送信者の公開鍵の有効性を確認して送信者の証明書の有効性を確認します。受信者は、送信者の証明書に署名した CA と同じ CA からの証明書を持っている必要があります。

ステップ 4 で、送信側システムの証明書を発行した CA を、受信システムが知らなければどうなるでしょうか? 多くの CA では階層的な トラスト・チェーンを形成できます。チェーンの各メンバは、上位権限者が署名した証明書を持っています。受信側システムで CA の証明書の有効性を確認する必要がある場合、このシステムは、CA の証明書の発行者の公開鍵を用いて、CA 証明書の署名を確認します。通常、この鍵は他の証明書の中に格納されています。受信側システムは、信頼できる CA または トラスト・チェーンのルートに到達するまで、この処理を繰り返します。

各々の証明書には、一意のシリアル番号が割り当てられています。証明書が破棄 (revoke) されると、そのシリアル番号は CRL (Certificate Revocation List) に入られます。送信者と受信者は、使用する証明書の有効性を確認する際には、破棄と期限切れの両方をチェックする必要があります。破棄されたかどうかをチェックするためには、送信者と受信者は、CA (複数の場合もある) から最新の CRL を定期的に取得しなければなりません。

4.5.1 証明書のエンコーディング

表 4-2 に、証明書に含まれるバイナリ・データをエンコードするさまざまな方法を示します。

表 4-2: 証明書のバイナリ・データをエンコードする方法

データのエンコード方法	説明
PEM (Privacy Enhanced Mail)	Base64 エンコード・バイナリとしてエンコード。

表 4-2: 証明書のバイナリ・データをエンコードする方法 (続き)

データのエンコード方法	説明
バイナリ	ASN.1 の DER (Distinguished Encoding Rules) に準拠したエンコード。
HEXL	16 進数文字列としてエンコード。各行の形式は次のとおりです。 <i>xxxxxxxx: yyyy yyyy yyyy yyyy yyyy yyyy yyyy</i> この形式で、 <i>xxxxxxxx</i> は行頭のデータのオフセット (16 進数)、 <i>yyyy yyyy yyyy yyyy yyyy yyyy</i> <i>yyyy yyyy</i> は 16 バイトまでの 16 進数データです。

証明書の使用に関するガイドラインは、4.5.2 項を参照してください。証明書の生成については、`ipsec_certmake(8)` を参照してください。

注意

証明書ベースの認証を効率的に使用するには、PKI (Public Key Infrastructure) または CA (Certification Authority) へのアクセスが必要になります。オペレーティング・システムに付属のユーティリティは、生産環境での証明書の作成や使用には不十分です。

4.5.2 証明書の使用に関するガイドライン

IPsec 構成で証明書を使用する際のガイドラインは次のとおりです。

- 証明書、CRL、非公開鍵は、現状では通常のファイルに格納されています。将来はこの情報の格納およびアクセス方法を改良する予定です。システムでの認証を安全なものにできるかどうかは、非公開鍵を安全に保てるかどうかにかかっています。鍵ファイルとそれを保存するディレクトリは、root ユーザのみがアクセスできるようにしてください。
- 公開鍵証明書を使用して接続が認証される場合、システムを識別するためにリモート・ピアに送信される証明書を指定する必要があります。認証には署名とデータの暗号化が伴うため、証明書ファイルと非公開鍵ファイルの両方を指定しなければなりません。他の証明書 (CA 証明書など) またはピア・システムの証明書の場合、非公開鍵がないの

で、証明書ファイルのみを指定します。証明書を使用した構成の例は、4.6.7.2 項 と 4.6.7.3 項 を参照してください。

- RSA 鍵を使用する証明書は、DSA よりも幅広く使用されています。すべてのベンダが DSA をサポートしているとは限りません。
- ピアごとに、使用する証明書は 1 つだけにしてください。各ピアに複数の証明書がある場合は、証明書の Subject Alternative Name が一意でなければなりません。
- 主要な PKI ベンダが発行する証明書が使用できます。証明書は、電子署名と鍵の暗号化に使用できることを示す適切な KeyUsage 拡張を備えている必要があります。ipsec_certmake ユーティリティを使用すると、PEM エンコード PKCS10 フォーマットの証明書要求ファイルを作成し、それを使用して適切な CA (Certificate Authority) の証明書を要求できます。CA やサードパーティの PKI ソフトウェアにアクセスできない場合、ipsec_certmake ユーティリティを使用すると、自分で署名した証明書階層をテスト用に生成できます。詳細は ipsec_certmake(8) を参照してください。
- RSA 暗号化モードを使用して認証を行う場合は、ピアの証明書を事前にシステムに構成しておく必要があります。これは、IKE 交換の初期段階に、ピアの公開鍵を使用してデータを暗号化しなければならないためです。RSA 署名モードでは、ピアの証明書を構成する必要はありません。これは、IKE 接続を通してピアが証明書を安全に送信できるためです。
- RSA 暗号化モードでは、使用する証明書の Subject Alternative Name の 1 つとして IP アドレスを指定します。
- 複数のネットワーク・インタフェースまたは複数のアドレスを持つホストでは、Subject Alternative Name として IP アドレスを使用する場合、ノードの IP アドレスごとに 1 つずつ、複数の証明書を作成する必要があります。この場合、IP アドレスは、別のタイプの Subject Alternative Name (たとえば、ドメイン名) より望ましいものです。
- 交換を成功させるためには、IKE のフェーズ 1 交換および フェーズ 2 交換で送信されるピア ID が重要です。システムが送信する ID がリモート・ピアのポリシーと一致しない場合、IKE 折衝は失敗します。ID には複数のタイプがあります。ベンダによっては、タイプのサブセットのみをサポートしていたり、交換される内容をどの程度厳密にチェッ

クするかという度合いが異なっている場合があります。以下のリストは、ID とその使用についての追加説明です。

- 証明書を使用する場合、フェーズ 1 ID は、証明書に格納されている SubjectAlternativeName の値から形成されます。通常、この値はシステムの IP アドレスですが、ドメイン名や電子メールアドレス (user@fully.qualified.domain) になることもあります。ベンダによっては、ID のフォーマットを 1 つしかサポートしていないものもあります。証明書に SubjectAlternativeName が含まれていない場合、通常、システムの IP アドレスが送信されます。
- 証明書には、SubjectAlternativeName の値が複数含まれていることがあります。すべてのベンダで、複数の値を持つ証明書を処理できるとは限りません。値の順序も、フェーズ 1 ID としてどの値を送るかに影響します。SubjectAlternativeName の値が 1 つしかない証明書を使用すると、相互運用に関する問題が少なくなります。
- フェーズ 2 では、セキュア・ゲートウェイは、ゲートウェイ動作を指定しているエンティティの ID を送信します。すなわち、接続の定義 (セキュア・ゲートウェイのポリシー) が ID に影響を与えます。たとえば、IPv4 アドレス 1.1.1.1 で選択するポリシーは、IPv4 サブネット 1.1.1.0/24 のポリシーを持ったピア・ゲートウェイとは一致しません。

4.6 IPsec の計画

IPsec および IKE (Internet Key Exchange) は、さまざまな構成と多数のオプションが使用できる複雑なプロトコルです。これらのプロトコルは、ホスト、ルータ、スタンドアロンの VPN (Virtual Private Network) ゲートウェイなどのさまざまなタイプのデバイスにも実装されています。ベンダは、それぞれ異なる方法でプロトコルを使用し、異なる省略時の値を使用しています。

IPv6 はどのノードにも構成できます。クラスタ・メンバに対しては、クラスタ・メンバごとに独立して IPv6 を構成できます。TruCluster に IPsec を実装する場合の注意事項については、4.6.3 項を参照してください。クラスタの構成については、『クラスタ管理ガイド』を参照してください。

ここでは、IPsec を構成する前に完了しておかなければならない作業について説明します。

4.6.1 IPsec サブセットがインストールされていることの確認

次のコマンドを入力して、IPsec サブセットがインストールされていることを確認します。

```
# setld -i | grep OSFIPSECBASE
```

IPsec サブセットがインストールされていない場合は、setld コマンドでインストールします。サブセットのインストールについての詳細は、setld(8)、または『インストレーション・ガイド』、または『システム管理ガイド』を参照してください。

IPsec サブセットのインストールが完了すると、システムは、呼び出されるといつでも IPsec モジュールを動的にカーネルにロードするように構成されています。

4.6.2 システムのネットワーク・トラフィックの記録

IPsec はシステムに出入りする IP パケットをすべて調べるため、セキュリティ・ポリシーでは、システムへの出入りが可能なトラフィックをすべて考慮する必要があります。SysMan を通して IPsec を開始した場合、システムは IP セキュア・モードになっています。このモードでは、重要なデータをそのまま送信してしまうリスクがあるときには、IP トラフィックをすべてブロックします。IP トラフィックがシステムに出入りできるためには、ipsecd デーモンが有効なポリシーで稼働している必要があります。

SysMan IPsec アプリケーションでは、IKE と DNS (Domain Name System) でよく必要になる接続を行うことができます。他のプロトコルに対するポリシーを追加しなければならないこともあります。たとえば、NIS (Network Information Service)、NTP (Network Time Protocol)、SMTP (Simple Message Transfer Protocol)、信頼できるサブネットに対して「すべてを許可する」ポリシーがあります。

また、ルーティング・デーモンを実行する場合、サブネット・ブロードキャスト・アドレスに対するトラフィックを許可する必要があります。

4.6.3 TruCluster への IPsec の実装

IPsec ポリシーを TruCluster に実装する際は、次の点に注意してください。

- クラスタ・インタコネクットのトラフィックは IPsec をバイパスします。これは、クラスタ・インタコネクットがブート処理の早い段階とシャット

ダウン処理の遅い段階でトラフィックを伝送するためです。この時点では IPsec は使用できません。外部トラフィックは、他のインタフェースを通してシステムに出入りします。

- 現在は、クラスタ別名アドレスを使用するトラフィックのアクセス制御保護のみがサポートされています。暗号化や認証を適用せずにクラスタ別名トラフィックを通すには、IPsec ポリシを作成しなければなりません。つまり、IPsec 保護なしでクラスタ別名トラフィックを通す必要があります。

4.6.4 IPsec 実装ガイドラインへの準拠

新しいピアで IPsec を確実に構成して動作させるためには、次のガイドラインに従ってください。

1. 可能であれば、ピアとの非セキュア接続が確立できることを確認します。これにより、IPsec と関係のないルーティングの問題を回避できます。
2. 事前共有鍵を使用して認証されるセキュア接続を構成します。これにより、IKE および PKI (Public Key Infrastructure) との相互運用に関する問題を同時にデバッグするのを回避できます。後で公開鍵認証を用いるように接続を変更する場合は、この時点では単純なテスト鍵を使用できます。
3. 必要に応じて、公開鍵証明書モードを使用して接続を構成します。

4.6.5 システムの性能に対する IPsec の影響の削減

IPsec を使用すると、各 IP パケットの処理に必要な CPU 時間が確実に増加します。この原因は、次のとおりです。

- どの IPsec 接続規則を適用するか決定するために、送受信されるパケットがすべて調べられる。
- 認証されるすべてのパケットで、HMAC 計算や HMAC チェックが必要になる。
- 暗号化で保護されるすべてのパケットで、暗号化と暗号解読が必要になる。特に、3DES 暗号化では、非 IPsec の場合と比べて、パケットごとにかなり大量の CPU 時間が必要になります。
- 主に公開鍵の暗号化処理のために、IKE 鍵交換動作のたびに CPU 処理が必要になる。

結果として、ネットワークのパケット処理のために CPU リソースの大部分を費やしている場合は、IPsec を有効にするとネットワークのスループットが大幅に低下するおそれがあります。ネットワークの使用量がそれほど多くないシステムでも、オーバーヘッドの増加が確認できることがあります。

IPsec が有効になっている場合、送受信する IP パケットごとに、IPsec ポリシを構成する接続のリストを調べる必要があります。ポリシの複雑さの程度によっては、得られる最大スループットが 25% またはそれ以上低下するおそれがあります。これは、暗号化や認証が実行されない場合でも発生します。認証と 3DES 暗号化を追加すると、プロセッサとネットワーク・インタフェースの速度に応じて、最大スループットが非 IPsec の場合の 10% 以下まで低下するおそれがあります。

IPsec 処理が性能に与える影響を小さくするには、次のガイドラインが役に立ちます。

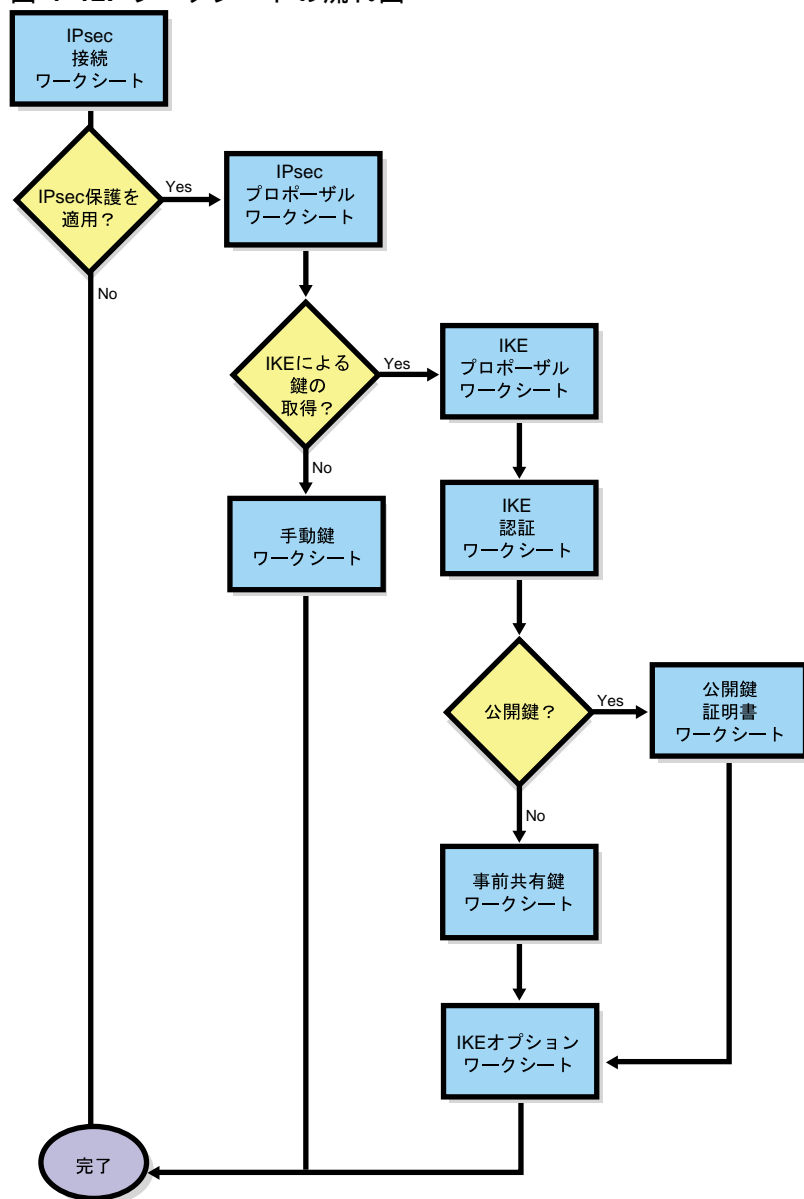
- ポリシ内の IPsec セキュア接続の数と、各セキュア接続にリストする IP アドレスの数を最小限にします。
- 新規のポリシ定義に自動的に挿入されるセキュア接続の `allow-dns-io` と `allow-ike-io` には、IPv6 アドレス用のセレクトアが含まれています。IPv6 を使用していない場合、これらのアドレスは削除できます。
- リスト内の後部の接続で、必要な DNS サーバへのアクセスを許可している場合は、`allow-dns-io` セキュア接続は不要です。
- トラフィックが指定されリモート IP ピアからのものであることを保証しなければならないが、トラフィック自体を秘密にする必要はない場合は、暗号化なしの AH または ESP の使用を考慮してください。認証なしで暗号化だけを使用したときには、セキュリティが確保できているとは見なされないことに注意してください。
- IKE および IPsec SA に対して適切な存続期間を設定して、鍵の再生成操作の必要回数を最小限に抑えます。
- できれば 3DES 暗号化の代わりに AES を使用します。AES は 3DES よりも 2.5 倍効率良く動作します。

4.6.6 構成の準備

IPsec ソフトウェアを構成する前に、システムと必要とする IPsec 接続のタイプについての情報を収集する必要があります。以下の項には、IPsec の構成

に必要な情報を記録するためのワークシートがあります。図 4-12 に、ワークシートを使用するときの基本的な順序を示します。

図 4-12: ワークシートの流れ図



ZK-1779U-AI

4.6.6.1 IPsec 接続のワークシート

図 4-13 に、IPsec 接続のワークシートを示します。以下の項では、このワークシートへ記入する情報について説明します。オンラインでマニュアルをご覧になっている場合は、印刷機能でワークシートを印刷してください。

図 4-13: IPsec 接続ワークシート

IPsec 接続ワークシート	
名前: _____	
セレクト	
リモートIPアドレス	
タイプ: <input type="checkbox"/> 単独IPv4 <input type="checkbox"/> IPv4サブネット <input type="checkbox"/> IPv4レンジ <input type="checkbox"/> 全IPv4 <input type="checkbox"/> 単独IPv6 <input type="checkbox"/> IPv6サブネット <input type="checkbox"/> IPv6レンジ <input type="checkbox"/> 全IPv6	
アドレス: _____	
IPサブネット・サイズ: _____	
終了アドレス: _____	
照合プロトコル: <input type="checkbox"/> 任意 <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> icmp <input type="checkbox"/> icmpv6 <input type="checkbox"/> ip <input type="checkbox"/> igmp	
照合ポート: _____	
ローカルIPアドレス	
タイプ: <input type="checkbox"/> 単独IPv4 <input type="checkbox"/> IPv4サブネット <input type="checkbox"/> IPv4レンジ <input type="checkbox"/> 全IPv4 <input type="checkbox"/> 単独IPv6 <input type="checkbox"/> IPv6サブネット <input type="checkbox"/> IPv6レンジ <input type="checkbox"/> 全IPv6	
アドレス: _____	
IPサブネット・サイズ: _____	
終了アドレス: _____	
照合プロトコル: <input type="checkbox"/> 任意 <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> icmp <input type="checkbox"/> icmpv6 <input type="checkbox"/> ip <input type="checkbox"/> igmp	
照合ポート: _____	
アクション	
<input type="checkbox"/> IPsecを適用	<input type="checkbox"/> 発信と着信 <input type="checkbox"/> 着信のみ <input type="checkbox"/> 発信のみ
<input type="checkbox"/> IPsecを適用しない	
<input type="checkbox"/> パケットを破棄	

名前

IPsec 接続の名前です。1 ~ 40 文字までの英数字、下線 (_), ハイフン (-) で構成されます。この実装では、特に指定しなければ IKE 交換と DNS (Domain Name System) 交換に対する接続を定義します。

リモート IP アドレス・セクタ

これは、送信パケットの宛先アドレス・フィールドと受信パケットの送信元アドレス・フィールドで、IPsec が照合するリモート IP アドレスです。これらのリモート IP アドレスを持つパケットが選択され、指定された IPsec アクションが実行されます。

タイプ

セクタの IP アドレス部分を指定する方法です。単独の IP アドレスを指定する場合は、「単独 IPv4」と「単独 IPv6」のいずれかにチェックを付けます。IP サブネット全体を指定する場合は、「IPv4 サブネット」と「IPv6 サブネット」のいずれかにチェックを付けます。IP アドレスの範囲を指定する場合は、「IPv4 レンジ」と「IPv6 レンジ」のいずれかにチェックを付けます。全 IP アドレスを指定する場合は、「全 IPv4」と「全 IPv6」のいずれかにチェックを付けます。

アドレス

IPv4 では、単独 IP アドレス、IP サブネット・アドレス、IP アドレス・レンジの開始アドレスのいずれかをドット表記 10 進数で表したものです。IPv6 では、単独 IP アドレス、IP サブネット・アドレス、IP アドレス・レンジの開始アドレスのいずれかを IPv6 アドレス形式で表したものです (IPv6 アドレスについては、3.3 節を参照してください)。

IP サブネット・サイズ

IP サブネット・マスクのサイズ (ビット数) です。範囲は、IPv4 の場合は 0 ~ 32 ビット、IPv6 の場合は 0 ~ 128 ビットになります。

終了アドレス

IPv4 では、IP アドレス・レンジの終了アドレスをドット表記 10 進数で表したものです。IPv6 では、IP アドレス・レンジの終了アドレスを IPv6 アドレス形式で表したものです。

照合プロトコル

セレクトで照合する上位層プロトコルです。このセレクトをすべてのプロトコルに一致させる場合は、「任意」にチェックを付けます。特定のプロトコルに一致させる場合は、適切なプロトコルにチェックを付けます。TCP、UDP、ICMP、ICMPv6、IP、IGMPの中から選択できます。

照合ポート

セレクトで照合するポート番号です。範囲は1～65535です。セレクトをすべてのポートに一致させる場合は、ここを空白にしておきます。

ローカル IP アドレス・セレクト

これは、送信パケットの送信元アドレス・フィールドと受信パケットの宛先アドレス・フィールドで、IPsecが照合するローカル IP アドレスです。これらのローカル IP アドレスを持つパケットが選択され、指定された IPsec アクションが実行されます。

タイプ

セレクトの IP アドレス部分を指定する方法です。単独の IP アドレスを指定する場合は、「単独 IPv4」と「単独 IPv6」のいずれかにチェックを付けます。IP サブネット全体を指定する場合は、「IPv4 サブネット」と「IPv6 サブネット」のいずれかにチェックを付けます。IP アドレスの範囲を指定する場合は、「IPv4 レンジ」と「IPv6 レンジ」のいずれかにチェックを付けます。全 IP アドレスを指定する場合は、「全 IPv4」と「全 IPv6」のいずれかにチェックを付けます。

アドレス

IPv4 では、単独 IP アドレス、IP サブネット・アドレス、IP アドレス・レンジの開始アドレスのいずれかをドット表記 10 進数で表したものです。IPv6 では、単独 IP アドレス、IP サブネット・アドレス、IP アドレス・レンジの開始アドレスのいずれかを IPv6 アドレス形式で表したものです。

IP サブネット・サイズ

IP サブネット・マスクのサイズ (ビット数) です。範囲は、IPv4 の場合は 0～32 ビット、IPv6 の場合は 0～128 ビットになります。

終了アドレス

IPv4 では、IP アドレス・レンジの終了アドレスをドット表記 10 進数で表したものです。IPv6 では、IP アドレス・レンジの終了アドレスを IPv6 アドレス形式で表したものです。

照合プロトコル

セレクトで照合する上位層プロトコルです。このセレクトをすべてのプロトコルに一致させる場合は、「任意」にチェックを付けます。特定のプロトコルに一致させる場合は、適切なプロトコルにチェックを付けます。TCP、UDP、ICMP、ICMPv6、IP、IGMPの中から選択できます。

照合ポート

セレクトで照合するポート番号です。範囲は 1 ~ 65535 です。セレクトをすべてのポートに一致させる場合は、ここを空白にしておきます。

アクション

ローカル・アドレス・セレクトとリモート・アドレス・セレクトに一致した IP パケットに対して実行する処理のタイプです。IPsec 処理を適用しない場合は、「IPsec を適用しない」にチェックを付けます。IPsec 処理を適用する場合は、「IPsec を適用」にチェックを付けます。パケットを破棄する場合は、「パケットを破棄」にチェックを付けます。

「IPsec を適用」にチェックを付けると、IPsec の処理は常に、受信と送信の両方向に適用されます。他の 2 つのアクションでは、そのアクションを適用する方向を指定する必要があります。全パケットにそのアクションを適用する場合は、「受信と送信」にチェックを付けます。受信パケットにそのアクションを適用する場合は、「受信のみ」にチェックを付けます。送信パケットにそのアクションを適用する場合は、「送信のみ」にチェックを付けます。

4.6.6.2 IPsec プロポーザルのワークシート

図 4-14 に、IPsec プロポーザルのワークシートを示します。IPsec 処理をパケットに適用したい場合 (IPsec 接続ワークシートの「IPsec を適用」にチェックを付けている場合) に限り、このワークシートへの記入が必要です。以下の項では、このワークシートへ記入する情報について説明しま

す。オンラインでマニュアルをご覧になっている場合は、印刷機能でワークシートを印刷してください。

図 4-14: IPsec プロポーザル・ワークシート

IPsec プロポーザル・ワークシート

プロポーザル・リスト: ☐ AH-ESP-IPCOMP-transport-proposals
☐ AH-ESP-IPCOMP-tunnel-proposals
☐ AH-ESP-transport-proposals
☐ AH-ESP-tunnel-proposals
☐ AH-transport-proposals
☐ AH-tunnel-proposals
☐ ESP-IPCOMP-transport-proposals
☐ ESP-IPCOMP-tunnel-proposals
☐ ESP-transport-proposals
☐ ESP-tunnel-proposals
☐ カスタム・リスト

リモート・セキュリティ・ゲートウェイの
IPアドレス: _____

ローカル・セキュリティ・ゲートウェイの
IPアドレス: _____

鍵の取得: ☐ IKE ☐ 手動構成

カスタム・プロポーザル・リスト

カスタム・プロポーザル・リスト名: _____

プロポーザル名: _____

プロポーザル・リスト

この接続に適用するプロポーザルを含むプロポーザル・リストの名前で
す。この接続と接続モードに対して使用する IPsec 保護のタイプに応じ
て、選択肢 1 つにチェックを付けます。プロポーザル・リスト内の

プロポーザルは、リストされている順番に折衝されます。両者が合意した最初のプロポーザルが選択されます。事前に定義されたプロポーザル・リストに、ニーズに合うものがない場合は、「カスタム・リスト」にチェックを付けます。

手動鍵交換を使用する場合は、事前に定義されたプロポーザル・リストはいずれも使用できません。1つのプロトコルに対して1つのプロポーザルを含むプロポーザル・リストを作成する必要があります。「カスタム・リスト」にチェックを付け、詳細は 4.6.6.3 項を参照してください。

プロポーザル・リスト名	保護タイプ
AH-ESP-IPCOMP-transport-proposals	SHA 1 または MD5 の認証と 3DES 暗号化を用いた、トランスポート・モードの AH および ESP 圧縮プロトコル
AH-ESP-IPCOMP-tunnel-proposals	SHA 1 または MD5 の認証と 3DES 暗号化を用いた、トンネル・モードの AH および ESP 圧縮プロトコル
AH-ESP-transport-proposals	SHA 1 または MD5 の認証と 3DES 暗号化を用いた、トランスポート・モードの AH および ESP プロトコル
AH-ESP-tunnel-proposals	SHA 1 または MD5 の認証と 3DES 暗号化を用いた、トンネル・モードの AH および ESP プロトコル
AH-transport-proposals	SHA 1 または MD5 の認証を用いた、トランスポート・モードの AH プロトコル
AH-tunnel-proposals	SHA 1 または MD5 の認証を用いた、トンネル・モードの AH プロトコル
ESP-transport-proposals	SHA 1 または MD5 の認証と 3DES 暗号化を用いた、トランスポート・モードの ESP プロトコル
ESP-tunnel-proposals	SHA 1 または MD5 の認証と 3DES 暗号化を用いた、トンネル・モードの ESP プロトコル

ESP-transport-proposals と ESP-tunnel-proposals は、IPsec で最も一般的に使用されるプロポーザルです。

事前に定義された IPsec プロポーザル・リストには、MD5 および SHA-1 HMAC で 3DES 暗号化を用いた場合の組み合わせがすべて含まれています。暗号化 (ESP) は、必ず認証とともに、すなわち AH または ESP 認証アルゴリズムとともに使用してください。暗号化されたパ

ケット (認証なしの暗号化) は、1 つのパケットの暗号化された内容を他のパケットに結合する攻撃に対して弱い可能性があります。

事前に定義された IP プロポーザルのリストには、DES 暗号化アルゴリズムは含まれていません。これは、現実的には十分な計算リソースを持つ敵によって破られる可能性があるためです。事前に定義された DES プロポーザルは含まれており、DES が必要な場合は SysMan IPsec アプリケーションでカスタム・プロポーザル・リストに組み込むことができます。

事前に定義された IPsec プロポーザル・リストには、AES 暗号化アルゴリズムは含まれていません。これは、広範囲に採用されていないためです。事前に定義された AES プロポーザルは含まれており、SysMan IPsec アプリケーションでカスタム・プロポーザル・リストに組み込むことができます。リモート・ピアが AES をサポートしている場合は、それを使用して IPsec の性能を改善してください。

リモート・セキュア・ゲートウェイの **IP** アドレス

IPsec トンネル接続のリモート終端にあるセキュア・ゲートウェイの IPv4 アドレス (ドット表記 10 進数) または IPv6 アドレス (IPv6 アドレス形式) です。トンネル・プロポーザルを含むプロポーザル・リストを選択した場合は、リモート・アドレスを指定する必要があります。アドレスを指定しない場合、IPsec はデフォルトでリモート・ピアのアドレスを使用します。

ローカル・セキュア・ゲートウェイの **IP** アドレス

IPsec トンネル接続のローカル終端にあるセキュア・ゲートウェイの IPv4 アドレス (ドット表記 10 進数) または IPv6 アドレス (IPv6 アドレス形式) です。トンネル・プロポーザルを含むプロポーザル・リストを選択した場合は、リモート・アドレスを指定する必要があります。アドレスを指定しない場合、IPsec はデフォルトでローカル・ホストのアドレスを使用します。

鍵の取得

IPsec 鍵を取得する方法です。IKE (Internet Key Exchange) プロトコルを使用して鍵を取得する場合は、「IKE」にチェックを付けます。これは一般的な使い方です。手動鍵を作成する場合は、「手動構成」にチェックを付けます。

カスタム・プロポーザル・リスト名

カスタム・リストを作成する(プロポーザル・リスト名の「カスタム・リスト」にチェックを付けた) 場合の、新規プロポーザル・リストの名前です。事前に定義されたプロポーザル・リストとそこに含まれるプロポーザルで、ほとんどの場合は十分です。

プロポーザル名

プロポーザル・リストに入れるプロポーザル(複数可) の名前です。IPsec プロポーザル名の形式は、次のとおりです。

protocol-mode-encryption-authentication_type

たとえば、esp-tn-3des-md5-96 は ESP プロトコル、トンネル・モード、3DES 暗号化、MD5 認証を表します。

ipsec-ah-tn-md5-96-and-esp-tn-3des-none プロポーザルは AH プロポーザルと ESP プロポーザルの組み合わせを表します。ESP プロポーザルの none という単語は認証なし(no authentication) を表すことに注意してください。この IPsec 実装では、可能性のあるすべての組み合わせに対してプロポーザルを事前に定義しています。

この接続と接続モードに対して使用する IPsec 保護のタイプに従って、プロポーザルの名前を記入します。プロポーザル・リスト内のプロポーザルは、リストされている順番に折衝されます。両者が合意した最初のプロポーザルが選択されます。事前に定義されたプロポーザル・リストにニーズに合うものがない場合、または手動鍵交換を使用している場合は、「カスタム・プロポーザル」にチェックを付けます。

4.6.6.3 IPsec カスタム・プロポーザルのワークシート

図 4-15 に、IPsec カスタム・プロポーザルのワークシートを示します。事前に定義されたプロポーザルの中に、環境に適したものがない場合(IPsec プロポーザルのワークシートのプロポーザル名で「カスタム・プロポーザル」にチェックを付けている場合)にのみ、このワークシートへの記入が必要です。以下の項では、このワークシートへ記入する情報について説明します。オンラインでマニュアルをご覧になっている場合は、印刷機能でワークシートを印刷してください。

図 4-15: IPsec カスタム・プロポーザル・ワークシート

IPsec カスタム・プロポーザル・ワークシート	
カスタム・プロポーザル名:	_____
タイプ:	<input type="checkbox"/> AH <input type="checkbox"/> ESP <input type="checkbox"/> IPCOMP <input type="checkbox"/> チェーン
モード:	<input type="checkbox"/> トランスポート <input type="checkbox"/> トンネル
圧縮アルゴリズム:	<input type="checkbox"/> 圧縮
認証アルゴリズム:	<input type="checkbox"/> MD5-96 <input type="checkbox"/> SHA1 <input type="checkbox"/> 暗号化のみ
暗号化アルゴリズム:	<input type="checkbox"/> 認証のみ <input type="checkbox"/> 3DES CBC <input type="checkbox"/> DES CBC
	<input type="checkbox"/> AES (128ビット鍵) <input type="checkbox"/> AES (192ビット鍵)
	<input type="checkbox"/> AES (256ビット鍵)
プロポーザルのチェーン:	_____
プロポーザルのチェーン:	_____
プロポーザルのチェーン:	_____
フェーズ 2 存続期間	
存続期間名:	_____
指定秒後、鍵を再生成:	_____
指定Kバイト後、鍵を再生成:	_____

カスタム・プロポーザル名

カスタム・プロポーザルを作成する場合の、新しいプロポーザルの名前です。ほとんどの場合は、事前に定義されたプロポーザルとそのパラメータで十分です。

タイプ

プロポーザルのタイプです。AH プロポーザルを定義する場合は、「AH」にチェックを付けます。ESP プロポーザルを定義する場合は、「ESP」にチェックを付けます。IP 圧縮プロポーザルを定義する場合は、「IPCOMP」にチェックを付けます。特定シーケンスの複数のプロポーザルで構成されるプロポーザルを定義する場合は、「チェーン」にチェックを付けます。手動鍵交換を使用する場合は、「チェーン」にはチェックを付けないでください。指定できるプロポーザルは 1 つだけです。

モード

IPsec プロトコルを使用する際のモードです。トランスポート・モードを使用する場合は「トランスポート」にチェックを付けます。トンネル・モードを使用する場合は「トンネル」にチェックを付けます。

圧縮アルゴリズム

パケットに適用する圧縮のタイプです。パケットは、IPsec 処理を適用する前に圧縮されます。圧縮を適用する場合は、「圧縮」にチェックを付けます。

認証アルゴリズム

パケットに適用する認証のタイプです。MD5 を使用する場合は「MD5-96」にチェックを付けます。SHA を使用する場合は「SHA1-96」にチェックを付けます。暗号化のみを使用する場合は「暗号化のみ」にチェックを付けます。

暗号化アルゴリズム

パケットに適用する暗号化のタイプです。DES を使用する場合は「DES」にチェックを付けます。triple-DES を使用する場合は「3DES」にチェックを付けます。AES を使用する場合は、適切なオプションにチェックを付けます。認証のみを使用する場合は、「認証のみ」にチェックを付けます。

プロポーザルのチェーン

定義しているプロポーザルに追加する他のプロポーザルの名前です。現在定義されているプロポーザルの名前を記入します。

フェーズ 2 SA 存続期間

IPsec 接続または SA の存続期間です。

存続期間名

存続期間指定の名前です。

指定 K バイト後、鍵を再生成

鍵の再生成を行わずに、接続が停止するまでに通すことができるデータの量 (K バイト単位) です。鍵の再生成は、データの約 80 ~ 90 パーセ

ントが通過したときに開始されます。新しい鍵が生成されて配信されると、接続が利用可能になります。

指定秒後、鍵を再生成

鍵の再生成を行わずに、接続が停止するまでに接続が存続できる時間(秒単位)です。鍵の再生成は、時間の約 80 ~ 90 パーセントが経過したときに開始されます。新しい鍵が生成されて配信されると、接続が利用可能になります。この秒数の 2 倍の間、接続が使用されなかった場合は、接続が削除されます。

4.6.6.4 IKE プロポーザルのワークシート

図 4-16 に、IKE プロポーザルのワークシートを示します。IKE を使用してパケットの認証および暗号化の鍵を取得する場合 (IPsec プロポーザル・ワークシートの「鍵の取得」フィールドで、「IKE」にチェックを付けている場合) に限り、このワークシートへの記入が必要です。以下の項では、このワークシートへ記入する情報について説明します。オンラインでマニュアルをご覧ください。印刷機能でワークシートを印刷してください。

図 4-16: IKE プロポーザル・ワークシート

IKE プロポーザル・ワークシート	
プロポーザル・リスト名:	<input type="checkbox"/> DSA-signature-proposals <input type="checkbox"/> Pre-Shared-Key-proposals <input type="checkbox"/> RSA-encryption-proposals <input type="checkbox"/> RSA-signature-proposals <input type="checkbox"/> カスタム・リスト
カスタム IKE プロポーザル・リスト	
カスタム・プロポーザル・リスト名:	_____
プロポーザル名:	<input type="checkbox"/> ike-dss-3des-md5 <input type="checkbox"/> ike-dss-3des-sha1 <input type="checkbox"/> ike-psk-3des-md5 <input type="checkbox"/> ike-psk-3des-sha1 <input type="checkbox"/> ike-rse-3des-md5 <input type="checkbox"/> ike-rse-3des-sha1 <input type="checkbox"/> ike-rss-3des-md5 <input type="checkbox"/> ike-rss-3des-sha1 <input type="checkbox"/> カスタム・プロポーザル

プロポーザル・リスト名

IKE 交換の認証と保護の方法を定義するプロポーザル・リストの名前です。プロポーザル・リスト内のプロポーザルは、リストされている順番に折衝されます。両者が合意した最初のプロポーザルが選択されます。事前に定義されたプロポーザル・リストに、ニーズに合うものがない場合は、「カスタム・リスト」にチェックを付けます。

IKE プロポーザル・リスト名	保護タイプ
DSA-signature-proposals	SHA 1 または MD5 のハッシュングと 3DES 暗号化を用いた DSA 署名
Pre-Shared-Key-proposals	SHA 1 または MD5 のハッシュングと 3DES 暗号化を用いた事前共有鍵
RSA-encryption-proposals	SHA 1 または MD5 のハッシュングと 3DES 暗号化を用いた RSA 暗号化
RSA-signature-proposals	SHA 1 または MD5 のハッシュングと 3DES 暗号化を用いた RSA 署名

注意

共有鍵の認証モードの中では、RSA 署名モードが、最も多くのベンダでサポートされているモードです。

カスタム・プロポーザル・リスト名

カスタム・リストを作成する場合 (プロポーザル・リスト名で「カスタム・リスト」にチェックを付けた場合) の、IKE プロポーザル・リストの名前です。事前に定義された IKE プロポーザル・リストとそこに含まれるプロポーザルで、ほとんどの場合は十分です。

プロポーザル名

IKE プロポーザル・リストに入れるプロポーザル (複数可) の名前です。IKE 交換に使用する保護のタイプに従って、プロポーザルにチェックを付けます。プロポーザル・リスト内のプロポーザルは、リストされた順番に折衝されます。両者が合意した最初のプロポーザルが選択されます。事前に定義された IKE プロポーザルのリストに、ニーズに合うものがない場合は、「カスタム・プロポーザル」にチェックを付けます。

IKE プロポーザル名	保護のタイプ
ike-dss-3des-md5	DSS 署名認証, 3DES 暗号化, MD5 ハッシング
ike-dss-3des-sha1	DSS 署名認証, 3DES 暗号化, SHA 1 ハッシング
ike-psk-3des-md5	事前共有鍵認証, 3DES 暗号化, MD5 ハッシング
ike-psk-3des-sha1	事前共有鍵認証, 3DES 暗号化, SHA1 ハッシング
ike-rse-3des-md5	RSA 暗号化認証, 3DES 暗号化, MD5 ハッシング
ike-rse-3des-sha1	RSA 暗号化認証, 3DES 暗号化, SHA1 ハッシング
ike-rss-3des-md5	RSA 署名認証, 3DES 暗号化, MD5 ハッシング
ike-rss-3des-sha1	RSA 署名認証, 3DES 暗号化, SHA1 ハッシング

IKE プロポーザル名の形式は、次のとおりです。

`ike-phase1_authentication-encryption_type-hash_algorithm`

4.6.6.5 IKE カスタム・プロポーザルのワークシート

図 4-17 に、IKE カスタム・プロポーザルのワークシートを示します。事前に定義されたプロポーザルの中に、環境に適したものがない場合 (IKE プロポーザルのワークシートの「プロポーザル名」で「カスタム・プロポーザル」にチェックを付けている場合) にのみ、このワークシートへの記入が必要です。以下の項では、このワークシートへ記入する情報について説明します。オンラインでマニュアルをご覧になっている場合は、印刷機能でワークシートを印刷してください。

図 4-17: IKE カスタム・プロポーザル・ワークシート

IKE カスタム・プロポーザル・ワークシート	
カスタム・プロポーザル名: _____	
暗号化アルゴリズム:	<input type="checkbox"/> DES CBC <input type="checkbox"/> 3DES CBC
認証方式:	<input type="checkbox"/> 事前共有鍵 <input type="checkbox"/> RSA暗号化 <input type="checkbox"/> DSS署名 <input type="checkbox"/> RSA署名
ハッシュ・アルゴリズム:	<input type="checkbox"/> MD5 <input type="checkbox"/> SHA1
フェーズ 1 存続期間	
存続期間名:	_____
指定秒後、鍵を再生成:	_____

カスタム・プロポーザル名

カスタム IKE プロポーザルを作成する場合の、新しいプロポーザルの名前です。ほとんどの場合は、事前に定義された IKE プロポーザルとそのパラメータで十分です。

暗号化アルゴリズム

IKE 交換に使用する暗号化アルゴリズムのタイプです。DES CBC を使用する場合は「DES CBC」にチェックを付けます。3DES CBC を使用する場合は「3DES CBC」にチェックを付けます。

認証方式

IKE フェーズ 1 交換に使用する認証方式のタイプです。使用する認証のタイプに応じて方式にチェックを付けます。RSA 署名方式は、サポートしているベンダが最も多い方式です。

方式名	説明
事前共有鍵	最も単純な方式です。この鍵は、IPsec 手動鍵と同じように、各システムでインストールと更新を手動で行う必要があります。
DSS 署名	認証は、DSS (Digital Signature Standard) を使用して、電子署名を生成し確認することによって行われます。DSS に基づく公開鍵を持つ証明書が必要です。
RSA 署名	DSS 署名と同じようなものですが、これは RSA 電子署名アルゴリズムを使用します。RSA 公開鍵を持つ証明書が必要です。
RSA 暗号化	認証は、RSA 公開鍵の暗号化アルゴリズムを用いて暗号化したデータを送信することで行われます。RSA 公開鍵を持つ証明書が必要です。公開鍵の操作が多く必要になるので、他の署名方式よりも低速になります。

ハッシュ・アルゴリズム

IKE 交換に使用するハッシュ・アルゴリズムのタイプです。MD5 を使用する場合は、「MD5」をチェックします。SHA 1 を使用する場合は、「SHA1」をチェックします。

フェーズ 1 存続期間

IKE 接続の存続期間です。

存続期間名

存続期間指定の名前です。

指定秒後、鍵を再生成

IKE 接続が停止するまでに IKE 接続が存続できる時間 (秒単位) です。IKE 接続は、新しいフェーズ 2 交換または新しい IP トラフィック用に必要になった時点で再度作成されます。

注意

「指定 K バイト後，鍵を再生成」フィールドは，IKE 接続では無視されます。

4.6.6.6 IKE 認証のワークシート

図 4-18 に，IKE 認証のワークシートを示します。以下の項では，このワークシートへ記入する情報について説明します。オンラインでマニュアルをご覧になっている場合は，印刷機能でワークシートを印刷してください。

図 4-18: IKE 認証ワークシート

IKE 認証ワークシート	
認証	
認証:	<input type="checkbox"/> 公開鍵証明書 <input type="checkbox"/> 事前共有 IKE 鍵
証明書	
公開鍵証明書名: _____	
証明書のエンコーディング: <input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL	
証明書ファイル: _____	
非公開鍵のエンコーディング: <input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL	
非公開鍵ファイル: _____	
CA 証明書: <input type="checkbox"/> Yes <input type="checkbox"/> No	
CRL 利用可能: <input type="checkbox"/> Yes <input type="checkbox"/> No	
CRL エンコーディング: <input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL	
CRL ファイル: _____	
事前共有 IKE 鍵	
鍵の名前: _____	
鍵の値: _____	
ローカル ID: <input type="checkbox"/> デフォルト <input type="checkbox"/> IPv4 アドレス <input type="checkbox"/> IPv6 アドレス	
<input type="checkbox"/> FQDM <input type="checkbox"/> 電子メール・アドレス <input type="checkbox"/> 16 進数の鍵	
ID 文字列: _____	

認証

IKE 交換を認証するために使用する方式です。事前共有シークレットを使用する場合は「事前共有 IKE 鍵」にチェックを付けます。公開鍵の証明書を使用する場合は、「公開鍵証明書」にチェックを付けます。

証明書

証明書は、IKE 交換のローカル・ホストを識別します。

公開鍵証明書名

IPsec 構成ファイル内で公開鍵証明書を識別するための名前です。証明書の実際の題名とは関係ありません。

証明書のエンコーディング

証明書のバイナリ・データに使用するエンコーディングのタイプです。証明書が PEM でエンコードされている場合は、「PEM」にチェックを付けます。証明書が DER でエンコードされている場合は、「バイナリ」にチェックを付けます。証明書が 16 進数としてエンコードされている場合は、「HEXL」にチェックを付けます。

証明書ファイル

証明書ファイルのフルパス名です。証明書ファイルの保存には /var/ipsec ディレクトリが使用できます。

非公開鍵のエンコーディング

証明書がシステムを認証する場合に、非公開鍵に使用するエンコーディングのタイプです。これは CA 証明書とピア証明書 (RSA 暗号化など) には適用できません。証明書が PEM を用いてエンコードされる場合は、「PEM」にチェックを付けます。証明書が DER を用いてエンコードされる場合は、「バイナリ」にチェックを付けます。証明書が 16 進数としてエンコードされる場合は、「HEXL」にチェックを付けます。

非公開鍵ファイル

非公開鍵ファイルへのフルパス名です。非公開鍵ファイルの保存には /var/ipsec ディレクトリが使用できます。これは CA 証明書とピア証明書 (RSA 暗号化など) には適用できません。

CA 証明書

この証明書が、他の証明書への署名に使用できるほど信頼できる場合は、「Yes」にチェックを付けます。それほど信頼できない場合は「No」にチェックを付けます。

CRL 利用可能

CA 証明書の場合、この証明書が署名した証明書で CRL (Certificate Revocation List) が利用できる場合は「Yes」にチェックを付けます。それ以外の場合は「No」にチェックを付けます。

CRL エンコーディング

CA 証明書の場合、CRL に使用されるエンコーディングのタイプです (CRL が利用できる場合)。CRL が PEM を用いてエンコードされる場合は、「PEM」にチェックを付けます。CRL が DER を用いてエンコードされる場合は、「バイナリ」にチェックを付けます。CRL が 16 進数としてエンコードされる場合は、「HEX」にチェックを付けます。

CRL ファイル

CA 証明書の場合、CRL ファイルのフルパス名です。CRL ファイルの保存には /var/ipsec ディレクトリが使用できます。

事前共有 IKE 鍵

事前共有鍵は、受信側のシステムに前もって渡されている認証鍵です。
鍵の名前

事前共有鍵の名前です。

鍵の値

鍵の値に対するテキスト文字列または 16 進数の文字列 (先頭が 0x) です。セキュリティを向上するには、テキストまたは 16 進数の長いランダムなシーケンスを使用します。

ローカル ID

IKE フェーズ 1 交換で事前共有鍵とともに送信された、送信側ホストの ID です。送信する特定のローカル ID を選択します。選択肢には、IPv4 アドレス、IPv6 アドレス、完全修飾ドメイン名 (FQDN)、電子

メール・アドレス，16 進数の鍵 ID があります。一般に，これはローカル・システムの IP アドレスまたは FQDN になります。IPsec の実装によって，要件が異なります。詳細は，リモート・システムのセキュリティ管理者にお問い合わせください。

ID 文字列

特定の ID タイプに対するテキスト文字列または 16 進数の文字列（先頭が 0x）です。

4.6.6.7 公開鍵証明書のワークシート

図 4-19 に，公開鍵証明書のワークシートを示します。root の証明書またはその他の公開鍵証明書を追加するには，このワークシートへの記入が必要です。以下の項では，このワークシートへ記入する情報について説明します。オンラインでマニュアルをご覧になっている場合は，印刷機能でワークシートを印刷してください。

図 4-19: IPsec 公開鍵証明書ワークシート

公開鍵証明書ワークシート	
名前:	_____
証明書エンコーディング:	<input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL
証明書ファイル:	_____
非公開鍵エンコーディング:	<input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL
非公開鍵ファイル:	_____
CA 証明書:	<input type="checkbox"/> Yes <input type="checkbox"/> No
CRL 利用可能:	<input type="checkbox"/> Yes <input type="checkbox"/> No
CRL エンコーディング:	<input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL
CRL ファイル:	_____

公開鍵証明書名

公開鍵証明書の名前です。この名前は，証明書の実際の題名とは関係ありません。

証明書エンコーディング

証明書のバイナリ・データに使用するエンコーディングのタイプです。証明書が PEM でエンコードされている場合は，「PEM」にチェックを

付けます。証明書が DER でエンコードされている場合は、「バイナリ」にチェックを付けます。証明書が 16 進数としてエンコードされている場合は、「HEXL」にチェックを付けます。

証明書ファイル

証明書ファイルのフルパス名です。証明書ファイルの保存には /var/ipsec ディレクトリが使用できます。

非公開鍵エンコーディング

証明書がシステムを認証する場合に、非公開鍵に使用するエンコーディングのタイプです。これは CA 証明書とピア証明書 (RSA 暗号化など) には適用できません。証明書が PEM を用いてエンコードされる場合は、「PEM」にチェックを付けます。証明書が DER を用いてエンコードされる場合は、「バイナリ」にチェックを付けます。証明書が 16 進数としてエンコードされる場合は、「HEXL」にチェックを付けます。

非公開鍵ファイル

非公開鍵ファイルへのフルパス名です。非公開鍵ファイルの保存には /var/ipsec ディレクトリが使用できます。これは CA 証明書とピア証明書 (RSA 暗号化など) には適用できません。

CA 証明書

この証明書が、他の証明書への署名に使用できるほど信頼できる場合は、「Yes」にチェックを付けます。それほど信頼できない場合は「No」にチェックを付けます。

CRL 利用可能

CA 証明書の場合、この証明書が署名した証明書で CRL (Certificate Revocation List) が利用できる場合は「Yes」にチェックを付けます。それ以外の場合は「No」にチェックを付けます。

CRL エンコーディング

CA 証明書の場合、CRL に使用されるエンコーディングのタイプです (CRL が利用できる場合)。CRL が PEM を用いてエンコードされる場合は、「PEM」にチェックを付けます。CRL が DER を用いてエンコー

ドされる場合は、「バイナリ」にチェックを付けます。CRL が 16 進数としてエンコードされる場合は、「HEXL」にチェックを付けます。

CRL ファイル

CA 証明書の場合、CRL ファイルのフルパス名です。CRL ファイルの保存には /var/ipsec ディレクトリが使用できます。

4.6.6.8 IKE オプションのワークシート

図 4-20 に、IKE オプションのワークシートを示します。省略時のオプション以外のオプションを指定する場合に限り、このワークシートへの記入が必要です。以下の項では、このワークシートへ記入する情報について説明します。オンラインでマニュアルをご覧になっている場合は、印刷機能でワークシートを印刷してください。

図 4-20: IKE オプション・ワークシート

IKE オプション・ワークシート	
SA キープアライブ:	<input type="checkbox"/> Yes <input type="checkbox"/> No
アグレッシブ・モード:	<input type="checkbox"/> Yes <input type="checkbox"/> No
パスMTUなし:	<input type="checkbox"/> Yes <input type="checkbox"/> No
一意のSAの作成:	<input type="checkbox"/> ポートごと <input type="checkbox"/> プロトコルごと <input type="checkbox"/> ホストごと <input type="checkbox"/> ネットワークごと
IKEグループ:	<input type="checkbox"/> デフォルト <input type="checkbox"/> グループ1 <input type="checkbox"/> グループ2 <input type="checkbox"/> グループ5
PFSグループ:	<input type="checkbox"/> なし <input type="checkbox"/> グループ1 <input type="checkbox"/> グループ2 <input type="checkbox"/> グループ5
フェース 1 およびフェース 2 の存続期間	
存続期間名: _____	
指定秒後、鍵を再生成: _____	
指定Kバイト後、鍵を再生成: _____	

SA キープアライブ

接続のコンテキストは、パケットが送受信されていないときにも維持されます。SA キープアライブを使用する場合は「Yes」、それ以外の場合は「No」にチェックを付けます。

アグレッシブ・モード

省略時のモード (メイン・モードと呼ばれる) より高速だが、折衝中の双方の ID を暗号化しない IKE 接続を確立するモードです。アグレッシブ・モードを使用する場合は「Yes」、使用しない場合は「No」にチェックを付けます。

パス MTU なし

システムによる MTU サイズの変更を無効にする場合は「Yes」、無効にしない場合は「No」にチェックを付けます。

一意の SA の作成

接続のポート、上位層プロトコル、ホスト、またはサブネットごとに一意の SA を作成します。使用するコンテキストを選択してください。省略したときには、トランスポート・モードではホストごとに一意の SA を作成し、トンネル・モードではネットワークごとに一意の SA を作成します。

IKE グループ

初期 Diffie-Hellman 交換に使用するグループです。これは、IKE プロポーザルより優先されます。グループ 1、2、5 のいずれかを選択します。省略時のグループはグループ 2 です。グループの番号が大きいほど、長い Diffie-Hellman 値が使用され安全ですが、CPU リソースの使用量が多くなります。古い IKE 実装との互換性が必要な場合以外は、グループ 1 は使用しないでください。

PFS グループ

PFS (Perfect Forward Secrecy) を使用する際の、初期 Diffie-Hellman 交換に使用するグループです。PFS を使用する場合、鍵生成処理は、接続に新しい鍵が必要になるたびに再起動されます。以前の鍵データから新しい鍵が生成されることはありません。省略時の設定では PFS を使用しません。

グループ 1、2、5 のいずれかを選択します。グループの番号が大きいほど、長い Diffie-Hellman 値が使用され安全ですが、CPU リソースの使用量が多くなります。

フェーズ 1 およびフェーズ 2 の SA 存続期間

IKE と IPsec SA の両方に対する省略時の存続期間です。この存続期間よりも、個別のプロポーザルで指定した存続期間の方が優先されます。

存続期間名

省略時の存続期間の名前です。

指定秒後、鍵を再生成

鍵の再生成を行わずに、接続が停止するまでに存続する時間 (秒単位) です。IPsec SA の場合、鍵の再生成は、時間の約 80 ~ 90 パーセントが経過したときに開始されます。新しい鍵が生成されて配信されると、接続が利用可能になります。省略時の値は、選択したプロポーザルによって異なります。この秒数の 2 倍の間、接続が使用されなかった場合は、接続が削除されます。

IKE SA の場合、指定された時間が経過した時点で接続は削除されます。接続は、追加のフェーズ 2 交換が必要になった時点で、または新しい IP トラフィックに応答して再度作成されます。

指定 K バイト後、鍵を再生成

鍵の再生成を行わずに、IPsec 接続が停止するまでに通すことができるデータの量 (K バイト単位) です。鍵の再生成は、データの約 80 ~ 90 パーセントが通過したときに開始されます。新しい鍵が生成されて配信されると、接続が利用可能になります。省略時の値は、選択したプロポーザルによって異なります。この存続期間は、IKE SA に対しては無視されます。

4.6.6.9 手動鍵のワークシート

図 4-21 に、IPsec 手動鍵のワークシートを示します。パケットの認証と暗号化のために手動で鍵を作成する場合 (IPsec プロポーザル・ワークシートの「鍵の取得」フィールドの「手動構成」にチェックを付けた場合) にのみ、このワークシートへの記入が必要です。以下の項では、このワークシートへ記入する情報について説明します。オンラインでマニュアルをご覧ください。印刷機能でワークシートを印刷してください。

注意

手動鍵を使用する場合、プロポーザルでは1つのプロトコルのみを指定していなければなりません。AHでは、認証アルゴリズムを1つだけ指定できます。ESPでは、1つの認証アルゴリズム、1つの暗号化アルゴリズム、またはそれぞれ1つを指定できます。複数の認証または暗号化アルゴリズムを指定するプロポーザルは使用できません。

図 4-21: IPsec 手動鍵ワークシート

手動鍵ワークシート	
鍵の名前:	_____
セキュリティ・パラメータ・インデックス:	_____
暗号鍵:	_____
認証鍵:	_____
処理のタイプ:	<input type="checkbox"/> 着信パケット <input type="checkbox"/> 発信パケット

鍵の名前

手動鍵の名前です。

セキュリティ・パラメータ・インデックス

対応する AH または ESP ヘッダ内の SPI (Security Parameters Index) を指定する、ゼロでない 32 ビットの数値です。IKE とともに手動鍵を使用する場合は、257 ~ 4095 の SPI 値を指定しなければなりません。この範囲の値は、IKE が自動的に割り当てることはありません。

暗号鍵

暗号化アルゴリズムで使用する暗号鍵を指定する、ASCII テキスト文字列または 16 進数の文字列 (先頭が 0x) です。次の表に、それぞれのアルゴリズムに必要な鍵の長さを示します。

アルゴリズム	ASCII 鍵の長さ (文字数)	Hex 鍵の長さ (桁数)
3DES	24 (192 ビット)	48 (192 ビット)
AES	16 (128 ビット)	32 (128 ビット)
	24 (192 ビット)	48 (192 ビット)
	32 (256 ビット)	64 (256 ビット)
DES	8 (64 ビット)	16 (64 ビット)

プロポーザルで暗号化を指定している場合にのみ、暗号鍵を指定します。

注意

ランダムに生成された 16 進数文字列は、一般に ASCII 文字列よりも安全です。

認証鍵

認証アルゴリズムで使用する認証鍵を指定する、ASCII テキスト文字列または 16 進数の文字列 (先頭が 0x) です。次の表に、それぞれのアルゴリズムに必要な鍵の長さを示します。

アルゴリズム	ASCII 鍵の長さ (文字数)	Hex 鍵の長さ (桁数)
HMAC MD5	16 (128 ビット)	32 (128 ビット)
HMAC SHA	20 (160 ビット)	40 (160 ビット)

プロポーザルで認証を指定している場合にのみ、認証鍵を指定します。

注意

ランダムに生成された 16 進数文字列は、一般に ASCII 文字列よりも安全です。

処理のタイプ

手動鍵を適用するパケットです。鍵を受信パケットに適用する場合は、「受信パケット」にチェックを付けます。鍵を送信パケットに適用する

場合は、「送信パケット」にチェックを付けます。鍵を送信と受信両方のパケットに適用する場合は、両方のボックスにチェックを付けます。

4.6.7 IPsec 構成例でのシステム構成

ここでは、4.1 節に示した各構成例について説明し、それぞれの例について、選択したシステムを構成する方法を示します。いずれの場合でも、記入したワークシートとその内容についての説明は、システムの IPsec を構成するうえで参考になります。場合によっては、構成を検討できるように別のオプションを示すこともあります。また、特定のトラフィックに対して接続を構成する方法についても説明します。

4.6.7.1 ホスト対ホスト接続の構成

図 4-1 では、ホスト A とホスト F がインターネット上のセキュア接続を通して通信しています。ホスト A の IPsec 接続ワークシートの記入例を次に示します。

IPsec 接続ワークシート	
名前: <u>HostF</u>	
セレクト	
リモートIPアドレス	
タイプ: <input checked="" type="checkbox"/> 単独IPv4 <input type="checkbox"/> IPv4サブネット <input type="checkbox"/> IPv4レンジ <input type="checkbox"/> 全IPv4 <input type="checkbox"/> 単独IPv6 <input type="checkbox"/> IPv6サブネット <input type="checkbox"/> IPv6レンジ <input type="checkbox"/> 全IPv6	
アドレス: <u>11.0.2.3</u>	
IPサブネット・サイズ: _____	
終了アドレス: _____	
照合プロトコル: <input checked="" type="checkbox"/> 任意 <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> icmp <input type="checkbox"/> icmpv6 <input type="checkbox"/> ip <input type="checkbox"/> igmp	
照合ポート: _____	
ローカルIPアドレス	
タイプ: <input checked="" type="checkbox"/> 単独IPv4 <input type="checkbox"/> IPv4サブネット <input type="checkbox"/> IPv4レンジ <input type="checkbox"/> 全IPv4 <input type="checkbox"/> 単独IPv6 <input type="checkbox"/> IPv6サブネット <input type="checkbox"/> IPv6レンジ <input type="checkbox"/> 全IPv6	
アドレス: <u>11.0.1.1</u>	
IPサブネット・サイズ: _____	
終了アドレス: _____	
照合プロトコル: <input checked="" type="checkbox"/> 任意 <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> icmp <input type="checkbox"/> icmpv6 <input type="checkbox"/> ip <input type="checkbox"/> igmp	
照合ポート: _____	
アクション	
<input checked="" type="checkbox"/> IPsecを適用 <input type="checkbox"/> IPsecを適用しない <input type="checkbox"/> パケットを破棄	
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </div> <div style="border-left: 1px solid black; padding-left: 10px;"> 発信と着信 着信のみ 発信のみ </div> </div>	

ホスト F の IPsec 接続ワークシートは，ホスト A のワークシートと同様ですが，リモートとローカルの IP アドレス欄の内容が逆になっている点異なります。

トラフィックが安全でないインターネットを通るため，ホスト A とホスト F は，トランスポート・モードの認証と暗号化の両方を必要とします。こ

の情報を指定するホスト A の IPsec プロポーザル・ワークシートの記入例を次に示します。

IPsec プロポーザル・ワークシート	
プロポーザル・リスト:	<input type="checkbox"/> AH-ESP-IPCOMP-transport-proposals <input type="checkbox"/> AH-ESP-IPCOMP-tunnel-proposals <input type="checkbox"/> AH-ESP-transport-proposals <input type="checkbox"/> AH-ESP-tunnel-proposals <input type="checkbox"/> AH-transport-proposals <input type="checkbox"/> AH-tunnel-proposals <input type="checkbox"/> ESP-IPCOMP-tunnel-proposals <input type="checkbox"/> ESP-IPCOMP-transport-proposals <input checked="" type="checkbox"/> ESP-transport-proposals <input type="checkbox"/> ESP-tunnel-proposals <input type="checkbox"/> カスタム・リスト
リモート・セキュア・ゲートウェイのIPアドレス:	_____
ローカル・セキュア・ゲートウェイのIPアドレス:	_____
鍵の取得:	<input checked="" type="checkbox"/> IKE <input type="checkbox"/> 手動構成

この構成では通信するホストが 2 つだけなので、事前共有鍵を使用して IKE 交換を保護します。ホスト A の IKE プロポーザル・ワークシートの記入例を次に示します。

IKE プロポーザル・ワークシート	
プロポーザル・リスト名:	<input type="checkbox"/> DSA-signature-proposals <input checked="" type="checkbox"/> Pre-Shared-Key-proposals <input type="checkbox"/> RSA-encryption-proposals <input type="checkbox"/> RSA-signature-proposals <input type="checkbox"/> カスタム・リスト

事前共有鍵の情報は、次に示すホスト A の IKE 認証ワークシートの記入例で指定されています。

IKE 認証ワークシート	
認証	
認証:	<input type="checkbox"/> 公開鍵証明書 <input checked="" type="checkbox"/> 事前共有 IKE 鍵
証明書	
公開鍵証明書名: _____ 証明書のエンコーディング: <input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL 証明書ファイル: _____ 非公開鍵のエンコーディング: <input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL 非公開鍵ファイル: _____ CA 証明書: <input type="checkbox"/> Yes <input type="checkbox"/> No CRL 利用可能: <input type="checkbox"/> Yes <input type="checkbox"/> No CRL エンコーディング: <input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL CRL ファイル: _____	
事前共有 IKE 鍵	
鍵の名前:	<u>key-for-host-f</u>
鍵の値:	<u>0x2a5fe219bc37dd46a314fb92</u>
ローカルID:	<input type="checkbox"/> デフォルト <input checked="" type="checkbox"/> IPv4アドレス <input type="checkbox"/> IPv6アドレス <input type="checkbox"/> FQDM <input type="checkbox"/> 電子メール・アドレス <input type="checkbox"/> 16進数の鍵
ID文字列:	<u>11.0.1.1</u>

この構成では、特殊な IKE オプションは必要ありません。

4.6.7.2 セキュア・ゲートウェイ対セキュア・ゲートウェイ接続の構成

図 4-2 では、セキュア GW A とセキュア GW B がインターネットを通してセキュア・トンネルを維持しています。このセキュア・トンネルは、地理的に離れた 2 つのサブネットを VPN で接続しています。セキュア GW A の IPsec 接続ワークシートの記入例を次に示します。

IPsec 接続ワークシート	
名前: <u>secure-gwy-2</u>	
セレクト	
リモートIPアドレス	
タイプ: <input type="checkbox"/> 単独IPv4 <input checked="" type="checkbox"/> IPv4サブネット <input type="checkbox"/> IPv4レンジ <input type="checkbox"/> 全IPv4 <input type="checkbox"/> 単独IPv6 <input type="checkbox"/> IPv6サブネット <input type="checkbox"/> IPv6レンジ <input type="checkbox"/> 全IPv6	
アドレス: <u>11.0.2.0</u>	
IPサブネット・サイズ: _____	
終了アドレス: _____	
照合プロトコル: <input checked="" type="checkbox"/> 任意 <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> icmp <input type="checkbox"/> icmpv6 <input type="checkbox"/> ip <input type="checkbox"/> igmp	
照合ポート: _____	
ローカルIPアドレス	
タイプ: <input type="checkbox"/> 単独IPv4 <input checked="" type="checkbox"/> IPv4サブネット <input type="checkbox"/> IPv4レンジ <input type="checkbox"/> 全IPv4 <input type="checkbox"/> 単独IPv6 <input type="checkbox"/> IPv6サブネット <input type="checkbox"/> IPv6レンジ <input type="checkbox"/> 全IPv6	
アドレス: <u>11.0.1.0</u>	
IPサブネット・サイズ: <u>24</u>	
終了アドレス: _____	
照合プロトコル: <input checked="" type="checkbox"/> 任意 <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> icmp <input type="checkbox"/> icmpv6 <input type="checkbox"/> ip <input type="checkbox"/> igmp	
照合ポート: _____	
アクション	
<input checked="" type="checkbox"/> IPsecを適用	
<input type="checkbox"/> IPsecを適用しない <input type="checkbox"/> パケットを破棄	<input type="checkbox"/> 発信と着信 <input type="checkbox"/> 着信のみ <input type="checkbox"/> 発信のみ

ここでは、4.6.7.1 項の場合と異なり、セレクトにはIPアドレスではなくサブネット・アドレスを指定する必要があることに注意してください。セキュア GW B の IPsec 接続ワークシートは、セキュア GW A のワークシートと同様ですが、リモートとローカルの IP アドレス欄の内容が逆になっている点異なります。

この構成に最適なプロポーザルは、ESP トンネル・プロポーザルです。リモートおよびローカルのセキュア・ゲートウェイの IP アドレスが必要です。IPsec プロポーザル・ワークシートの記入例を次に示します。

IPsec プロポーザル・ワークシート	
プロポーザル・リスト:	<input type="checkbox"/> AH-ESP-IPCOMP-transport-proposals <input type="checkbox"/> AH-ESP-IPCOMP-tunnel-proposals <input type="checkbox"/> AH-ESP-transport-proposals <input type="checkbox"/> AH-ESP-tunnel-proposals <input type="checkbox"/> AH-transport-proposals <input type="checkbox"/> AH-tunnel-proposals <input type="checkbox"/> ESP-IPCOMP-tunnel-proposals <input type="checkbox"/> ESP-IPCOMP-transport-proposals <input type="checkbox"/> ESP-transport-proposals <input checked="" type="checkbox"/> ESP-tunnel-proposals <input type="checkbox"/> カスタム・リスト
リモート・セキュア・ゲートウェイのIPアドレス:	<u>16.142.242.1</u>
ローカル・セキュア・ゲートウェイのIPアドレス:	<u>16.142.244.1</u>
鍵の取得:	<input checked="" type="checkbox"/> IKE <input type="checkbox"/> 手動構成

セキュア GW 2 の IP プロポーザル・ワークシートでは、ローカルとリモートのセキュア・ゲートウェイの IP アドレスが逆になっています。

2 つのゲートウェイは、IKE 交換を保護するための RSA 署名プロポーザルを折衝します。IKE プロポーザル・ワークシートの記入例を次に示します。

IKE プロポーザル・ワークシート	
プロポーザル・リスト名:	<input type="checkbox"/> DSA-signature-proposals <input type="checkbox"/> Pre-Shared-Key-proposals <input type="checkbox"/> RSA-encryption-proposals <input checked="" type="checkbox"/> RSA-signature-proposals <input type="checkbox"/> カスタム・リスト

公開鍵証明書の情報は、次の IKE 認証ワークシートに記録されています。

IKE 認証ワークシート	
認証	
認証:	<input checked="" type="checkbox"/> 公開鍵証明書 <input type="checkbox"/> 事前共有IKE鍵
証明書	
公開鍵証明書名: <u>secure-gwyl-cert</u>	
証明書のエンコーディング: <input checked="" type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL	
証明書ファイル: <u>/var/ipsec/sql.pem</u>	
非公開鍵のエンコーディング: <input checked="" type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL	
非公開鍵ファイル: <u>/var/ipsec/sql.private.pem</u>	
CA 証明書: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
CRL 利用可能: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
CRL エンコーディング: <input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL	
CRL ファイル: _____	

上記のワークシートでは、暗号化操作のために証明書ファイルと非公開鍵ファイルを指定しました。

この構成では、PFS (Perfect Forward Secrecy) を使用して、追加の鍵を生成するために既存の鍵を使用しないことを保証しています。この情報は、次に示す記入済みの IKE オプション・ワークシートで指定しています。

IKE オプション・ワークシート	
SA キープアライブ:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
アグレッシブ・モード:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
パスMTUなし:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
一意のSAの作成:	<input checked="" type="checkbox"/> ポートごと <input type="checkbox"/> プロトコルごと <input type="checkbox"/> ホストごと <input type="checkbox"/> ネットワークごと
IKEグループ:	<input type="checkbox"/> デフォルト <input type="checkbox"/> グループ1 <input checked="" type="checkbox"/> グループ2 <input type="checkbox"/> グループ5
PFSグループ:	<input type="checkbox"/> なし <input type="checkbox"/> グループ1 <input checked="" type="checkbox"/> グループ2 <input type="checkbox"/> グループ5

セキュア GW A では公開鍵証明書の情報を指定しているので、管理者は、対応する公開鍵証明書用に、root 証明書または他の認定された署名の証明

書情報も指定しなければなりません。記入済みの IPsec 公開鍵証明書ワークシートを次に示します。

公開鍵証明書ワークシート	
名前:	<u>root-cert</u>
証明書エンコーディング:	<input checked="" type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL
証明書ファイル:	<u>/var/ipsec/root.pem</u>
非公開鍵エンコーディング:	<input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL
非公開鍵ファイル:	_____
CA 証明書:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
CRL 利用可能:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
CRL エンコーディング:	<input type="checkbox"/> PEM <input type="checkbox"/> バイナリ <input type="checkbox"/> HEXL
CRL ファイル:	_____

4.6.7.3 ホスト対セキュア・ゲートウェイ接続の構成

図 4-3 では、ホスト D はインターネット上のセキュア・トンネルを通して、セキュア・ゲートウェイと通信を行います。ホスト D の IPsec 接続ワークシートの記入例を次に示します。

IPsec 接続ワークシート	
名前: <u>secure-gwy</u>	
セレクト	
リモート IP アドレス	
タイプ: <input type="checkbox"/> 単独 IPv4 <input checked="" type="checkbox"/> IPv4 サブネット <input type="checkbox"/> IPv4 レンジ <input type="checkbox"/> 全 IPv4 <input type="checkbox"/> 単独 IPv6 <input type="checkbox"/> IPv6 サブネット <input type="checkbox"/> IPv6 レンジ <input type="checkbox"/> 全 IPv6	
アドレス: <u>11.0.1.0</u>	
IP サブネット・サイズ: <u>24</u>	
終了アドレス: _____	
照合プロトコル: <input checked="" type="checkbox"/> 任意 <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> icmp <input type="checkbox"/> icmpv6 <input type="checkbox"/> ip <input type="checkbox"/> igmp	
照合ポート: _____	
ローカル IP アドレス	
タイプ: <input checked="" type="checkbox"/> 単独 IPv4 <input type="checkbox"/> IPv4 サブネット <input type="checkbox"/> IPv4 レンジ <input type="checkbox"/> 全 IPv4 <input type="checkbox"/> 単独 IPv6 <input type="checkbox"/> IPv6 サブネット <input type="checkbox"/> IPv6 レンジ <input type="checkbox"/> 全 IPv6	
アドレス: <u>11.0.3.1</u>	
IP サブネット・サイズ: _____	
終了アドレス: _____	
照合プロトコル: <input checked="" type="checkbox"/> 任意 <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> icmp <input type="checkbox"/> icmpv6 <input type="checkbox"/> ip <input type="checkbox"/> igmp	
照合ポート: _____	
アクション	
<input checked="" type="checkbox"/> IPsec を適用 <input type="checkbox"/> IPsec を適用しない <input type="checkbox"/> パケットを破棄	
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <input type="checkbox"/> 発信と着信 <input type="checkbox"/> 着信のみ <input type="checkbox"/> 発信のみ </div> </div>	

リモート IP アドレス・セレクトに IP サブネットを指定し、ローカル IP アドレス・セレクトに単独 IP アドレスを指定していることに注意してください。セキュア・ゲートウェイの IPsec 接続ワークシートは、ホスト D のワークシートと同様ですが、リモートとローカルの IP アドレス欄の内容が逆になっている点が異なります。

ホスト D は自分自身のセキュア・ゲートウェイとして機能しているため、この構成での最適なプロポーザルは、前の構成と同じように、ESP トンネル・プロポーザルです。この構成でも、リモートおよびローカルのセキュア・ゲートウェイの IP アドレスが必要になります。IPsec プロポーザル・ワークシートの記入例を次に示します。

IPsec プロポーザル・ワークシート	
プロポーザル・リスト:	<input type="checkbox"/> AH-ESP-IPCOMP-transport-proposals <input type="checkbox"/> AH-ESP-IPCOMP-tunnel-proposals <input type="checkbox"/> AH-ESP-transport-proposals <input type="checkbox"/> AH-ESP-tunnel-proposals <input type="checkbox"/> AH-transport-proposals <input type="checkbox"/> AH-tunnel-proposals <input type="checkbox"/> ESP-IPCOMP-tunnel-proposals <input type="checkbox"/> ESP-IPCOMP-transport-proposals <input type="checkbox"/> ESP-transport-proposals <input checked="" type="checkbox"/> ESP-tunnel-proposals <input type="checkbox"/> カスタム・リスト
リモート・セキュア・ゲートウェイのIPアドレス:	<u>16.142.242.1</u>
ローカル・セキュア・ゲートウェイのIPアドレス:	<u>11.0.3.1</u>
鍵の取得:	<input checked="" type="checkbox"/> IKE <input type="checkbox"/> 手動構成

セキュア・ゲートウェイの IPsec プロポーザル・ワークシートでは、ローカルとリモートのセキュア・ゲートウェイの IP アドレスが逆になります。

また、この構成では IKE 認証に RSA 署名プロポーザルを使用します。公開鍵証明書情報は、次の IKE 認証ワークシートの例に記録されています。

IKE 認証ワークシート

認証

認証: ☒ 公開鍵証明書 ☐ 事前共有IKE鍵

証明書

公開鍵証明書名: secure-gwy-cert

証明書のエンコーディング: ☒ PEM ☐ バイナリ ☐ HEXL

証明書ファイル: /var/ipsec/sqwy.pem

非公開鍵のエンコーディング: ☒ PEM ☐ バイナリ ☐ HEXL

非公開鍵ファイル: /var/ipsec/sq-private.pem

CA 証明書: ☐ Yes ☒ No

CRL 利用可能: ☐ Yes ☒ No

CRL エンコーディング: ☐ PEM ☐ バイナリ ☐ HEXL

CRL ファイル: _____

前の構成と同じように、管理者は、対応する公開鍵証明書用に、root 証明書または他の認定された署名の証明書情報も指定しなければなりません。記入済みの IPsec 公開鍵証明書ワークシートを次に示します。

公開鍵証明書ワークシート

名前: root-cert

証明書エンコーディング: ☒ PEM ☐ バイナリ ☐ HEXL

証明書ファイル: /var/ipsec/root.pem

非公開鍵エンコーディング: ☐ PEM ☐ バイナリ ☐ HEXL

非公開鍵ファイル: _____

CA 証明書: ☒ Yes ☐ No

CRL 利用可能: ☐ Yes ☒ No

CRL エンコーディング: ☐ PEM ☐ バイナリ ☐ HEXL

CRL ファイル: _____

4.6.7.4 特定のトラフィックに対する接続の構成

前述の構成では，さまざまなシステムの間ですべてのトラフィックの安全を確保する方法を示しました。しかし，すべてのトラフィックではなく，特定のプロトコルやアプリケーション（たとえば，ファイル転送プロトコル，FTP）のトラフィックのみを安全にしたい場合もあります。FTP にはポート 20 にデータ・チャンネルがあり（データのトラフィック用），ポート 21 にコントロール・チャンネル（コマンドと応答用）があります。ここでは，省略時の接続に加えて，IPsec 保護が FTP トラフィックに適用されるように，図 4-1 のホスト A と ホスト F を構成する方法について説明します。

ホスト A に対して，次のセレクトタで FTP サーバ接続を作成します。

- リモート・セレクトタ (IPv4 アドレス 11.0.2.3，TCP プロトコル，任意のポート)
- ローカル・セレクトタ (IPv4 アドレス 11.0.1.1，TCP プロトコル，ポート 21)
- ローカル・セレクトタ (IPv4 アドレス 11.0.1.1，TCP プロトコル，ポート 20)

また，次のセレクトタで FTP クライアント接続を作成します。

- リモート・セレクトタ (IPv4 アドレス 11.0.2.3，TCP プロトコル，ポート 21)
- リモート・セレクトタ (IPv4 アドレス 11.0.2.3，TCP プロトコル，ポート 20)
- ローカル・セレクトタ (IPv4 アドレス 11.0.1.1，TCP プロトコル，任意のポート)

次に，適切なアクションとプロポーザルを選択します。

ホスト F の場合も FTP クライアント接続と FTP サーバ接続を作成しますが，ローカルとリモートの IPv4 アドレスが逆になります。

FTP トラフィックのみを保護する場合は，FTP 接続が動作しない場合に備えて，保護なしですべてのトラフィックを通す接続をそれぞれのノードに作成します。このようにすると，ホストはネットワーク接続から孤立しません。リモートおよびローカルのセレクトタは，すべての IPv4 アドレス，任意のプロトコル，任意のポートに対するものになります。または，他のトラフィックを保護する場合は，FTP 接続の後に他の接続を作成できます。

4.7 IPsec の構成

共通デスクトップ環境 (CDE) のアプリケーション・マネージャの SysMan Menu アプリケーションを使用すると、IPsec の構成ができます。ここでは、システムを IPsec ホストとして構成する方法とセキュア・ゲートウェイとして構成する方法を説明します。

4.7.1 ホストの構成

ホストに IPsec を構成するには、次のように操作します。

1. SysMan Menu で [ネットワーク] [追加ネットワーク・サービス] [インターネット・プロトコル・セキュリティ (IPsec) の設定] を選択して、IPsec のメイン・ウィンドウを表示します。

または、コマンド行で次のコマンドを入力します。

```
# /usr/sbin/sysman ipsec
```

IPsec を初めて構成する場合は、情報ダイアログ・ボックスが表示され、IPsec を有効にする前にセキュア接続を定義するように通知されることがあります。セキュア接続を定義せずに IPsec を有効にすると、システムに出入りするパケットはすべて破棄され、トラフィックが流れなくなります。[了解] を選択します。

IPsec メイン・ウィンドウには、構成されたセキュア接続と構成された公開鍵証明書が表示されます。

2. ウィンドウの上部で [このシステムで IP セキュリティ (IPsec) を有効にする] を選択します。
3. [追加] を選択します。「セキュア接続の追加/変更」ダイアログ・ボックスが表示されます。
4. 接続名を入力します。
5. [追加] を選択してリモート IP アドレス・セレクタを追加します。「セレクタの追加/変更」ダイアログ・ボックスが表示されます。次の操作を実行します。
 - a. セレクタのタイプを選択します。
 - b. IP アドレス (単一のホストと通信している場合)、サブネット・アドレス (セキュア・ゲートウェイと通信している場合)、最初のアドレス (アドレス・レンジと通信している場合) を入力します。

- c. IP サブネットを選択した場合は、サブネット・マスクのサイズを入力します。
 - d. アドレス・レンジを選択した場合は、最後のアドレスを入力します。
 - e. 照合する上位層プロトコルを選択します。特に指定しなければ、すべてのプロトコルが選択されます。
 - f. セレクタを特定のポート番号に制限する場合は、照合するポート番号を入力します。特に指定しなければ、すべてのポート番号が選択されます。
 - g. [了解] を選択してデータを確定し、「セレクタの追加/変更」ダイアログ・ボックスを閉じます。リモート・アドレスとローカル・アドレスの追加が終了したら、手順 7 に進みます。
6. [追加] を選択してローカル IP アドレス・セレクタを追加します。手順 5a に進みます。
7. セレクタに一致したパケットに適用するアクションを選択します。省略時のアクションは、IPsec 保護の適用です。
8. [次へ] を選択してデータを確定し、「セキュア接続の追加/変更」ダイアログ・ボックスを閉じます。「接続の追加/変更: IPsec プロポーザル」ダイアログ・ボックスが表示されます。次の操作を実行します。
- a. プロポーザル・リストから IPsec プロポーザルを選択します。
 - b. セキュア・ゲートウェイと通信する場合は、セキュア・ゲートウェイ (リモート) の IP アドレスとシステムの IP アドレス (ローカル) を指定します。
 - c. IKE を使用して鍵を取得するか、手動設定を使用するかを指定します。[次へ] を選択して、データを確定して「接続の追加/変更: IPsec プロポーザル」ダイアログ・ボックスを閉じます。
- 手動設定を選択し、プロポーザルが 1 つだけのカスタム・プロポーザル・リストを作成した場合は、「接続の追加/変更: マニュアル・キー」ダイアログ・ボックスが表示されます。手順 9 に進んでください。IKE プロトコルを選択した場合は、「接続の追加/変更: IKE プロポーザル」ダイアログ・ボックスが表示されます。手順 11 に進んでください。

9. [追加] を選択して手動鍵を追加し、「Modify Keys: IPsec キーの追加/変更」ダイアログ・ボックスを表示します。次の操作を実行します。
 - a. 鍵名を入力します。
 - b. SPI (Security Parameter Index) を入力します。
 - c. 選択したプロポーザルに必要なアルゴリズムの鍵を入力します。
[了解] を選択してデータを確定し、「Modify Keys: IPsec キーの追加/変更」ダイアログ・ボックスを閉じます。
10. 受信パケット, 送信パケット, その両方のパケット, のいずれに鍵を適用するかを選択します。追加の鍵を指定する場合は, 手順 9 に進みます。手動鍵の指定が終了した場合は, 手順 18 に進みます。
11. プロポーザル・リストから IKE プロポーザルを選択します。[次へ] をクリックして, データを確定して「接続の追加/変更: IKE プロポーザル」ダイアログ・ボックスを閉じ, 「接続の追加/変更: IKE 認証」ダイアログ・ボックスを表示します。
12. 公開鍵証明書または事前共有鍵で IKE 交換を認証するかどうかを選択します。
13. 公開鍵証明書を選択した場合は, [追加] を選択して IKE 証明書を追加します。「証明の追加/変更」ダイアログ・ボックスが表示されます。次の操作を実行します。
 - a. 証明書名を入力し, 証明書のエンコード方式を選択し, 証明書ファイルのローカル・パスを入力します。
 - b. この証明書がシステムを認証する場合は, エンコード方式を選択して, 非公開鍵ファイルのローカル・パスを入力します。
 - c. この証明書を他の証明書への署名に使用する場合は, [CA 証明] を選択します。それ以外の場合は, 手順 f に進みます。
 - d. CRL (Certificate Revocation List) が使用できない場合は, [証明取消リスト (CRL) がありません] を選択します。手順 f に進みます。
 - e. CRL のエンコード方式を選択して, CRL ファイルのローカル・パスを入力します。
 - f. [了解] を選択してデータを確定し, 「証明の追加/変更」ダイアログ・ボックスを閉じます。

14. IKE 交換のための証明書を選択します。手順 17 に進みます。
15. 事前共有鍵を選択した場合は、[IKE 共有キーの追加] を選択します。
「IKE キーの追加/変更」ダイアログ・ボックスが表示されます。次の操作を実行します。
 - a. 鍵名と鍵の値を入力します。
 - b. ローカル ID タイプを選択します。
 - c. ID 文字列 (通常は、IP アドレスまたはドメイン名) を入力します。
 - d. [了解] を選択してデータを確定し、「IKE キーの追加/変更」ダイアログ・ボックスを閉じます。
16. IKE 交換のための事前共有鍵を選択します。
17. [次へ] を選択して「接続の追加/変更: IKE 認証」ダイアログ・ボックスを閉じ、「接続の追加/変更: オプションの IKE パラメータ」ダイアログ・ボックスを表示します。次の操作を実行します。
 - a. オプションのパラメータを選択します。
 - b. 初期 Diffie-Hellman 交換用の IKE グループ番号を選択します (IKE プロポーザルと異なる場合)。
 - c. PFS (Perfect Forward Secrecy) を使用している場合は、今後の Diffie-Hellman 交換用のグループ番号を選択します。
 - d. プロポーザルで存続期間を指定していない場合は、省略時の存続期間を選択します。
 - e. [Finish] を選択してデータを確定し、「接続の追加/変更: オプションの IKE パラメータ」ダイアログ・ボックスを閉じます。
18. 接続が作成されたことを通知するダイアログ・ボックスが表示されます。[了解] を選択してこのダイアログ・ボックスを閉じます。
19. 追加の公開鍵証明書を指定する必要がある場合は、「公開キーの証明」フィールドで [追加] を選択して、証明書の情報を入力する「証明の追加/変更」ダイアログ・ボックスを表示します。次の操作を実行します。
 - a. 証明書名を入力し、証明書のエンコード方式を選択し、証明書ファイルのローカル・パスを入力します。

- b. 証明書がシステムを認証する場合は、非公開鍵のエンコード方式を選択し、非公開鍵ファイルのローカル・パスを入力します。
- c. この証明書を他の証明書への署名に使用する場合は、[CA 証明] を選択します。それ以外の場合は、手順 f に進みます。
- d. CRL (Certificate Revocation List) が利用できない場合は、[証明取消リスト (CRL) がありません] を選択します。手順 f に進みます。
- e. CRL のエンコード方式を選択し、CRL ファイルのローカル・パスを入力します。
- f. [了解] を選択してデータを確定し、「証明の追加/変更」ダイアログ・ボックスを閉じます。

20. IPsec のメイン・ウィンドウで [了解] を選択して構成情報を保存します。IPsec がシステム上ですでに実行されているかどうかにかかわらず、「IPsec を再起動しますか?」ダイアログ・ボックスが表示されます。IPsec を起動または再起動する場合は [了解] を選択し、それ以外の場合は [いいえ] を選択します。[いいえ] を選択した場合は、IPsec を起動または再起動するためにはシステムをリブートしなければなりません。

相互運用に関する問題の解決方法については、4.5.2 項を参照してください。

4.7.2 セキュア・ゲートウェイの構成

ルータやゲートウェイに IPsec を構成する前に、システムが IP ルータとして構成されていることを確認してください。システムを IP ルータとして構成する方法についての詳細は、2.3.5 項を参照してください。

ルータやゲートウェイに IPsec を構成するには、次のように操作します。

1. SysMan Menu で [ネットワーク] [追加ネットワーク・サービス] [IPsec (Internet Protocol Security) の設定] を選択して、IPsec のメイン・ウィンドウを表示します。

または、コマンド行で次のコマンドを入力します。

```
# /usr/sbin/sysman ipsec
```

IPsec を初めて構成する場合は、情報ダイアログ・ボックスが表示され、IPsec を有効にする前にセキュア接続を定義するように通知されることがあります。セキュア接続を定義せずに IPsec を有効にすると、シ

システムに出入りするパケットはすべて破棄され、トラフィックが流れなくなります。 [了解] を選択します。

IPsec メイン・ウィンドウには、構成されたセキュア接続と構成された公開鍵証明書が表示されます。

2. ウィンドウの上部で [Enable IP Security (IPsec)] を選択します。
3. [追加] を選択します。「セキュア接続の追加/変更」ダイアログ・ボックスが表示されます。
4. 接続名を入力します。
5. [追加] を選択してリモート IP アドレス・セレクトアを追加します。「セレクトアの追加/変更」ダイアログ・ボックスが表示されます。次の操作を実行します。
 - a. セレクトアのタイプを選択します。
 - b. IP アドレス (単一のホストと通信している場合)、サブネット・アドレス (セキュア・ゲートウェイと通信している場合)、最初のアドレス (アドレス・レンジと通信している場合) を入力します。
 - c. IP サブネットを選択した場合は、サブネット・マスクのサイズを入力します。
 - d. アドレス・レンジを選択した場合は、最後のアドレスを入力します。
 - e. 照合する上位層プロトコルを選択します。特に指定しなければ、すべてのプロトコルが選択されます。
 - f. セレクトアを特定のポート番号に制限する場合は、照合するポート番号を入力します。特に指定しなければ、すべてのポート番号が選択されます。
 - g. [了解] を選択してデータを確定し、「セレクトアの追加/変更」ダイアログ・ボックスを閉じます。リモート・アドレスとローカル・アドレスの追加が終了したら、手順 7 に進みます。
6. [追加] を選択してローカル IP アドレス・セレクトアを追加します。手順 5a に進みます。
7. セレクトアに一致したパケットに適用するアクションを選択します。省略時のアクションは、IPsec 保護の適用です。

8. [次へ] を選択してデータを確定し、「セキュア接続の追加/変更」ダイアログ・ボックスを閉じます。「接続の追加/変更: IPsec プロポーザル」ダイアログ・ボックスが表示されます。次の操作を実行します。
 - a. プロポーザル・リストから IPsec プロポーザルを選択します。
 - b. セキュア・ゲートウェイまたはホストと通信する場合は、リモート・システムの IP アドレスとシステムの IP アドレス (ローカル) を指定します。
 - c. IKE を使用して鍵を取得するか、手動設定を使用するかを指定します。[次へ] を選択して、データを確定して「IPsec プロポーザル」ダイアログ・ボックスを閉じます。

手動設定を選択し、プロポーザルが 1 つだけのカスタム・プロポーザル・リストを作成した場合は、「接続の追加/変更: マニュアル・キー」ダイアログ・ボックスが表示されます。手順 9 に進んでください。IKE プロトコルを選択した場合は、「接続の追加/変更: IKE プロポーザル」ダイアログ・ボックスが表示されます。手順 11 に進んでください。
9. [追加] を選択して手動鍵を追加し、「マニュアル・キー: IPsec キーの追加/変更」ダイアログ・ボックスを表示します。次の操作を実行します。
 - a. 鍵名を入力します。
 - b. SPI (Security Parameter Index) を入力します。
 - c. 選択したプロポーザルに必要なアルゴリズムの鍵を入力します。

[了解] を選択してデータを確定し、「マニュアル・キー: IPsec キーの追加/変更」ダイアログ・ボックスを閉じます。
10. 受信パケット、送信パケット、その両方のパケット、のいずれに鍵を適用するかを選択します。追加の鍵を指定する場合は、手順 9 に進みます。手動鍵の指定を終了する場合は [Finish] を選択します。手順 18 に進みます。
11. プロポーザル・リストから IKE プロポーザルを選択します。[次へ] をクリックして、データを確定して「接続の追加/変更: IKE プロポーザル」ダイアログ・ボックスを閉じ、「接続の追加/変更: IKE 認証」ダイアログ・ボックスを表示します。

12. 公開鍵証明書または事前共有鍵で IKE 交換を認証するかどうかを選択します。
13. 公開鍵証明書を選択した場合は、[追加] を選択して IKE 証明書を追加します。「証明の追加/変更」ダイアログ・ボックスが表示されます。次の操作を実行します。
 - a. 証明書名を入力し、証明書のエンコード方式を選択し、証明書ファイルのローカル・パスを入力します。
 - b. 証明書がシステムを認証する場合は、エンコード方式を選択して、非公開鍵ファイルのローカル・パスを入力します。
 - c. この証明書を他の証明書への署名に使用する場合は、[CA 証明] を選択します。それ以外の場合は、手順 f に進みます。
 - d. CRL (Certificate Revocation List) が使用できない場合は、[証明取消リスト (CRL) がありません] を選択します。手順 f に進みます。
 - e. CRL のエンコード方式を選択して、CRL ファイルのローカル・パスを入力します。
 - f. [了解] を選択してデータを確定し、「証明の追加/変更」ダイアログ・ボックスを閉じます。
14. IKE 交換のための証明書を選択します。手順 17 に進みます。
15. 事前共有鍵を選択した場合は、[Add an IKE pre-shared key] を選択します。「IKE キーの追加/変更」ダイアログ・ボックスが表示されます。次の操作を実行します。
 - a. 鍵名と鍵の値を入力します。
 - b. ローカル ID タイプを選択します。
 - c. ID 文字列 (通常は、IP アドレスまたはドメイン名) を入力します。
 - d. [了解] を選択してデータを確定し、「IKE キーの追加/変更」ダイアログ・ボックスを閉じます。
16. IKE 交換のための事前共有鍵を選択します。

17. [次へ] を選択して「接続の追加/変更: IKE 認証」ダイアログ・ボックスを閉じ、「接続の追加/変更: オプションの IKE パラメータ」ダイアログ・ボックスを表示します。次の操作を実行します。
 - a. オプションのパラメータを選択します。
 - b. 初期 Diffie-Hellman 交換用の IKE グループ番号を選択します (IKE プロポーザルと異なる場合)。
 - c. PFS (Perfect Forward Secrecy) を使用している場合は、今後の Diffie-Hellman 交換用のグループ番号を選択します。
 - d. プロポーザルで存続期間を指定していない場合は、省略時の存続期間を選択します。
 - e. [Finish] を選択してデータを確定し、「接続の追加/変更: オプションの IKE パラメータ」ダイアログ・ボックスを閉じます。
18. 接続が作成されたことを通知するダイアログ・ボックスが表示されます。[了解] を選択してこのダイアログ・ボックスを閉じます。
19. 追加の公開鍵証明書を指定する必要がある場合は、「公開キーの証明」フィールドで [追加] を選択して、証明書の情報を入力する「証明の追加/変更」ダイアログ・ボックスを表示します。次の操作を実行します。
 - a. 証明書名を入力し、証明書のエンコード方式を選択し、証明書ファイルのローカル・パスを入力します。
 - b. 証明書がシステムを認証する場合は、非公開鍵のエンコード方式を選択し、非公開鍵ファイルのローカル・パスを入力します。
 - c. この証明書を他の証明書への署名に使用する場合は、[CA 証明] を選択します。それ以外の場合は、手順 f に進みます。
 - d. CRL (Certificate Revocation List) が利用できない場合は、[証明取消リスト (CRL) がありません] を選択します。手順 f に進みます。
 - e. CRL のエンコード方式を選択し、CRL ファイルのローカル・パスを入力します。
 - f. [了解] を選択してデータを確定し、「証明の追加/変更」ダイアログ・ボックスを閉じます。
20. IPsec のメイン・ウィンドウで [了解] を選択して構成情報を保存します。IPsec がシステム上ですでに実行されているかどうかにかかわら

ず、「IPsec を再起動しますか?」ダイアログ・ボックスが表示されます。IPsec を起動または再起動する場合は [了解] を選択し、それ以外の場合は [いいえ] を選択します。[いいえ] を選択した場合は、システムをリブートして IPsec を起動または再起動するか、または `ipsecd` デーモンを起動または再ロードします (4.8.1 項を参照)。

相互運用に関する問題の解決方法については、4.5.2 項を参照してください。

4.8 構成後の作業

SysMan アプリケーションを使用して IPsec を構成した後は、次の操作を行います。

- IPsec デーモンの管理 (4.8.1 項)
- SA のモニタリング (4.8.2 項)
- IPsec のモニタリング (4.8.3 項)

4.8.1 IPsec デーモンの管理

通常は、SysMan IPsec アプリケーションを使用して新しい接続を作成した場合や既存の接続を変更した場合に、IPsec と IPsec デーモン (`ipsecd`) を起動します。

SysMan から IPsec を起動すると、システムは IP セキュア・モードになります。このモードでは、システムは、誤って重要なデータを暗号化せずに送信してしまうよりも、IP トラフィックをすべてブロックする方が良いという原則で動作します。IP トラフィックをシステムに出入りさせるには、`ipsecd` デーモンが正しいポリシーで動作していなければなりません。最初に IPsec を構成してテストするときには、制限がきつくなりすぎることがあります。

システムの IP セキュア・モードを終了させるには、次のコマンドを入力します。

```
# /sbin/init.d/ipsec unsecure
```

新規接続の作成、または既存の接続の変更を行った後でも、IPsec デーモン (`ipsecd`) の起動、停止、再ロードはいつでも行えます。

SysMan から IPsec を有効にした後で `ipsecd` を起動するには、次のコマンドを入力します。

```
# /sbin/init.d/ipsec start
```

ipsecd を停止するには、次のコマンドを入力します。

```
# /sbin/init.d/ipsec stop
```

システムが IP セキュア・モードの場合、システムに出入りする IP トラフィックはなくなります。SysMan から IPsec 処理を無効にした場合、システムは「IP セキュア」モードから抜け出します。

ipsecd を再ロードするには、次のコマンドを入力します。

```
# /sbin/init.d/ipsec reload
```

これにより、ipsecd は強制的に SPD ファイルを再度読み取り、新しいセキュリティ・ポリシーを強制します。既存の SA は、構成された存続期間が満了するまで有効のままになります。

詳細は ipsecd(8) を参照してください。

4.8.2 セキュリティ・アソシエーションのモニタリング

IPsec のこの実装では、ipsecd デーモンは実行中に IPsec SA および IKE SA の情報を収集します。netstat コマンドを実行すると、IPsec と IKE SA の両方をモニタリングできます。

IPsec SA を (冗長モードで) モニタリングするには、次のコマンドを入力します。

```
# /usr/sbin/netstat -x -v
Current Inbound: AH: 0  ESP: 1  IPCOMP: 1
Current Outbound: AH: 0  ESP: 1  IPCOMP: 1
Total Inbound: AH: 0  ESP: 1  IPCOMP: 1
Total Outbound: AH: 0  ESP: 1  IPCOMP: 1

Type      Local / Remote Selector      SPI      Pkts  Errors
AuthErr  CiphErr  Replays  Algorithms
Lifetime (used/total)
ipc/tr/o 16.140.64.106
16.140.64.223
0 0 0 deflate
85/1800 seconds
esp/tr/o 16.140.64.106
16.140.64.223
0 0 0 3des-cbc/hmac-sha1-96
85/1800 seconds 5/204800 KB
ipc/tr/i 16.140.64.106
16.140.64.223
0 0 0 deflate
85/1800 seconds
esp/tr/i 16.140.64.106
16.140.64.223
0 0 0 3des-cbc/hmac-sha1-96
85/1800 seconds 7/204800 KB
```

この表示では、各接続に対して別々の入力および出力の SA があります。接続が AH と ESP の両方で保護されている場合、それぞれに SA があります。フィールドの説明は、次のとおりです。

Type	SA のタイプ。ah または esp, tn (トンネル) または tr (トランスポート), i (受信パケット) または o (送信パケット)。
Errors	暗号解読 (CiphErr), 認証 (AuthErr), リプレイ (Replays) チェックに失敗したパケットの数。
Algorithms	SA が使用する暗号化および HMAC アルゴリズム。
Lifetime	SA の存続期間。経過秒数 / ハード存続期間の秒数, および転送 K バイト数 / ハード存続期間の K バイトで表されます。

IKE SA を (冗長モードで) モニタリングするには、次のコマンドを入力します。

```
# /usr/sbin/netstat -X -v

Total Phase-1: 1   Failed Phase-1: 0
Total QM: 1   Failed QM: 0

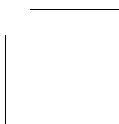
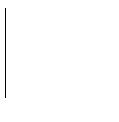
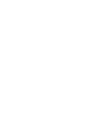
I/R Local / Remote Identifiers          Bytes
I  ipv4(16.140.64.106)                   756
   ipv4(16.140.64.223) (at 16.140.64.223:500)
   Pre-shared Keys / 3des-cbc / sha1 / hmac-sha1
   Created: Fri Nov 02 2001 10:15:40
   Used: Fri Nov 02 2001 10:15:41
   Expires: Fri Nov 02 2001 11:15:40
   I-Cookie: 0x575059dd31000000 R-Cookie: 0x1aa850255c000003
```

I/R は、ホストが Initiator (開始システム) と Responder (応答システム) のいずれであるかを示します。I または R の前にアスタリスク (*) がある場合、IKE 折衝が継続中です。Bytes は、SA を介して送られたデータのバイト数です。また、IKE 認証モード (暗号化、ハッシュ、HMAC アルゴリズム)、SA が作成された時刻、最終使用時刻、満了日時、Initiator および Responder のクッキーも表示されます。クッキーは、SPI に類似しており、このペアで IKE SA が一意に識別されます。

4.8.3 IPsec のモニタリング

`netstat` コマンドを使用して、IPsec カーネル・パケット処理エンジンをモニタリングすることもできます。IPsec がカーネルに構成されていれば、これらの統計情報を表示できます。表示するには、次のコマンドを入力します。

```
# netstat -p ipsec
ipsec:
    11992495 total packets processed by IPsec engine
    11990029 IP packets processed by IPsec engine
    0 AH headers processed
    26 ESP headers processed
    14 IPCOMP headers processed
    8 packets triggered an IKE action
    2477 packets dropped by IPsec
    11987544 packets passed through by IPsec
```



Mobile IPv6

IPv6 (Internet Protocol Version 6) は、拡張可能なヘッダ構造、アドレスの自動構成、セキュリティ (IPsec)、トンネリングなどの機能を通じて移動性 (mobility) をサポートするように設計されています。Mobile IPv6 はこれらの機能の上に構築され、モバイル・ノードが、ノードの IP アドレスを変更することなしにリンク間を移動できるようにする動作を定義しています。このようにして、モバイル・ノードが他のネットワークに移動しても、透過的にモバイル・ノードとの間でパケットのルーティングができます。

Mobile IPv6 の実装には、次のような制限があります。

- TruCluster システムではサポートされていません。
- IETF Internet Draft for *Mobility Support in IPv6* (draft-ietf-mobileip-ipv6-15.txt) のセクション 4.4 で規定されているように Binding Update 認証はサポートしていません。これには、セクション 5.6 で定義されている Authentication Data Sub-option も含まれます。このため、この実装の使用は、攻撃を受けるおそれのないテスト環境に限定されます。これは、認証されていないバインドを受け入れて、システムの統一性が失われる可能性があるためです。

この章の内容は次のとおりです。

- Mobile IPv6 の経緯 (5.1 節)
- Mobile IPv6 の環境 (5.2 節)
- Mobile IPv6 の動作 (5.3 節)
- Mobile IPv6 の準備 (5.4 節)
- Mobile IPv6 の構成 (5.5 節)
- Mobile IPv6 環境のモニタリング (5.6 節)

問題解決については、10.4 節を参照してください。

5.1 Mobile IPv6 の経緯

通信の分野では、移動性の強化がトレンドになっています。携帯電話はすでに、ビジネスや個人の通信形態を変革しています。コンピュータ、特にラップトップ・コンピュータやハンドヘルド・コンピュータも移動性を備えていますが、これらはまだ携帯電話のような連続的な接続性は備えていません。

今日では、WAP (Wireless Application Protocol) や GPRS (General Packet Radio Service) を使用する基本的なデータ・サービスがあります。しかし、次のようなトレンドによって、声とデータをフルに利用できるモバイル通信の要求が生まれています。

- 3G (第 3 世代) ネットワークの開発
- ビデオ、音声、画像など、大容量でさまざまなタイプのコンテンツのインターネット上での利用
- ワイヤレス契約者とインターネット・ユーザの増大
- 音声およびデータの機能を備えた集合型デバイスの開発

5.2 Mobile IPv6 の環境

Mobile IPv6 環境では、ノードには次のような役割があります。

モバイル・ノード

取り付け位置をリンク間で変更することができ、変更後もホーム・アドレスから到達できる IPv6 ノード (ホストまたはルータ)。

コレスポンデント・ノード

モバイル・ノードと通信するピア IPv6 ノード。コレスポンデント・ノード (ホストまたはルータ) は、モバイル・ノードでも静止ノードでもかまいません。Mobile IPv6 の Tru64 UNIX 実装を使用すると、システムをコレスポンデント・ノードにすることができます。

ホーム・エージェント

モバイル・ノードが現在の気付アドレス (care-of address) を登録する、モバイル・ノードのホーム・リンク上にあるルータ。

これらのノードの相互関連を理解するには、次の用語に関する理解が必要です。

ホーム・アドレス

モバイル・ノードがホーム・リンク上またはホーム位置にある場合の、モバイル・ノードの IPv6 アドレス。このアドレスのサブネット・プレフィックスはホーム・ネットワークのサブネット・プレフィックスになります。モバイル・ノードは、常にホーム・アドレスで参照できます。ホーム・アドレスは変わりません。

気付アドレス (care-of address)

モバイル・ノードが外部リンクまたはホーム以外の位置にある場合の IPv6 アドレス。このアドレスのサブネット・プレフィックスは外部ネットワークのサブネット・プレフィックスになります。モバイル・ノードには複数の気付アドレスが設定できますが、モバイル・ノードのホーム・エージェントに登録した気付アドレスは、1 次気付アドレスと呼ばれます。

バインディング

モバイル・ノードのホーム・アドレスと気付アドレスの対応付け。この対応付には存続期間もあります。各ノードは全バインディングのキャッシュを維持します。バインディング・キャッシュの内容を表示する方法については、11.4 節を参照してください。

5.3 Mobile IPv6 の動作

図 5-1、図 5-2、図 5-3 では、コレスポンデント・ノード、ホーム・エージェント、モバイル・ノードの間の相互作用を 3 種類のシナリオで図示しています。

図 5-1 では、モバイル・ノードはホーム・リンク上にあります。これは定位置と考えられます。コレスポンデント・ノードからモバイル・ノードのホーム・アドレスに送られたパケットは、一般的な IP ルーティング・メカニズムによって配信されます。

図 5-1: ホーム位置にあるモバイル・ノードとの通信
外部ネットワーク

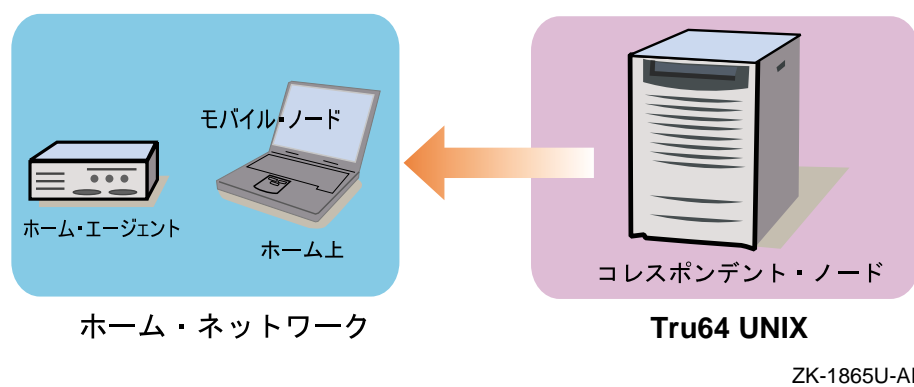
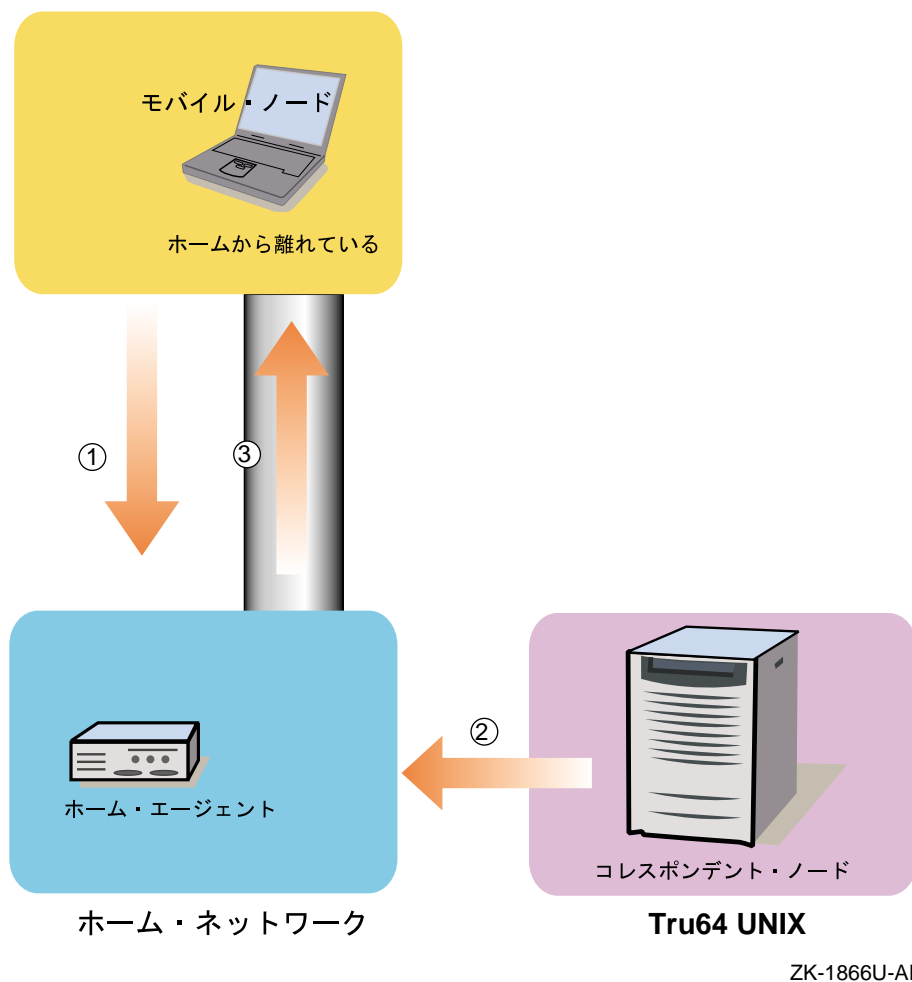


図 5-2 では、モバイル・ノードは外部リンクに移動しています。ノードは、現在ホームから離れていると見なされます。

図 5-2: ホームから離れているモバイル・ノードとの通信 – その 1
外部ネットワーク



外部リンクでは、次のようなイベントが発生します。

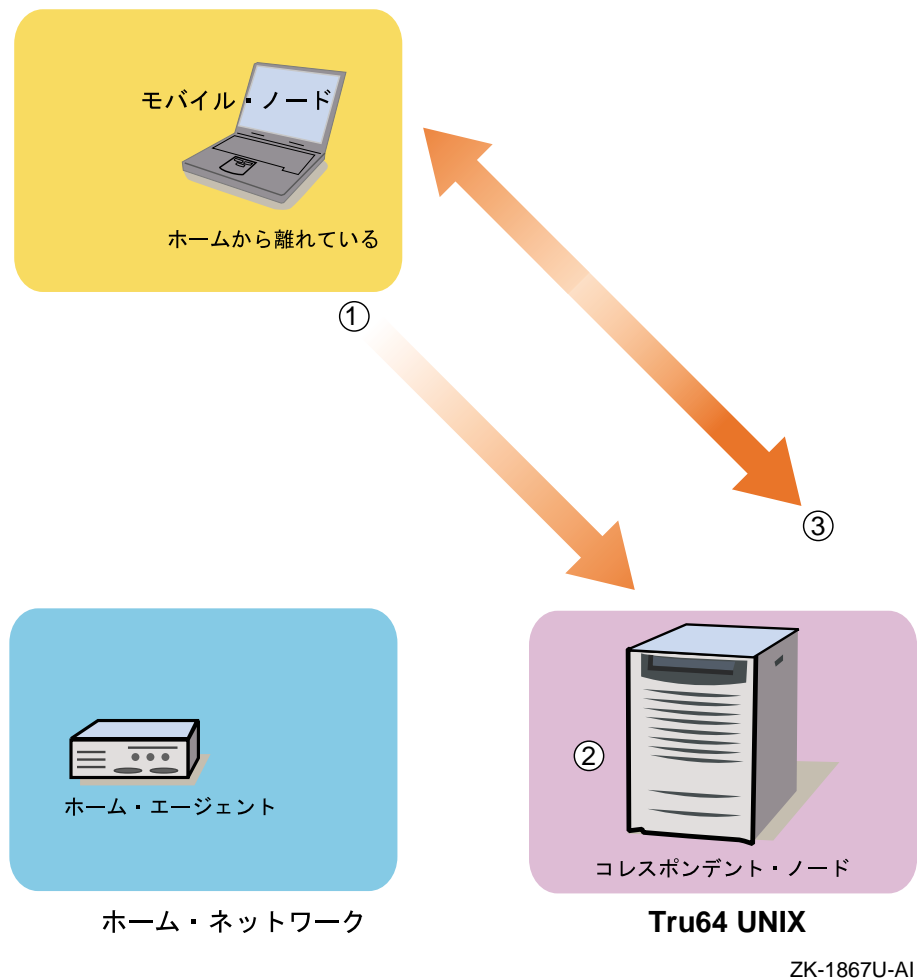
- ① モバイル・ノードは気付アドレスを構成し、ホーム・エージェントに Binding Update を送信することで、そのアドレスをホーム・エージェントに登録します。この新しいアドレスが、モバイル・ノードの 1 次気付アドレスになります。

ホーム・エージェントは、モバイル・ノードに Binding Acknowledgement を返すことで、Binding Update に対して肯定応答を行います。

- ② コレスポネント・ノードからモバイル・ノードのホーム・アドレスに送られたパケットは、ホーム・リンクに到達します。
- ③ ホーム・エージェントはパケットを横取りし、それをカプセル化し、モバイル・ノードの登録気付アドレスへのトンネル処理を行います。

図 5-3 では、モバイル・ノードはトンネル処理されたパケットをホーム・エージェントから受信します。

図 5-3: ホームから離れているモバイル・ノードとの通信 – その 2
外部ネットワーク



トンネリングされたパケットをモバイル・ノードが受信した後に、次のようなイベントが発生します。

- ① モバイル・ノードは、トンネリングされたパケットのヘッダで、1 次気付アドレスを認識します。モバイル・ノードはオリジナルの送信側コレスポンデント・ノードに、モバイル・ノードのバインディング・キャッシュのエントリがないと見なします。エントリがあれば、コレスポンデント・ノードはルーティング・ヘッダを使用してモバイル・ノードにパケットを直接送信していたはずですが、次に、Binding Update をコレスポンデント・ノードに送信します。
- ② コレスポンデント・ノードは、ホーム・アドレスと気付アドレスの間にバインディングを作成します。
- ③ パケットは、コレスポンデント・ノードとモバイル・ノードの間を直接流れます。このような、ルートの最適化には次のような効果があります。
 - ・ 一般に、三角ルーティングと呼ばれるルーティングの排除。
 - ・ モバイル・ノードのホーム・エージェントとホーム・リンクでの輻輳の排除。
 - ・ ホーム・エージェント、ホーム・リンク、ホーム・リンクにつながる中間のネットワークで障害が発生した場合の影響の削減。これは、これらのノードおよびリンクが、モバイル・ノードへのパケット配信にほとんど関与していないためです。

モバイル・ノードがホームから離れている場合、モバイル・ノードは必ずホーム・アドレス・オプションを送信して、受信側に自分のホーム・アドレスを通知します。このようにして、受信側はそのパケットが所属する接続を正確に識別できるようになります。

モバイル・ノードがホーム・リンクに戻ると、モバイル・ノードはホーム・エージェントとコレスポンデント・ノードに Binding Update を送信し、バインディングをクリアします。

5.4 Mobile IPv6 の準備

ここでは、Mobile IPv6 を構成する前に必要な作業について説明します。

また、システムを PIPv6 ホスト・ノードまたはルータとして構成する必要があります。詳細は 3.7 節 を参照してください。

5.4.1 カーネルでの IPv6 サポートの確認

Mobile IPv6 サポートは、IPv6 サブセットの一部として含まれています。次のコマンドを入力して、IPv6 サブセットがインストールされていることを確認します。

```
# sysconfig -q ipv6
```

ipv6: サブシステム属性が表示されない場合は、3.6.1 項 で述べた手順に従って IPV6 オプションの選択とインストールを行います。サブセットのインストールについての詳細は、setld(8)、『インストール・ガイド』、『システム管理ガイド』を参照してください。

5.4.2 カーネルでの Mobile IPv6 サポートの確認

次のコマンドを入力して、Mobile IPv6 サポートがカーネルに構成されていることを確認します。

```
# sysconfig -q ipv6 mobileipv6_enabled
```

mobileipv6_enabled 属性が定義されていない場合、カーネルに Mobile IPv6 は構成されていません。正しいカーネルを実行しているか確認してください。正しいカーネルを実行している場合は、doconfig コマンドでカーネルを再構成します。詳細は 3.6.1 項 を参照してください。

mobileipv6_enabled が定義されていても 1 が設定されていない場合は、次のコマンドで再構成します。

```
# sysconfig -r ipv6 mobileipv6_enabled=1
mobileipv6_enabled: reconfigured
```

これで、システムはコレスポンデント・ノードとして動作できるようになります。コレスポンデント・ノードはルータとしてパケットを転送することもできます。システムをルータとしても使用する場合は、5.5 節 を参照してください。

5.5 Mobile IPv6 の構成

ここでは、IPv6 ノードをコレスポンデント・ノードとして構成する方法、および IPv6 ルータとして動作するコレスポンデント・ノードとして構成する方法を説明します。

5.5.1 コレスポンデント・ノードの構成

カーネルに IPv6 サポートが組み込まれていることが確認できれば、システムはコレスポンデント・ノードとして機能し、ホーム・エージェントを通してモバイル・ノードと通信できるようになり、Binding Update をモバイル・ノードから受信した後は、モバイル・ノードと直接通信できるようになります。これ以上の構成は不要です。

IPv6 インストール後の作業については、3.8 節を参照してください。

5.5.2 コレスポンデント・ノードおよびルータの構成

コレスポンデント・ノードを IPv6 ルータとしても動作させる場合は、次の手順で操作します。

1. システムを IPv6 ルータとして構成します。詳細は 3.7.2 項を参照してください。
2. システムのブート時に、ip6rtrd デーモンが Mobile IPv6 環境で機能するようにします。まず、次のコマンドを実行してデーモンのフラグを取得します。

```
# rcmgr get IP6RTRD_FLAGS
```

次に、`-m` オプションをフラグに追加します。直前のコマンドでフラグが表示されなかった場合は、次のコマンドでフラグに `-m` オプションを追加します。

```
# rcmgr set IP6RTRD_FLAGS "-m"
```

3. `/etc/ip6rtrd.conf` ファイルを編集して、Router Advertisement の間隔を次のように変更します。

```
#
# Sample ip6rtrd configuration file
#
interface interface-name {
    MinRtrAdvInterval 0 /* Min = seconds */
    MinRtrAdvIntervalMsec 500 /* + milliseconds */
    MaxRtrAdvInterval 1 /* Max = seconds */
    MaxRtrAdvIntervalMsec 500 /* + milliseconds */
}
```

これにより、IPv6 ルータは要求によらないマルチキャストの Router Advertisement を 0.5 ~ 1.5 秒おきに送信し、モバイル・ノードの移動を早く検出できるようにします。詳細は `ip6rtrd.conf(4)` を参照してください。

4. 次のコマンドで IPv6 を再起動します。

```
# /usr/sbin/rcinet restart inet6
```

IPv6 インストール後の作業については、3.8 節を参照してください。

5.6 Mobile IPv6 環境のモニタリング

Mobile IP 環境をモニタリングするには、次のものを使用します。

- `tcpdump` コマンド
- `netstat` コマンド
- IPv6 デーモンのログ・ファイル

5.6.1 tcpdump の使用

`tcpdump` ユーティリティは、IPv6 パケットの取り込み、解析、出力を行います。Binding Update および Acknowledgement オプションは、IPv6 パケットの IPv6 Destination Option ヘッダに含まれています。`tcpdump` を使用するには、カーネルに PACKETFILTER オプションを構成する必要があります。詳細は `packetfilter(8)` を参照してください。

可能なパケットをすべて表示するには、インタフェースを Promiscuous および Copyall モードに構成してから、次のように `tcpdump` コマンドを実行します。

```
# pfconfig +p +c interface
# tcpdump -i interface -s 1500 [-x] [ipv6]
```

詳細は `tcpdump(8)` を参照してください。

5.6.2 netstat の使用

`netstat -b` コマンドを使用すると、現在の移動バインディングとその属性がモニタリングできます。コマンドの出力例を次に示します。

```
# netstat -b
```

```
Mobile IPv6 Binding Cache
```


Home Address	Care-of Address	Flags	Refs	Sequence#	Lifetime
testhome	testcoa	A	1	1	43
1	2	3	4	5	6

上記の例では、次のことがわかります。

- 1** モバイル・ノードは、ホーム・アドレス testhome を持っています。
- 2** 現在、気付アドレス testcoa に到達できます。
- 3** Binding Update に対して肯定応答を行うように要求しました (A フラグ)。
- 4** このバインディング・データ構造には、現在 1 つの参照があります。
- 5** Binding Update でシーケンス番号に 1 を設定しています。
- 6** このバインディングの存続期間は 43 秒残っています。存続期間が満了すると、エントリはキャッシュから削除されます。

netstat -bs コマンドを使用すると、移動バインディングに関する統計情報がモニタリングできます。コマンドの出力例を次に示します。

```
# netstat -bs
Mobile IPv6:
  1 entry in binding cache
  1 add
  0 deletes
  0 changes
  0 frees
  3 lookups
```

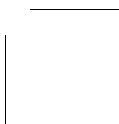
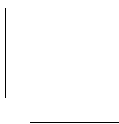
詳細は 11.4 節 および netstat(1) を参照してください。

5.6.3 IPv6 デーモンのログ・ファイル

ip6rtrd デーモンは、情報イベントと重要なイベントを /var/adm/syslog.dated/date/daemon.log ファイルに記録します。詳細は 11.9 節 を参照してください。

ip6rtrd デーモンのデバッグ情報のロギングを有効にするには、次のコマンドを実行します。

```
# rcmgr set IP6RTRD_FLAGS "-d -l -m /usr/tmp/ip6rtrd.log"
# /usr/sbin/rcinet restart inet6
```



ATM (非同期転送モード) ネットワークには、次のような機能があります。

- セル・スイッチングによる 25 M/bps ~ 622 M/bps , あるいはそれ以上の伝送スピード
- 豊富な高品質のサービス
- 個々の接続についてリソースが予約された , コネクション型相互接続。これらの接続は , 2 つのアプリケーション間の対話 , または多くのアプリケーションおよびプロトコル間の多くの対話が多重化されている接続に適しています。

ATM ネットワークにより , 特にローカル・エリア・ネットワークで実行されるアプリケーションで必要とされる高速で短い待ち時間 (交換方式の全二重ネットワーク基盤) が実現されます。

この章では、次の項目について説明しています。

- ATM ネットワーク環境 (6.1 節)
- ATM 構成の準備 (6.2 節)
- ATM サブシステムの構成方法 (6.3 節)
- ATM サブシステムの管理方法 (6.4 節)

ATM 用のデバイス・ドライバおよびカーネル・モジュールの作成方法については、『*Asynchronous Transfer Mode*』を参照してください。問題解決のための情報は、10.6 節を参照してください。

6.1 ATM 環境

ATM ネットワークは、次の要素から構成されています。

- スイッチ
仮想チャネル識別子 (VCI) および仮想パス識別子 (VPI) のリストを保持しており、1 つのエンド・システムを別のシステムに接続し、

ATM セルをセル内に含まれる VCI/VPI 情報に基づいて、1 つのエンド・システムから別のシステムへの転送すなわち交換 (スイッチ) を行う特別なシステム。

- エンド・システム

スイッチに物理的に接続されていて、スイッチを経由して他のエンド・システムと通信するシステム。

オペレーティング・システムの ATM 環境では、次の構成が可能です。

- CLIP (Classical Internet Protocol)
- LANE (Local Area Network Emulation)
- IP スイッチング

以下の各項では、これらの構成のそれぞれについて、およびそれぞれの構成におけるシステムの役割について説明します。

6.1.1 Classical IP 環境

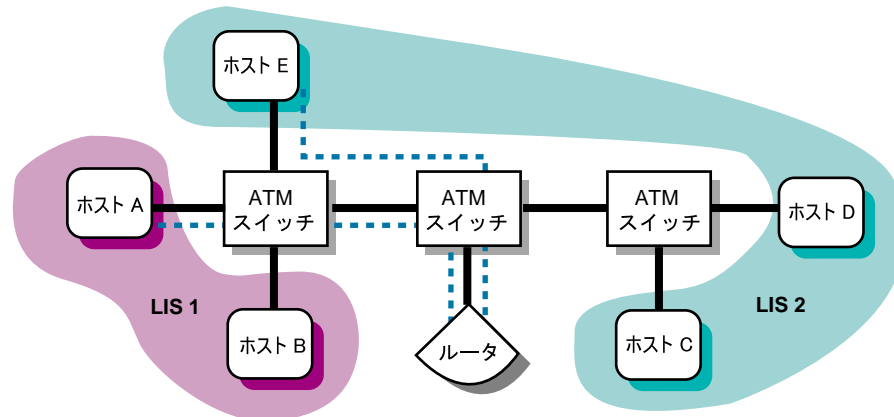
Classical IP 環境は、RFC 1577 で説明されているように、ユニキャスト IP トラフィックを ATM ネットワークで伝送する手段を提供します。この環境では、相互に通信できるホストは LIS (Logical IP Subnetwork) として分類されます。1 つの ATM ネットワークには、複数の LIS が含まれることがあります。1 つの LIS では、すべてのホストおよびルータについて、次の必要条件があります。

- 同じ IP ネットワーク番号や IP サブネットワーク番号とマスクを持っていること。
- ATM ネットワークに直接接続されていること。
- LIS 以外のメンバにはルータを経由してアクセスすること。
- 交換仮想回線 (SVC) では、ARP (Address Resolution Protocol) を使用して、IP プロトコル・アドレスから ATM ハードウェア・アドレスを取得すること。SVC およびパーマネント仮想サーキット (PVC) では、逆 ARP を使用して ATM ハードウェア・アドレスから IP プロトコル・アドレスを取得すること。
- 同一 LIS 内の他のメンバと通信できること (メッシュ・トポロジ)。

図 6-1 は、2 つの LIS を持つ ATM ネットワークを示しています。ホスト A および B は LIS 1 のメンバであり、ホスト C、ホスト D、およびホスト E

は、LIS 2 のメンバです。この図では、ホスト A とルータ間およびホスト E とルータ間の仮想回路 (VC) も示しています。これらのホストは同じスイッチに接続されているため、相互通信を実行する VC を確立しているように見えますが、別の LIS 内のメンバとの通信はすべてルータを経由しなければならないため、VC を確立することはできません。

図 6-1: ATM ネットワークでの Classical IP



ZK-1307U-AI

6.1.2 LAN Emulation 環境

LANE (LAN Emulation) 環境では、ATM Forum で定義されているように、複数のホストがエミュレート LAN (ELAN) と呼ばれる 1 つのエンティティにグループ化されます。LANE 環境には、次のような特徴があります。

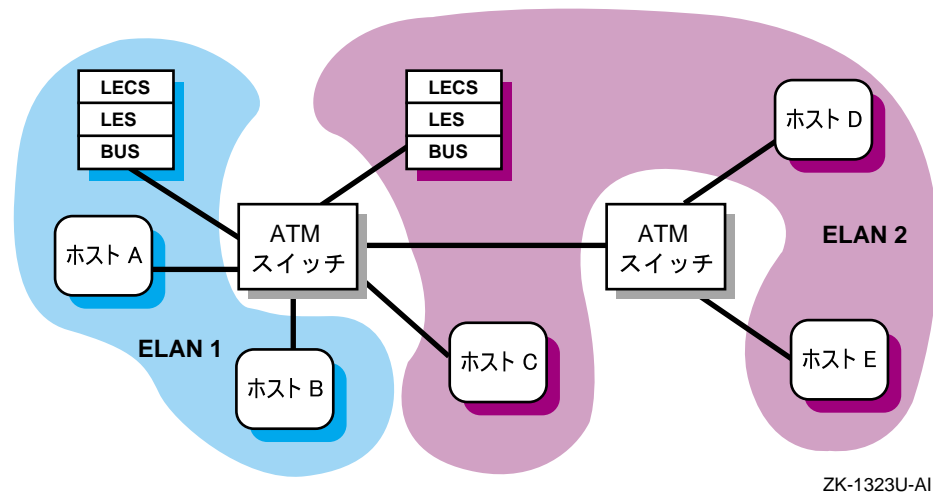
- 48 ビットのメディア・アクセス制御 (MAC) アドレスでホストを識別します。
- Classical IP 環境とは異なり、ポイント・ツー・ポイント接続またはマルチキャスト・サーバのいずれかを通じて、マルチキャストおよびブロードキャスト・サービスをサポートします。
- IEEE ブロードキャスト LAN を使用する任意のプロトコルをサポートします。

さらに、LANE インタフェース (elan) が、NetRAIN によってサポートされています。詳細については、nr(7) を参照してください。

図 6-2 は、2 つのエミュレート LAN を含む ATM ネットワークを示しています。ホスト A およびホスト B は、ELAN 上の LEC (LAN Emulation

Clients) です。ホスト C、ホスト D、およびホスト E は、ELAN 2 上の LEC です。LECS (LAN Emulation Configuration Server)、LES (LAN Emulation Server)、および BUS (Broadcast and Utility Server) のサーバ機能は通常 ATM スイッチ上に常駐しますが、2 つの異なるシステムとして表現されます。

図 6-2: ATM ネットワークでのエミュレート LAN



6.1.3 IP スイッチング

注意

IP スイッチングをサポートしているのは、旧バージョンとの互換性を維持するためだけであり、将来のリリースではサポートされなくなる予定です。新しいアプリケーションの開発では、この機能は使用しないでください。

IP スイッチング環境は、1 つの IP スイッチに接続された 1 つ以上のホストから構成されます。各ホストは、それぞれの物理接続が異なるサブネットとなるポイント・ツー・ポイント物理接続によって IP スイッチに接続されます。ホストと IP スイッチ間の通信は、動的に作成された PVC 上で実行されます。

IP スイッチは、IP ルーティングや IP トラフィックのクラス分けの機能を実行する IP コントローラ・ソフトウェアが追加された、典型的な ATM スイッチです。この環境では、1 つのホストから別のホストに転送される、同一の

プロトコル・タイプおよびサービスのタイプを持ち、パケット・ヘッダに示されているその他の特性が同一である一連のパケットは、フローと呼ばれます。長く遅延されているフローを IP コントローラが検出すると、ATM スイッチに対して適切なハードウェア接続を確立し、IP コントローラを迂回して ATM セルをデスティネーションに直接転送します。これにより、そのスイッチおよびネットワーク全体のスループットが向上します。

このオペレーティング・システムの IP スイッチングの実装は、Ipsilon Networks 社の参照モデルに基づいており、次のような特性があります。

- IP だけをサポートします。
- マルチキャスト・サービスおよびブロードキャスト・サービスをサポートします。
- システムが ARP サーバまたはマルチキャスト・サーバとして機能する必要がありません。
- IFMP (Ipsilon Flow Management Protocol) を使用して、制御情報を IP スイッチと交換します。
- ATM Forum シグナリング (options UNI3X) がシステム上に構成されている必要がありません。
- 必要とされる構成手順が Classical IP および LAN Emulation より少なく済みます。

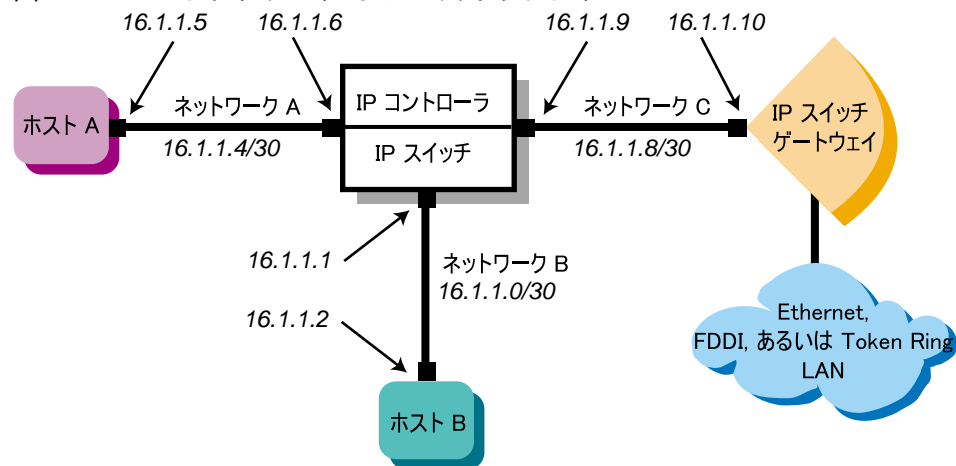
ATM での IP スイッチングには、次のような制限事項があります。

- 1 つのホスト当たり 1 つの IP スイッチング・インタフェース (ips) だけがサポートされています。
- IP スイッチング用のドライバを使用した場合、そのドライバでは他の ATM プロトコルは使用できません。
- tcpdump および packetfilter ユーティリティは、ips インタフェースではサポートされていません。

図 6-3 は、IP スイッチ、IP スイッチ・ゲートウェイ、いくつかのホスト、および従来型の LAN ネットワークを持つ、単純な ATM ネットワークを示しています。ホスト A (16.1.1.5)、ホスト B (16.1.1.2)、および IP スイッチ・ゲートウェイ (16.1.1.10) は、それぞれ異なるサブネット上 (16.1.1.4/30, 16.1.1.0/30, 16.1.1.8/30) にあります。IP スイッチ・ゲートウェイはルー

ティング・プロトコルを実行し、他のサブネットへのルートを従来型の LAN 上のホストに通知します。

図 6-3: ATM ネットワークでの IP スイッチング



ZK-1305U-AI

IP スイッチング・サブネットワークで推奨されるネットワーク・マスク長は、30 ビットです。このようにすると、各ホスト・アドレスに対し、サブネットワーク・アドレスに 1 ビット、ブロードキャスト・アドレスに 1 ビットの合計 2 ビットを使用することができます。サイズの大きなネットマスクを使用することにより、接続されるホストが少ないサブネットワーク上の IP アドレス空間を節約することができます。

6.2 ATM の計画

この節では、ATM ソフトウェアを構成する前に完了する必要がある作業について説明します。

6.2.1 ATM サブセットがインストールされていることの確認

次のコマンドを入力して、ATM サブセットがインストールされていることを確認します。

```
# setld -i | grep ATM
```

すべてのサブセットがインストールされていない場合には、setld コマンドを使用してそれらのサブセットをインストールします。サブセットのイ

ンストレーションについての詳細は、setld(8) または『インストール・ガイド』を参照してください。

注意

OSFATMBINOBJECT サブセットをインストールする必要はありません。

6.2.2 ATM のカーネルへの構成

ATM サブセットをインストールした後、次のコマンドを実行して、必要な ATM サポートがカーネル内にあることを確認します。

```
# sysconfig -q atm
```

atm: が表示されない場合は、スーパーユーザとしてログインし、次の手順を実行します。

1. doconfig コマンドを実行して、新しいカーネルを作成します。カーネルの再作成についてよくわからない場合には、『システム管理ガイド』を参照してください。
2. プロンプトが表示されたら、表 6-1 で説明されているカーネル・オプションを 1 つ以上選択します。

注意

ATM ハードウェアがすでにインストールされている場合は、options ATM が必須オプションとして自動的に選択されます。

3. 次のコマンドを実行し、新しいカーネルを使用してシステムをリブートします。

```
# shutdown -r now
```

このコマンドにより、システムは直ちにシャットダウンされ、自動的にリブートされます。

表 6-1: ATM カーネル・オプション

オプション	目的
options ATM	基本 ATM サポート (必須)
options UNI3X	LANE または Classical IP による ATM Forum シグナリング
options ATMILMI3X	ATM Forum ILMI (Integrated Layer Management) サポート
options ATMIP	Classical IP サービス
options LANE	ATM Forum LANE (LAN Emulation)
options ATMIFMP	IP スイッチング

6.2.3 構成の準備

ATM サポートがカーネル内にあることを確認できれば、ATM を構成できます。ATM を構成するには、ATM アダプタと、次の 1 つ以上のインタフェースを構成する必要があります。

- Classical IP 論理インタフェース
- LAN Emulation 論理インタフェース
- IP スイッチング論理インタフェース

必要な情報は、設定して使用しようとしている環境によって異なります。

6.2.3.1 アダプタに関する情報

図 6-4 は、ATM セットアップ・ワークシートです。以下の各項では、このワークシートに記録する必要がある情報について説明します。本書をオンラインで参照している場合は、印刷機能を使用して、このワークシートのコピーを印刷することができます。

図 6-4: ATM 設定ワークシート

ATM 設定ワークシート			
アダプタ名:	_____	_____	_____
ROM ESIs:	_____	_____	_____
追加ESIs:	_____	_____	_____
ネットワーク・レイヤ:	<input type="checkbox"/> SONET	<input type="checkbox"/> SDH	
フロー制御:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
ILMI:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
シグナリング:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
VCアカウンティング:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
UNIバージョン:	<input type="checkbox"/> 3.0	<input type="checkbox"/> 3.1	

アダプタ名

ATM ネットワーク・インタフェースのデバイス名。lta ネットワーク・インタフェースなど。

ROM ESI

システムおよびローカル・スイッチに登録しようとしているアダプタの、ROM エンド・システム識別子 (ESI) アドレス。すべてのアダプタの ROM ESI アドレスを登録するには、このフィールドを空白のままにしておきます。

スイッチによって割り当てられたアドレス・プレフィックスの数によっては、1 つまたはそれ以上の ATM アドレスを作成することができます。ドライバは最高 64 の ROM ESI アドレスを管理することができますが、一般的にアダプタの ROM ESI アドレスはごくわずかです。

追加 ESI

システムおよびローカル・スイッチに登録しようとしている追加の ESI アドレス。1 つの ESI アドレスには、12 桁の 16 進数が含まれています。

ネットワーク・レイヤ

SONET (Synchronous Optical Network) をアダプタで使用可能にする場合は、「SONET」をチェックします。SDH (Synchronous Digital Hierarchy) モードを、SONET および SDH 物理インタフェースの両方をサポートする ATM アダプタで使用可能にする場合は、「SDH」をチェックします。

フロー制御

アダプタでのベンダ固有のフロー制御を使用可能にする場合は、「Yes」をチェックします。それ以外の場合には、「No」をチェックします。アダプタは、このタイプのフロー制御をサポートしていなければなりません。Compaqのアダプタおよびスイッチは、FLOWmasterベンダ・フロー制御をサポートしています。

ILMI

ILMI (Integrated Layer Management Interface) をアダプタで使用可能にする場合は、「Yes」をチェックします。それ以外の場合には、「No」をチェックします。Classical IP を交換仮想回線 (SVC) で使用するには、ILMI を使用可能にしておかなければなりません。

シグナリング

アダプタでのシグナリングを使用可能にする場合は、「Yes」をチェックします。それ以外の場合には、「No」をチェックします。Classical IP を SVC で使用する場合は、SVC を使用可能にしておかなければなりません。

VC アカウンティング (シグナリングのみ)

仮想回路 (VC) リリースのロギングを使用可能にする場合は、「Yes」をチェックします。それ以外の場合には、「No」をチェックします。

UNI バージョン (シグナリングのみ)

アダプタで使用するシグナリングのバージョン。UNI (User-Network Interface) V3.0 を使用する場合は、「3.0」をチェックします。UNI V3.1 を使用する場合は、「3.1」をチェックします。省略時の値は 3.0 です。

6.2.3.2 Classical IP に関する情報

図 6-5 は、ATM Classical IP ワークシートです。以下の各項では、このワークシートに記録する必要のある情報について説明します。本書をオンラインで参照している場合は、印刷機能を使用して、このワークシートのコピーを印刷してください。

図 6-5: ATM クラシカル IP ワークシート

ATM クラシカル IP ワークシート			
ATM ホスト・ファイル			
ATM アドレス:	ホスト名:	別名:	
_____	_____	_____	
_____	_____	_____	
_____	_____	_____	
_____	_____	_____	
_____	_____	_____	
LIS			
LIS 番号: _____			
ARP			
ARP: <input type="checkbox"/> クライアント <input type="checkbox"/> サーバ			
ATMアドレス: _____			
IPアドレス: _____			
PVC			
VCI: _____			
VPI: _____			
リモート・クラシカルIP: <input type="checkbox"/> Yes <input type="checkbox"/> No			
リモートIPアドレス: _____			

ATM アドレス

/etc/atmhosts ファイルに追加する, ATM ネットワーク上の ATM ARP サーバの ATM アドレス。

ホスト名

/etc/atmhosts ファイルに追加する, ATM ネットワーク上の ATM ARP サーバの名前。

別名

/etc/atmhosts ファイルに追加する, ATM ARP サーバの別名。

LIS 番号

論理 IP サブネット (LIS) のインタフェース番号。1 つの ATM ドライバに複数の LIS インタフェースを作成することができます。

ARP

システムが ARP サーバとして機能するようにする場合は、「サーバ」をチェックします。それ以外の場合には、「クライアント」をチェックします。

ATM アドレス (ARP クライアントのみ)

ATM ARP サーバの ATM アドレスであり、`/etc/atmhosts` ファイルに表示されるホスト名または別名、あるいはセクタ・バイト付きの 40 桁の AESA (ATM End System Address)。また、ARP サーバは、ATM ネットワークに接続されていなければなりません。

注意

ATM Forum では、NSAP スタイルのアドレスを AESA と呼んでいます。

IP アドレス (ARP クライアントのみ)

ATM ARP サーバ・マシンの IP アドレス。

VCI (PVC のみ)

PVC の仮想チャネル識別子 (VCI)。

VPI (PVC のみ)

PVC の仮想パス識別子 (VPI)。

リモート・クラシカル IP (PVC のみ)

リモート・ホストがクラシカル IP を RFC 1577 の定義に従ってサポートしている場合には、「Yes」をチェックします。それ以外の場合には、「No」をチェックします。

リモート IP アドレス (PVC のみ)

リモート・ホストがクラシカル IP をサポートしていない場合には、そのリモート・ホストの IP アドレスを入力します。

6.2.3.3 LAN エミュレーションに関する情報

図 6-6 は、ATM LAN Emulation ワークシートです。以下の各項では、このワークシートに記録する必要がある情報について説明します。本書をオンラインで参照している場合は、印刷機能を使用して、このワークシートのコピーを印刷することができます。

図 6-6: ATM LAN エミュレーション・ワークシート

ATM LAN エミュレーション・ワークシート		
ATM ホスト・ファイル		
ATM アドレス:	ホスト名:	別名:
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
LANE		
ELAN 番号: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>		
ELAN 名: <input type="text"/>		
モード: <input type="checkbox"/> 省略時の LECS <input type="checkbox"/> 指定 LECS <input type="checkbox"/> LES		
LECS 名: <input type="text"/>		
LES 名: <input type="text"/>		
MTU サイズ: <input type="checkbox"/> 1516 <input type="checkbox"/> 4544 <input type="checkbox"/> 9234 <input type="checkbox"/> 8190		

ATM アドレス

/etc/atmhosts ファイルに追加する、ATM ネットワーク上の LES (LAN Emulation Server) の ATM アドレス。

ホスト名

`/etc/atmhosts` ファイルに追加する、ATM ネットワーク上の LES の名前。

別名

`/etc/atmhosts` ファイルに追加する LES の別名があれば、その名前。

ELAN 番号

LEC (LAN Emulation Client) インタフェース・ユニット番号。

ELAN 名

結合するエミュレート LAN の名前。これはオプションです。エミュレート LAN 名は、すでに ATM スイッチ上で構成されたものでなければなりません。エミュレート LAN 名が ATM スイッチ上で構成されない場合には、LEC は省略時のエミュレート LAN を結合します。

モード

省略時の LECS (LAN Emulation Configuration Server) に接続する場合は、「省略時の LECS」をチェックします。LEC は、ILMI MIB 要求を使用して LECS に接続し、LECS アドレスを取得します。この要求に失敗すると、LEC は周知の LECS のアドレスを使用します。特定の LECS に接続する場合は、「指定 LECS」をチェックします。いずれの場合でも、LEC は LECS に接続して LEC アドレスを取得します。

LES に直接接続する場合は、「LES」をチェックします。

LECS 名

LECS の ATM アドレスであり、`/etc/atmhosts` ファイルに表示されるホスト名または別名、あるいはセクタ・バイト付きの 40 桁の ATM AESA アドレス。特定の LECS に接続するには、その LECS のアドレスを入力します。最高 4 つまで指定することができます。

LES 名

LES の ATM アドレスであり、`/etc/atmhosts` ファイルに表示されるホスト名または別名、あるいはセクタ・バイト付きの 40 桁の ATM

AESA アドレス。LEC が LES に直接接続して、構成フェーズを迂回するようにする場合は、その LES アドレスを入力します。

MTU サイズ

最大伝送単位 (MTU) のサイズ。サポートされている MTU サイズは、1516、4544、9234、および 18190 です。仮想 LAN 名を使用して指定されている場合には、そのエミュレート LAN はすでに ATM スイッチ上に構成され、指定された MTU サイズをサポートできるようになっていなければなりません。指定された MTU サイズに対応して構成されていない場合には、その要求は無視されます。

6.2.3.4 IP スイッチングに関する情報

図 6-7 は、ATM IP スイッチング・ワークシートです。以下の各項では、このワークシートに記録する必要がある情報について説明します。本書をオンラインで参照している場合は、印刷機能を使用して、このワークシートのコピーを印刷することができます。

図 6-7: ATM IP スイッチング・ワークシート

ATM IP スイッチング・ワークシート			
ホスト・ファイル			
	ホスト名:	インターネット・アドレス:	別名:
	_____	_____	_____
	_____	_____	_____
	_____	_____	_____
	_____	_____	_____
	_____	_____	_____
	_____	_____	_____
IP スイッチング			
アダプタ名:	_____	_____	_____
ips 番号:	_____	_____	_____
SNAP VCI:	_____	_____	_____
ルーティング:	<input type="checkbox"/> gated	<input type="checkbox"/> routed	<input type="checkbox"/> 静的経路
静的経路			
デスティネーション:	_____		
ゲートウェイ:	_____		
ネットマスク:	_____		

ホスト名

/etc/hosts ファイルに追加する，サブネットワーク上のホストの
名前。

インターネット・アドレス

/etc/hosts ファイルに追加する，サブネットワーク上のホストの
IP アドレス。

別名

/etc/hosts ファイルに追加する，サブネットワーク上のホストの別
名があれば，その名前。

アダプタ名

ネットワーク・インタフェースのデバイス名。 `lta` ネットワーク・インタフェースなど。

ips 番号

IP スwitチング (`ips`) ・インタフェース番号。 複数のアダプタを使用している場合には、それぞれのアダプタに、個別のインタフェース番号が割り当てられます。

SNAP VCI

IFMP (Ipsilon Flow Management Protocol) が省略時の SNAP (Subnetwork Attachment Point) VCI として使用する仮想チャネル識別子 (VCI) 番号です。 省略時の VCI は 15 です。 この番号は、IFMP がデスティネーション・ホスト上で使用する VCI 番号、またはポイント・ツー・ポイント・インタフェースに関連付けられたスイッチに一致しなければなりません。

ルーティング

内部ルーティング・テーブルを使用する方式です。 `gated` デーモンを使用する場合には、「`gated`」をチェックします。 `routed` デーモンを使用する場合には、「`routed`」をチェックします。 スタティック・ルートを使用する場合には、「静的経路」をチェックします。

デスティネーション (静的経路のみ)

デスティネーション・サブネットワークの IP アドレス。

ゲートウェイ (静的経路のみ)

IP スwitチ上での IP コントローラの IP アドレス。

ネットマスク (静的経路のみ)

デスティネーション・サブネットワークのネットマスク。

6.3 ATM の構成

必要な ATM の計画が完了し、正しい ATM ハードウェアをインストールした後、ATM ソフトウェアを構成することができます。 CDE (Common

Desktop Environment) のアプリケーション・マネージャから ATM 設定アプリケーションを使用して、ATM を構成します。次の項目を構成することができます。

- ATM アダプタ
- Classical IP
- LAN Emulation
- IP スイッチング

ATM 設定アプリケーションを使用する方法の詳細については、1.2.1 項で指定されているように SysMan Menu アプリケーションを起動し、6.3.1 項を参照してください。

オプションとして、`atmsetup -old` コマンドを実行すると、以前のリリースで利用可能だった `atmsetup` スクリプトを使用できます。詳細は、オンライン・ヘルプおよび `atmsetup(8)` を参照してください。

6.3.1 ATM アダプタの構成

ATM 論理インタフェースを使用する前に、アダプタを構成しておかなければなりません。ATM アダプタを構成するには、次の手順に従ってください。

1. SysMan Menu から [ネットワーク] [基本ネットワーク・サービス] [ATM (Asynchronous Transfer Mode) の設定] を選択して、ATM 設定メイン・ウィンドウを表示します。

代わりに、次のコマンドをコマンド行から入力することもできます。

```
# /usr/sbin/sysman atm
```

または、次のように入力します。

```
# atmsetup
```

ATM 設定メイン・ウィンドウには、未構成アダプタ、構成されたアダプタ、および構成された論理インタフェースが表示されます。

2. 「未設定のアダプタ」フィールドからアダプタを 1 つ選択します。
3. [設定] を選択します。「アダプタの設定/修正」ダイアログ・ボックスが表示されます。

4. このアダプタについて、すべての ROM ESI (Endpoint System Identifier) を登録しない場合には、[ROM ESI の登録] を選択します。省略時の設定では、アダプタのすべての ROM ESI アドレスが登録されます。
5. このアダプタに追加の ESI (ソフト ESI と呼ばれます) を登録するには、[ソフト ESI の登録] を選択します。
6. このアダプタに送信 CBR (Constant Bit Rate) またはペーシング・オプションを設定するには、[CBR/ペーシング・オプションの設定] を選択します。「CBR/ペーシング・オプションの設定」ダイアログ・ボックスが表示されます。設定が終了したら、[了解] を選択してダイアログ・ボックスをクローズして変更を保存します。
7. このアダプタがサポートするネットワーク物理層のタイプとして、SONET または SDH を指定します。
8. このアダプタでフロー制御 (FLOWmaster) を使用可能にするかどうかを指定します。
9. このアダプタで ILMI (Integrated Local Management Interface) を使用可能にするかどうかを指定します。
10. このアダプタでシグナリングを使用可能にするかどうかを指定します。
11. すべての仮想回路 (VC) リリースのロギングを使用可能にするかどうかを指定します。
12. UNI (User-Network Interface) のバージョンを選択します。
13. 構成内容を確認後 [了解] を選択して、「アダプタの設定/修正」ダイアログ・ボックスをクローズします。以上で、ATM 論理インタフェースを構成できるようになります。

アダプタの構成を変更することもできます。詳細は、オンライン・ヘルプおよび `atmsetup(8)` を参照してください。

6.3.2 Classical IP の構成

Classical IP を構成する前に、ATM アダプタを構成しておかなければなりません。ホストに Classical IP を構成するには、次の手順を実行します。

1. ATM スイッチ上で PVC マッピングを作成します (PVC のみ)。
2. `atmhosts` ファイルにサーバを追加します。

3. `hosts` データベースへホストを追加します。
4. ATM 設定アプリケーションを実行します。
5. Classical IP 論理インタフェースを構成します。
6. スタティック・ルートを追加します (SVC のみ)。
7. PVC の設定を確認します (PVC のみ)。

以下の各項では、これらの各手順について説明します。

6.3.2.1 ATM スイッチへの PVC マッピングの作成

ATM スイッチが必要な環境で PVC を使用する場合には、ATM スイッチに PVC マッピングを作成する必要があります。マッピングの作成方法は、使用する ATM スイッチのタイプによって異なります。詳細は、使用している ATM スイッチのドキュメントを参照してください。

6.3.2.2 `atmhosts` ファイルへのサーバの追加

`/etc/atmhosts` ファイルを編集して、ATM ARP サーバのアドレスを ATM ネットワークに追加することができます。`/etc/atmhosts` ファイルには、ATM ホスト名から ATM ハードウェア・アドレスへのマッピング情報が含まれています。このファイルには、ATM ネットワーク上の特定のサービスのための、ATM ESI および AESA も含まれています。このファイルにエントリを追加すると、アドレスまたはサービスを、長い 16 進数の文字列ではなく、名前で指定できるようになります。

`/etc/atmhosts` ファイルのエントリは、次のいずれかです。

- 最初の文字がシャープ記号 (#) で始まるコメント行
- アドレス指定

アドレス指定は `/etc/hosts` ファイルの IP アドレス指定に似ており、その形式は次のとおりです。

```
atm_addr hostname [ alias ... ]
```

`atm_addr` パラメータは、ESI または AESA から構成することができます。

次の表は、アドレス・タイプ、およびそれぞれのタイプで必要とされる 16 進数のアドレスの桁数を示しています。

アドレス・タイプ	アドレスの桁数
ESI	12 桁の 16 進数
AESA	38 桁の 16 進数
セクタ・バイト付きの AESA	40 桁の 16 進数

`hostname` パラメータには、プリント可能な文字であれば何でも使用することができます。

次の例は、`/etc/atmhosts` ファイルのエントリを示しています。

```
08002b2fe740 myhost.esi 1
47840f01020300002122313208002b2fe740 myhost 2
47840f01020300002122313208002b2fe7403a myhost.ip 3
```

- 1 myhost をスイッチで登録するときに使用する ESI を指定します。
- 2 myhost の AESA を指定します。これはネットワーク・プレフィックスおよび ESI であり、ネットワークが認識できるアドレスです。
- 3 RFC 1577「*Classical IP and ARP over ATM*」の本オペレーティング・システムでの実装のための、myhost 上のサービスのセクタ・バイト付きの AESA を指定します。

注意

省略時の設定では、`atmhosts` ファイルには PVC のエントリが含まれています。このエントリは、削除したり変更したりしないでください。

6.3.2.3 hosts データベースへのホストの追加

ホストが接続する LIS (Logical IP Subnet) 上に存在するすべての ATM ホストに対応する IP アドレスを `hosts` データベースに追加します。ローカル・ホストおよび ATM ARP サーバの IP アドレスを確認してください。環境によっては、ホスト名およびアドレスは、ローカルな `/etc/hosts` ファイル、あるいは DNS または NIS で配布されるファイルのいずれかに置くことができます。

これらの IP アドレスは、`/etc/hosts` ファイルを直接編集するか、CDE のアプリケーション・マネージャの SysMan Menu アプリケーションを実行することによって、`/etc/hosts` ファイルに入力することができます。詳細は、2.3.7 項を参照してください。

6.3.2.4 ATM 設定アプリケーションの実行

Classical IP をシステム上に構成するには、次の手順に従ってください。

1. SysMan Menu の [ネットワーク] [基本ネットワーク・サービス] [ATM (Asynchronous Transfer Mode) の設定] を選択して、ATM 設定メイン・ウィンドウを表示します。

代わりに、次のコマンドをコマンド行から入力することもできます。

```
# /usr/sbin/sysman atm
```

または、次のように入力します。

```
# atmsetup
```

ATM 設定メイン・ウィンドウには、未構成アダプタ、構成されたアダプタ、および構成された論理インタフェースが表示されます。

2. [追加] を選択します。「インタフェースの追加」ダイアログ・ボックスが表示されます。
3. [Classical IP] を選択します。「インタフェースの追加」ダイアログ・ボックスがクローズされます。「Classical IP インタフェースの追加/修正」ダイアログ・ボックスが表示されます。
4. Classical IP 論理インタフェースを追加するアダプタを選択します。
5. 省略時の論理インタフェース番号を使用しない場合には、別の番号を入力します。
6. システムが ARP クライアントまたは ARP サーバとして動作するかどうかを指定します。
7. システムが ARP クライアントになる場合には、ARP サーバの ATM アドレスまたは別名を入力します。次に、ARP サーバの IP アドレスを入力します。

8. 論理インタフェースの PVC を指定する場合には、[PVC] を選択します。「PVC の追加/修正」ダイアログ・ボックスが表示されます。次の手順を実行します。
 - a. 仮想回路の仮想パス識別子 (VPI) を入力します。
 - b. 仮想回路の仮想チャンネル識別子 (VCI) を入力します。
 - c. リモート・ホストのエンティティが RFC 1577 で定義されているように Classical IP をサポートするかどうかを指定します。
 - d. リモート・ホストが Classical IP をサポートしていない場合は、リモート・ホストの IP アドレスを入力します。
 - e. 構成内容を確認後 [了解] を選択して、「PVC の追加/修正」ダイアログ・ボックスをクローズします。
9. [了解] を選択して、「Classical IP インタフェースの追加/修正」ダイアログ・ボックスをクローズします。
10. ATM 設定メイン・ウィンドウで [了解] を選択し、変更を保存します。システムに ATM インタフェースが存在しない場合には、「Start ATM Now」ダイアログ・ボックスが表示されます。ATM サブシステムを起動するには、[了解] を選択します。それ以外の場合には、[いいえ] を選択します。[いいえ] を選択した場合には、システムをリブートして、ATM サブシステムを起動しなければなりません。

システムに ATM インタフェースが存在している場合には、「Reboot Required」ダイアログ・ボックスが表示されます。[了解] を選択し、メッセージに肯定応答します。ATM サブシステムを起動するには、システムをリブートしなければなりません。

アダプタの構成を変更することもできます。詳細は、オンライン・ヘルプおよび atmsetup(8) を参照してください。

6.3.2.5 Classical IP 論理インタフェースの構成

ATM 設定アプリケーションを実行し、(アプリケーション内から、またはシステムをリブートして) ATM 構成要素を起動すれば、Classical IP (lis) インタフェースを構成できます。lis インタフェースを構成する方法については、2.3.1 項を参照してください。

6.3.2.6 スタティック・ルートの追加 (SVC のみ)

ネットワーク・トポロジおよびネットワーク内の論理 IP サブネットワーク (LIS) の数および構成によって、別の LIS サブネット上にあるホストに接続するには、他のホストへのスタティック・ルートを追加しなければならない場合があります。ルーティング・テーブルにスタティック・ルートを追加する方法については、2.3.6 項を参照してください。

6.3.2.7 PVC の構成の確認 (PVC のみ)

PVC が構成された後、`atmarp -a` コマンドを実行して、構成を確認します。PVC が構成されていれば、次のような出力が表示されます。

```
# atmarp -a
Number of entries : 1

IP Address :   atm66 (16.142.128.66)
ATM Address :   PVC
Flags :        Complete Permanent
VCs :          vpi    vci    VC Type
               ---    ---    -
               0      999    PVC
```

6.3.3 LAN エミュレーションの構成

ホストに LAN エミュレーションを構成するには、次の手順を実行します。

1. `atmhosts` ファイルにサーバを追加します。
2. `hosts` データベースへホストを追加します。
3. ATM 設定アプリケーションを実行します。
4. LAN Emulation 論理インタフェースを構成します。

以下の各項では、これらの手順について説明します。

6.3.3.1 `atmhosts` ファイルへのサーバの追加

`/etc/atmhosts` ファイルを編集するのは、LES (LAN Emulation Server) アドレスを指定するか、LECS (LAN Emulation Configuration Server) アドレスを自分の ATM ネットワークで指定する場合に限られます。`/etc/atmhosts` ファイルには、ATM ホスト名から ATM ハードウェア・アドレスへのマッピングが含まれています。このファイルには、ATM ネットワーク上の特定のサービスの ATM ESI および AESA も含まれています。

/etc/atmhosts ファイルの編集方法についての詳細は、6.3.2.2 項を参照してください。

6.3.3.2 hosts データベースへのホストの追加

ホストが接続する任意のエミュレート LAN (ELAN) 上に存在するすべての ATM ホストの IP アドレスを hosts データベースに追加します。ローカル・ホストの IP アドレスを確認します。環境によっては、ホスト名およびアドレスは、ローカルな /etc/hosts ファイル内、あるいは DNS または NIS で配布されるファイルのいずれかに置くことができます。

これらの IP アドレスは、/etc/hosts ファイルを直接編集するか、CDE のアプリケーション・マネージャの SysMan Menu アプリケーションを実行することによって、/etc/hosts ファイルに入力することができます。詳細は、2.3.7 項を参照してください。

6.3.3.3 ATM 設定アプリケーションの実行

システムに LAN Emulation を構成するには、次の手順に従ってください。

1. SysMan Menu の [ネットワーク] [基本ネットワーク・サービス] [ATM (Asynchronous Transfer Mode) の設定] を選択して、ATM 設定メイン・ウィンドウを表示します。

代わりに、次のコマンドをコマンド行から入力することもできます。

```
# /usr/sbin/sysman atm
```

または、次のように入力します。

```
# atmsetup
```

ATM 設定メイン・ウィンドウには、未構成アダプタ、構成されたアダプタ、および構成された論理インタフェースが表示されます。

2. [追加] を選択します。「インタフェースの追加」ダイアログ・ボックスが表示されます。
3. [LAN Emulation] を選択します。「インタフェースの追加」ダイアログ・ボックスがクローズされます。「LAN Emulation インタフェースの追加/修正」ダイアログ・ボックスが表示されます。
4. LAN エミュレーション論理インタフェースを追加するアダプタを選択します。

5. 省略時の論理インタフェース番号を使用しない場合には、別の番号を入力します。
6. 特定のエミュレート LAN を結合するには、結合するエミュレート LAN の名前を入力します。
7. システムがエミュレート LAN に登録されるモードを選択します。特定の LECS (LAN Emulation Configuration Server) (2 番目の選択肢) に接続する場合には、LECS 名または別名も入力します。LES (LAN Emulation Server) に直接接続する場合 (3 番目の選択肢) にも、LES 名または別名を入力します。
8. 省略時の MTU サイズである 1516 以外のサイズを指定するには、別の MTU サイズを選択します。
9. [了解] を選択して、「LAN Emulation インタフェースの追加/修正」ダイアログ・ボックスをクローズします。
10. ATM 設定メイン・ウィンドウで [了解] を選択し、変更を保存します。システムに ATM インタフェースが存在しない場合には、「Start ATM Now」ダイアログ・ボックスが表示されます。ATM サブシステムを起動するには、[了解] を選択します。それ以外の場合には、[いいえ] を選択します。[いいえ] を選択した場合には、システムをリブートして、ATM サブシステムを起動しなければなりません。

システムに ATM インタフェースが存在する場合には、「Reboot Required」ダイアログ・ボックスが表示されます。[了解] を選択し、メッセージに肯定応答します。ATM サブシステムを起動するには、システムをリブートしなければなりません。

注意

ELAN を ATM スイッチに結合できるのは、それぞれのアダプタで 1 度だけです。同じ ELAN を同じアダプタに何度も結合してはいけません。同じ ELAN を同じスイッチに結合するには、別のアダプタをインストールして、そこから ELAN を結合しなければなりません。

アダプタの構成を変更することもできます。詳細は、オンライン・ヘルプおよび atmsetup(8) を参照してください。

6.3.3.4 LAN エミュレーション論理インタフェースの構成

ATM 設定を実行し、ATM 構成要素を (アプリケーション内部からまたはシステムをブートすることによって) 起動した後、LAN Emulation (elan) インタフェースを構成します。elan インタフェースを構成する方法については、2.3.1 項を参照してください。

6.3.4 IP スイッチングの構成

ホストに IP スイッチングを構成するには、次の手順を実行します。

1. `hosts` ファイルに IP アドレスを追加します。
2. IP スイッチング論理インタフェース作成するために、ATM 設定アプリケーションを実行します。
3. スイッチング論理インタフェースを構成します。
4. ルーティング・テーブルヘルトを追加します。

以下の各項では、これらの手順について説明します。

6.3.4.1 `hosts` ファイルへの IP アドレスの追加

`/etc/hosts` ファイルを編集して、ホストが接続するそれぞれの IP スイッチング・サブネットワークの IP アドレスを追加します。それぞれのサブネットについて、ポイント・ツー・ポイント・リンクの両端 (ホスト側と IP コントローラ側) に対する IP アドレスのペア、サブネットの IP アドレス、およびサブネットのブロードキャスト・アドレスを追加します。たとえば、図 6-3 の構成の `/etc/hosts` ファイルは、次のとおりです。

```
# IP Switching subnet A
16.1.1.4  networka-net
16.1.1.5  hosta.corp.com          hosta          atm5
16.1.1.6  ipsctrlhosta.corp.com ipsctrlhosta   atm6
16.1.1.7  networka-broadcast
# IP Switching subnet B
16.1.1.0  networkb-net
16.1.1.1  ipsctrlhostb.corp.com ipsctrlhostb   atm1
16.1.1.2  hostb.corp.com        hostb          atm2
16.1.1.3  networkb-broadcast
# IP Switching subnet C
16.1.1.8  networkc-net
```

```
16.1.1.9   ipsctrlhostc.corp.com   ipsctrlhostc   atm9
16.1.1.10  ipgwy.corp.com                 ipgwy          atm10
16.1.1.11  networkc-broadcast
```

これらの IP アドレスは、`/etc/hosts` ファイルを直接編集するか、CDE のアプリケーション・マネージャの SysMan Menu アプリケーションを実行することによって、`/etc/hosts` ファイルに入力することができます。詳細は、2.3.7 項を参照してください。

6.3.4.2 ATM 設定アプリケーションの実行

システムに IP スイッチングを構成するには、次の手順に従ってください。

1. SysMan Menu の [ネットワーク] [基本ネットワーク・サービス] [ATM (Asynchronous Transfer Mode) の設定] を選択して、ATM 設定メイン・ウィンドウを表示します。

代わりに、次のコマンドをコマンド行から入力することもできます。

```
# /usr/sbin/sysman atm
```

または、次のように入力します。

```
# atmsetup
```

ATM 設定メイン・ウィンドウには、未構成アダプタ、構成されたアダプタ、および構成された論理インタフェースが表示されます。

2. [追加] を選択します。「インタフェースの追加」ダイアログ・ボックスが表示されます。
3. [IP スイッチング] を選択します。「インタフェースの追加」ダイアログ・ボックスがクローズされます。「IP スイッチング・インタフェースの追加/修正」ダイアログ・ボックスが表示されます。
4. IP Switching 論理インタフェースを追加するアダプタを選択します。
5. 省略時の論理インタフェース番号を使用しない場合には、別の番号を入力します。
6. 仮想チャネル識別子 (VCI) を省略時の設定から変更するには、[オプション] を選択します。「IP スイッチング・オプションの修正」ダイアログ・ボックスが表示されます。次の手順を実行してください。
 - a. 目的の SNAP VCI の値が 15 (省略時の値) 以外であれば、それを入力します。

注意

この SNAP VCI の値は、ポイント・ツー・ポイント・インタフェースに関連付けられているスイッチで、IFMP が使用する VCI の値と一致していなければなりません。

- b. 接続を送信し、受信するために使用する VCI の範囲を入力します。
 - c. [了解] を選択して変更を保存し、「IP スイッチング・オプションの修正」ダイアログ・ボックスをクローズします。
7. [了解] を選択して、「IP スイッチング・インタフェースの追加/修正」ダイアログ・ボックスをクローズします。
8. ATM 設定メイン・ウィンドウで [了解] を選択し、変更を保存します。システムに ATM インタフェースが存在しない場合には、「Start ATM Now」ダイアログ・ボックスが表示されます。ATM サブシステムを起動するには、[了解] を選択します。それ以外の場合には、[いいえ] を選択します。[いいえ] を選択した場合には、システムをリブートして、ATM サブシステムを起動しなければなりません。

システムに ATM インタフェースが存在する場合には、「Reboot Required」ダイアログ・ボックスが表示されます。[了解] を選択し、メッセージに肯定応答します。ATM サブシステムを起動するには、システムをリブートしなければなりません。

アダプタの構成を変更することもできます。詳細は、オンライン・ヘルプおよび `atmsetup(8)` を参照してください。

6.3.4.3 IP スイッチング論理インタフェースの構成

ATM 設定アプリケーションを実行し、ATM 構成要素を (アプリケーション内部からまたはシステムをブートすることによって) 起動した後、IP スイッチング (`ips`) インタフェースを構成します。 `ips` インタフェースを構成する方法については、2.3.1 項を参照してください。

6.3.4.4 ルートの追加

ネットワーク・トポロジおよびホスト上のインタフェースの数によっては、システムに複数のインタフェースがあり、省略時のルートが別のネットワー

ク上の別のゲートウェイである場合に、他のホストへのルートを追加しなければならないことがあります。次の手順のいずれかを実行します。

- `gated` デーモンまたは `routed` デーモンを起動し、システムのルーティング・テーブルを自動的に更新します。
- デスティネーション・ネットワークのルーティング・テーブルにスタティック・ルートを追加します。SysMan Menu の [ネットワーク] [基本ネットワーク・サービス] [スタティック・ルートの設定 (/etc/routes)] を選択します。「スタティック・ルートの設定 (/etc/routes)」ダイアログ・ボックスが表示されます。デスティネーション・サブネットワークの IP アドレス、および IP スイッチ上の IP コントローラのアドレスを指定する必要があります。たとえば、図 6-3 のホスト A で IP スイッチングを構成している場合に、16.1.1 ネットワーク上のすべてのトラフィックを IP スイッチを経由してルーティングするには、デスティネーション・アドレスとして 16.1.1/24 を CIDR (Classless Inter-Domain Routing) 形式で指定し、16.1.1.6 をゲートウェイ・アドレスとして指定します。

システムが通信する必要のある、それぞれの追加のネットワークについてのエントリを追加します。詳細は、2.3.6 項を参照してください。

6.4 ATM 環境の管理

ATM 環境の管理では、次の構成要素の管理を行います。

- ATM ネットワークおよび ATM ネットワークに関する情報の表示
- シグナリング・モジュール
- Classical IP 環境
- LAN Emulation 環境
- IP スイッチング
- ATM サブシステムのメッセージ

以下の各項では、これらの構成要素の管理方法について説明します。

6.4.1 ATM ネットワークと、ATM ネットワークに関する情報の表示

ATM ネットワークを管理し、ATM ネットワークに関する情報を表示するには、`atmconfig` コマンドを使用します。このコマンドは、基本 ATM モ

ジュールおよびデバイス・ドライバだけを制御し、特定の収束化モジュールやシグナリング・プロトコルについては制御しません。atmconfig コマンドを使用すると、次の操作を実行することができます。

- デバイス・ドライバの有効化および無効化
- PVC の作成および削除
- SVC の削除
- ESI の作成および削除
- 現在アクティブな VC およびドライバの状態表示
- 構成バッチ・ファイルの処理

詳細は、atmconfig(8) を参照してください。

6.4.2 シグナリング・モジュール

エンド・システムで ATM UNI シグナリングを管理するには、atmsig コマンドを使用します。atmsig コマンドを使用すると、次の作業を実行することができます。

- シグナリング・モジュールに関する状態情報の表示
- ILMI およびシグナリングの有効化および無効化
- Q.SAAL および Q.93B (2931) の各種タイマ値および統計値の読み取りおよび変更

シグナリング・モジュールは、常に、指定されたインタフェースに関連付けられており、ドライバ名によって識別することができます。インタフェースが無効である場合には、シグナリング・モジュールも無効です。インタフェースを再びオンラインにするときには、シグナリング・モジュールを有効にしなければなりません。

詳細は、atmsig(8) を参照してください。

6.4.3 Classical IP 環境

エンド・システムで Classical IP を管理するには、atmarp コマンドを使用します。atmarp コマンドを使用すると、次の作業を実行することができます。

- 論理 IP サブネット (LIS) インタフェースの作成
- ATM ARP テーブルのエントリの作成および削除

- ATM ARP テーブルのエントリの表示
- エントリのパーマネント・フラグの切り替え
- ローカル・ホストの ATM 構成状態の表示
- VC および Classical IP をサポートしないリモート IP エントリの間に関連付けの作成および削除

詳細は、`atmarp(8)` を参照してください。

6.4.4 LAN Emulation 環境

LAN Emulation 環境の管理には、次のような作業が含まれています。

- LEC (LAN Emulation Client) の管理
- LE-ARP (LAN Emulation Address Resolution Protocol) の表示

以下の各項では、これらの作業について説明します。

6.4.4.1 LAN Emulation Client の管理

LEC を管理するには、`atmelan` コマンドを使用します。`atmelan` コマンドを使用すると、次の作業を実行することができます。

- LEC のネットワーク・インタフェースとしての作成および構成
- カウンタ、パラメータ、およびそれぞれの LEC の状態の表示

詳細は、`atmelan(8)` を参照してください。

6.4.4.2 LE-ARP テーブルの表示

それぞれの `elan` インタフェースに対する LE-ARP テーブルを表示するには、`learp` コマンドを使用します。エミュレート LAN のアドレス・マッピングが表示されます。それぞれのエントリは、MAC (Media Access Control) アドレス、状態、ATM アドレス、およびフラグから構成されます。詳細は、`learp(8)` を参照してください。

6.4.5 IP スイッチング

エンド・システムの IP スイッチングを管理するには、`atmifmp` コマンドを使用します。`atmifmp` コマンドを使用すると、次の作業を実行することができます。

- IP スイッチングの有効化および無効化

- IP スイッチングの構成の表示
- IP スイッチングの統計値の表示またはクリア
- IP スイッチングのフロー情報の表示

詳細は、`atmifmp(8)` を参照してください。

6.4.6 ATM サブシステムのメッセージ

ATM サブシステムは、`/var/adm/syslog.dated/date/kern.log` ファイルに状態メッセージとエラー・メッセージを記録します。このメッセージ・ファイルの内容は、`SysMan Menu` ユーティリティのイベント・ビューアで見ることができます。イベント・ビューアについての詳細は、11.9 節を参照してください。

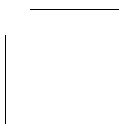
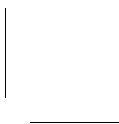
省略時の設定では、ATM サブシステムはサブシステム初期化メッセージ、重要な状態変更、および重大なエラー状況を記録します。ATM サブシステムが表示するメッセージのレベルを、すべての構成要素にわたって一括して上げるには、次のコマンドを使用します。

```
# sysconfig -r atm global_msg_level=2
```

メッセージ・レベルは、サブシステムの構成要素ごとに上げることもできます。たとえば、`LANE` のメッセージ・レベルを上げて、セッション初期化情報を参照できるようにするには、次のコマンドを使用します。

```
# sysconfig -r lane lane_msg_level=2
```

詳細は、`sys_attrs_atm(5)` を参照してください。



DHCP (Dynamic Host Configuration Protocol) を使用すると、IP アドレスの集中管理および管理の自動化が可能になります。グラフィカル・アプリケーションを使用すると複数のコンピュータの構成を一度に行うことができ、その構成は、確実に一貫性が保たれ、正確であることが保証されます。ポータブル・コンピュータをネットワークに接続する際にも、自動的に構成が行われます。

この章では次のことを説明します。

- Tru64 UNIX システムの DHCP インプリメンテーション (7.1 節)
- DHCP 構成の準備 (7.2 節)
- xjoin および SysMan Menu ユーティリティを使用して DHCP サーバを構成する方法 (7.3 節)
- DHCP クライアント・アドレッシングの管理方法 (7.4 節)

Tru64 UNIX における DHCP のインプリメンテーションは、JOIN Systems 社の JOIN Server Version 4.1 をベースにしています。DHCP についての詳細は、DHCP(7) リファレンス・ページおよび『*JOIN Server Administrator's Guide*』を参照してください。『*JOIN Server Administrator's Guide*』は、JOIN Systems 社から HTML ファイルで提供されており、下記のファイルをブラウザでオープンすることにより参照できます。

`/usr/doc/join/TOC.html`

トラブルシューティング情報については、10.7 節を参照してください。

注意

Tru64 UNIX Version 4.0F から、DHCP データベース・ファイルは新しいフォーマットで保存されます。この新しいフォーマットは、古いフォーマットとは互換性がありません。この変更の理由、影響のあるファイルの一覧、および新しいフォーマットへの変換方法についてはオンライン・ドキュメントで説明しています。

す。このドキュメント、README-DB237 と変換ユーティリティ conv185-237 は、`/etc/joyin` ディレクトリに置かれています。

7.1 DHCP 環境

DHCP 環境では、システムには次の役割があります。

- サーバ

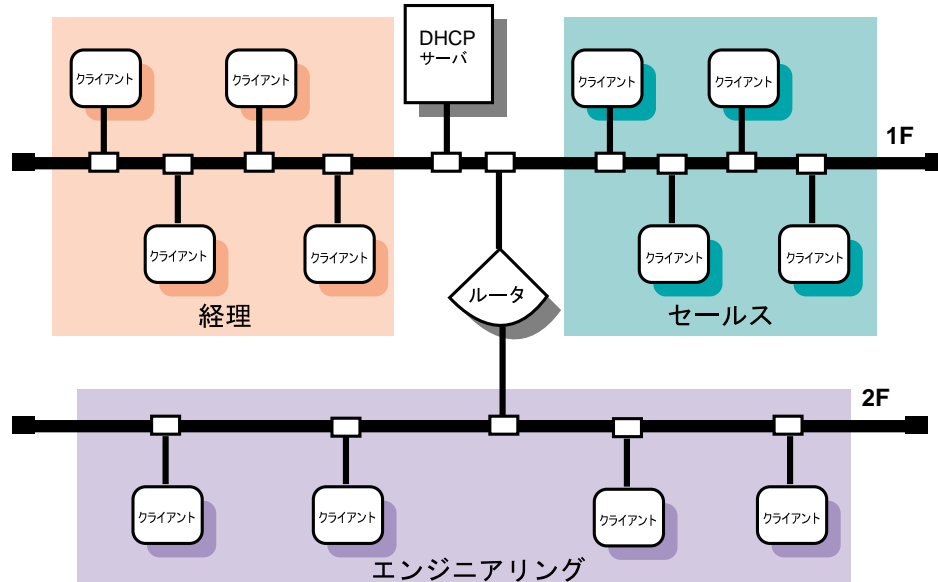
ネットワーク上の他のシステムに DHCP および BOOTP サービスを提供するシステム。1つのサブネットワーク上に複数のサーバが存在できますが、各サーバの IP アドレスの範囲は重複してはなりません。DHCP サーバをサポートしているクラスタ・メンバの場合、フェイルオーバを利用したコモン・データベースを使用しているすべてのクラスタ・メンバの唯一の DHCP サーバになります。他のクラスタに固有の情報については、『クラスタ管理ガイド』を参照してください。

- クライアント

DHCP サーバに構成情報を要求するシステム。クラスタのメンバを DHCP クライアントとして使用することはできません。クラスタのメンバには静的アドレッシングを使用します。

ある企業のローカル・エリア・ネットワーク (LAN) における DHCP の構成例を図 7-1 に示します。この LAN (acme-net) の DHCP サーバは、3つの業務分野のクライアントに IP アドレスを提供するように構成されています。この構成では、ルータは BOOTP パケットを送信するように構成しなければなりません。DHCP パケットは、DHCP 拡張を持つ BOOTP パケットです。詳細は `bprelay(8)` を参照してください。

図 7-1: DHCP の構成 (acme-net)



ZK-1146U-AIJ

7.1.1 DHCP パラメータの割り当て

DHCP 環境では、DHCP パラメータは次のエンティティに割り当てられます。

- グループ

グループ・パラメータは、同じ構成値を共有するネットワーク上のすべてのクライアント(ノード)に適用されます。これらのクライアントをグループ化することにより、ネットワーク構成を簡単に実現し保守することができます。各ノードに対してパラメータを定義するのではなく、(クライアントの)グループに対してパラメータを定義します。グループ・パラメータを定義したら、その設定を使用して他のサブネットワークやノードを構成することができます。

論理領域、機能領域、物理領域、または任意の方法でノードをグループ化することができます。グループを他のグループ、サブネットワーク、およびノードとグループ化することもできます。

- サブネットワーク

サブネットワーク・パラメータは、サブネットワーク上のすべてのクライアント(ノード)に適用されます。サブネットワークをグループとみなすこともできますが、グループはサブネットワーク・アドレスを共有しています。サブネットワークは、他のサブネットワークやノードとグループ化することができます。

- ノード

ノード・パラメータは、ネットワーク上の個々のクライアント(ノード)に適用され、通常はサブネットワーク・パラメータまたはグループ・パラメータより優先されます。

これらのエンティティとそのパラメータは、ネットワーク上で相互に階層的な関係があります。たとえば図 7-1 は、2 つのサブネットワークと 3 つのグループ(アカウントिंग、セールス、およびエンジニアリング) からなる acme-net と呼ばれるビジネス・ネットワークを示しています。DHCP 管理者は、このネットワークを、個々のノードを含む 2 つのサブネットワーク (floor1 および floor2) からなる acme-net という名前の 1 つのグループと見ることができます。

acme-net グループは階層のトップ・レベルであり、ネットワーク上のすべてのシステムに適用されるパラメータを指定します。次のレベルの floor1 サブネットワークは floor1 サブネットワーク上のすべてのノードに適用されるパラメータを、floor2 サブネットワークは floor2 サブネットワーク上のすべてのノードに適用されるパラメータを指定します。グループごとにパラメータを割り当てることが必要な場合は、DHCP 管理者は、アカウントिंग・グループおよびセールス・グループから構成される floor1 サブネットワークの各グループに個々のノードを割り当てます。ただしこの 2 つのグループは同一サブネットワーク上にあるので、別のグループ・パラメータを割り当てて必要はありません。

図 7-1 がサブネットワーク(ルータ)を持たない単一 LAN の場合、DHCP 管理者は、このネットワークを個々のノードを含む 3 つのグループ(アカウントिंग、セールス、およびエンジニアリング) から構成される acme-net という 1 つのグループとみることができます。

1 つの Ethernet またはサブネットワーク番号を定義するためにグループを使用することもできます。またこの設定を使用して、他のノードまたはサブネットワークを構成することもできます。

7.1.2 DHCP とセキュリティ

MAC (Media Access Control) アドレス・データベースを作成して、DHCP サーバへのクライアント・アクセスを制限することができます。MAC アドレス・データベースを作成すると、データベースに登録されたアドレスを持つクライアントだけが IP アドレスを受け取ることができます。詳細は 7.4.4 項を参照してください。

7.2 DHCP の計画

DHCP を構成する前に必要な作業について説明します。

7.2.1 DHCP ソフトウェアのインストールの確認

DHCP サーバ・システムに対して、次のコマンドを実行して DHCP サーバがインストールされていることを確認します。

```
# setld -i | grep OSFINET
```

サブセットがインストールされていない場合は、setld コマンドを使用してサブセットをインストールします。サブセットのインストールについての詳細は、setld(8) または『インストレーション・ガイド』を参照してください。

DHCP クライアント・システムに対して、DHCP クライアント・ソフトウェアは必須サブセットとともにインストールされます。

7.2.2 構成の準備

DHCP ソフトウェアがインストールされていることを確認したら、xjoin ユーティリティを使用して DHCP を構成できます。

- サーバ・パラメータの指定
- グループ、ノード、およびサブネットワークの基本 DHCP パラメータの指定

指定する情報は、DHCP 環境の定義により異なります。この後の項で DHCP の構成に必要な情報を記録するためのワークシートを示します。

7.2.2.1 サーバ/セキュリティ・パラメータ

図 7-2 は、DHCP サーバ/セキュリティ・パラメータ・ワークシートを示しています。本書をオンラインで参照している場合、印刷機能を使用してこの

ワークシートを印刷することができます。この後の項では、ワークシートに記録する必要のある情報について説明します。

図 7-2: DHCP サーバ/セキュリティ・パラメータ・ワークシート

DHCPサーバ/セキュリティ・パラメータ・ワークシート	
BOOTP アドレスを プールから割り当てる:	True <input type="checkbox"/> False <input type="checkbox"/>
BOOTP 互換:	True <input type="checkbox"/> False <input type="checkbox"/>
省略時のリース・タイム:	_____
ネーム・サービス:	/etc/hosts <input type="checkbox"/> DNS <input type="checkbox"/> NIS <input type="checkbox"/>
Ping タイムアウト:	_____
仮割り当てリスト残留時間:	_____
既知の MAC アドレスに制限:	True <input type="checkbox"/> False <input type="checkbox"/>
IP レンジ	
サブネットワーク・アドレス:	_____
DHCP サーバ:	_____
IP レンジ:	_____
ホスト名リスト	
ドメイン名:	_____
DHCP サーバ:	_____
ホスト名プレフィックス:	_____
ホスト名:	_____

BOOTP アドレスをプールから割り当てる

BOOTP クライアントへのアドレスをプールから割り当てるよう DHCP サーバを設定する場合は、True をチェックします。アドレスの割り当ては永続します。/etc/bootptab ファイルでアドレスが構成された (これが普通の方法です) BOOTP クライアントを DHCP サーバがサポートするよう設定する場合は、False をチェックします。これが省略時の設定です。

BOOTP 互換

クライアントが BOOTP アドレスを要求した場合に、DHCP サーバだけでなく BOOTP サーバとしてサーバを機能させたい場合は、True をチェックします。BOOTP クライアントをサポートしない場合は、

False をチェックします。BOOTP サーバだけを構成したい場合は、7.4.6 項を参照してください。

省略時のリース・タイム

ノード、サブネットワーク、またはグループに対して明示的に構成していない場合の、クライアントの DHCP 専用の省略時の時間(日、時間、分、および秒単位)。

ネーム・サービス

サーバが使用するネーム・サービス。DHCP サーバに対してネーム・サービスを構成しなければなりません。ネーム・サービスは、ネットワーク上の他のシステムに対する認証、ルート、アドレスおよびネーミング関連機能を実行するために使用されます。サーバは、次のタイプのネーム・サービスを使用できます。

- ローカル・ネーム・サービスは、動的に割り当てられた名前とアドレスに関する情報を使用して /etc/hosts ファイルを更新します。
- DNS (Domain Name System) は、ホスト名を数値 IP アドレスに自動的に変換します。
- NIS (Network Information Service) を使用すると、ホスト名情報をネットワーク上に分散することができます。

Ping タイムアウト

ping タイムアウトまでの時間(1/1000 秒)。ping コマンドは、ネットワーク上のクライアントが使用できるかどうかを確認します。ping プログラムがクライアントに要求を送信した場合、クライアントは要求に応答して、クライアントの IP アドレスを返します。Ping タイムアウト・パラメータは、一定の時間、他に IP アドレスを使用しているクライアントがないことを確認します。タイムアウトの後、ping コマンドは確認を中止します。

仮割り当てリスト残留時間

IP アドレスが、別のデバイスに割り当てられる候補となるまでに、仮の割り当てリストにとどまる最大時間(時間、分、および秒単位)を入力します。これにより、解放された IP アドレスがすぐに再度使用されることがなくなります。

既知の **MAC** アドレスに制限

MAC アドレスが一致するクライアントに IP アドレスを割り当てる場合は、True をチェックします。そうでない場合は、False をチェックします。サーバへのクライアント・アクセスの制限についての詳細は、7.4.4 項を参照してください。

IP レンジとは、ネットワーク上のクライアントに割り当てることのできる IP アドレスの範囲です。同一サブネットワーク上に複数の DHCP サーバが存在することはできますが、各サーバが管理する IP アドレス・レンジは重複してはなりません。IP レンジには、次の情報を指定します。

サブネットワーク・アドレス

サブネットワークは、単一 TCP/IP ネットワークの論理的な一部分です。サブネットワーク IP 番号は、ネットワークの1つのセグメントを識別します。ネットワーク数が増加すると、IP アドレスのルーティングは複雑になります。サブネットワークを使用すると、ネットワーク・アドレスを割り当てる場合に柔軟性が増し、ネットワーク番号の管理が容易になります。IP アドレスは、次の情報から構成されます。

- ネットワーク・アドレス
- サブネットワーク・アドレス
- ホスト・アドレス

IP アドレスは4つのフィールドに分割され、各フィールドはピリオドで区切られます。各フィールドはアドレスの要素を表します。たとえば、通常の IP アドレスは次のように表されます。

128.174.139.47

この例で 128.174 はネットワーク・アドレスであり、139 はサブネットワーク・アドレスであり、47 はホスト・アドレスです。そのためサブネットワーク・アドレスは 128.174.139.0 になります。

DHCP サーバ

DHCP サーバの IP アドレス。

IP レンジ

選択したサブネットワーク上のクライアントに割り当てる固有の IP アドレスのグループです。前出のサブネットワーク・アドレスの例を使

用すると、サブネットワーク上に 25 のクライアントが存在する場合、IP アドレスの範囲は 128.174.139.47 から 128.174.139.72 です。サブネットワーク・アドレスは、複数の対応する IP アドレス・レンジを持つことができます。

サーバとクライアントの間にあるルータが BOOTP パケットを送信する場合、DHCP サーバは複数のサブネットワーク上でクライアントを構成することができます。ブート・ファイルおよび BOOTP パラメータについての詳細は、7.2.2.2 項 および bprelay(8) を参照してください。

ホスト名リストには、IP アドレスを割り当てる時にクライアントに割り当てられる名前が含まれます。ホスト名リストには、次の情報を指定します。

ドメイン名

ドメインは、管理を目的としてまとめられた、複数のコンピュータを表します。管理の容易さを考慮して、通常、ドメイン名は企業に対して割り当てられます。たとえば、ドメインが、ネットワークの新しいサービスにアクセスできるように変更された場合は、そのドメインの一部である各コンピュータも、自動的に新しいサービスにアクセスできます。

NIC ドメイン・レジスターにより割り当てらるたドメイン名を正確に入力します。この際、最上位のドメイン拡張子(たとえば school.edu, company.com, city.gov) も含めます。

DHCP サーバ

DHCP サーバの IP アドレス。

ホスト名プレフィックス

特定のホスト名のプレフィックスを入力します。ホスト名のプレフィックスは、コンピュータがホスト名を要求した際に割り当て可能な名前がない場合に使用します。たとえば、Company.com ドメインを使用している場合に、Hostname リスト・ボックスの名前がすべて割り当て済みでホスト名のプレフィックスが net12host であると、ホスト名を要求する 2 つのコンピュータは、ホスト名として net12host1 と net12host2 を受け取ることになります。

ホスト名

ホスト名を要求するシステムに割り当てるホスト名。

7.2.2.2 基本的な DHCP パラメータ

図 7-3 は、基本的な DHCP パラメータ・ワークシートを示しています。本書をオンラインで参照している場合、印刷機能を使用してこのワークシートを印刷することができます。この後の項で、ワークシートに記録する必要のある情報について説明します。

図 7-3: DHCP 基本パラメータ・ワークシート

DHCP基本パラメータ・ワークシート	
構成のタイプ:	ノード <input type="checkbox"/> サブネット <input type="checkbox"/> グループ <input type="checkbox"/>
構成名:	_____
メンバのグループ:	_____
グループ・メンバ:	_____
ネットあるいはサブネットワークの	
IP アドレス:	_____
ハードウェア・アドレス:	_____
ハードウェア・タイプ:	_____
BOOTPパラメータ	
ブート・ファイル:	_____
ブート・ファイル・サーバ・アドレス:	_____
ブート・ファイル・サイズ:	_____
DNS ドメイン名:	_____
DNS サーバ IP アドレス:	_____

ホーム・ディレクトリ:	_____
ホスト IP アドレス:	_____
ルータ:	_____

クライアント・ホスト名の送信:	True <input type="checkbox"/> False <input type="checkbox"/>
サブネットワーク・マスク:	_____
TFTP ルート・ディレクトリ:	_____
ブロードキャスト・アドレス:	_____
サブネットワークはローカル:	True <input type="checkbox"/> False <input type="checkbox"/>
マスクの供給:	True <input type="checkbox"/> False <input type="checkbox"/>
DHCP 再割り当て時間:	_____
DHCP 更新時間:	_____
リース時間:	_____

構成のタイプ

ノードの構成を行う場合は「ノード」を、サブネットワークの構成を行う場合は「サブネット」をチェックしてください。グループの構成を行う場合は「グループ」をチェックします。

構成名

ノード、グループ、またはサブネットワークの名前。

メンバのグループ

ノード、サブネットワーク、およびグループ構成に対して、DHCP パラメータ値を継承する構成の名前を指定します。グループに対して定義されたパラメータは、この構成にも適用されます。

グループ・メンバ

グループの構成の場合、このグループを構成するノード、サブセット、およびグループ。

ネットあるいはサブネットワークの IP アドレス

サブネットワーク構成の場合の、サブネットワークの IP アドレス。IP アドレスのフォーマットは、`ddd.ddd.ddd.ddd`です。たとえばサブネットワークが `16.128` の場合は、`16.128.0.0` のように最後にゼロを追加する必要があります。

ハードウェア・アドレス

ノード構成の場合の、クライアント・ノードのイーサネット・アドレス。

ハードウェア・タイプ

ノード構成の場合の、システムを識別するための名前。

ノード、サブネットワーク、およびグループ構成の場合、BOOTP パラメータを使用すると、ネットワーク上のホストに構成情報を渡す方法を指定することができます。BOOTP パラメータには、次の情報を指定します。

ブート・ファイル

クライアントの省略時のブート・イメージの完全パス名。

ブート・ファイル・サーバ・アドレス

ブート・ファイルを格納するサーバの IP アドレス。IP アドレスのフォーマットは、`ddd.ddd.ddd.ddd`です。

ブート・ファイル・サイズ

クライアント用の省略時のブート・イメージを、512 オクテット・ブロック単位で表した長さ。ファイルの長さは、10 進数で指定します。

DNS ドメイン名

ドメイン・ネーム・システムを使用してホスト名を決定する場合に、クライアントが使用するドメイン名。

DNS サーバ IP アドレス

クライアントが使用できる DNS ネーム・サーバの IP アドレスのリスト。これは任意の順番にリストできます。アドレスのフォーマットは `ddd.ddd.ddd.ddd` です。

ホーム・ディレクトリ

ブート・ファイル名で指定されていない場合の、ブート・ファイルのパス名。

ホスト IP アドレス

BOOTP クライアントのホスト IP アドレス。アドレスのフォーマットは `ddd.ddd.ddd.ddd`です。

ルータ

ルータの IP アドレスのリスト。アドレスのフォーマットは `ddd.ddd.ddd.ddd`です。

クライアント・ホスト名の送信

クライアントのホスト名を送信する場合は、「True」をチェックします。送信しない場合は「False」をチェックします。

サブネットワーク・マスク

クライアントのサブネットワーク・マスク。サブネットワーク・マスクを使用すると、アドレスにサブネットワーク番号を追加できるようになり、アドレスの割り当てがより複雑になります。DHCP 応答でサブネットワーク・マスクとルータ・オプションの両方を指定する場合は、サブネットワーク・マスク・オプションを最初に指定しなければなりません。サブネットワーク・マスクのフォーマットは `ddd.ddd.ddd.ddd` です。

TFTP ルート・ディレクトリ

TFTP (Trivial File Transfer Protocol) のルート・ディレクトリ。

サブネットワークおよびグループ構成の場合、IP レイヤ・パラメータはホスト単位の IP レイヤの操作に影響を与えます。必要な IP レイヤ・パラメータを次に示します。

ブロードキャスト・アドレス

クライアントのサブネットワークで使用中のブロードキャスト・アドレス。アドレスのフォーマットは `ddd.ddd.ddd.ddd` です。

サブネットワークはローカル

クライアントが接続される IP ネットワークのすべてのサブネットワークが、クライアントが直接接続しているネットワークのサブネットワークと同じ MTU (maximum transfer unit) を使用する場合は、「True」をチェックします。同じ MTU を使用しない場合は「False」をチェックします。クライアントは、直接接続されているネットワークのサブネットワークがより小さな MTU を使用する可能性も考慮してください。

マスクの供給

クライアントが、サブネットワーク・マスク要求に ICMP を使って応答する場合は、「True」をチェックします。それ以外の場合は「False」をチェックします。

この他のパラメータについては、『*JOIN Server Administrator's Guide*』(</usr/doc/join/TOC.html>) を参照してください。

ノード、グループ、およびサブネットワーク構成の場合、リース・パラメータを使用すると、IP リース時間に関する情報を指定することができます。リース時間は、IP アドレスが使用される時間の長さを決定します。リース・パラメータには、次の情報を指定します。

DHCP 再割り当て時間

クライアントがネットワーク上の任意のサーバに対して新しいリースを要求するまでのアドレスの割り当てからの時間間隔を秒単位で示します。

DHCP 更新時間

クライアントが元のサーバからリースされた期間を延長しようとするまでのアドレスの割り当てからの時間間隔を秒単位で示します。

リース時間

DHCP サーバが、DHCP クライアントの IP アドレスの使用を許可する時間。月、日、時間、分または秒単位で示します。たとえば 2 months 5 days 45 minutes と示します。実際のリース時間は、クライアントとサーバが決定します。

7.3 DHCP サーバの構成

xjoin ユーティリティを使用して、DHCP サーバを構成します。xjoin ユーティリティを起動するには、次のコマンドを実行します。

```
# /usr/bin/X11/xjoin
```

次に示すサーバ情報を構成することができます。

- サーバ/セキュリティ・パラメータ
- IP レンジ
- ホスト名
- サブネットワーク
- DHCP クライアント・ノード
- グループ

これらのパラメータに変更を加えた後、xjoin のウィンドウの右下にある [Add/Update] ボタンをクリックし、サーバ構成ファイルを更新します。

xjoin ユーティリティを終了するには、[File] メニューの [Exit] を選択します。詳細は、xjoin(8) および『*JOIN Server Administrator's Guide*』(</usr/doc/join/TOC.html>) を参照してください。

xjoin ユーティリティで DHCP サーバを構成した後、joind デーモンを起動して DHCP サーバを有効にします。この方法については、7.3.7 項を参照してください。

7.3.1 サーバ/セキュリティ・パラメータの構成

サーバ/セキュリティ・パラメータを構成するには、次の手順に従ってください。

1. xjoin メイン・ウィンドウで、[Server/Security] タブをクリックします。
2. ウィンドウの左側にある [Server] を選択します。
3. プルダウン・メニューから、[Server/Security] パラメータを選択します。
4. サーバ・パラメータを選択します。
5. 「True」または「False」を選択、あるいは値を入力します。
6. 構成したいすべてのサーバ・パラメータに対して、手順 4 と 5 の操作を行います。
7. [Add/Update] ボタンを選択し、新しいサーバ・パラメータでサーバを更新します。

7.3.2 IP レンジの構成

IP レンジを構成するには、次の手順に従ってください。

1. xjoin メイン・ウィンドウで、[Server/Security] タブをクリックします。
2. ウィンドウの左側にある [Server] を選択します。
3. プルダウン・メニューから [IP Range] を選択します。
4. [New IP Range] を選択します。

5. 各 IP レンジ に対して、サブネットワーク・アドレス、サーバ・アドレス、および IP レンジ を入力します。IP レンジ は次のように入力します。
 - a. サブネットワーク (ネットワーク、サブネットワーク、およびホスト・アドレス) の IP アドレス・レンジの開始アドレスを入力します。
 - b. [Tab] キーを押し、次のフィールドに移動します。
 - c. IP アドレス・レンジの終了アドレスを入力します。
6. 各々の新しい IP レンジ に対して、手順 4 と 5 の操作を行います。
7. [Add/Update] ボタンをクリックし、新しい IP レンジでサーバを更新します。

7.3.3 ホスト名リストの構成

Accept Client Name Server パラメータを False に設定する場合のみ、ホスト名リストを構成します。Accept Client Name Server パラメータを True に設定すると、サーバはクライアントが提案した名前を自動的に受け付けますので、ホスト名リストは構成しないでください。

ホスト名を構成するには、次の手順に従ってください。

1. xjoin メイン・ウィンドウで、[Server/Security] タブをクリックします。
2. ウィンドウの左側にある [Server] を選択します。
3. プルダウン・メニューから、[Hostname Lists] を選択します。
4. [New Hostname List] を選択します。
5. ドメイン名、DHCP サーバ名、ホスト名のプレフィックス、およびホスト名を入力します。
6. 各ホスト名リストに対して、手順 4 と 5 の操作を繰り返します。
7. [Add/Update] ボタンをクリックし、新しいホスト名リストでサーバを更新します。

7.3.4 サブネットワークの構成

サブネットワークを構成するには、次の手順に従ってください。

1. xjoin メイン・ウィンドウで [Subnets] タブを選択します。
2. ウィンドウの左側にある [New Record] を選択します。
3. [Name] パラメータを選択します。サブネットワーク構成の名前 (たとえば Subnet3) を入力します。
4. [Member of Group] パラメータを選択します。サブネットワークのメンバになるグループの名前を入力します。
5. [Net or Subnet IP Address] パラメータを選択します。ネットワークのサブネットワーク部分を識別するネットまたはサブネット IP アドレスを入力します。
6. [Broadcast Address] パラメータを選択します。このサブネットワークのブロードキャスト・アドレスを入力します。
7. 基本 DHCP パラメータに関する情報を入力します。これらのパラメータについては、7.2.2 項および『*JOIN Server Administrator's Guide*』(</usr/doc/join/TOC.html>) を参照してください。

[Subnets] タブのすべてのパラメータの値を変更する必要はありません。ユーザのネットワーク構成に関係するパラメータの値だけを変更します。
8. [Add/Update] ボタンをクリックし、新しいサブネットワーク構成情報でサーバを更新します。
9. `/etc/join/netmasks` ファイルを編集して、ユーザのネットワーク内の各サブネットワークに対するエントリを追加します。各エントリのフォーマットを次に示します。

```
subnet_address subnet_mask
```

7.3.5 DHCP クライアント・ノードの構成

ノードを構成するには、次の手順に従ってください。

注意

クラスタのメンバを DHCP クライアントとして使用することはできません。クラスタのメンバには静的アドレッシングを使用してください。

1. xjoin メイン・ウィンドウで [Nodes] タブを選択します。
2. ウィンドウの左側にある [New Record] を選択します。
3. [Name parameter] を選択します。ノード構成の名前 (たとえば Client5) を入力します。
4. [Hardware Type] パラメータを選択し、ノードが接続されているネットワークのタイプ (たとえば Token Ring, Ether3, Pronet, Arcnet, または 0) を入力します。
5. [Hardware Address/Client ID] パラメータを選択し、ノードのハードウェア・アドレスまたはクライアント ID を入力します。手順 5 で [Hardware Type] にゼロを定義した場合は、クライアント ID (ユーザが定義する英数字文字列) を入力します。

ノードのハードウェア・アドレス(MAC アドレス)を使用している場合は、そのアドレスを *nn:nn:nn:nn:nn:nn* のフォーマットで入力します (たとえば, 08:00:26:75:31:81)。ハードウェア・アドレスは、ワークステーションが製造された時に割り当てられ、ワークステーションの電源を入れたり、リブートしたりすると表示されます。ハードウェア・アドレスはイーサネット・アドレスとも呼ばれます。

注意

本書で使用しているアドレスは、すべて例にすぎません。実際に使用する場合は、例で出てくるアドレスを使用しないでください。

6. [Member of Group] パラメータを選択し、ノードがメンバになるグループの名前を入力します。

7. DHCP の基本パラメータに関する情報を入力します。これらのパラメータについては、7.2.2 項および『*JOIN Server Administrator's Guide*』(</usr/doc/join/TOC.html>) を参照してください。

[Nodes] タブのすべてのパラメータの値を変更する必要はありません。ユーザのネットワーク構成のためのパラメータの値だけを変更します。

8. [Add/Update] ボタンをクリックし、新しいノード構成情報でサーバを更新します。

DHCP によっては、MAC アドレス・フィールドはいつでもクライアントのネットワーク・アダプタの実 MAC アドレスであるとは限りません。以下の Microsoft クライアントは、サーバに送信する前に MAC アドレスを変更することが知られています。

- Windows 95
- Windows NT
- Windows for Workgroups with Microsoft TCP/IP

これらのクライアントはハードウェア・タイプを利用した MAC アドレスの前に置かれます。MAC アドレス・タイプは 0、長さは 7 (6 の代わり) です。たとえば、イーサネット・アドレスが 11:22:33:44:55:66 の場合、静的 IP マッピングのために次のことを指定する必要があります。

- MAC アドレス: 01:11:22:33:44:55:66
- MAC タイプ: 0
- MAC 長: 7

MAC アドレスをこのように指定しない場合、クライアントは DHCP サーバからの IP アドレスを修正するために異常終了します。

詳細については、ご使用の Microsoft 製品のドキュメントを参照してください。

7.3.6 グループ・パラメータの設定

グループを定義するには、次の手順に従ってください。

1. xjoin メイン・ウィンドウで [Groups] タブを選択します。
2. ウィンドウの左側にある [New Record] を選択します。

3. [Name parameter] を選択します。グループ構成の名前 (たとえば Global) を入力します。
4. [Member of Group] パラメータを選択します。適切であれば、新しいグループがメンバになるグループの名前を入力します。
5. [Group Members] パラメータを選択し、グループのメンバになるサブネットワーク名または他のグループ名を入力します。[Tab] キーを押して、各エントリ間を移動します。
6. DHCP の基本パラメータに関する情報を入力します。これらのパラメータについての詳細は、7.2.2 項および『*JOIN Server Administrator's Guide*』 (/usr/doc/join/TOC.html) を参照してください。
[Groups] タブのすべてのパラメータの値を変更する必要はありません。ユーザ特有のネットワーク構成を記述するパラメータの値だけを変更します。
7. [Add/Update] ボタンをクリックし、新しいグループ構成でサーバを更新します。

7.3.7 DHCP サーバの起動 (joind)

OSFINET オプション・サブセットをインストールし、インストレーション・スクリプトを実行し、サーバを構成したら、Common Desktop Environment (CDE) のアプリケーション・マネージャの SysMan Menu アプリケーションを使用して DHCP サーバを起動し、新しい構成を実装します。SysMan Menu アプリケーションを起動するには、第 1 章の指示に従ってください。

DHCP サーバを起動するには、次の手順を行ってください。

1. SysMan Menu の [ネットワーク] [追加ネットワーク・サービス] [DHCP サーバ (joind) の設定] を選択して、「DHCP サーバとしてシステムを設定」ダイアログ・ボックスを表示します。
代わりに、次のコマンドをコマンド行に入力することができます。

```
# /usr/bin/sysman joind
```


ユーティリティは、このシステムを DHCP サーバにするかどうか聞いてきます。
2. 「はい」ラジオ・ボタンを選択して、joind デーモンを使用可能にします。

3. デバッグのレベルを設定します。省略時の設定は 0 で、デバッグ情報は何も出力されません。値が高くなるほど、より詳細なデバッグ情報が生成されます。
4. 適切なラジオ・ボタンを選択して、ログ・レベルを設定します。
5. [了解] を選択して変更を保存します。ユーティリティは、変更を確認してデーモンをその場で起動するかどうか選択を求めるためのダイアログ・ボックスを表示します。
6. [はい] を選択するとデーモンが起動され、その場で変更が適用されます。[いいえ] を選択すると、変更は次にシステムをリブートした時に適用されます。
選択内容を確認するメッセージが表示されます。
7. [了解] を選択してこのメッセージを消去し、「DHCP サーバとしてシステムを設定」ダイアログ・ボックスを閉じます。

「DHCP サーバとしてシステムを設定」ダイアログ・ボックスでは、`joind` デーモンを使用不可にしたり、停止したりすることもできます。追加情報については、SysMan Menu オンライン・ヘルプを参照してください。

注意

`kill -9` コマンドを使用して DHCP サーバ・デーモンを停止しないでください。データベース・ファイルが壊れる原因になるためです。代わりに、「DHCP サーバとしてシステムを設定」ダイアログ・ボックス、または `kill -HUP` コマンドを使用してください。

`joind` デーモンの詳細については、`joind(8)` を参照してください。

7.4 DHCP の管理

この項では、次に挙げる DHCP 関連の作業の実施方法について説明します。

- DHCP クライアントの起動
- DHCP クライアント構成のモニタ
- クライアント IP アドレスの永久的なマッピング
- DHCP サーバへのアクセスの制限

- BOOTP クライアントの構成
- DHCP アドレス割り当ての無効化

7.4.1 DHCP クライアントの起動

SysMan Menu ユーティリティを使用してネットワーク・インタフェースを構成する際には、IP アドレスの取得方法を指定する必要があります。DHCP サーバによって動的に割り当てられるアドレスを使用する場合には、適切なダイアログ・ボックスで「DHCP を使用」のラジオ・ボタンを選択し、ネットワーク・サービスを再起動します。ネットワーク・インタフェースの構成についての詳細は、2.3.1 項を参照してください。

その後に DHCP クライアントが起動され、DHCP を使用して DHCP サーバから IP アドレスを取得します。これ以降、デーモンはオペレーティング・システムがブートされるたびに毎回その動作を行います。

省略時の設定では、Tru64 UNIX DHCP クライアントはホスト名も DHCP サーバから受信するものと想定します。ただし、ネットワーク環境内の DHCP サーバのタイプと構成によっては、サーバがクライアントからホスト名を受信することもあります。

さらに、サーバが、クライアントのホスト名とダイナミック IP アドレスで DNS または NIS を更新しない場合もあります。その結果、システムは正常に機能しなくなります。CDE (Common Desktop Environment) では、ローカル・システムのホスト名と IP アドレスの対応が、`/etc/hosts` データベース、DNS または NIS で一致している必要があるためです。

このような環境で DHCP サーバにホスト名を送信するようにクライアントを構成しなければならない場合は、次の手順に従います。

1. 2.3.1 項で述べたように、SysMan Menu ユーティリティでネットワーク・インタフェースを構成します。適切なダイアログ・ボックスで [Use DHCP] ラジオ・ボタンを選択します。
2. SysMan Menu を終了し、次のコマンドを入力してシステムのホスト名を設定します。

```
# rcmgr set HOSTNAME "hostname"
```

システムが DNS ドメインの一部になっている場合は、完全修飾ホスト名を指定します。たとえば、システムの名前が `yellowtail` で

tuna.ocean.com ドメイン内にある場合は「yellowtail.tuna.ocean.com」と入力します。

3. テキスト・エディタで `/etc/hosts` ファイルを開き、次のような `localhost` のエントリを見つけます。

```
127.0.0.1      localhost
```

行末にシステムのホスト名を別名として追加します。たとえば、システムのホスト名が `yellowtail` の場合は、次のように入力します。

```
127.0.0.1      localhost    yellowtail
```

4. システムをリブートします。

これでシステムは正しく動作するはずですが、システムのブートが通常より遅く、ネットワークに問題があることを示すエラー・メッセージが表示される場合は、CDE が正しく動作していないおそれがあります。必要があれば、次のようにログインしてアクセスを回復し、問題を修正してください。

1. CDE のログイン画面で [オプション] プルダウン・メニューをクリックし、[セッション] [フェイルセーフ・セッション] を選択します。
2. ログインして必要な修正を行い、リブートします。リブート時、CDE セッションは通常のデスクトップ設定に自動的に戻ります。

7.4.2 DHCP クライアント構成のモニタリング

最初の DHCP サーバの構成が終わったら、`/var/joy/log` ファイルの内容を確認するか、あるいは次の操作を行って、DHCP クライアントの状態をチェックすることができます。

1. ルートで DHCP サーバ・ホストにログインします。
2. 次のコマンドを実行して `xjoin` ユーティリティを起動します。

```
# /usr/bin/X11/xjoin
```
3. `xjoin` メイン・ウィンドウの [Server/Security] タブをクリックします。
4. プルダウン・メニューから [Active IP Snapshot] を選択します。
「Active IP Snapshot」ウィンドウに構成済みの DHCP クライアントが表示されます。

5. ウィンドウの左側にある [record] をクリックします。ウィンドウの右側は、クライアントのその時点での構成情報をすべて表示します。

xjoin ユーティリティを使用してクライアントの構成情報を修正したり、ハードウェア・アドレスを IP アドレスに永久的にマップしたり、ファイルをアクティブな IP データベースにインポートしたり、ウィンドウからレコードを削除したりできます。詳細は xjoin(8) および『*JOIN Server Administrator's Guide*』(/usr/doc/join/TOC.html) を参照してください。

7.4.3 クライアント IP アドレスの永久的なマッピング

多くの場合クライアントには、IP アドレス・プールで最初に利用できる IP アドレスが割り当てられます。ただし、クライアントのハードウェア・アドレスまたは、MAC (Media Access Control) アドレスに IP アドレスを永久にマップ、または割り当てたいこともあります。ハードウェア・アドレスにマッピングされた IP アドレスは、ユーザが定義済みの IP アドレスでなくても構いません。クライアントのハードウェア・アドレスに IP アドレスを永久にマップするためには、次の手順に従ってください。

1. ルートで DHCP サーバにログインします。
2. 次のコマンドを実行して xjoin ユーティリティを起動します。

```
# /usr/bin/X11/xjoin
```
3. xjoin メイン・ウィンドウで、[Server/Security] タブをクリックします。
4. プルダウン・メニューから [Active IP Snapshot] を選択します。
「Active IP Snapshot」ウィンドウが表示されます。
5. [New Record] を選択します。
6. 各パラメータの値を入力します。各エントリを入力したら、Return または Tab を押します。「Lease Expiration」フィールドには、IP アドレスの割当てが DHCP データベースに保管されるように、整数 -1 を指定してください(これで期限切れになりません)。
7. [Add/Update] ボタンをクリックします。これにより新しいレコードがデータベースに追加されます。
8. 各 MAC アドレスに対して、手順 5 から 7 の操作を行います。

7.4.4 DHCP サーバへのアクセスの制限

「既知の MAC アドレスに制限」サーバ・パラメータを True に設定した場合のみ、DHCP サーバへのクライアントのアクセスを制限します (詳細は 7.2.2.1 項を参照してください)。「既知の MAC アドレスに制限」サーバ・パラメータを True に設定したら、DHCP サーバへのアクセス、および DHCP サーバからの IP アドレス割り当てを受けることが許される MAC アドレスのリストを作成する必要があります。このサーバ・パラメータを False に設定した場合は、MAC アドレスのリストを作成する必要はありません。

DHCP サーバへのアクセスが許可される MAC アドレスのリストを作成するには、次の手順に従ってください。

1. xjoin メイン・ウィンドウで、[Server/Security] タブをクリックします。
2. プルダウン・メニューから [Preload MAC Addresses] を選択します。「Preload MAC Addresses」ウィンドウが表示されます。
3. [New Record] を選択します。
4. 各パラメータの値を入力します。各エントリを入力したら Return キーを押します。
5. [Add/Update] ボタンをクリックして、新しいレコードをデータベースに追加します。
6. DHCP サーバにアクセスさせたい各 MAC アドレスに対して、手順 3 から 5 の操作を行います。

上記の操作を行うかわりに、jdbmod コマンドを使用して MAC アドレス・データベースにファイルをインポートすることができます。インポートするファイルのフォーマットについての詳細は、jdbmod(8) を参照してください。

MAC アドレス・データベースからレコードを削除するには、ウィンドウの左側の [MAC address] を選択して [Delete] ボタンをクリックします。

7.4.5 BOOTP クライアントの構成

BOOTP だけを使用してクライアントを登録するには、次の手順に従ってください。

1. ルートでログインします。

2. 次のコマンドを実行して xjoin ユーティリティを起動します。

```
# /usr/bin/X11/xjoin
```

3. xjoinメイン・ウィンドウで、[Nodes] タブをクリックします。
4. ブートファイル名、ホスト IP アドレス、サブネットワーク・マスクを含む BOOTP クライアント情報、およびその他必要な情報を入力します。基本 BOOTP パラメータは、中央の欄のキー・パラメータの下にあります。他のパラメータを表示するには、プルダウン・メニューの [Basic DHCP Parameters] をクリックし [DHCP parameters] を選択します。
5. [File/Update] を選択し、これらの変更を有効にします。

7.4.6 DHCP アドレス割り当ての無効化

DHCP アドレス割り当てを使用不能にし、BOOTP および DHCP サーバ・デーモンを使用して (/usr/sbin/joind) BOOTP 要求にだけ応答したい場合もあります。DHCP および BOOTP サーバですべての DHCP アドレス割り当て機能を使用不能にするには、すべてのサブネットワークに対して IP アドレスの範囲を指定しないで(これが省略時の設定)ください。IP アドレスの範囲が定義されていなければ、DHCP クライアント要求に対してサーバが DHCP 応答を送信することはありません。

DHCP アドレス割り当てを使用不能にすると、このサーバで以前に登録した DHCP クライアントは、リース・タイムアウトになるまで有効です。つまり、サーバはクライアント・リースを更新できません。

ポイント・ツー・ポイント接続

Tru64 UNIXシステムは、Serial Line Internet Protocol (SLIP) および Point-to-Point Protocol (PPP) を使用して、ポイント・ツー・ポイント接続をサポートします。

この章では、次に挙げる接続のダイヤル・イン・システムとダイヤル・アウト・システムを準備し、構成する方法について説明します。

- SLIP 接続 (8.1 節)
- PPP 接続 (8.2 節)
- 一般的なモデム接続 (8.3 節)

SLIP のトラブルシューティング情報については 10.8 節 を、PPP のトラブルシューティング情報については 10.9 節 を参照してください。

8.1 SLIP (Serial Line Internet Protocol)

SLIP (Serial Line Internet Protocol) は、2 つのホスト間のシリアル・ライン上で IP を実行する際に使用するプロトコルです。2 つのホスト間は、直接またはモデムを使用した電話回線を通じて接続できます。TCP/IP コマンド (`rlogin`, `ftp`, `ping` など) は、SLIP 接続で実行できます。

8.1.1 SLIP 環境

SLIP 環境で、システムが非常に近接している場合には、相互に直接接続できます。また、離れている場合には、モデムと電話回線を通じて接続できます。図 8-1 に、それぞれについての単純な SLIP 構成の例を示します。図 8-2 には、2 つのシステム間の SLIP 接続について示します。ここで、HOSTB は、ゲートウェイ・システムとして動作します。

図 8-1: 単純な SLIP 構成のサンプル

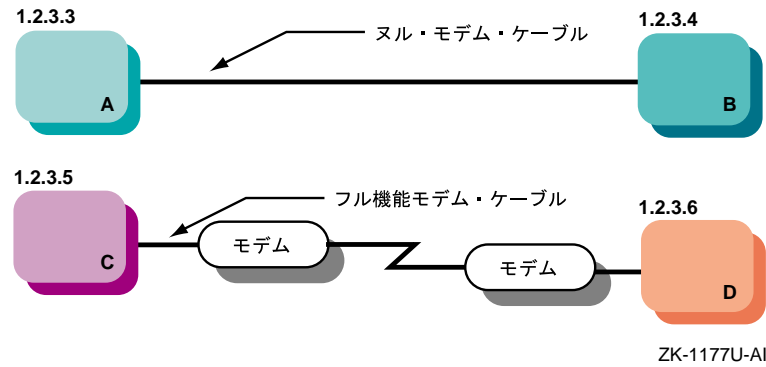
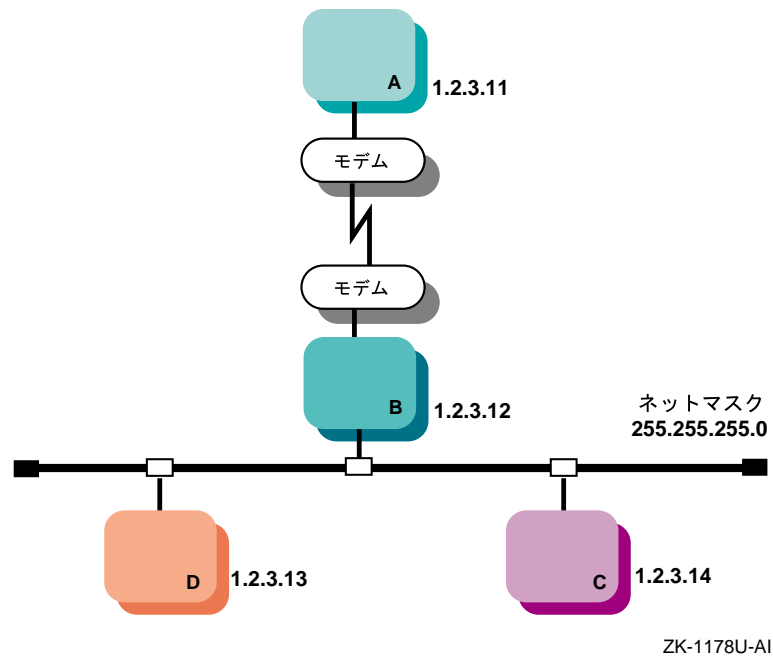


図 8-2: ゲートウェイ・システムを使用した SLIP 構成



8.1.2 SLIP の計画

この項では、SLIP を構成する前に必要な作業について説明します。

8-2 ポイント・ツー・ポイント接続

8.1.2.1 ハードウェアの確認

ハードウェアの確認を行う際には、ケーブルとモデムの両方を確認してください。

適切なケーブルを使用していることを確認してください。適切なケーブルを使用しないと、信号が劣化して、ソフトウェアが正常に機能しないおそれがあります。2 台のコンピュータを直結する場合には、以下のガイドラインに従って適切なケーブルを使用してください。

- パラレル・ケーブルではなくシリアル・ケーブルを使用します。
- 2 台のコンピュータを直結するために設計されたヌル・モデム・ケーブルを使用します。
- 少なくとも 9 芯のシールド・ケーブルを使用します (DECconnect ケーブルは、シリアル接続に使用するには芯線の数が多いので使用しません)。
- ケーブルの両端にあるコネクタのオス/メスとピン数を確認します。一般に、適切なケーブルの両端には、オスの DB25 または DB9 ピン・コネクタが付いています。使用するシリアル・ポートが不明確な場合は、コンピュータに付属のハードウェア・マニュアルを参照してください。

2 台のコンピュータがモデムと電話回線で接続されている場合、モデム・ケーブルのガイドラインについては 8.3.1 項を参照してください。

SLIP でモデムを使用する場合、最も良い結果を得るには次のガイドラインに従ってください。

- 38,400 ビット/秒 (bps) のシリアル・ポート速度を処理できるモデムを使用します。準備したモデムが 38,400 bps のシリアル・ポート速度を処理できない場合には、そのモデムで設定できる速度の最高値に設定します。
- V.42bis 圧縮に準拠している V.34bis のモデムを使用します。また、V.42bis と MNP (Microcom Network Protocol) はともに他方のプロトコルのサブセットを実装しているので、MNP をサポートするモデムも使用できます。
- モデムは 8 ビット、パリティなしに設定して、電話回線に接続します。
- 可能な場合は、ハードウェア・フロー制御を使用します。高速モデムは、回線品質が低下すると、より低いデータ・レートに頻繁にフォール・バックします。

注意

SLIP では、ソフトウェア・フロー制御 (XON/XOFF) は使用しないでください。このフロー制御を使用すると、データ・ストリームが壊れるため、IP 上の TCP 層がオーバーランに対する再送要求を発行します。

8.1.2.2 構成の準備

通信用ハードウェアを確認すると、SLIP を実行するシステムを設定できます。

図 8-3 は SLIP を構成する際に必要な情報を記録できる SLIP 設定ワークシートを示しています。この後の項では、このワークシートに記録する必要がある情報について説明します。本書をオンラインで参照している場合には、プリント機能を使用してこのワークシートをプリントできます。

図 8-3: SLIP 設定ワークシート

SLIP設定ワークシート	
接続のタイプ:	<input type="checkbox"/> ケーブル <input type="checkbox"/> モデム
システムのタイプ:	<input type="checkbox"/> ダイアル・イン <input type="checkbox"/> ダイアル・アウト
ローカル IP アドレス:	_____
ネットワーク・マスク:	_____
デスティネーション IP アドレス:	_____
ターミナル名:	_____
速度:	_____
SLIP ログイン情報:	_____
ダイアル・アウト・システム	
startslip サブコマンド:	_____

ダイアル・イン・システム	
slhosts ファイル・オプション:	_____
ゲートウェイ:	<input type="checkbox"/> Yes <input type="checkbox"/> No

接続のタイプ

2 つのシステムがヌル・モデム・ケーブルで接続されている場合は、「ケーブル」を選びます。2 つのシステムが、モデム・ケーブル、

モデム，および 1 本の電話回線で接続されている場合は「モデム」を選びます。

システムのタイプ

システムがリモート・システムからの呼び出しに応答するように設定する場合は，「Dial-in」を選びます。システムがリモート・システムを呼び出すように設定する場合は，「Dial-out」を選びます。

ローカル IP アドレス

システムの SLIP インタフェースの IP アドレス。各 SLIP インタフェースには，IP アドレスが必要です。SLIP についての詳細は，『*Tru64 UNIX 概要*』および `startslip(8)` を参照してください。

ネットワーク・マスク

ネットワークのサブネット・マスク。これは両方のシステムで同じでなければなりません。ネットワーク・マスクについての詳細は，2.2 節を参照してください。

デスティネーション IP アドレス

デスティネーション・システムの SLIP インタフェース IP アドレス。

ターミナル名

ケーブル接続している `/dev` ディレクトリにある有効なターミナル・デバイス名。これは，絶対パス名（たとえば `/dev/tty00`），または `/dev` ディレクトリ内の名前（たとえば `tty00`）のいずれでもかまいません。ターミナル・ラインの指定についての詳細は，`startslip(8)` を参照してください。ターミナル・デバイスについては，`port(7)` を参照してください。

速度

システムとシステム，またはシステムとモデムを接続する場合に使用する，シリアル・ポートの速度。省略時の速度は，9600 bps です。速度についての詳細は，`startslip(8)` を参照してください。

SLIP ログイン情報

SLIP 接続のログイン情報。これには、ユーザ名、パスワード、およびログイン・シーケンス (たとえば、ダイヤル・アウト接続で使用するログイン・プロンプト) があります。

startslip サブコマンド

表 8-1 に、ダイヤル・アウト・システムの場合に、ユーザが作成する設定スクリプト・ファイルで指定する最小限の startslip サブコマンドを示します。表 8-2 には、オプションの startslip サブコマンドを示します。

表 8-1: 必須 startslip サブコマンド

サブコマンド	必要な情報
myip	使用しているシステムの IP アドレス
dstip	デスティネーション・システムの IP アドレス
netmask	サブネットワークのネットワーク・マスク
hardwired	なし。2 つのシステムをヌル・モデム・ケーブルで接続するように指定します。
modemtype	直接接続していない場合に、使用するモデムのタイプ
opentty	シリアル・ラインと回線速度。
dial	ダイヤルする電話番号
expect	シリアル・ラインで受信する予定の情報 (たとえばログイン・シーケンス)
send	シリアル・ラインで転送したい情報
connslip	構成されているネットワーク・インタフェース。そのネットワーク・インタフェースにシリアル・ラインを接続します。

表 8-2: オプションの **startslip** サブコマンド

サブコマンド	説明
debug	指定されたログ・ファイルにデバッグ・メッセージを生成します。
gateway	デスティネーション・システムが、LAN 上の別のシステムへのゲートウェイであることを指定します。
icmpsup	ICMP (Internet Control Message Protocol) 通信を抑えます。ICMP 通信 (ping コマンドで生成されるものなど) は、SLIP 接続での送信が許可されません。これによって、より重要な通信用に回線の帯域幅が確保されます。
tcppauto	ローカル・システムは、リモート・システムが TCP ヘッダを圧縮していることを検出すると、TCP ヘッダを圧縮します。このオプションは、リモート・システムが TCP ヘッダの圧縮を行っているかどうか分からない場合に便利です。 注意: <code>tcppauto</code> オプションが両方のシステムで有効になっている場合、TCP ヘッダは圧縮されません。2 つのシステムのうちいずれかは、TCP ヘッダの圧縮を明示的に有効にしなければなりません。
tcppcomp	SLIP 接続で送信する前に TCP ヘッダを圧縮します。TCP ヘッダを圧縮すると、データ転送が速くなります。リモート・システムは、リモート・エンドに到達したときにヘッダの圧縮を解除できるように、このオプションをサポートしていなければなりません。

startslip サブコマンドの完全なリストについては、**startslip(8)** を参照してください。

slhosts ファイル・オプション

表 8-3に、ダイアル・イン・システムの場合に、`/etc/slhosts` ファイルで指定する各 SLIP リンクのオプションのリストを示します。

表 8-3: **slhosts** ファイル・オプション

サブコマンド	説明
debug	デバッグ・メッセージを生成して、 <code>daemon.log</code> ファイルに格納します。

表 8-3: slhosts ファイル・オプション (続き)

サブコマンド	説明
icmpsup	ICMP (Internet Control Message Protocol) トラフィックを制限します。ICMP トラフィック (ping コマンドで生成されるものなど) は、SLIP 接続での送信ができません。これによって、より重要な通信用に回線の帯域幅が確保されます。
tcputo	ローカル・システムは、リモート・システムが TCP ヘッダを圧縮していることを検出すると、TCP ヘッダを圧縮するように指定します。このオプションは、リモート・システムが TCP ヘッダの圧縮を行っているかどうか分からない場合に便利です。これは、省略時の設定です。
tcpcomp	SLIP 接続で送信する前に TCP ヘッダを圧縮します。TCP ヘッダを圧縮すると、データ転送が速くなります。リモート・システムは、リモート・エンドに到達したときにヘッダの圧縮を解除できるようにこのオプションをサポートしていなければなりません。tcpcomp オプションと tcputo オプションを同時に指定しないでください。

詳細については、slhosts(4) を参照してください。

ゲートウェイ

ダイヤル・イン・システムで、ご使用のシステムが LAN にアクセスする場合に、ダイヤル・アウト・システムのゲートウェイとして動作するときは、Yes を選びます。それ以外の場合には、No を選びます。

8.1.3 SLIP の構成

SLIP を構成するには、通信ハードウェアが適正なことを確認し、構成ワークシートを完成します。SLIP 環境にあるシステムは、次のいずれかの役割を果たすことができます。

- ダイヤル・イン・システム
- ダイヤル・アウト・システム

ダイヤル・イン接続とダイヤル・アウト接続の両方を構成するには、いくつかのシステム・ファイルを編集し、startslip プログラムを使用します。

8.1.3.1 ダイヤル・イン・システムの構成

ダイヤル・イン・システムを構成するには、ルートとしてログインし、次の手順を行ってください。

1. モデムを使用している場合は、ダイヤル・イン・アクセス用にモデムを設定します。詳細については、8.3.2 項を参照してください。

注意

SLIP のダイヤル・イン・アクセスには、`getty` プロセスを使用してください。

2. `/etc/passwd` ファイルを編集して、SLIP ユーザ専用のエントリを作成します。ログイン・シェル・フィールドには、`/usr/sbin/startslip` を指定します。ここに指定するログイン名は、`/etc/slhosts` ファイルでエントリを検索するのに使用します。たとえば、次のように指定します。

```
slip1:password:20:20:Remote SLIP User:/usr/users/guest:/usr/sbin/startslip
```

3. `/etc/slhosts` ファイルを編集し、ワークシートの情報を使用してログイン名のエントリを作成します。`/etc/slhosts` ファイルのエントリは、次のような構文で記述します。

login_name remote_ip local_ip netmask option

たとえば、図 8-1 でホスト D がダイヤル・イン・システムの場合は、次のようなエントリになります。

```
slip1 1.2.3.6 1.2.3.5 255.255.255.0 nodebug
```

詳細については、`slhosts(4)` を参照してください。

4. `/etc/inittab` ファイルを編集して、SLIP を実行する各ターミナル・デバイスについてエントリを作成します。`/etc/inittab` ファイルのエントリは、次の構文で記述します。

Identifier:Runlevel:Action:Command

たとえば、次のようにします。

```
nullmodem:3:respawn:/usr/sbin/getty /dev/tty00 M38400 vt100
```

詳細については、`inittab(4)` を参照してください。

- 5. `init q` コマンドを実行して、すぐに `getty` プロセスをスタートします。
- 6. LAN 上の別のシステムにアクセスするため、ダイヤル・イン・システムをダイヤル・アウト・システムへのゲートウェイにする場合は、ダイヤル・イン・システムを IP ルータとして構成してから、さらに `gated` デーモンを実行する必要があります。基本的なネットワーク設定の説明については、第 2 章を参照してください。

SLIP の使用中に問題が発生した場合は、10.8 節を参照してください。

8.1.3.2 ダイヤル・アウト・システムの構成

リモート・システムへのコールをシステムから行いたい場合は、ダイヤル・アウト接続を構成します。ダイヤル・アウト接続を構成するには、ルートとしてログインし、次の手順に従ってください。

- 1. モデムを使用している場合は、使用しているモデム名のエントリが、`/etc/acucap` ファイルにあることを確認します。`/etc/acucap` ファイルにモデムのエントリがない場合は、次の手順に従ってください。
 - a. 使用しているモデムに類似したエントリをコピーします。
 - b. 使用しているモデムの属性に合わせて、モデムの属性を変更します。このエントリの同期化文字列 (ss) に、表 8-4 にリストされている AT コマンドを含め、ダイヤル・アウト・アクセス用にモデムを設定します。もう一方のモデムの設定は、そのままかまいません。

表 8-4: ダイヤル・アウト・アクセス用のモデム・コマンド

コマンド	説明
<code>at&c1</code>	通常のキャリア検出 (CD) 動作。もう一方のモデムのキャリア検出信号を受信するまで、キャリア検出信号を ON にしないようにモデムを設定します。
<code>at&d2</code>	通常のデータ端末レディ (DTR) 動作。この設定は、DTR が OFF になった場合に回線を切るようにモデムを設定します。たとえば、ユーザがシステムからログオフした場合がこれに相当します。
<code>ate1</code>	エコーをオンにします。
<code>atq0</code>	リザルト・コードを表示します。
<code>ats0=0</code>	電話に応答しません。

さらに、デバッグ・オプション (db) を含めます。デバッグを ON にすると、モデムは、ファイル内のモデム属性の調整に使用するための補足情報を提供します。詳細については、acucap(4) を参照してください。

2. `getty` コマンドを使用してモデムからシステムにアクセスする場合に、すでに `getty` プロセスが実行されているときは、次の手順に従ってください。

- a. `/etc/inittab` ファイルを編集して、モデム・エントリのアクション・フィールドを、次のように `respawn` から `off` に変更します。

```
modem:23:off:/usr/sbin/getty /dev/tty00 M38400 vt100
```

詳細については、`inittab(4)` を参照してください。

- b. `init q` コマンドを実行して、`getty` プロセスを終了します。

3. `/usr/spool/locks` ディレクトリ内で `LCK..ttypn` ロック・ファイルの有無を調べます。SLIP 用に構成している端末デバイスのロック・ファイルがあれば、それを削除してください。

端末デバイス経由で接続を確立すると、他のアプリケーションによって接続が切られないようにするために、システムがロック・ファイルを生成します。この接続が正しい手続きを経ずに切断されると、ロック・ファイルが残り、新しい接続が確立できなくなります。

4. SLIP ダイアル・アウト接続用の `startslip` サブコマンドを含むファイルを作成するには、次の手順に従ってください。

- a. 新しいスクリプト・ファイルに、`startslip(8)` からサンプル・スクリプト・ファイルをコピーします。
- b. `tip` コマンドを使用して、リモート・システムにダイアル・アウトしてログインし、ワークシートにあるプロンプトおよびログイン・シーケンスをそのまま書き込みます。
- c. スクリプト・ファイルを編集し、プロンプトとログインの情報を使用して `expect` サブコマンドを変更します。次に、ワークシートの情報を使用して、その他のサブコマンドを変更します。

注意

サンプル・スクリプト・ファイルは、ファイルの先頭で `debug` サブコマンドとデバッグ・ファイル名を指定しています。

詳細については、`startslip(8)` を参照してください。

5. `-i filename` オプションを使用して、`startslip` コマンドを呼び出します。`filename` には、`startslip` サブコマンドを含んでいるファイルの名前を指定します。

`startslip` コマンドは、接続するとバックグラウンドで実行されます。電話番号 (存在する場合) およびプロセス ID は、`/var/run/ttyxx.tel-pid` ファイルにログが取られます。

SLIP の使用中に問題が発生した場合は、10.8 節を参照してください。

8.1.4 SLIP ダイアル・アウト接続の終了

SLIP ダイアル・アウト接続を終了するには、次の手順に従ってください。

1. 次のコマンドを使用して、強制終了する `startslip` プロセスのプロセス ID を調べます。

```
# cat /var/run/ttyxx.tel-pid
phonenum 8021455 pid 821
```

このコマンドの `ttyxx` には、SLIP 接続に使用するターミナル・ラインを指定します。システムで複数の SLIP 接続を行っている場合に、`/var/run` ディレクトリには、複数のファイルが存在します。

2. 手順 1 で特定したプロセス ID を指定し、次のコマンドを使用して、`startslip` プロセスを強制終了します。

```
# kill 821
```

`SIGKILL` (`kill -9`) は使用しないでください。このプロセスを `SIGKILL` で終了させると、`tty` ファイルが壊れてしまう可能性があります。

また、モデムの電源を切ってダイアル・アウト接続を終了する方法もあります。

8.2 PPP (Point-to-Point Protocol)

PPP (Point-to-Point Protocol) では、シリアル・リンクでデータグラムを送信する標準的な方法と、リンクの両端にあるシステム (ピア) がリンクのさまざまなオプション特性を折衝するための標準的な方法が提供されます。PPP を使用すると、シリアル・リンクで IP データグラムを送信することができ、ピア・マシン間で TCP/IP 接続ができます。

Tru64 UNIX の PPP サブシステムは、パブリック・ドメインの `ppp-2.3.1` がベースになっており、IP データグラムをサポートしています。PPP についての詳細は、RFC 1661、RFC 1662、RFC 1332、および RFC 1334 を参照してください。

2 つのシステム間で PPP 接続を確立するということは、基本的には、リンクの両端でシリアル・リンクを設定し、`pppd` デーモンを実行することを意味します。

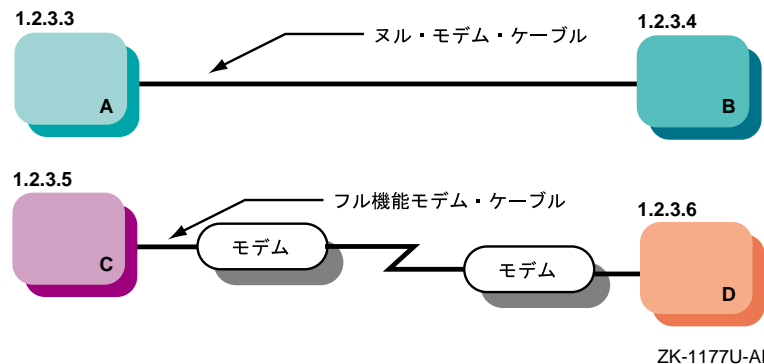
PPP 環境内のシステムは次の役割を持ちます。

- ダイアル・アウト・システム
- ダイアル・イン・システム

8.2.1 PPP 環境

非常に近接している PPP を使用しているシステムは、相互に直接接続することができます。また、離れている場合も、モデムと電話回線を通じて接続できます。図 8-4 に、相互に接続された 2 つのシステム間の PPP 接続の例を 2 つ示します。

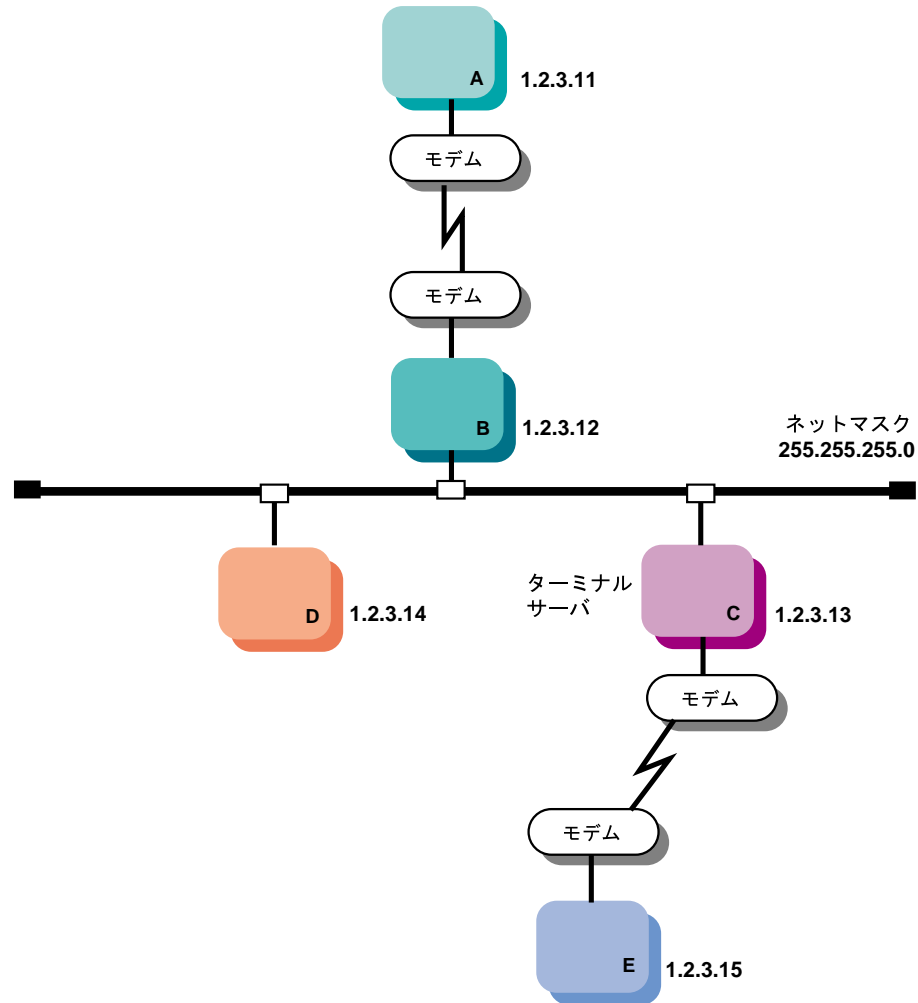
図 8-4: 単純な PPP の構成



ZK-1177U-AI

図 8-5は、2つの PPP 接続を示します。1つ目は、ホスト A とホスト B の間にあり、ホスト B がゲートウェイ・システムとして動作しています。2つ目は、パーソナル・コンピュータ E とホスト D の間にあり、ターミナル・サーバ C を介しています。後者の構成は、自宅で仕事をしている従業員がワーク・システムにダイヤル・インする場合に、ごく一般的に使用されるものです。

図 8-5: ネットワーク PPP 構成



ZK-1176U-AI

8.2.1.1 chat スクリプト

chat スクリプトを使用すると、PPP 接続のダイヤル・アウト処理を自動化することができます。リモート・システムからの出力を待ち、指定どおりの応答を返すように構成することができます。

chat スクリプトのそれぞれのエントリは、次の形式になっています。

string_chat_expects string_chat_sends

たとえば、chat スクリプトには、次のような情報が含まれることがあります。

```
ABORT "NO CARRIER" 1
ABORT "NO DIALTONE"
ABORT "ERROR"
ABORT "NO ANSWER"
ABORT "BUSY"
"" at 2
"" atdt2135476 3
CONNECT 4
login: myname 5
Password: "\qmypassword" 6
"$ " "\qpppd" 7
```

この chat スクリプトが実行されると、次の処理が実行されます。

- 1 指定したメッセージを受信したときには、PPP 接続を終了するように chat プログラムに指示します。
- 2 chat プログラムがモデムを初期化します。
- 3 chat プログラムは何も待たず、モデムにダイヤル・コマンドを送信します。
- 4 chat プログラムは CONNECT メッセージを待ち、キャリッジ・リターンを送信します (暗黙に指定)。
- 5 chat プログラムは login: 文字列を待ち、myname 文字列を送信します。
- 6 chat プログラムは Password: 文字列を待ち、mypassword 文字列を送信します。 \q により、-v オプションを使用すると、chat はパスワードを記録できなくなります。
- 7 chat プログラムはシェル・プロンプト (\$) を待ち、pppd を送信して、リモート・コンピュータで pppd デーモンを起動します。 \q により、以前の \q の効果が取り消されます。

接続するそれぞれのリモート・システムに対して、ユニークな chat スクリプトを作成することができます。スクリプトが完成したら、pppd デーモンの引数として chat コマンド文字列を指定することで、そのスクリプトを使用してシステムに接続することができます。たとえば次のようにします。

```
% pppd /dev/tty01 38400 connect 'chat -f /etc/ppp/chat-script'
```

このコマンドを実行すると、pppd デーモンはシリアル・ポートをオープンして、chat プログラムがリモート・モデムにダイヤル・アウトできるようにします。chat プログラムがモデム接続を確立すると、pppd デーモンはその後、リモート・システムとの間で PPP 接続のネゴシエーションを行います。

chat コマンドおよび chat スクリプトの詳細については、chat(8) を参照してください。

8.2.1.2 PPP オプション

pppd を呼び出す場合には、コマンド行に PPP オプションを指定できます。これらのオプションは、接続の速度、ローカルおよびリモート IP アドレス、ネットワーク・インタフェースのネットマスクといった基本の設定をすることができます。また、フロー制御のタイプ、権限、使用するルーティングといった高度な構成をすることもできます。

PPP 接続を初期化するたびに、ある一定の設定を使用する場合は、次のファイルを編集することによって、接続の都度自動的にこれらの設定を使用可能にすることができます。

- /etc/ppp/options — このファイルには、ユーザの省略時設定オプションやコマンド行オプションの前に読み取られる、システムの省略時設定オプションが含まれています。このファイルには、pppd デーモンを実行するときに常に使用する必要があるオプションが、すべて含まれています。

注意

/etc/ppp/options ファイルが存在し、pppd から読み取り可能でなければなりません。そうでない場合、デーモンは実行されません。このファイルには、root だけが書き込めるようにアクセス許可を設定してください。

- /etc/ppp/options.tty.xx
このファイルには、シリアル・ポート (/tty.xx) 固有のオプションが含まれています
- \$HOME/.ppprc

このファイルには、コマンド行オプションの前に読み取られる、ユーザの省略時設定オプションが含まれています。

構成によっては、一定のパラメータでは、あるオプション・ファイルは他のファイルを抑えることもあります。たとえば、`/etc/ppp/options` ファイルのパラメータの値の 1 セットを指定するとします。すると `/etc/ppp/options.tty.xx` ファイルにある同じパラメータの値の違うセットを指定することになり、指定したシリアル・ポートを介して接続する際には、後者のファイルの設定が使用されます。

SysMan Menu ユーティリティで PPP オプション・ファイルの作成と変更ができます (詳細は 8.2.3.2 項を参照してください)。また、オプション・ファイルのテンプレートを `/etc/ppp.common/options` から `/etc/ppp` ディレクトリにコピーして、その新しいファイルをテキスト・エディタで編集することもできます。

pppd オプションについての説明は、`pppd(8)` を参照してください。

8.2.1.3 認証

PPP を構成するときには、以下の 3 つのプロトコルのいずれかを実装して、ピア・システムの身元を確認できます。これらのプロトコルは、それぞれパスワードまたはシークレットを交換して認証処理を実施します。

- PAP (Password Authentication Protocol)

通常のログイン処理と似ています。クライアントがユーザ名とパスワードをサーバ・システムに送信し、サーバがそれを信頼できるユーザのデータベースと比較します。ログイン情報がデータベース内の情報と一致すると、サーバは PPP 接続を許可します。

- CHAP (Challenge Handshake Authentication Protocol)

サーバは、自身のローカル・システム名と、ランダムに生成したチャレンジ文字列をクライアント・システムに送信します。クライアントはサーバのシステム名を使用して、関連するシークレットをデータベース内で検索します。次に、シークレットとチャレンジ文字列の組み合わせを元にして暗号化した応答を作成してサーバに送信します。サーバ側で同じ結果が得られた場合は、クライアントがシークレットを知っていることが確認され、PPP 接続が許可されます。

- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)

Microsoft 社独自のプロトコル。CHAP と似ていますが、サーバがローカル・システム名をクライアント・システムに送信しない点が異なります。データベース内で正しいシークレットを検索するには、クライアント・システムがサーバのシステム名を事前に知っていなければなりません。また、暗号化されたチャレンジ応答を生成する際に、クライアントはログイン用に、関連するユーザ名をサーバに送ります。ドメイン名も送ることがあります。

CHAP ベースのプロトコルでは、高いセキュリティが得られます。これは、認証に使用するシークレットが暗号化されるためです。PAP シークレットの暗号化はオプションです。さらに、ログイン処理の後も、CHAP ベースのプロトコルはクライアント・システムの正当性を定期的を確認します。PAP ではクライアントの認証を 1 度しか行わないため、第 3 者が間に入って、クライアントに成りすますことができます。

ダイヤル・アウト・システムを構成している場合は、インターネットのサービス・プロバイダに連絡して、使用している暗号化のタイプを確認してから、適切な PPP オプションとシークレットをシステムに設定しなければなりません。ダイヤル・イン・システムを構成している場合は、使用している環境に必要なセキュリティのレベルを決定しなければなりません。高い安全性を必要とする接続には、CHAP ベースの認証プロトコルを使用することをお勧めします。

SysMan Menu を使用すると、各プロトコルで使用するデータベース・ファイルを作成して編集することができます (詳細は 8.2.3.2 項を参照)。またはオプションとして、テキスト・エディタを使用して、以下のいずれかの形式のエントリを作成することでファイルを管理することもできます。ファイルを保存する際は、読み取りアクセスがルート・ユーザのみに許されていることを確認してください。そうしないと、システム上の他のユーザがパスワードやシークレットを参照できてしまいます。

注意

/etc/ppp ディレクトリには、認証に使用されるシークレット情報のファイルが置かれています。NFS を用いてエクスポートされた他のホストからアクセスできるようなパーティションには、このディレクトリを配置しないでください。

PAP シークレットは `/etc/ppp/pap-secrets` ファイルに格納されており、次のような形式です。

client server secret [address...]

- *client* — 認証されるクライアントの名前、またはユーザのログイン名。 特定しない場合はワイルドカード (*) を使用します。
- *server* — 認証を要求するマシンの名前。 特定しない場合はワイルドカード (*) を使用します。
- *secret* — クライアントとサーバの両方が知っているパスワードまたはシークレット。
- *address* — クライアントが使用できるゼロ個以上のホスト名または IP アドレス (このフィールドはサーバでのみ使用します)。

たとえば、ユーザ名が `ichiro` でパスワードが `blade` のユーザが、サーバ `gatekeeper.forest.com` への接続に PAP 認証を使用しなければならない場合、各マシンの `/etc/ppp/pap-secrets` ファイルには次のようなエントリが必要です。

```
ichiro gatekeeper.forest.com blade
```

サーバの管理者がクライアント・システムを特定のホスト名に限定したい場合、サーバの `/etc/ppp/pap-secrets` ファイルでは、`address` フィールドを次のように記述する必要があります。

```
ichiro gatekeeper.forest.com blade palm.forest.com
```

CHAP シークレットは `/etc/ppp/chap-secrets` ファイルに格納されており、次のような形式です。

client server secret [address...]

- *client* — 認証されるクライアントの名前。
- *server* — 認証を要求するマシンの名前。
- *secret* — クライアントとサーバの両方が知っているパスワードまたはシークレット。
- *address* — クライアントが使用できるゼロ個以上のホスト名または IP アドレス (このフィールドはサーバでのみ使用します)。

たとえば、home という名前のクライアントが、サーバ work への接続に CHAP 認証を使用しなければならない場合、各マシンの /etc/ppp/chap-secrets ファイルには、次のようなエントリが必要です。

```
home    work    "open sesame"
```

この例に示すように、シークレットに空白が含まれている場合は、1つのフィールドと解釈させるために引用符で囲む必要があります。

サーバの管理者がクライアント・システムを特定のホスト名に限定したい場合、/etc/ppp/chap-secrets ファイルでは、address フィールドを次のように記述する必要があります。

```
home    work    "open sesame"  home.gingerbread.com house.gingerbread.com
```

この場合、クライアントは、サーバに接続した際に home または house として認識されます。

MS-CHAP シークレットも /etc/ppp/chap-secrets ファイルに格納されていますが、エントリの形式は次のようになっています。

username server secret

- *user* — 認証されるユーザのログイン名。Microsoft のドメイン名を含めることができます。
- *server* — 認証を要求するマシンの名前。 特定しない場合はワイルドカード (*) を使用します。
- *secret* — クライアントとサーバの両方が知っているパスワードまたはシークレット。

たとえば、Tru64 UNIX クライアントのユーザ bill が、Microsoft Windows RAS サーバ keymaster へのダイヤル・アウトで MS-CHAP 認証を使用しなければならない場合、Tru64 UNIX クライアントの /etc/ppp/chap-secrets ファイルには、次のようなエントリが必要です。

```
bill    keymaster    fireworks
```

サーバがスタンドアロン・システムでない場合は、エントリを次のように指定します。ここで、finance は、Microsoft Windows ネットワークのドメイン名です。

```
finance\\bill    *    fireworks
```

Microsoft Windows RAS サーバを使用したダイヤル・アウト接続の設定についての詳細は、8.2.3.6 項を参照してください。

8.2.2 PPP の準備

この項では、PPP を構成する前に行う必要がある作業について説明します。

8.2.2.1 ハードウェアの確認

PPP で使用するハードウェアを確認する際には、SLIP と同じ一般的なガイドラインが使用できます。 8.1.2.1 項 を参照してください。

8.2.2.2 カーネルでの PPP サポートの確認

次のコマンドを入力することによって、PPP がカーネル内でサポートされていることを確認します。

```
# sysconfig -s ppp
```

PPP がロードされず構成できない場合は、次のことを行います。

1. ルートとしてログインします。
2. doconfig プログラムを実行し、Point-to-Point (PPP) オプションを選択して、カーネルを再作成します。
3. 現在の /vmunix カーネル・ファイルのバックアップ・コピーを作成します。
4. 新たに作成した /sys/HOSTNAME/vmunix カーネル・ファイルを /vmunix ファイルにコピーします。
5. システムをリブートします。

8.2.2.3 構成の準備

カーネルでの PPP サポートを確認したら、PPP を構成することができます。必要に応じて、以降の項で説明している内容を参照して、PPP 接続を確立するために必要な PPP オプションを把握してください。

これらの項では、一般的に使用される PPP オプションについてのみ説明しています。PPP オプションの詳細については、pppd(8) と SysMan Menu のオンライン・ヘルプを参照してください。

8.2.2.3.1 基本的な接続オプション

図 8-6 に、PPP 設定のワークシートを示します。ここでは、このワークシートに記入する情報について説明します。本書をオンラインで参照している場合は、印刷機能でワークシートを印刷してください。

図 8-6: PPP 設定ワークシート

PPP設定ワークシート	
システムのタイプ:	<input type="checkbox"/> ダイヤル・イン <input type="checkbox"/> ダイヤル・アウト
ローカル IP アドレス:	_____
リモート IP アドレス:	_____
ネットワーク・マスク:	_____
ターミナル名:	_____
速度:	_____
認証レベル:	_____
認証タイプ:	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP
オプション:	_____

システムのタイプ

システムがリモート・システムからの呼び出しに応答する場合は、「Dial-in」にチェックをします。システムがリモート・システムへ呼び出しをプレースする場合は、「Dial-out」にチェックをします。

ローカル IP アドレス

ローカル・システムの IP アドレス。

ダイヤル・イン・システムでは、システムをローカル・エリア・ネットワーク用に構成済みの場合、このアドレスはすでに割り当てられています。これはプライマリ・ネットワーク・インタフェースのアドレスです。システムがインターネットに接続されていない場合は、IP アドレスを割り当てなければなりません。

ダイヤル・アウト・システムでは、ISP に接続する場合、通常は ISP が IP アドレスを割り当てます。IP アドレスを指定する必要はありません。アドレスの割り当てを行わないリモート・ホストに接続する場合、そのホストがすでにインターネットに接続されていれば、ローカル・システムには、リモート・ホストと同じサブネットワークのアドレスを割

り当てます。リモート・ホストがインターネットに接続されていなければ、任意の IP アドレスをローカル・システムに割り当てます。

インターネットに接続されていない 2 つのシステムの間に PPP 接続を設定する場合、192.168.*.* の範囲のアドレスが使用できます。このアドレスは、RFC 1918 によって、プライベート・ネットワーク用に確保されています。

リモート IP アドレス

リモート・システムの IP アドレス。

ダイアル・イン・システムでは、リモート・システム自身が割り当てたアドレスを使用することもできますが、セキュリティ上は、ローカル・システムがリモート・ホストにアドレスを割り当てる方が良いでしょう。

ダイアル・アウト・システムでは、ISP に接続する場合、通常はこのアドレスを指定する必要はありません。他のタイプのリモート・ホストに接続する場合は、セキュリティを強化するために、このアドレスを指定した方が良いでしょう。

ネットワーク・マスク

ご使用のネットワークのサブネットワーク・マスク。両方のシステムで同じでなければなりません。ネットワーク・マスクについての詳細は、2.2 節を参照してください。

ダイアル・アウト・システムでは、ISP に接続する場合、通常はネットワーク・マスクを指定する必要はありません。

ターミナル名

/dev ディレクトリにある有効なターミナル・デバイスの名前です。これは、絶対パス名 (たとえば /dev/tty01)、または /dev ディレクトリ内の名前 (たとえば tty01) のいずれでもかまいません。ターミナル・デバイスの詳細については、ports(7) を参照してください。

速度

システム間の接続に使用するモデム (またはヌル・モデム) とターミナル・ライン仕様の速度です。モデムが回線速度を自動的に検知するか、またはホスト間の接続にヌル・モデム・ケーブルを使用している場

合には、ホストがサポートできる最大レートまで任意のレートを指定できます。通常は 38400 bps です。

ワークシートの「アドレス解決とルーティング」セクションでは、ローカル・アドレスとルーティング・テーブルへの変更を制御するためのオプションを記述します。また、ローカル IP アドレスの割り当てを制御するオプションについても記述します。

ARP (Address Resolution Protocol)

ダイヤル・イン接続で、ローカル・システムの ARP テーブルにリモート・システムのエントリを明示的に追加する場合は、「追加」を選択します。明示的にエントリを追加しない場合は、「無効」を選択します。

必要に応じてシステムが ARP テーブルを自動的に変更できるようにする場合は、「自動」を選択します。

システム・ルーティング・テーブル

ダイヤル・アウト接続で、リモート・ゲートウェイ・システムのエントリをローカル・システムのルーティング・テーブルに明示的に追加する場合は、「追加」を選択します。明示的にエントリを追加しない場合は、「無効」を選択します。

必要に応じてシステムがルーティング・テーブルを自動的に変更できるようにする場合は、「自動」を選択します。

IP アドレス・ネゴシエーションの無効化

リモート・システムにローカル IP アドレスを受け入れさせたいときには、「Yes」を選択します。リモート・システムがローカル IP アドレスを指定するようにしたい場合は、「No」を選択します。

ピアによるローカル IP アドレスの指定

リモート・システム (ISP) がローカル IP アドレスを割り当てるようにしたい場合は、「Yes」を選択します。自分でローカル IP アドレスを指定したい場合は、「No」を選択します。

ワークシートの「通信」セクションには、性能と信頼性を改善するために PPP 接続を微調整する際のオプションを記述します。

注意

接続を確立できない場合や接続を維持できない場合を除いて、この設定は変更しない方が良いでしょう。

MRU (Maximum Receive Unit)

システムが受信できるパケットの最大サイズ (バイト数) を指定します。IPv4 リンクでは、MRU の最小値は 128 ですが、最良の値は 296 (TCP/IP ヘッダに 40 バイト、データに 256 バイト) です。省略時の PPP options ファイルでは 296 です。

IPv6 接続では、MRU の最小値は 1298 ですが、最良の値は 1500 です。カーネルで IPv6 が有効になっている場合、使用するかどうかにかかわらず、PPP は自動的に IPv6 アドレスを構成します。そのため、MRU の値は 1298 以上に設定する必要があります。あるいは、PPP リンクで IPv6 を使用しない場合は、noip6 オプションを指定します。noip6 オプションは、SysMan Menu では指定できません。コマンド行の pppd コマンドで指定するか、または手動で適切な options ファイルを編集して指定する必要があります。options ファイルの詳細は 8.2.1.2 項を参照してください。

非同期文字変換マップ

シリアル回線では受信できない制御文字を含む、32 ビットの 16 進数を指定します。この値は、省略時の 200a000 のままにしておくことをお勧めします。この値は、シリアル・リンクに telnet リンクが含まれる場合に適した値です。

ソフトウェア・フロー制御

システムがハードウェア・フロー制御をサポートしていない場合は、「Yes」を選択してソフトウェア・フロー制御 (XON/XOFF) を有効にします。それ以外の場合は「No」を選択してソフトウェア・フロー制御をしないことをお勧めします。

ハードウェア・フロー制御

明示的にハードウェア・フロー制御 (RTS/CTS) を有効にするには、「有効」を選択します。明示的にハードウェア・フロー制御を無効にするには、「無効」を選択します。

省略時の「変更しない」のままにしておき、可能な場合にはシリアル接続のハードウェア・フロー制御を行うようにすることをお勧めします。

最大 **LCP** エコー要求

接続を切る前に送信する LCP (Link Control Protocol) エコー要求フレームの最大数を指定します。省略時設定の LCP エコー要求フレーム送信回数である 5 回を過ぎても、ローカル・システムがリモート・システムから応答を受信しない場合は、リンクがアクティブでないと見なし、接続を切ります。

LCP エコー要求間隔

ローカル・システムが LCP エコー要求フレームをリモート・システムに送信する間隔を指定します。省略時の値は 60 秒です。

デバッグの有効化

デバッグを有効にする場合は「Yes」、有効にしない場合は「No」を選択します。

メッセージはすべて、`/etc/syslog.conf` ファイルで指定されたファイルに書き込まれます。接続できないか、接続を維持できない場合は、ログ・ファイルを利用してトラブルシューティングができます。

8.2.2.3.2 認証オプション

図 8-7 に、PPP 認証ワークシートを示します。ここでは、このワークシートに記入する情報について説明します。本書をオンラインで参照している場合は、印刷機能でワークシートを印刷してください。

注意

認証は、ピア・システムとの最初の接続が成功するまで有効にしないようにしてください。

図 8-7: PPP 認証ワークシート

PPP 認証ワークシート	
ダイヤルアウト用ローカル・システム:	_____
ドメイン名:	_____
リモート・システム名:	_____
ピア認証:	<input type="checkbox"/> 自動 <input type="checkbox"/> 必要 <input type="checkbox"/> 無効
ダイヤルイン用ローカル・システム名:	<input type="checkbox"/> 自動 <input type="checkbox"/> ホスト名
	<input type="checkbox"/> システム名: _____
PAP 認証:	<input type="checkbox"/> 自動 <input type="checkbox"/> 必要 <input type="checkbox"/> 無効
PAP 認証用ユーザ名:	_____
PAPに/etc/passwd を使用:	<input type="checkbox"/> Yes <input type="checkbox"/> No
PAPシークレット・ファイルの暗号化:	<input type="checkbox"/> Yes <input type="checkbox"/> No
CHAP 認証:	<input type="checkbox"/> 自動 <input type="checkbox"/> 必要 <input type="checkbox"/> 無効

ダイヤル・アウト用ローカル・システム名

ダイヤル・アウト認証のためのローカル・システム名を指定します。

ドメイン名

ダイヤル・アウト認証のためのローカル・システム名に付加するドメイン名を指定します。

リモート・システム名

ダイヤル・アウトまたはダイヤル・イン認証のためのリモート・システム名を指定します。

ピア認証

リモート・ホストが、あらかじめ割り当てられたものと同じホスト名と IP アドレスを指定して、認証を受けるように強制したい場合は、「必要」を選択します。認証を必要としない場合は「無効」を選択します。システムが自動的に認証要求に応答するようにするには、「自動」を選択します。

一般に、システムが LAN に接続されている場合は、リモート・ホストが認証を受けるように強制し、リモート・ホストの IP アドレスを身元に基づいて制限することをお勧めします。認証を強制しない場

合、リモート・ホストは、ローカル・サブネット上の他のホストに成りますことがあります。

ダイヤル・イン用ローカル・システム名

ダイヤル・イン・システムで、ホスト名をローカル・システム名として使用する場合には、「ホスト名」を選択します。システムが自動的にローカル・システム名を選択する(ホスト名、または未定義の場合はリモート・システムが選択した名前として)ようにするには、「自動」を選択します。

特定のローカル・システム名を指定する必要がある場合は、フィールドにそれを記入します。

認証が有効な場合、ローカル・システム名は、リモート・システムが期待しているシステム名と一致していなければなりません。ただし、`/etc/rc.config` ファイル内で定義されているローカル・システムのホスト名と一致している必要はありません。

PAP 認証

リモート・ホストが PAP 認証を受けるように強制したい場合は、「必要」を選択します。PAP 認証を必要としない場合や PAP 認証に回答しない場合は「無効」を選択します。

システムが自動的に PAP 認証要求に回答するようにするには、「自動」を選択します。

PAP 認証用ユーザ名

PAP 認証用のユーザ名を指定します。リモート・ホストが PAP 認証を必要とする場合、`pppd` コマンド行にユーザ名を指定する必要があります。8.2.3.5 項を参照してください。

PAP に `/etc/passwd` を使用

PAP 認証に `/etc/ppp/pap-secrets` ファイル以外に `/etc/passwd` ファイルも使用する場合は、「Yes」を選択します。それ以外の場合は「No」を選択します。

PAP シークレット・ファイルの暗号化

PAP 認証に暗号化したシークレットのみを使用する場合は「Yes」を選択します。それ以外の場合は「No」を選択します。

CHAP 認証

リモート・ホストが CHAP 認証を受けるように強制したい場合は、「必要」を選択します。CHAP 認証を必要としない場合や CHAP 認証に応答しない場合は「無効」を選択します。

システムが自動的に CHAP 認証要求に応答するようにするには、「自動」を選択します。

8.2.3 PPP を使用したダイアル・アウト・システムの構成

システムがリモート・システムに発呼する場合には、次のタスクを実行して、ダイアル・アウト接続を確立しなければなりません。

- 初期通信の設定
- options ファイルの作成
- シークレット・ファイルの作成
- メッセージ・ロギングの設定
- PPP 接続の開始

以下の各項では、これらの構成タスクについて説明します。8.2.3.6 項では、Microsoft Windows Remote Access Server (RAS) に接続する場合に必要な追加手順について説明します。

8.2.3.1 ダイアル・アウト・システムの初期通信の設定

システムをモデムに物理的に接続するか、またはリモート・システムに直結した後、次の手順を実行します。

1. /usr/spool/locks ディレクトリ内で LCK..tty`nn` ロック・ファイルの有無を調べます。PPP 用に構成している端末デバイスのロック・ファイルがあれば、それを削除してください。

端末デバイス経由で接続を確立すると、他のアプリケーションによって接続が切られないようにするために、システムがロック・ファイルを生

成します。この接続が正しい手続きを経ずに切断されると、ロック・ファイルが残り、新しい接続が確立できなくなります。

2. モデムを使用して PPP 接続を確立する場合は、モデムとの通信ができることを確認します。
 - a. `/etc/remote` ファイルを編集して、`kdebug` エントリをコピーします。
 - b. 新しいエントリを修正して、システム名、端末デバイス名 (システムに応じて `tty00` または `tty01`)、速度、パリティを指定します。詳細については `remote(4)` を参照してください。
 - c. `tip` コマンドを使用して、次のようにモデムにアクセスします。

```
% tip system_name
```

`system_name` は、`/etc/remote` ファイルに格納されています。
 - d. モデムが AT コマンド言語を使用している場合には、次のコマンドを入力します。

```
at RETURN
```

モデムが quiet モードでなければ、OK メッセージで応答します。モデムが動作していることが確認できたら、`~` と `Ctrl/D (~^D)`、または `~` とピリオド (`~.`) を入力して `tip` セッションを終了します。`tip` コマンドの詳細については `tip(1)` を参照してください。
3. リモート・システムの管理者またはインターネット・サービス・プロバイダ (ISP) に問い合わせ、次の情報を入手します。
 - リモート・システムが動的に割り当てる場合を除き、リモート IP アドレスとネットマスク
 - エスケープ処理を実行する必要がある文字
 - リモート・サービスにログインして使用する方法
4. 8.2.1.1 項の説明に従って `chat` スクリプトを作成し、ダイアル・アウト処理を自動化します。

————— 注意 —————

`tip` コマンドを使用すると、ダイアル・アウトしてリモート・システムにログインし、接続処理に関する追加情報を収

集することができます。 chat スクリプトで使用するための
正確なプロンプト，ログイン・シーケンス，pppd スタート
アップ・シーケンスを記録しておきます。

8.2.3.2 ダイアル・アウト・システムの options ファイルの作成

Common Desktop Environment (CDE) のアプリケーション・マネージャの
SysMan Menu を使用して，PPP の options ファイルを作成します。 SysMan
Menu アプリケーションを起動するには，1.2.1 項 の手順に従ってください。

ダイアル・アウト・システムの options ファイルを作成するには，次の手順
に従ってください。

1. SysMan Menu から [ネットワーク] [追加ネットワーク・サービス]
[シリアル・ライン・ネットワーク] [Point-to-Point Protocol (PPP)]
[オプション・ファイルの作成] を選択して，「PPP オプション・ファイ
ルの設定」ダイアログ・ボックスを表示します。

代わりに，次のコマンドをコマンド行から入力することもできます。

```
# /usr/bin/sysman ppp_options
```

2. 表示されるリストからファイルを 1 つクリックし，[修正] を選択します。
あるいは，次の手順を実行して，新しい options ファイルを作成します。
 - a. [新規ファイル...] オプションを選択して，「Create PPP オプショ
ン・ファイル名」ダイアログ・ボックスを表示します。
 - b. 新しいファイル名を入力し，[了解] をクリックします。

「PPP オプション・ファイルの修正」ダイアログ・ボックスが表示
されます。

3. [Dial-Out Options の設定] を選択し [設定] をクリックして，「Dial-Out
Options の設定」ダイアログ・ボックスを表示します。 PPP 設定ワーク
シートで収集した情報を使用して，各フィールドに入力します。

pppd オプションの完全なリストについては，pppd(8) とオンライン・ヘル
プを参照してください。

4. [了解] を選択し，「Dial-Out Options の設定」ダイアログ・ボック
スを閉じます。

5. 追加の PPP オプションを構成するには、[Advanced PPP Options] を選択します。対応するダイアログ・ボックス内で各メニューを選択し、PPP 設定ワークシートと PPP 認証ワークシートで収集した情報を、必要に応じてフィールドに入力します。
終了したら、「Advanced PPP Options」ダイアログ・ボックスで [了解] を選択してダイアログ・ボックスを閉じます。
6. 「PPP オプション・ファイルの修正」ダイアログ・ボックスの [了解] を選択して変更を保存し、ダイアログ・ボックスを閉じます。
7. [終了] を選択し、「PPP オプション・ファイルの設定」ダイアログ・ボックスを閉じます。

SysMan Menu ユーティリティを使用すると、options ファイルをコピー、変更、および削除することができます。詳細は、オンライン・ヘルプを参照してください。

8.2.3.3 シークレット・ファイルの作成

chap-secrets および pap-secrets ファイルには、8.2.1.3 項で説明されているように、認証に使用できるエントリが含まれています。以下の各項では、これらのファイルにエントリを作成する方法について説明します。

8.2.3.3.1 PAP-secrets ファイルのエントリの作成

Common Desktop Environment (CDE) のアプリケーション・マネージャの SysMan Menu を使用して、pap-secrets ファイルを作成します。SysMan Menu アプリケーションを起動するには、1.2.1 項の手順に従ってください。

pap-secrets ファイルにエントリを作成するには、次の手順に従ってください。

1. SysMan Menu から [ネットワーク] [追加ネットワーク・サービス] [シリアル・ライン・ネットワーク] [Point-to-Point Protocol (PPP)] [pap-secrets ファイルの修正] を選択して、「pap-secrets ファイルの修正」ダイアログ・ボックスを表示します。
代わりに、次のコマンドをコマンド行から入力することもできます。

```
# /usr/bin/sysman pap
```
2. [追加] を選択して、「Add pap-secrets エントリ」ダイアログ・ボックスを表示します。必要な情報を入力します。

3. [了解] を選択して現在の変更を保存し、このダイアログ・ボックスを閉じます。「pap-secrets ファイルの修正」ダイアログ・ボックスには新しいエントリが表示されます。
4. 必要な回数だけ、手順 2 および 3 を繰り返します。
5. [終了] を選択して、「pap-secrets ファイルの修正」ダイアログ・ボックスを閉じます。

PAP-secrets ファイルのエントリを変更したり削除したりするためにも、SysMan Menu ユーティリティを使用することができます。詳細は、オンライン・ヘルプを参照してください。

8.2.3.3.2 CHAP-secrets ファイルのエントリの作成

Common Desktop Environment (CDE) のアプリケーション・マネージャの SysMan Menu を使用して、chap-secrets ファイルを作成します。SysMan Menu アプリケーションを起動するには、1.2.1 項の手順に従ってください。

chap-secrets ファイルにエントリを作成するには、次の手順に従ってください。

1. SysMan Menu から [ネットワーク] [追加ネットワーク・サービス] [シリアル・ライン・ネットワーク] [Point-to-Point Protocol (PPP)] [chap-secrets ファイルの修正] を選択して、「chap-secrets ファイルの修正」ダイアログ・ボックスを表示します。
代わりに、次のコマンドをコマンド行から入力することもできます。

```
# /usr/bin/sysman chap
```
2. [追加] を選択して、「Add chap-secrets エントリ」ダイアログ・ボックスを表示します。必要な情報を入力します。
3. [了解] を選択して現在の変更を保存し、このダイアログ・ボックスを閉じます。「chap-secrets ファイルの修正」ダイアログ・ボックスには新しいエントリが表示されます。
4. 必要な回数だけ、手順 2 および 3 を繰り返します。
5. [終了] を選択して、「chap-secrets ファイルの修正」ダイアログ・ボックスを閉じます。

CHAP-secrets ファイルのエントリを変更したり削除したりするためにも、SysMan Menu ユーティリティを使用することができます。詳細は、オンライン・ヘルプを参照してください。

8.2.3.4 メッセージ・ロギングの設定

メッセージ・ロギングを設定するには、次の手順を実行します。

1. 次のように、`/etc/syslog.conf` ファイルを編集します。

注意

`/etc/syslog.conf` ファイル内のホワイト・スペースには、タブ文字を使用しなければならず、スペース文字は使用できません。詳細は、`syslogd(8)` を参照してください。

- a. `local2` ファシリティ (`pppd` デーモンおよび `chat` プログラムで使用) を、次のように、メッセージの宛先として `/dev/console` を指定している行に追加します。

```
kern.debug;local2.notice                                /dev/console
```

この例では、`notice` の重大度が指定されています。この重大度およびロギング・システムの一般的な情報については、『システム管理ガイド』を参照してください。

- b. 次のエントリをこのファイルに追加して、`ppp-log` ファイルを作成します。

```
local2.debug                                /etc/ppp/ppp-log
```

- c. 編集内容を保存して、ファイルを閉じます。

2. 次のコマンドで PPP ログ・ファイルを作成します。

```
# touch /etc/ppp/ppp-log
```

3. 次のコマンドを入力して `syslogd` デーモンを終了し、再起動します。

```
# /sbin/init.d/syslog stop
# /sbin/init.d/syslog start
```

8.2.3.5 PPP 接続の開始

システムの PPP ダイアル・アウト接続の構成が終了したら、ローカル・システムで `pppd` デーモンを起動してリモート・システムに接続します。たとえば次のコマンドは、`chat` スクリプトを実行して、`tty01` を通してリモート・システムへの PPP 接続を確立します。

```
% pppd /dev/tty01 38400 connect 'chat -f /etc/ppp/chat-script'
```

PPP オプション・ファイルで端末名と速度のオプションをすでに設定している場合は、次のように、それらのオプションなしで `pppd` を実行できます。

```
% pppd connect 'chat -f /etc/ppp/chat-script'
```

PAP 認証が必要なリモート・システムとの PPP 接続を開始する場合、次のように、`pppd` コマンドにユーザ名を指定する必要があります。

```
% pppd user username connect 'chat -f /etc/ppp/chat-script'
```

PPP 接続のモニタリングと切断についての詳細は、8.2.5 項を参照してください。

注意

`ppp` インタフェースのアドレスを構成する際には、`ifconfig` コマンドは使用しないでください。`pppd` デーモンは、アドレスを割り当て、インタフェースを実行中と見なします。

8.2.3.6 Microsoft Windows Remote Access Server への接続

この項では、Tru64 UNIX システムから Microsoft Windows Remote Access Server (RAS) へのダイアル・アウト接続を確立する方法について説明します。

次の情報を、`/etc/ppp/chap-secrets` ファイルに入力する必要があります。

- Microsoft Windows ドメインのログイン名とパスワード
- Microsoft Windows ドメイン名

`/etc/ppp/chap-secrets` ファイルの作成方法の詳細については、8.2.3.3.2 項 および `pppd(8)` を参照してください。

8.2.3.6.1 RAS サーバの構成

RAS サーバへのダイヤル・アウト・アクセスが可能になるように Tru64 UNIX システムを構成するには、次の手順を実行します。

1. ルートとしてログインします。
2. `/etc/ppp/chap-secrets` ファイルを作成します。たとえば、`money` というサーバに、`monopoly` というユーザ名および `candlestick` というパスワードを使用してダイヤル・アウトするには、次のように `chap-secrets` ファイルを作成します。

```
#
# secret for logging into an RAS server
#
monopoly money candlestick
```

3. このユーザおよびリモート名引数を使用して `pppd` コマンドを実行し、サーバ `money` への `secret` を選択します。たとえば、次のようになります。

```
# pppd tty00 38400 user monopoly remotename money \
connect 'chat -f /etc/ppp/chat-script'
```

ダイヤル・アウトした RAS サーバがスタンドアロン・サーバ、またはドメイン・コントローラではない場合には、ユーザ名の前にドメイン名を付加する必要があります。この操作をコマンド行から実行するには、次のようなコマンドを入力します。 `empire` がドメイン名です。

```
# pppd tty00 38400 user 'empire\\monopoly' remotename money \
connect 'chat -f /etc/ppp/chat-script'
```

注意

この例では、バックスラッシュ文字をエスケープ処理するために、一重引用符が必要です。

代わりに、次のように、この情報を `/etc/ppp/chap-secrets` ファイルに追加することもできます。

```
#
# secret for logging into an RAS server
#
empire\\monopoly money candlestick
```

また、chat プログラムを使用した場合でも、ダイヤル・アウト接続を確立するために必要なダイアログを自動化することができます。chat プログラムの使用方法については、8.2.1.1 項を参照してください。

認証の実行中には、Microsoft Windows は、そのノード名を PPP ピアに送信しません。このため、この PPP ピアは、chap-secrets ファイルから正しい secret を選択するために、あらかじめ Microsoft Windows システムのノード名を認識していなければなりません。これは、pppd デーモンの remotename オプションを設定することによって可能です。この操作が実行されていないと、認証が失敗し、PPP リンクが切断されます。

8.2.3.6.2 Microsoft CHAP の認証の問題の解決

認証が失敗すると、Microsoft CHAP (MS-CHAP) は、エラー・コードを返します。エラー・メッセージを記録するには、pppd コマンドを debug オプションを使用して起動します。エラー・コードの形式は、次のとおりです。

```
rcvd [CHAP Failure id=0x0 "E=NUM R=1"]
```

NUM は、MS-CHAP が返すエラー・コードです。

エラー・コードには、次のようなものがあります。

エラー・コード	説明
E=646	このアカウントでは、ログイン時間が制限されている。この時間は、ログオンできない。
E=647	このアカウントは、使用不可になっている。
E=648	このアカウントのパスワードの有効期限が過ぎている (pppd デーモンは、パスワードの変更をネゴシエートできない点に注意)。
E=649	ダイヤル・インが許可されていない。
E=691	RAS Server が、ユーザ名を確認できない。パスワードが間違っているか、ユーザ名の前にドメイン名を付ける必要がある。

8.2.4 PPP でのダイヤル・イン・システムの構成

システムがリモート・システムからの着呼に応答するようにするには、ダイヤル・イン接続を確立しなければなりません。次のタスクを実行する必要があります。

- 初期通信の設定
- options ファイルの作成
- シークレット・ファイルの作成
- メッセージ・ロギングの設定

最初の 2 つの構成タスクについては、以下の各項で説明します。残りの構成タスクについては、8.2.3.3 項と 8.2.3.4 項を参照してください。

8.2.4.1 ダイアル・イン・システムの初期通信の設定

システムをモデムに物理的に接続するか、またはリモート・システムに直結した後、次の手順を実行します。

1. モデムを使用する場合は、モデムにダイアル・イン・アクセスを設定します。詳細は 8.3.2 項を参照してください。
2. `/usr/spool/locks` ディレクトリ内で `LCK..tty n` ロック・ファイルの有無を調べます。PPP 用に構成する端末デバイスのロック・ファイルがあれば、それを削除してください。

端末デバイス経由で接続を確立すると、他のアプリケーションによって接続が切られないようにするために、システムがロック・ファイルを生成します。この接続が正しい手続きを経ずに切断されると、ロック・ファイルが残り、新しい接続が確立できなくなります。

3. `/etc/passwd` ファイルを編集して、PPP ユーザの専用エントリを作成します。ログイン・シェル・フィールドには `/usr/sbin/startppp` を指定します。これは、ダイアル・イン接続用の `pppd` デーモンを起動します。たとえば、次のようになります。

```
ppp1:password:20:20:Remote PPP User:/usr/users/guest:/usr/sbin/startppp
```

4. `/etc/inittab` ファイルを編集して、PPP を実行するターミナル・デバイスごとにエントリを作成します。たとえば、次のようになります。

```
nullmodem:3:respawn:/usr/sbin/getty /dev/tty00 M38400 vt100
```

詳細は、`inittab(4)` を参照してください。

5. `init q` コマンドを実行して、直ちに `getty` プロセスを実行します。
6. ダイアル・イン・システムが、ダイアル・アウト・システムが LAN 上の他のシステムにアクセスするためのゲートウェイになる場合には、このダイアル・イン・システムを IP ルータとして構成しなければならず、

gated デーモンを実行しなければなりません。 /etc/gated.conf ファイルを編集して、rip 文の nobroadcast オプションを (指定されている場合は) 削除します。基本的なネットワーク設定情報については、第 2 章を参照し、gated オプションについては、gated.conf(4) を参照してください。

8.2.4.2 ダイアル・イン・システムの options ファイルの作成

Common Desktop Environment (CDE) のアプリケーション・マネージャの SysMan Menu を使用して、PPP options ファイルを作成します。SysMan Menu アプリケーションを起動するには、1.2.1 項の手順に従ってください。

ダイアル・イン・システムの options ファイルを作成するには、次の手順に従ってください。

1. SysMan Menu から [ネットワーク] [追加ネットワーク・サービス] [シリアル・ライン・ネットワーク] [Point-to-Point Protocol (PPP)] [オプション・ファイルの作成] を選択して、「PPP オプション・ファイルの設定」ダイアログ・ボックスを表示します。

または、コマンド行で次のコマンドを実行します。

```
# /usr/bin/sysman ppp_options
```

2. 表示されるリストからファイルを 1 つクリックし、[修正] を選択します。あるいは、次の手順を実行して、新しい options ファイルを作成します。
 - a. [新規ファイル] オプションを選択して、「Create PPP オプション・ファイル名」ダイアログ・ボックスを表示します。
 - b. 新しいファイル名を入力し、[了解] をクリックします。

「PPP オプション・ファイルの修正」ダイアログ・ボックスが表示されます。

3. [Dial-In Options の設定] を選択し [設定] をクリックして、「Dial-In Options 設定」ダイアログ・ボックスを表示します。PPP 設定ワークシートで収集した情報を使用して、各フィールドに入力します。

pppd オプションの詳細なリストは、pppd(8) とオンライン・ヘルプを参照してください。

4. [了解] を選択して、「Dial-In Options の設定」ダイアログ・ボックスを閉じます。

5. 追加の PPP オプションを構成するには、[Advanced PPP Options] を選択します。関連するダイアログ・ボックスでメニュー項目を選択して、PPP 設定ワークシートと PPP 認証ワークシートで収集した情報を、必要に応じてフィールドに入力します。
終了したら、「Advanced PPP Options」ダイアログ・ボックスで [了解] を選択してダイアログ・ボックスを閉じます。
6. 「PPP オプション・ファイルの修正」ダイアログ・ボックスの [了解] を選択して変更を保存し、ダイアログ・ボックスを閉じます。
7. [終了] を選択し、「PPP オプション・ファイルの設定」ダイアログ・ボックスを閉じます。

また、SysMan Menu ユーティリティを使用すると、options ファイルをコピー、変更、および削除することができます。詳細は、オンライン・ヘルプを参照してください。

PPP オプション・ファイルの作成が終了したら、8.2.3.3 項と 8.2.3.4 項で、シークレット・ファイルの作成とメッセージ・ロギングの設定方法を参照してください。

8.2.5 PPP 接続のモニタリングと終了

pppd デーモンが起動されると、最初に必要に応じてシリアル接続またはモデム接続を確立します。次に、その接続を通して PPP リンクを確立します。PPP リンクが正常に確立され、8.2.3.4 項で述べたようにメッセージのロギングを有効にしていた場合、デーモンは接続に関する基本的な情報を、コンソールのログに記録します。たとえば次のようなものです。

```
Aug 7 17:35:43 packrat pppd[79322]: pppd 2.3.1 started by jensen, uid 283
Aug 7 17:36:24 packrat pppd[79322]: Connect: ppp0 <-> /dev/tty01
Aug 7 17:36:32 packrat pppd[79322]: local IP address 201.146.128.25
Aug 7 17:36:32 packrat pppd[79322]: remote IP address 201.146.128.2
```

メッセージのロギングを有効にすると、トラブルシューティングのために ppp-log ファイルを表示して、接続処理に関する詳細な情報を得ることもできます。たとえば次のようなものです。

```
% more /etc/ppp/ppp-log
.
.
Aug 7 18:07:35 packrat pppd[79605]: sent [PAP AuthReq id=0x1 user="jensen"
password="sailboa"]
Aug 7 18:07:35 packrat pppd[79605]: pap_sauth: Sent id 1.
Aug 7 18:07:35 packrat pppd[79605]: Timeout 120012d80:14000a318 in 3 seconds.
Aug 7 18:07:38 packrat pppd[79605]: sent [PAP AuthReq id=0x2 user="jensen"
password="sailboa"]
```

```

Aug  7 18:07:38 packrat pppd[79605]: pap_sauth: Sent id 2.
Aug  7 18:07:38 packrat pppd[79605]: Timeout 120012d80:14000a318 in 3 seconds.
Aug  7 18:07:38 packrat pppd[79605]: rcvd [PAP AuthNak id=0x2 ""]
Aug  7 18:07:38 packrat pppd[79605]: pap_rauthnak: Rcvd id 2.
Aug  7 18:07:38 packrat pppd[79605]: Remote message:
Aug  7 18:07:38 packrat pppd[79605]: PAP authentication failed
.
.

```

上記の ppp-log ファイルの抜粋では、PAP 認証に失敗しています。理由としては、/etc/pap-secrets ファイル内でユーザがパスワードのスペルを間違えていることが考えられます。

PPP インタフェースに対応する統計情報を表示するには、次のように netstat および pppstats コマンドを実行します。

```

% netstat -I ppp0
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Coll
ppp0 1500 <Link> 18 0 22 0 0
ppp0 1500 201.146.128 p82.dialup.company 18 0 22 0 0

% pppstats
IN PACK VJCOMP VJUNC VJERR | OUT PACK VJCOMP VJUNC NON-VJ
1132 26 0 0 0 | 1425 33 0 0 33

```

これらのコマンドについての詳細は、pppstats(8) と netstat(1) を参照してください。

PPP リンクを終了するには、次のコマンドを実行して、pppd デーモンのいずれか 1 つに TERM または INTR シグナルを送信します。

```
# kill `cat /etc/ppp/pppxx.pid`
```

上記のコマンドの pppxx には、PPP 接続に使用していた pppd インタフェースを指定します。kill コマンドは、関連するプロセスに対して停止、クリーン・アップ、終了を行うように通知します。

モデムが接続されているハードウェア・シリアル・ポート上で pppd デーモンが実行されている場合には、モデムが切れると pppd が HUP シグナルを取得し、クリーン・アップして終了します。これは、ドライバとその現在の設定値によって決まります。

pppd デーモンを終了させる手段として、SIGKILL (kill -9) は使用しないでください。SIGKILL を使用すると pppd が異常終了し、tty ファイルが壊れてしまう可能性があります。

8.3 モデム使用時のガイドライン

Tru64 UNIX システムでは、さまざまなモデムを使用して、近接していないシステムと相互にポイント・ツー・ポイント接続を行うことができます。これらの接続には、SLIP (Serial Line Internet Protocol)、PPP (Point-to-Point Protocol)、および UNIX 間コピー・プログラム (UUCP) が使用されます。さらに、これらの接続は、基本的なダイアル・アウト接続やダイアル・イン接続にすることもできます。たとえば、リモート・システムの管理を行うためにリモート・システムにログインすることができます。

この節では、すべての接続タイプについて、Tru64 UNIX システムでモデムを使用するための一般的なガイドラインを示します。SLIP 接続と PPP 接続については 8.1.2.1 項を、UUCP 接続については『ネットワーク管理ガイド：サービス編』を、それぞれ参照してください。

8.3.1 正しいモデム・ケーブルの使用方法

システムのシリアル・ポートにモデムを接続するには、適正なケーブルを使用しなければなりません。適正なケーブルを使用しないと、信号が劣化して、ソフトウェアが正常に機能しなくなる可能性があります。

ケーブルは、モデムに付属しているものを使用するのが最善です。付属のケーブルがない場合は、次のガイドラインに従って、適切な代替りのケーブルを選んでください。

- パラレル・ケーブルではなくシリアル・ケーブルを使用します。
- 2 台のコンピュータを直結するために設計されたヌル・モデム・ケーブルは使用しないでください。
- 少なくとも 9 芯のシールド・ケーブルを使用します (DECconnect ケーブルは、モデムを完全に制御するには芯線の数がないので使用しません)。
- ケーブルの両端にあるコネクタの、オス/メスとピン数を確認します。モデムに接続する側のケーブルの端は、慣習的に 25 ピンのオス・コネクタです。コンピュータに接続する側の端は、通常は 9 ピンまたは 25 ピンのメス・コネクタです。使用するシリアル・ポートが不明確な場合は、コンピュータに付属のハードウェア・マニュアルを参照してください。

適切なケーブルは通常、「モデム・ケーブル」と明記して販売されています。

8.3.2 ダイヤル・イン・アクセス用のシステムの構成

適正なケーブルでモデムと電話回線を接続してから、次の手順に従ってください。

1. `/etc/remote` ファイルを編集して、`kdebug` エントリと類似のエントリを作成します。たとえば、モデムが `tty00` に接続されていて、38400 のボー・レートでモデムにアクセスしようとする場合には、次のようなエントリを作成してください。

```
b38400:dv=/dev/tty00:br#38400:pa=none
```

注意

モデムの中には、その速度を、シリアル・ポートの速度に合わせて設定するものがあります。必ず、`getty` または `uugetty` に指定する速度と同じ速度を使用して、モデムにアクセスしてください。そうしないと、速度の不一致のためにログインできない場合があります。

2. `/usr/spool/locks` ディレクトリ内で `LCK..ttynn` ロック・ファイルの有無を調べます。モデム用に構成している端末デバイスのロック・ファイルがあれば、それを削除してください。端末デバイス経由で接続を確立すると、他のアプリケーションによって接続が切られないようにするために、システムがロック・ファイルを生成します。この接続が正しい手続きを経ずに切断されると、ロック・ファイルが残り、新しい接続が確立できなくなります。

3. 次のように `tip` コマンドを使用して、モデムにアクセスします。

```
% tip b38400
```

`tip` ユーティリティは、`connected` メッセージで応答します。これで、モデムと通信することができます。

4. モデムが AT コマンド言語を使用している場合は、次のコマンドを入力します。

```
at Return
```

モデムが `quiet` モードでなければ、OK メッセージで応答します。

~ と Ctrl/D (~^D), または ~ とピリオド (~.) を入力すると, tip セッションはいつでも終了できます。tip コマンドについての詳細は, tip(1) を参照してください。

5. 8.3.2.1 項 に指定されているダイアル・イン・アクセス用のモデムを構成します。
6. /etc/inittab ファイルを編集して, モデムのエントリを作成します。非共用モードでモデム回線を使用する場合は, 次のようにエントリを作成します。

```
modem:23:respawn:/usr/sbin/getty /dev/tty00 M38400 vt100
```

共用モード(ダイアル・アウトおよびダイアル・イン接続)でモデム回線を使用する場合は, getty ユーティリティではなく uugetty ユーティリティを使用して, 次のようなエントリを作成します。

```
modem:23:respawn:/usr/lib/uucp/uugetty -r -t 60 tty00 38400
```

uugetty ユーティリティでは, tip および cu ユーティリティを使用できますが, ファイル・ロック機構の違いから他社製のユーティリティは使用できない場合があります。

注意

uugetty ユーティリティを使用したい場合は, UNIX-to-UNIX Copy Facility サブセットをインストールする必要があります。

7. ルートとして次のコマンドを入力して, getty または uugetty のプロセスをスタートします。

```
# init q
```

getty または uugetty プロセスは, スタートするとスリープ状態に移行し, ダイアルされるまで待機します。

8.3.2.1 ダイアル・イン・アクセス用モデムの設定

ダイアル・イン・アクセス用のモデムを構成するには, AT コマンド・セットを使用して, さまざまなコマンドをモデムに送信する必要があります。表 8-5 は必要な AT コマンドのリストです。これらのコマンドの設定は多くのモデムの場合, 一般的には省略時の設定と同じですが, モデムが正し

く構成されているか確認するために、もう一度これらのコマンドを入力することができます。

表 8-5: ダイヤル・イン・アクセス用のモデム・コマンド

コマンド	説明
at&c1	通常のキャリア検出 (CD) 動作。もう一方のモデムのキャリア検出信号を受信するまで、キャリア検出信号を ON にしないようにモデムを設定します。
at&d2	通常のデータ端末レディ (DTR) 動作。この設定は、DTR が OFF になった場合に回線を切るようにモデムを設定します。たとえば、ユーザがシステムからログオフした場合がこれに該当します。
atq1	モデムを quiet モードに設定します。リザルト・コードはシステムに送信されません。
ate0	エコーをオフにします。これによって、getty プロセスを発行しているログイン・プロンプトが、モデムによってエコー・バックされなくなります。
ats0=n	応答するまで待機するベルの数を指定します。n = 0 (zero) の場合には、モデムは応答しません。
at&w0	NVRAM に現在のモデムの設定値を保存します。ほとんどのモデムは、設定を保存して再利用するためのユーザ・プロファイルを備えています。このコマンドは、設定を省略時のプロファイル (0) に保存します。

これらのコマンドは個々にでも、1 つのコマンドとしても入力できます。次に例を示します。

```
at&c1&d2q1e0s0=n&w0 Return
```

結果を確かめるために以下のコマンドを入力します。(e0 コマンドを利用してエコーを止めるため、これらの文字は画面上には表示されません。)

```
at&v Return
```

アクティブなプロファイルと保存プロファイル 0 に、入力した値が反映されます。アクティブな (現在の) プロファイルはモデムの電源を切ると失われますが、保存プロファイル内のモデム設定は保持され、再利用することができます。

指定された設定に加えて、コンピュータとモデム間の接続に使用するフロー制御のタイプを構成します。オペレーティング・システムはハードウェアおよびソフトウェアの両方のフロー制御をサポートします。使用しているコン

コンピュータがハードウェア・フロー制御をサポートしている場合、適切なコマンドを使用して、モデムとシリアル・ラインがハードウェア・フロー制御を使用するように設定します。ハードウェア・フロー制御がサポートされていない場合は、ソフトウェア・フロー制御を使用します。詳しい情報については、ご使用のコンピュータおよびモデムのマニュアルを参照してください。

8.3.3 ダイアル・アウト・アクセス用のシステムの構成

適正なケーブルでモデムと電話回線を接続してから、次の手順に従ってください。

1. `modemtype` サブコマンドを使用して指定したモデム名のエントリが、`/etc/acucap` ファイルにあることを確認します。`/etc/acucap` ファイルにモデムのエントリがない場合は、次の手順に従ってください。

- a. 使用しているモデムと類似したエントリをコピーします。次のエントリは、US Robotics モデム用のもので、共用モードで `tip` コマンドと共用しています。

```
us|US|US Robotics (28.8 fax/data modem):\n:cr:hu:ls:re:ss=AT\rATE1Q0&C0X0&A0\r:sr=OK:\n:sd#250000:di=ATD:dt\r:\n:dd#50000:fd#50:os=CONNECT:ds=\d+++\dATZ\r\dATS0=2\r:\n:ab=\d+++\dATZ\r\dATS0=2:
```

- b. ご使用のモデムの属性と一致するようにモデムの属性を変更し、デバッグ・オプション (db) を含めます。デバッグを ON にすると、モデムから、ファイル内のモデム属性の調整に使用するための補足情報が提供されます。詳細については、`acucap(4)` を参照してください。

2. 8.3.3.1 項に指定されているように、呼び出すシステム用のエントリを `/etc/remote` に作成します。

3. `getty` プロセスを使用して、モデムからシステムにアクセスする場合に、すでに `getty` ユーティリティが実行されているときは、次の手順に従ってください。

- a. `/etc/inittab` ファイルを編集して、モデム・エントリの Action フィールドを `respawn` から `off` に変更します。

```
modem:23:off:/usr/sbin/getty /dev/tty00 M38400 vt100
```

詳細については、`inittab(4)` を参照してください。

b. `init q` コマンドを実行して、`getty` プロセスを終了します。

4. `/usr/spool/locks` ディレクトリ内で `LCK..ttynn` ロック・ファイルの有無を調べます。モデム用に構成している端末デバイスのロック・ファイルがあれば、それを削除してください。

端末デバイス経由で接続を確立すると、他のアプリケーションによって接続が切られないようにするために、システムがロック・ファイルを生成します。この接続が正しい手続きを経ずに切断されると、ロック・ファイルが残り、新しい接続が確立できなくなります。

5. 次のように、`tip` コマンドを使用して、`-baud_rate` フラグとダイヤル・アウトする電話番号を指定します。

```
% tip -38400 8881234
```

この例では、`tip` はボー・レートから負記号 (-) を削除し、`tip` コマンド名とボー・レートを連結して、文字列 `tip38400` を作成します。次に `tip` は、`/etc/remote` ファイルで、この文字列と一致するエントリを検索します。`/etc/remote` ファイルのエントリは、モデムを初期化する `us38400` エントリのケーパビリティ情報をポイントしています。

コマンド行で電話番号を指定することによって、さまざまな電話番号の発信接続に対して、同じモデム属性を共用できます。

リモート・システムをログオフして `tip` ユーティリティを終了すると、保存していた設定がリストアされて、次のユーザがモデムを使用できるようになります。共用モードで使用する場合は、モデムはダイヤルイン・アクセス用に使用できます。

`~` と `Ctrl/D` (`~^D`)、または `~` とピリオド (`~.`) を入力すると、`tip` セッションはいつでも終了できます。`tip` コマンドについての詳細は、`tip(1)` を参照してください。

8.3.3.1 `/etc/remote` ファイルのエントリの作成

`/etc/remote` ファイルには、確立するダイヤル・アウト接続に関する情報が格納されます。

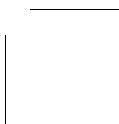
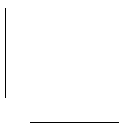
このファイルを使用すると、ターミナル・デバイス名、接続速度、およびモデムを定義する `/etc/acucap` ファイルを入力することができます。たとえば、次の 2 つのエントリは、8.3.3 項の手順 1a で指定されたモデムのもので、

```
tip38400:tc=us38400 [1]
us38400|38400 Baud dial out via US Robotics modem:\ [2]
:el=^U^C^R^O^D^S^Q@:ie=#%$:oe=^D:\ [3]
:dv=/dev/tty00:br#38400:ps=none:at=us:du: [4]
```

- [1] モデムの共用ファシリティを指定する us38400 エントリをポイントします。
- [2] us38400 エントリの最初の行です。
- [3] 行の終端文字，および入力および出力ファイルの終端記号を定義します。
- [4] 接続を開始するデバイス，速度，パリティ，/etc/acucap エントリの名前，およびダイヤル・アップ回線を定義します。

任意の数のリモート・システムに接続するには，このような汎用的なエントリを使用します。

オプションとして，アクセスするそれぞれのリモート・システムのためのエントリを作成することもできます。そのようなエントリには，電話番号など，これらのシステム固有の設定を含めることができます。詳細は，remote(4) を参照してください。



LAT 接続

LAT (Local Area Transport) プロトコルは、端末や PC、プリンタ、モデムなど、ローカル・エリア・ネットワーク (LAN) 上のデバイスが接続されたターミナル・サーバとホスト・コンピュータ・システムとの間の通信をサポートします。Tru64 UNIX の LAT は、STREAMS ベースのドライバです。

この章では次のことを説明します。

- Tru64 UNIX システムでの LAT の実装 (9.1 節)
- LAT 構成の準備 (9.2 節)
- LAT ドライバの構成方法 (9.3 節)
- 各種の LAT 接続の設定方法 (9.4 節)

LAT の概要についての情報は、`lat_intro(7)` を参照してください。トラブルシューティング情報については、10.10 節を参照してください。

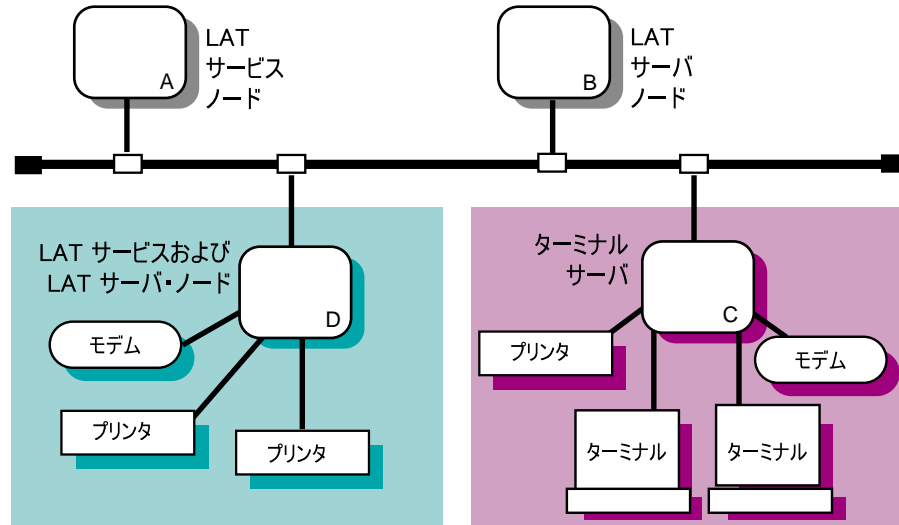
9.1 LAT 環境

LAT 環境では、システムは次の役割を担っています。

- サービス・ノード
LAN のユーザに LAT サービスを提供し、サーバ・ユーザからの接続を受け付けるシステム。
- サーバ・ノード
発信接続用に構成されるターミナル・サーバまたはシステム。サーバ・ノードによって、このノードに接続しているユーザは、LAT サービス・ノードから提供される LAT サービスへ発信ポートを介して、LAT セッションを開始できます。

図 9-1 に、LAT サーバ・ノードと LAT サービス・ノードを使用した LAN の例を示します。

図 9-1: サンプルの LAT ネットワーク構成



ZK-1179U-AI

また、LAT ソフトウェアによって、ホスト・アプリケーションは、アプリケーション・ポートとして指定されたサーバ・ポートとの接続を開始してリモート・デバイスにアクセスできます。この節では、以下の項目について説明します。

- LAT 接続のタイプ
- LAT ネットワークにおけるアクセス制御
- リモート・サーバに対するパスワードの指定
- 負荷分散

9.1.1 LAT 接続のタイプ

次の LAT 接続のタイプが認められています。

- 端末/ホスト間接続 (Terminal-to-host connections)

ターミナル・サーバに接続されている端末のユーザが、LAT サービスに接続する基本的な LAT 接続です。たとえば図 9-1 で、ターミナル・サーバ C に接続されている端末のユーザが、ホスト A のサービスに接続する場合、端末/ホスト間接続が使用されます。

- ホスト開始接続 (Host-initiated connections)

ターミナル・サーバに接続されているビット・シリアル同期デバイスが、LAT ホストのユーザ作成アプリケーションと通信する接続です。たとえば図 9-1 で、ホスト A がホスト D のプリンタを使用するように設定されている場合、ホスト開始接続が使用されます。

- 発信接続 (Outgoing connections)

LAT サーバ・ノードのユーザが、`llogin` コマンドを使用して LAT サービスに接続する際に使用されます。たとえば図 9-1 で、ホスト B のユーザがホスト A 上の LAT サービスに接続する場合、発信接続が使用されます。

- Lattelnets ゲートウェイ接続 (Lattelnets gateway connections)

ターミナル・サーバに接続されている端末のユーザが、Tru64 UNIX ホストを介してリモート・ホストに接続するような場合に使用されます。たとえば図 9-1 で、ホスト D の Lattelnets サービスに接続しているターミナル・サーバ C に接続されている端末のユーザは、Lattelnets ゲートウェイ接続を使用しています。

9.1.2 LAT ネットワークでのアクセス制御方法

LAT ネットワークは本来ローカルなので、LAT 環境で高度な制御ができ、LAT デバイスへ物理的にアクセスできます。物理的なアクセスの制御だけではなく、次の機能によって LAT アクセスを制御できます。

- LAT ターミナル・サーバのログイン・パスワード

ターミナル・サーバにアクセスするためにパスワードの入力を要求できます。詳細については、ご使用のターミナル・サーバのマニュアルを参照してください。

- LAT グループ

LAT グループを設定して、ホストの通信を特定のグループに制限できます。

- LAT サービス・ノードでそのグループを指定するには `latcp -g -a` コマンドを実行します。
- LAT サーバ・ノードでそのグループを指定するには、`latcp -u` コマンドを実行します。

- ターミナル・サーバでそのグループを指定する方法は、ご使用のターミナル・サーバのマニュアルを参照してください。

一般にグループは、LAT ネットワークを論理的な小単位に細分化して、サーバとサービス・ノード間のメッセージの通信量を制限するために、ネットワーク・マネージャ、システム管理者、サーバ・マネージャによって設定されます。グループを利用することにより、サーバによる情報の保持の対象となるサービス・ノード数を制限し、サーバの LAT データベースのサイズを管理するのにも役立ちます。

注意

グループを利用してアクセスを制限することはできますが、この機能は、セキュリティ機構として提供されるものではありません。

LAT サービス・ノードとの接続を確立するためには、ターミナル・サーバ・ポート上で有効なグループ、または LAT サービス・ノード上の発信ポートが、そのサービス・ノード上の最低 1 つのグループと一致する必要があります。同様に、ターミナル・サーバまたはサーバ・ノードがサービス・ノードからのメッセージを処理するには、ターミナル・サーバ・ポートで有効なグループ、またはサーバ・ノードで有効な発信ポート・グループが、サービス・ノード上の最低 1 つのグループと一致する必要があります。一致するグループがない場合は、サービス・ノードからのメッセージが無視されてしまいます。

LAT のサービス・ノード・グループおよび発信ポート・グループを有効にする方法については、`latcp(8)` を参照してください。

9.1.3 リモート・サービスのパスワードの指定方法

パスワードで保護されているリモート・サービスにアクセスする場合、LAT プロトコルはパスワードを要求します。パスワードによって保護されたサービスを提供するターミナル・サーバで、パスワードのチェック機能が有効になっている場合には、アプリケーション・ポートをマップするときにパスワードを指定しなければなりません。パスワードを指定しないと、ターミナル・サーバからサービスに接続しようとしてもすべて拒否されます。詳細については `latcp(8)` を参照してください。

9.1.4 負荷分散

LAN上で2つ以上のノードが同じサービスを提供している場合に、ターミナル・サーバは、希望のサービスに対するランク付けが一番高いノードに接続します。このランク付けは、サービスを提供するノードの現在の負荷に基づきます。この処理は負荷分散と呼ばれます。

負荷分散は異種環境で機能します。したがって、同じ名前を持つサービス・ノードが、異なるオペレーティング・システムを実行することもできます。

9.2 LAT の計画

この節では、LAT を構成する前に必要な作業について説明します。

9.2.1 LAT サブセットがインストールされていることの確認

次のコマンドを入力して、LAT サブセットがインストールされていることを確認します。

```
# setld -i | grep OSFLAT
```

LAT サブセットがインストールされていない場合は、`setld` コマンドを使ってインストールします。サブセットのインストールについての詳細は、`setld(8)` または『インストレーション・ガイド』を参照してください。

LAT サブセットのインストール後、システムをリブートして LAT モジュールをカーネルにロードします。システムは、ブート時に LAT モジュールをカーネルへ動的にロードするように構成されています。

9.2.2 カーネルでの DLB サポートの確認

LAT サブセットをインストールしたら、次のコマンドを実行して、DLB (Data Link Bridge) がカーネルでサポートされていることを確認してください。

```
# sysconfig -q dlb
```

`dlb`: プロンプトが表示されない場合は、スーパーユーザとしてログインして、次の手順を実行してください。

1. 構成ファイルを編集して、次のエントリを追加します。

```
options DLB
```

省略時の構成ファイルは、`/sys/conf/HOSTNAME` です。 `HOSTNAME` は、ご使用のホスト・プロセッサ名で、すべて大文字です。

2. doconfig コマンドを実行して、新しいカーネルを構成します。カーネルの再構成についての詳細は、『システム管理ガイド』を参照してください。
3. 次のコマンドを実行して、新しいカーネルでシステムをリブートします。

```
# shutdown -r now
```

このコマンドによってシステムはただちにシャットダウンされ、自動的にリブートされます。

9.2.3 構成の準備

カーネルで DLB がサポートされていることを確認したら、latsetup ユーティリティを使用して LAT を構成できます。

図 9-2 は、LAT を構成する際に必要な情報を記録することのできる LAT 設定ワークシートを示しています。本書をオンラインで閲覧している場合は、プリント機能を使用してこのワークシートをプリントできます。この後の項では、ワークシートに記録する必要がある情報について説明します。

図 9-2: LAT 設定ワークシート

LAT 設定ワークシート	
ブート時の LAT の自動スタート:	<input type="checkbox"/> Yes <input type="checkbox"/> No
tty デバイスのタイプ:	_____
LAT tty デバイスの数:	_____
/etc/inittab の LAT エントリ (getty) の数:	_____

ブート時の LAT の自動スタート

省略時の設定では、/sbin/init.d/lat のスタートアップおよびシャットダウン・スクリプトは、実行レベル 3 に達すると LAT を自動的にスタートさせて、実行レベル 3 を終了すると LAT を自動的に停止します。LAT を自動的にスタートさせたくない場合は、No の欄を選択してください。それ以外の場合は、Yes の欄を選択してください。

tty デバイスのタイプ

各 LAT 接続用のターミナル・デバイス (tty) のタイプ。Tru64 UNIX は SVR4 および BSD のデバイス・タイプをサポートしますが、SVR4

フォーマットだとデバイス数が制限されないので、SVR4 デバイスを使用することをお勧めします。

SVR4 デバイスの特殊ファイルのフォーマットは次のとおりです。

`/dev/lat/n`

`n` には 620 ~ 4370 の値が使用されます。たとえば `/dev/lat/620` , `/dev/lat/777` , および `/dev/lat/4000` は SVR4 デバイスを指定します。

BSD デバイスの特殊ファイルのフォーマットは次のとおりです。

`/dev/ttyWX`

`W` には 0 ~ 9 の値が入り、`X` には 0 ~ 9、小文字の `a ~ z`、大文字の `A ~ Z` のいずれかの 1 つの英数字が入ります。たとえば `/dev/tty02` , `/dev/tty0e` , および `/dev/tty9f` は BSD LAT ターミナル・デバイスを指定します。ただし、すべての BSD ターミナル・デバイス名が、大文字小文字を区別するわけではありません。デバイス特殊ファイル `/dev/tty9f` と `/dev/tty9F` は、両方とも `TTY9F` に変換されます。

このフォーマットを使用すると、システムで実行する UUCP などのすべてのシリアル・デバイスが使用できる BSD ターミナル・デバイスを、最高 620 まで指定できます。したがって、LAT で使用できる BSD デバイスの数は、620 未満になる可能性があります。

LAT tty デバイスの数

同時に着信する LAT 接続の数、アプリケーション・ポートの数、および必要な発信接続の数の総数です。

`/etc/inittab` の LAT エントリ (`getty`) の数

`/etc/inittab` ファイルに追加する LAT の `getty` エントリの数です。これは、必要な同時着信 LAT 接続数です。

9.3 LAT の構成方法

この節では、次の各作業の実施方法について説明します。

- `latsetup` ユーティリティによる LAT の構成
- LAT の手動による起動と停止
- LAT 起動ファイルの作成

- `inittab` ファイルのカスタマイズ
- 特定のネットワーク・アダプタ上での LAT の実行

9.3.1 `latsetup` による LAT の構成

`latsetup` ユーティリティを使用して、システムの LAT を構成したり管理したりします。`latsetup` を使用するには、LAT および DLB は実行カーネルに組み込み、ご使用のシステムを実行レベル 3 または 4 にして、スーパーユーザとしてログインする必要があります。詳細については、`latsetup(8)` を参照してください。

`latsetup` ユーティリティには、次の機能があります。

- LAT デバイスの特殊ファイルの作成。
- `/etc/inittab` ファイルに対する `getty` エントリの追加または削除。
- `init q` コマンドの実行。
- LAT ドライバのスタートまたは停止。
- LAT 自動スタートアップおよびシャットダウンの有効化または無効化。有効にすると、実行レベル 3 に達したときに自動的に LAT がスタートします。

NetRAIN セットを構成する NetRAIN 仮想インタフェースまたはアダプタ上で LAT を構成することはできません。LAT は NetRAIN 上では、サポートされていません。

`latsetup` ユーティリティを起動するには、SysMan Menu から次のように選択します。[ネットワーク] [追加ネットワーク・サービス] [LAT (Local Area Transport) の設定]。別の方法としては、コマンド・ライン上で次のコマンドを入力します。

```
# /usr/sbin/latsetup
```

ご使用の端末が Curses をサポートしていない場合には、`-nocurses` フラグを指定する必要があります。このフラグによって、コマンド行モードで `latsetup` ユーティリティを実行できます。

注意

同じマシンで複数の `latsetup` プロセスを同時に実行しないでください。誤った情報が `latsetup` のユーザに提供されて、`/etc/inittab` ファイルを壊す可能性があります。

9.3.2 LAT のスタートおよび停止

手動で LAT をスタートするには、次のコマンドを入力してください。

```
# /sbin/init.d/lat start
```

手動で LAT を停止するには、次のコマンドを入力してください。

```
# /sbin/init.d/lat stop
```

LAT セッション内から LAT を停止すると、そのセッションは終了します。

9.3.3 LAT スタートアップ・ファイルの作成

LAT の自動スタートアップおよびシャットダウンを有効にしている場合、システムが実行レベル 3 に達すると、カーネルに LAT をロードして `/sbin/init.d/lat` スクリプトを実行します。このスクリプトは、`/etc/latstartup.conf` ファイルが存在する場合に、このファイル内の `latcp` コマンドを読み取って実行し、LAT をスタートします。`latcp` コマンドについての詳細は、`latcp(8)` を参照してください。

`/etc/latstartup.conf` ファイルがない場合、LAT は省略時のパラメータ値でスタートします。表 9-1 に、LAT パラメータとその省略時の値を示します。

表 9-1: LAT パラメータ

パラメータ	省略時の値
ノード名	ホスト名
マルチキャスト・タイマ	60 秒
ネットワーク・アダプタ	ブロードキャスト・メディアに接続されているすべてのネットワーク・アダプタ。NetRAIN セットを構成する NetRAIN 仮想インタフェース (nr) およびそれらのアダプタを除く。
サービス名	LAT のノード名パラメータからの値。各サービスは次のパラメータを持ちます。

表 9-1: LAT パラメータ (続き)

パラメータ	省略時の値	
	パラメータ	省略時の値
	サービスの説明	Compaq Tru64 UNIX Version X.X LAT SERVICE
	レーティング	ダイナミック
	グループ・コード	0
	エージェントの状態	無効
発信ポート・グループ	グループ 0	
学習されたサービスの最大数	100	

ご使用のシステムで LAT をカスタマイズする場合は、`/etc/latstartup.conf` ファイルを作成して `latcp` コマンドを含むように変更できます。たとえば、あるノード名を定義したり、サービス名を追加したりできます。

注意

ご使用のシステムがクラスタの場合、Context-Dependent Symbolic Link (CDSL) として `/etc/latstartup.conf` ファイルを作成する必要があります。詳細については、『システム管理ガイド』を参照してください。

例 9-1 に、`/etc/latstartup.conf` ファイルの例を示します。

例 9-1: `/etc/latstartup.conf` ファイルの例

```
/usr/sbin/latcp -n testnode [1]
/usr/sbin/latcp -A -a lattelnet14 -i "LAT/telnet" -o [2]
/usr/sbin/latcp -A -a testservice [3]
/usr/sbin/latcp -g 0,21,52 -a testservice [4]
/usr/sbin/latcp -A -a boundservice -p 620,621 [5]
/usr/sbin/latcp -c200 [6]
/usr/sbin/latcp -A -p 630 -O -V finance [7]
/usr/sbin/latcp -u 0,1,41,97 [8]
/usr/sbin/latcp -e ln0 [9]
```

- ① LAT ノード名を変更します。
- ② LAT/Telnet 接続に使用できるオプション・サービスを追加します。
LAT/Telnet ゲートウェイについての詳細は、9.4.4 項を参照してください。
- ③ アンバウンドの対話式サービス `testservice` を追加します。
- ④ サービス `testservice` にグループ 0, 21, および 52 を追加します。
- ⑤ バウンド・サービスを追加して、2つの LAT デバイスをバインドします。620 および 621 は、SVR4スタイルの LAT デバイスです。
- ⑥ 学習されたサービスの数を 200 まで増加します。
- ⑦ サービス `finance` に発信ポートをマップします。
- ⑧ 発信ポート・グループ 0, 1, 41, および 97 を追加します。
- ⑨ `ln0` アダプタを追加します。

`latstartup.conf` ファイル内では、サービスを追加する `latcp` コマンドを、このサービス名を必要とする `latcp` コマンドより先に配置する必要があります。例 9-1 の 3 行目および 4 行目で、この点について示しています。

9.3.4 inittab ファイルのカスタマイズ

`/etc/inittab` ファイルを変更して、`getty` 以外のプログラムを使用するように設定できます。たとえば、`/etc/inittab` ファイルに次のエントリを追加して、LAT デバイス 620 でユーザ定義プログラム `myownprogram` が使われるように構成できます。

```
lat620:34:respawn:/usr/sbin/myownprogram /dev/lat/620
```

この例では、デバイス `/dev/lat/620` に絶対パス名を使用しています。

LAT によるユーザ定義プログラムの使用方法については、9.4.5 項を参照してください。`/etc/inittab` および `getty` ユーティリティについての詳細は、`inittab(4)` および `getty(8)` を参照してください。

`/etc/inittab` ファイルを変更して次のようなエントリを追加すると、初期構成後に手動で作成した LAT デバイスを追加することもできます。

```
lat621:34:respawn:/usr/sbin/getty lat/621 console vt100
```

2 番目のフィールド (34) には、エントリを処理する実行レベルを指定します。この例では、`getty` プロセスは実行レベル 3 または 4 のいずれかで生成されます。さらにこの例では、相対パス名 `lat/621` を使用しています。

9.3.5 特定のネットワーク・アダプタでの LAT の実行

ご使用のシステムが複数のネットワーク・アダプタで構成されている場合、省略時の設定では、`latcp` プログラムは、LAT プロトコルをサポートできるすべてのアダプタで LAT プロトコルの使用をスタートしようとします (NetRAIN セットを構成する NetRAIN 仮想インタフェースおよびアダプタを除きます)。別の論理ネットワークに接続されているアダプタの場合でも、これが理想的な状態です。ただし、単一の論理ネットワークに接続されているアダプタの場合には、LAT プロトコルは 1 つのアダプタでだけ実行してください。このように指定するには、`latcp -e adapter` コマンドを `/etc/latstartup.conf` ファイルに追加してください。詳細については、`latcp(8)` を参照してください。

`netstat -i` コマンドを使用して、システムに定義されているアダプタの名前を調べてください。

9.4 LAT 接続の構成

この節では、次の各作業の実施方法について説明します。

- LAT 経由の印刷を目的としたプリンタ設定
- ホスト側が開始する接続の設定
- 発信接続の設定
- LAT/Telnet ゲートウェイの設定
- 専用またはオプションのサービスの作成
- 端末の専用 `tty` デバイスの提供

9.4.1 プリンタの設定方法

以降の項では、LAT 経由で印刷を行うためのプリンタの設定方法について説明します。プリンタを正しく構成すると、ホストが起動するコネクションを通して、ローカルの LAT ホストからプリンタにアクセスすることができます (9.4.2 項を参照)。

本書は LAT サービスの確立方法について説明しており、プリンタ設定の情報を詳細まで網羅しているわけではありません。プリンタの設定方法についての詳細は、『システム管理ガイド』、`printconfig(8)`、`lprsetup.dat(4)`、および `lprsetup(8)` を参照してください。

プリンタの設定を開始する前に、次の情報を収集しておく必要があります。

- プリンタを接続するターミナル・サーバ名
- 次のうちいずれか一方または両方
 - プリンタを接続するポート名
 - リモート・プリンタに割り当てられているサービス名
- ターミナル・サーバのマニュアル
- プリンタのマニュアル

注意

この節の例では、DECserver 700 サーバを使用しています。実際に設定を行う場合には、ご使用のターミナル・サーバに添付されたマニュアルを参照してください。

9.4.1.1 ターミナル・サーバでのプリンタの設定方法

プリンタを設定するには、次の手順に従ってください。

1. ターミナル・サーバのシリアル・インタフェースにプリンタを接続します。
2. ターミナル・サーバのマニュアルで指定されているターミナル・サーバ・コマンドを使用して、Tru64 UNIX サービス・ノードからのホスト開始要求を介して、接続されているリモート・プリンタにサーバがアクセスできるように設定します。サービス・ノードは、ローカルの LAT ホストを指します。
3. プリンタのマニュアルを参照して、プリンタの文字サイズ、フロー制御、パリティ、および速度を調べます。
4. プリンタの特性とターミナル・サーバのポート設定値を比較します。次のようなコマンドを入力すれば、ターミナル・サーバのコンソールにこの設定値を表示できます。

```
Local> SHOW PORT 7 CHARACTERISTICS
```

このコマンドによって、ポート 7 の特性が表示されます。次に、ターミナル・サーバの最低限のポートの設定値を示します。

文字サイズ:	プリンタの文字サイズ
フロー制御:	XON (または、プリンタによっては-CTS/RTS)
速度:	プリンタの速度
アクセス:	リモート
自動ボー:	不可
自動接続:	不可

ターミナル・サーバのポート設定値がプリンタ特性と一致しない場合は、DEFINE コマンドを使用してターミナル・サーバのポート設定値を定義してください。次に例を示します。

```
Local> DEFINE PORT 7 SPEED 9600
```

5. ポートの設定値を定義したら、そのポートをログアウトして新しい設定値を初期化します。次に例を示します。

```
Local> LOGOUT PORT 7
```

9.4.1.2 ポート構成のテスト方法

プリンタおよびターミナル・サーバ・ポートでプリンタ特性が一致していることを確認するには、ターミナル・サーバで TEST PORT コマンドを使用します。たとえば構成が正しい場合には、DECserver 700で次のコマンドを実行すると、ポート 7 に接続されているプリンタに文字のテスト・パターンがプリントされます。

```
Local> TEST PORT 7
```

プリンタは、ターミナル・サーバのコンソールで [Break] キーを押さない限り、24 行のテスト・データをプリントします。データがプリントされない場合や誤っている場合には、ポートまたはプリンタが間違っていて設定されているか、またはハードウェアに問題があります。

9.4.1.3 プリンタ用のサービス・ノードの設定方法

サービス・ノード (ローカル LAT ホスト) では、latcp コマンドを使用して、ターミナル・サーバ上のリモート・ポートまたはリモート・サービスに

未使用のアプリケーション・ポートをマップします。 9.4.1.1 項のプリンタには、ターミナル・サーバ名、およびポート名またはサービス名のいずれかを使用してください。

たとえば次のコマンドは、サーバ LOCSEER 用のローカル・アプリケーション・ポート 621 を、リモート・プリンタ・ポート port07 にマップします。

```
# latcp -A -p 621 -H LOCSEER -R port07
```

次のコマンドは、リモート・プリント・ポートの代わりにリモート・プリンタのサービス名を指定しています。

```
# latcp -A -p 621 -H LOCSEER -V REMprinter07
```

詳細については、latcp(8) を参照してください。

9.4.1.4 サービス・ノードでのプリント・スプーラの設定方法

リモート・プリンタのプリント・スプーラを設定するには、lprsetup コマンドを使用してください。次のシンボルは、ホストが開始する接続を介してリモート・プリンタにアクセスできるように、サービス・ノード (ローカル LAT ホスト) の printcap ファイルで設定する必要があります。

- ct
接続タイプ。
- lp
出力時にオープンするデバイス名。

次の例に、LAT プリンタの /etc/printcap エントリを示します。

```
lp25|lp0:\
:af=/usr/adm/lpacct:\
:ct=LAT:\ ①
:lf=/usr/adm/lperr:\
:lp=/dev/lat/621:\ ②
:mx#0:\
:of=/usr/lbin/lpf:\
:sd=/usr/spool/lpd:
```

- ① ct シンボルに LAT を指定します。
- ② サービス・ノードを設定する際に、latcp コマンドで使った LAT アプリケーション・ポート (tty デバイス) を指定します。lp シンボルには完全パス名を指定する必要があります。

9.4.1.5 プリンタのテスト方法

プリンタを設定したら、ファイルをプリントして、すべてのものが正常に動作することを確認めます。たとえば、プリンタ名が `lp25` で `test` がテキスト・ファイルである場合は、次のコマンドを実行してプリンタをテストできます。

```
# lpr -Plp25 test
```

プリンタが動作しない場合は、すべての設定が正しいかどうかを確認してください。 `printcap` エントリが `lf` エントリを定義している場合は、対応するログ・ファイルを調べて、発生した可能性のあるエラーを確認することができます。

9.4.2 ホスト側が開始する接続の設定方法

ホスト側が開始する接続は、ターミナル・サーバに接続されているビット・シリアル同期デバイスが、適切に構成されたシステム上でユーザが開発したアプリケーションと通信できる接続です。このようなデバイスの例には、端末、モデム、別のホスト・コンピュータ・システムへの通信ポート、およびプリンタがあります。プリンタ接続についての詳細は、9.4.1 項に説明があります。

この節では、ホスト側が開始する接続用にシステムを設定する方法と、これらの接続を活用する、アプリケーション開発のためのガイドラインについて説明します。

9.4.2.1 ホスト側が開始する接続用のシステムの設定方法

ご使用のシステムをホスト側が開始する LAT 接続用に設定するには、次の手順に従ってください。

1. `latcp -A -p` コマンドを使用して、ターミナル・サーバ上のリモート・ポートまたはサービスに、システムのアプリケーション・ポート (tty デバイス) をマップします。次の例では、623 はアプリケーション・ポート、T1301A はターミナル・サーバ名、PORT_6 はターミナル・ポート名です。

```
# /usr/sbin/latcp -A -p 623 -HT1301A -R PORT_6
```

また、この例でポート名の代わりにサービス名を指定することもできます。

2. tty デバイスの保護ビット、所有者、およびグループが、接続用に適切に設定されているかどうかを確認します。通常のユーザが tty デバイスをオープンしたり読み取ったりできるようにする場合は、デバイスを world 読み取り可能にしてください。
3. サーバ・ポートの特性をポートに接続されているデバイスの特性と一致させ、さらにホストが接続を開始できるようにサーバ・ポートを設定します。詳細については、デバイスおよびターミナル・サーバのマニュアルを参照してください。

9.4.2.2 プログラム・インタフェース

ホストが開始する接続を適用するように開発されたアプリケーションは、次の例外を除いて、tty デバイスのアプリケーションに非常によく似ています。

- プログラムは、デバイスの特殊ファイルを使用して LAT ドライバと通信します。ホスト・プログラムが LAT の tty デバイスに対して open 呼び出しを実行する場合、LAT ドライバはターゲット・サーバ上のターゲット・ポートまたはサービスに接続しようとします。ドライバは、`errno` 変数に成功または失敗のコードを報告します。
- open 呼び出しが成功すると、ユーザ・プログラムは、データ転送を処理する `read` および `write` のシステム・コールを実行し、デバイス制御情報を処理する通常の `ioctl` を実行します。
- LAT 接続は、デバイスの `close` システム・コールによって終了します。

ホストが開始する接続に使用できるプログラム例として、`/usr/examples/lat` ディレクトリに `dial.c` アプリケーション・プログラムを用意しています。この例にアクセスするには、`OSFEXAMPLES` オプション・サブセットをインストールする必要があります。

Tru64 UNIX の LAT は、STREAMS ベースの tty 設計です。LAT の tty デバイスをオープンすると、POSIX 回線制御規則モジュール `ldterm` が LAT ドライバ上のストリームに組み込まれます。アプリケーションが `ldterm` による追加処理を必要としない場合は、ストリームからこのモジュールを削除する必要があります。

`/usr/examples/lat` ディレクトリに含まれている `lined.c` アプリケーション・プログラムは、Clist ベースの tty と STREAMS tty 環境でターミナル (tty) 回線制御規則がどのように変更されるかを示します。このサンプル・プログラムにアクセスするには、`OSFEXAMPLES` オプション・サブセッ

トをインストールする必要があります。さらに、`strchg` コマンドを使用して、ユーザの標準入力の STREAMS 構成を変更できます。

詳細については、`autopush(8)`および`strchg(1)`を参照してください。

9.4.3 発信接続の設定方法

発信接続では、ローカル・ユーザが `llogin` コマンドを使用して、リモート・ホストのサービスに接続できます。発信接続を行うには、リモート・ホスト上の指定されたサービスをローカル・ホストのターミナル・デバイスの特殊ファイルと対応させます。`llogin` コマンドについての詳細は、`llogin(1)`および『*Tru64 UNIX ユーザーズ・ガイド*』を参照してください。

9.4.3.1 発信接続用のシステムの設定方法

LAT 発信接続用にシステムを設定するには、次の手順に従ってください。

1. `latcp -A -p` コマンドを使用して、リモート・システムのポートまたはサービスにシステムの発信ポート (tty デバイス) をマップします。次の例では、621 は発信ポート、`REMOTE_SERVICE` はリモート・ノードのサービス名です。

```
# /usr/sbin/latcp -A -p 621 -O -V REMOTE_SERVICE
```

次の例のようにリモート・ノード名とポート名を指定することもできます。この例では、`titan` がノード名、`PORT_1` がポート名です。

```
# /usr/sbin/latcp -A -p 621 -O -H titan -R PORT_1
```

2. 次のコマンドを使用して、リモート・サービスがシステムで利用できる学習されたサービスであることを確認します。

```
# /usr/sbin/latcp -d -l
```

サービスが表示されない場合、学習されたサービスが最大数に達しています。この場合は、このサービスは使用できます。発信接続を試みると、ローカル・ホストはリモート・サービスが使用できるかどうかを調べます。使用できる場合は、発信 LAT 接続が実行されます。

学習されたサービスの最大数を増加させるには、`latcp -c` コマンドを使用してください。学習済みサービスについての詳細は、`latcp(8)`および`lat_intro(7)`を参照してください。

9.4.3.2 プログラム・インタフェース

発信接続を適用するために開発されたアプリケーションは、ホストが開始する接続用に開発されたアプリケーションと同じガイドラインに従います。詳細については 9.4.2.2 項を参照してください。

`/usr/examples/lat` ディレクトリ内の `getdate.c` アプリケーション・プログラムは、発信接続で使用するプログラムの例です。このサンプル・プログラムにアクセスするには、`OSFEXAMPLES` オプション・サブセットをインストールする必要があります。

9.4.4 LAT/Telnet ゲートウェイの設定方法

LAT/Telnet ゲートウェイ・サービスによって、LAT ターミナル・サーバのユーザは、Tru64 UNIX ホストを介して Telnet プロトコルを実行するリモート・ホストに接続できます。ユーザは、最初にローカルの Tru64 UNIX システムにログインする必要はありません。構成されている場合は、自由に `rlogin` コマンドを使用してリモート・ホストに直接接続できます。

LAT/Telnet ゲートウェイを設定するには、次の手順に従ってください。

1. `latcp` コマンドを使用して、LAT/Telnet サービスを定義します。次に例を示します。

```
# /usr/sbin/latcp -A -a lattelnet -i "LAT/telnet gateway" -o
```

-o フラグは、オプション・サービスであることを表します。オプション・サービスは、LAT 用に特別に作成した特殊なアプリケーションと一緒に使用します。これらのサービスは、特殊なアプリケーションを占有して使用するために、LAT tty デバイスにバインドされています。

2. `/etc/inittab` ファイルを編集して、手順 1 で作成した `lattelnet` サービスを生成したい LAT デバイスのエントリを変更します。

選択した LAT 端末は、ゲートウェイ専用になります。選択した端末の数によって、システムが同時に提供できる LAT/Telnet ゲートウェイ・セッションの最大数が決まります。たとえば次の例は、3 つのデバイスの LAT/Telnet ゲートウェイ・エントリを示します。これは、このシステムが 3 つの同時セッションを提供できることを意味します。

```
lat624:34:respawn:/usr/sbin/lattelnet lat/624 lattelnet
lat625:34:respawn:/usr/sbin/lattelnet lat/625 lattelnet
lat626:34:respawn:/usr/sbin/lattelnet lat/626 lattelnet
```

Telnet の代わりに rlogin コマンドを使用する場合は、`/etc/inittab` エントリの `lattelnet` プログラムの 3 番目の引数として、`/usr/bin/rlogin` を指定します。次に例を示します。

```
lat624:34:respawn:/usr/sbin/lattelnet lat/624 lattelnet /usr/bin/rlogin
```

3. `init` コマンドで `inittab` ファイルを読み取り、`init q` コマンドを使用してゲートウェイを起動します。

4. `ps` コマンドを使用して、`lattelnet` プロセスがスタートしたことを確認します。

`lattelnet` プログラムは、`syslogd` デーモンを使用して、`/var/adm/syslog.dated/date/daemon.log` ファイルへメッセージのログを取ります。このファイルを調べて、エラー・メッセージが生成されなかったことを確認してください。

5. `CONNECT` コマンドを入力して、LAT ターミナル・サーバからゲートウェイに接続します。たとえば、ゲートウェイとして、`LOCAL` というローカル・ノードを使用して、`REMOTE` というリモート・ノードに接続するには、次のように入力します。

```
Local> CONNECT LATTELNET NODE LOCAL DEST REMOTE
```

このコマンド行は、Telnet と rlogin のどちらでも使用できます。

また、Telnet で接続する場合は、サービス名 `LATTELNET` を入力して、希望のリモート・ノードのプロンプトになるまで待ちます。次の例に、ターミナル・サーバのユーザがサービス `LATTELNET` に接続し、リモート・ノード `MYTRIX` からのログイン・プロンプトを待っているときに起きる状態を示します。

```
Local> CONNECT LATTELNET
LAT to TELNET gateway on printf
telnet> OPEN MYTRIX
Trying...
Connected to mytrix.
Escape character is '^]'.
mytrix login:
```

9.4.5 専用またはオプションのサービスの作成方法

専用サービスは、自分用の特殊アプリケーションと組み合わせて使用できます。`/usr/examples/lat` ディレクトリに次のような特殊アプリケーション・プログラムが提供されています。

- `latdate.c`

日付と時刻をユーザに提供します。

- `latdlogin.c`

DECnet へのログイン用に LAT/DECnet ゲートウェイを提供します。

専用サービスの設定は、LAT/Telnet ゲートウェイの設定に似ています。
9.4.4 項を参照してください。専用オプションを設定するには、次の手順に従ってください。

1. ルートでログインします。
2. アプリケーション・コードを入力してコンパイルしたら、希望のディレクトリに実行可能ファイルをコピーします。
3. `latcp -A -a` コマンドを使用して、サービスを追加します。次に例を示します。

```
# /usr/sbin/latcp -A -a showdate -i "LAT/date service" -o
```

`-o` は、専用のサービスであることを指定します。

4. `/etc/inittab` ファイルを編集して、専用の `tty` デバイスのエントリを追加します。次に例を示します。

```
lat630:3:respawn:/usr/sbin/latdate lat/630 showdate
```

注意

同時に実行するすべてのサービスには `/etc/inittab` エントリが必要です。この例では、`latdate` サービスのユーザは一度に1人だけ許可されます。

5. `init q` コマンドを使用して、`init` に `inittab` ファイルを読み取らせて、サービスをスタートします。

LAT 端末でサービスを使用するには、`CONNECT` コマンドを実行してください。次に例を示します。

```
Local> CONNECT SHOWDATE
```

Tru64 UNIX ホストは、バウンド・インタラクティブ・サービスおよびアンバウンド・インタラクティブ・サービスも提供できます。詳細については、

lat_intro(7) を参照してください。これらのサービスの作成に使用するコマンドの情報については、latcp(8) を参照してください。

9.4.6 端末の専用 tty デバイスの提供

ターミナル・サーバ・ポートに接続されている端末は、特定の Tru64 UNIX LAT ホストに専用 tty デバイスを提供できます。この構成は、端末ユーザにホスト上の特定アプリケーション (データベースなど) へのアクセスを許可するが、セキュリティ上の理由によって、他のアプリケーションやホストへのアクセスを許可したくない場合に役立ちます。

端末を構成すると、端末は必ず LAT ホスト上の、指定された tty デバイ스에接続されます。端末のユーザは、セッションを切り替えたり、別のホストに接続したり、そのホストの別の tty デバイ스에接続したりすることはできません。

9.4.6.1 専用 tty デバイスの設定方法

端末の専用 tty デバイスを設定するには、次の手順に従ってください。

1. 端末が接続されているターミナル・サーバ名とポート名を調べます。次のターミナル・サーバ・コマンドには、サーバ名およびポート名がそれぞれ示されています。

```
Local> SHOW SERVER
Local> SHOW PORT number
```

number 変数は、ターミナル・サーバのポート番号です。

2. LAT ホストで latcp -A -p コマンドを使用して、ターミナル・サーバ・ポートにアプリケーション・ポート (tty デバイス) をマップします。たとえば次のコマンドは、ターミナル・サーバ LATTERM のポート 2 に、SVR4 デバイス (アプリケーション・ポート 630) をマップします。

```
# latcp -A -p630 -H LATTERM -R PORT_2
```

詳細については、latcp(8) を参照してください。

3. LAT ホストで、アプリケーション・ポートとしてマップされた tty デバイス用の /etc/inittab ファイルに、getty エントリを追加します。次に例を示します。

```
lat630:34:respawn:/usr/sbin/getty          lat/630 console vt100
```

4. ターミナル・サーバでポートのアクセスを REMOTE に定義して、ポートからログアウトします。次に例を示します。

```
Local> DEFINE PORT 2 ACCESS REMOTE  
Local> LOGOUT PORT 2
```

5. 設定したターミナル・サーバ・ポートに接続されている端末で、Return キーを押します。システムのプロンプトが表示されて、端末が専用 tty デバイスに接続されます。

この手順を繰り返す必要がある場合は、`/etc/inittab` ファイルから `getty` エントリを削除し、`init q` コマンドを実行して、最初の手順からスタートしてください。

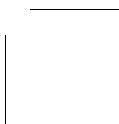
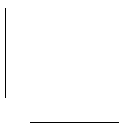
9.4.6.2 専用 tty デバイスの削除方法

専用 tty デバイスをターミナル・ポートから削除し、このポートに接続されている端末が任意のホストに接続できるようにするには、次を実行します。

1. 同じサーバの別の端末にログインします。
2. ポートのアクセスを LOCAL に設定して、ポートからログアウトします。次に例を示します。

```
Local> DEFINE PORT 2 ACCESS LOCAL  
Local> LOGOUT PORT 2
```

3. アプリケーション・ポートをアンマップして、`/etc/inittab` ファイルから `getty` エントリを削除します。



10

ネットワークおよびネットワーク・サービスに関する問題の解決

この章では、ネットワークおよびネットワーク・サービス・ソフトウェアを使用する際に発生する問題を解決するための診断用マップについて説明します。この章とともに適切なマニュアルを参照することにより、多くの問題をユーザ・レベルで解決することができます。

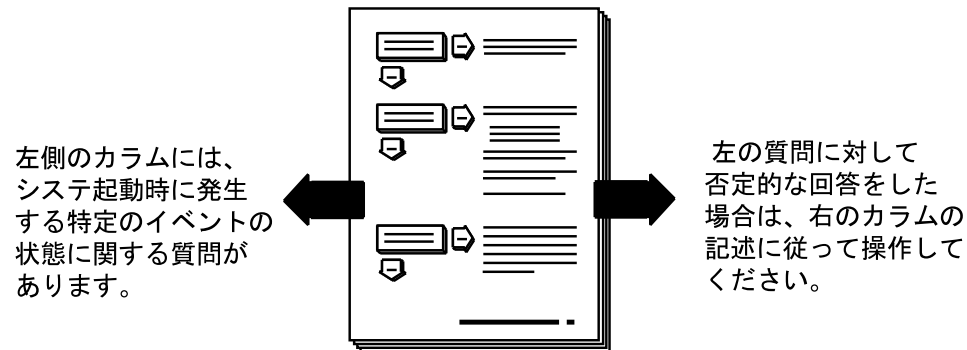
10.1 節と 10.2 節には診断マップの使用方法と、マップ内での開始位置を問題の種類ごとに示しています。それ以降の各節には診断マップがあり、次に挙げる各種の接続に関する問題を解決するための方法を説明しています。

- IPv4 (10.3 節)
- IPv6 (10.4 節)
- Mobile IPv6 (10.4.3 項)
- IPsec (IP security) (10.5 節)
- ATM (10.6 節)
- DHCP (10.7 節)
- SLIP (10.8 節)
- PPP (10.9 節)
- LAT (10.10 節)

10.1 診断マップの使用方法

ネットワークおよびネットワーク・サービスに関する問題は、さまざまな原因によって発生します。この章の診断マップは、問題の原因を特定するために役立ちます。同様の診断マップは、『ネットワーク管理ガイド：サービス編』にも記載されています。次の図に、診断マップの使用方法を示します。

図 10-1: 診断マップの使用方法



問題を切り分けた後、診断マップは、さまざまな問題解決ツールやユーティリティの使用方法について他の章を参照するように指示します。また、場合によっては、特定のデバイスやソフトウェア製品のマニュアルを参照するように指示します。

レイヤード・ソフトウェアを通してネットワークおよびネットワーク・サービス・ソフトウェアを使用している場合には、本書で説明していない問題が発生する場合があります。詳しい情報については、該当する製品のマニュアルを参照してください。

10.2 準備

問題の解決を開始する前に、通信ハードウェアが使用できる状態になっていることを確認してください。次のことを確認します。

- システムのケーブルが物理的に適切に接続（イーサネット・ケーブルの接続およびトランシーバーの接続）されていること。詳細は、システムおよび通信ハードウェア装置のマニュアルを参照してください。
- ネットワーク・イベントを監視するためにイベント・ロギングが使用可能になっていること。イベント・ロギングの開始とイベント・メッセージについての詳細は、『システム管理ガイド』を参照してください。

既知の問題に関する最新の情報については、各製品のリリース・ノートを参照してください。

10-2 ネットワークおよびネットワーク・サービスに関する問題の解決

IPv6 ネットワークで発生した問題に効率的に対処するためには、次の用語も
十分理解してから、問題解決を行ってください。

オンリンク・ノード

使用しているシステムと同じサブネットワークに接続されているノード。この場合のサブネットワークとは、LAN、PPP のシリアル接続、IPv6 over IPv4 構成済みトンネルのいずれかです。使用しているシステムとオンリンク・ノードの間には IPv6 ルータは存在しません。構成済みトンネルの場合には、トンネルの接続先側のノードがオンリンク・ノードです。

オフリンク・ノード

使用しているシステムと同じサブネットワークには接続されていないノード。システムとオフリンク・ノードの間には、少なくとも 1 つの IPv6 ルータが存在します。

図 3-4 では、ホスト A がユーザのシステムだとすると、ホスト B がオンリンク・ノード、ホスト C とホスト D がオフリンク・ノードになります。

表 10-1 は、問題解決の際に、まず診断マップのどの部分を参照すればよいかを示しています。

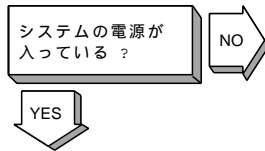
表 10-1: 問題解決のスタート・ポイント

問題の種類	スタート・ポイント
uucp コマンドのエラー	『ネットワーク管理ガイド：サービス編』の「UUCP に関する問題の解決」
ネットワーク・コマンドのエラー	10.8 節 (SLIP 接続を使用している場合) 10.9 節 (PPP 接続を使用している場合) 10.3 節 10.4 節
ATM ネットワークへの接続	10.6 節 10.6.1 項 (Classical IP を使用している場合) 10.6.2 項 (LANE を使用している場合) 10.6.3 項 (IP 交換を使用している場合) 10.3 節 10.4 節

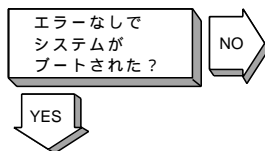
表 10-1: 問題解決のスタート・ポイント (続き)

問題の種類	スタート・ポイント
DHCP を使用しての IP アドレスの取得	10.7 節 10.3 節 10.4 節
NTP を使用している場合にシステム時間を修正	『ネットワーク管理ガイド：サービス編』の「NTP に関する問題の解決」
ホスト名情報の取得	『ネットワーク管理ガイド：サービス編』の「DNS/BIND クライアントに関する問題の解決」(DNS/BIND を使用している場合) 『ネットワーク管理ガイド：サービス編』の「NIS クライアントに関する問題の解決」(NIS を使用している場合)
ファイルへのアクセス	『ネットワーク管理ガイド：サービス編』の「NFS クライアントに関する問題の解決」(NFS を使用している場合) 『ネットワーク管理ガイド：サービス編』の「AutoFS に関する問題の解決」(AutoFS を使用している場合) 10.3 節 10.4 節
LAT を使用したホストへの接続	10.10 節
未知のエラー	10.3 節
未知の IPv6 エラー	10.4 節
メールの送信または受信	『ネットワーク管理ガイド：サービス編』の「sendmail に関する問題の解決」 『ネットワーク管理ガイド：サービス編』の「POP および IMAP に関する問題の解決」(メール・システムに POP または IMAP を使用している場合)

10.3 IPv4 ネットワークに関する問題の解決



システムに電源を入れます。システムのマニュアルを参照して、スタートアップ手順および問題解決の方法について確認してください



Network Information Service (NIS) を実行していて、NIS デモンを起動した後、リモート・ファイル・システムをマウントする前にシステムがハングする場合は、ypbind 要求に応答する NIS サーバがありません。ドメイン内に NIS サーバがあることがわかっている場合は、サーバが応答するまで待ちます。ブート・プロシージャは続行されます。

Local Area Transport (LAT) に問題がある場合は、次のメッセージが表示されます。

```
getty: cannot open "/dev/ttyxx"
```

LAT に関する問題の解決手順については、10.10 節を参照してください。

ご使用のシステムが Network File System (NFS) クライアントで、リモート・ファイル・システムまたはディレクトリのマウント中にハングする場合は、次の手順に従ってください。

1. システムとネットワーク間のケーブルおよび接続部を調べます。
2. ネットワーク上の、`/etc/fstab` ファイルに記述されているサーバが、すべて使用可能になるまで待ちます。システムは、その後でブートを続行します。
3. NFS サーバが停止している場合にクライアント・システムをブートするには、次の手順に従ってください。
 - a. システムを停止します。
 - b. シングルユーザ・モードでシステムをブートし、ローカル・ファイル・システムで `fsck` コマンドを実行します。
 - c. `/etc/fstab` ファイルを編集し、`bg` (バックグラウンド) オプションをサーバのエントリに追加します。詳細は、`fstab(4)` および `mount(8)` を参照してください。

- d. 次のコマンドを使用してシステムをリブートします。

```
# /sbin/reboot
```

fstab ファイルのエントリに `bg` オプションが指定されている場合は、サーバが起動して NFS サーバとして機能し始めると、リモート・ファイル・システムまたはディレクトリが自動的にマウントされます。

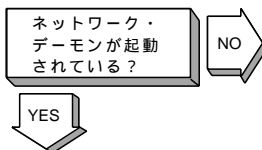


ネットワークが構成されたかどうか見るためには、次の手順に従ってください。

1. 使用しているシステムがこの環境では初めてであり、ネットワーク上で使用するために最近システムを構成した場合、ネットワーク・アダプタ・モードがコンソール・レベルで正しく設定されているかどうか確認します。たとえば、10base2 イーサネット・ネットワークを持っているにもかかわらず、システムが 10baseT イーサネットを使用するように構成されている場合、適切なコンソール値に設定されるまでシステムはネットワークの確認に失敗します。詳細については、『インストレーション・ガイド』にある、フル・インストレーションにあらかじめ必要なタスクを参照してください。
2. `rcmgr` ユーティリティを使用して、`/etc/rc.config` ファイル内の `NUM_NETCONFIG` エントリの値を表示します。

```
# rcmgr get NUM_NETCONFIG
```

値が 0 の場合は、ネットワークを構成するために SysMan Menu ユーティリティを実行します。詳しくは、2.3 節を参照してください。

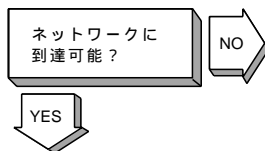


ネットワーク・デーモン (`inetd`) が実行されていることを確認します。次のコマンドを入力します。

```
# ps -e | grep inetd
```

実行中の `inetd` デーモンがない場合は、次のコマンドを使用して `inetd` デーモンを起動します。

```
# /sbin/init.d/inetd start
```

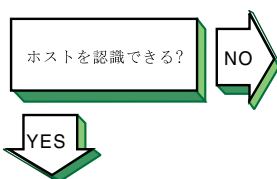


リモート・ホストのネットワークに到達できない場合は、次のメッセージが表示されます。

```
network is unreachable
```

次の手順に従ってください。

1. `netstat -i` コマンドを使用して、ローカル・ホストのネットワーク・デバイスが適切に構成されていることを確認します。ネットワーク・デバイスの構成についての説明は、2.3 節を参照してください。
2. `netstat -r` コマンドを使用して、ローカル・ホストのルーティング・テーブルが正しいことを確認します。
3. 各インターネット・プロトコル (IP) ルータのルーティング・テーブルのパスをトレースして、リモート・ホストのネットワークのエントリがあることを確かめます。IP ルータのルーティング・テーブルの正しくない部分は修正します。この手順を実行するには、ネットワーク・トポロジについての完全な知識が必要です。
4. リモート・ホストに対する、ローカル・ホストのアドレスから名前への変換が正しいことを確認します。「ホストを認識できる？」の解決手順を参照してください。
5. リモート・ホストへのパスにあるすべてのルータを調べ、それらのセキュリティ機能が有効になっているためにリモート・ホストに到達できないかどうかを調べます。



リモート・ホストが未知の場合は、次のメッセージが表示されます。

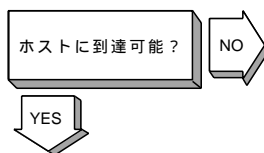
```
unknown host
```

次の手順に従ってください。

1. 有効なホスト名を使用してリモート・ホストに到達しようとしているかどうかを確かめます。
2. リモート・ホストが別の名前ドメインに属していないか、またはユーザがフル・ドメイン名を指定しているかを確かめます。
3. サイトが、名前からアドレスへの変換に DNS (Domain Name System) を使用している場合は、`/etc/svc.conf` ファイルを調べ、`hosts` データベース・エントリのサービ

スとして `bind` が指定されているかどうかを確認めます。指定されていない場合は、`/etc/svc.conf` ファイルを編集して、そのエントリを追加します。また、DNS サービスがリモート・ホストについての情報を持っているかどうかを確認します。『ネットワーク管理ガイド：サービス編』の「DNS/BIND クライアントに関する問題の解決」で説明されている手順を参照してください。

4. サイトが、名前からアドレスへの変換に NIS ネーム・サービスを使用している場合は、`/etc/svc.conf` ファイルを調べ、`hosts` データベース・エントリのサービスとして `yp` (NIS) が指定されているかどうかを確認めます。指定されていない場合は、`/etc/svc.conf` ファイルを編集して、そのエントリを追加します。また、NIS サービスがリモート・ホストについての情報を持っているかどうかを確認します。『ネットワーク管理ガイド：サービス編』の「NIS クライアントに関する問題の解決」で説明されている手順を参照してください。
5. `/etc/svc.conf` ファイルにリストされている名前からアドレスへの変換メカニズムが `local` だけの場合は、`/etc/hosts` ファイルにはリモート・ホストについての情報がありません。詳細については、`svc.conf(4)` を参照してください。



リモート・ホストに到達できない場合は、次のメッセージが表示されます。

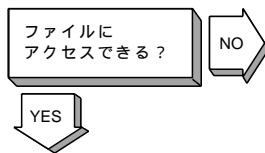
```
host is unreachable
```

次の手順に従ってください。

1. ローカル・ホストとネットワーク間のケーブル接続を確認めます。
2. `ping` コマンドを使用して、リモート・ホストが実行されていることを確認します。
3. `netstat -i` コマンドを使用して、ローカル・ホストのネットワーク・デバイスが適切に構成されていることを確認します。ネットワーク・デバイスの構成についての説明は、2.3 節を参照してください。
4. `netstat -r` コマンドを使用して、ローカル・ホストのルーティング・テーブルが正しいことを確認します。 `ping`

コマンドを使用して、IP ルータが到達可能であるかどうかを確認します。

5. リモート・ホストに対するローカル・ホストのアドレス-名前変換が正しいことを確かめます。「ホストを認識できる？」の解決手順を参照してください。
6. リモート・ホストへのパスにあるすべてのルータを調べ、それらのセキュリティ機能が有効になっているためにリモート・ホストに到達できないのかどうかを判断します。



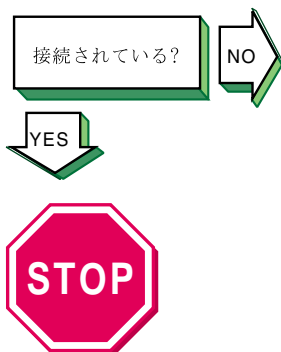
コマンド `rcp` または `rsh` を使用してファイルにアクセスできない場合は、次のメッセージが表示されます。

`permission denied`

次の手順に従ってください。

1. ユーザがリモート・ホストへアクセスしようとしたのかどうかを確認めます。リモート・ホストは、リモートからのアクセスを意図的に禁止していることがあります。
2. 正しいホスト定義およびユーザ定義がリモート・ホストのユーザの `.rhosts` ファイルにあることを確かめます。
3. `/etc/hosts.equiv` ファイルが正しく設定されていることを確かめます。
4. リモート・システムの `.rhosts` ファイルにコピーされたディレクトリ、およびファイルの保護が正しいことを確かめます。

NFS を使用している場合は、『ネットワーク管理ガイド：サービス編』に記載されている NFS に関する問題解決の情報を参照してください。



まだ問題がある場合は、サービス担当者に報告してください(第 12 章 参照)。

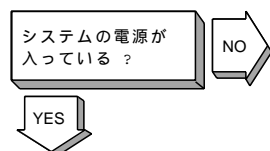
接続が切断されると、次のメッセージが表示されます。

connection timed out

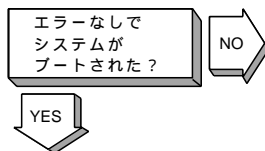
次の手順に従ってください。

1. ネットワークをテストして、問題が、ローカル・ホスト、リモート・ホスト、またはその 2 つの間にあるホストのうちのどこにあるかを調べます。ネットワークのテストについての詳細は、第 11 章を参照してください。
2. 問題のあるホストを発見したら、次の手順に従ってください。
 - a. ネットワーク・デバイスが適切に構成されていることを確認します。ローカル・ホストのブロードキャスト・アドレスおよびアドレス・マスクが正しいことを確認します。ネットワーク・デバイスの構成上の情報については、2.3 節を参照してください。
 - b. ローカル・ホストの `/etc/hosts` ファイルに、ローカル・ホストの正しい IP アドレスがあることを確認します。
 - c. ローカル・ホストからネットワークへのケーブル接続が損なわれることなく適切に行われていることを確認します。
 - d. ローカル・エリア・ネットワーク (LAN) で接続している場合には、アドレス解決プロトコル (ARP) のエントリが正しいこと、およびシステムが LAN に正しく接続されていることを確認します。
 - e. ワイド・エリア・ネットワーク (WAN) で接続している場合には、システムが WAN に正しく接続されていること、およびモデムが正常に動作していることを確認します。

10.4 IPv6 ネットワークに関する問題の解決



システムに電源を投入します。システムのスタートアップ手順と問題解決については、システムのマニュアルを参照してください。



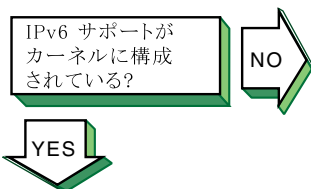
ブート時にネットワーク関連のエラーや警告が表示された場合には、次の手順で対処します。

1. 次のコマンドを実行し、システムのブート時に IPv6 を使用不能にします。
2. システムをリブートします。問題が解決しない場合には、10.3 節に進んでください。
3. 次のコマンドを実行して、IPv6 を起動します。

```
# rcmgr set IPV6 "no"
```

```
# /usr/sbin/rcinet inet6
```

同じ問題が発生するようであれば、誤りがないか /etc/rc.config ファイル、/etc/ip6rtrd.conf ファイル、および /etc/routes ファイルの内容をチェックしてください。



必要な IPv6 サポートがカーネルに構成されていることを確認します。次のコマンドを実行します。

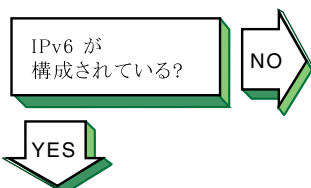
```
# sysconfig -s ipv6 | grep configured
```

何も表示されない場合には、IPv6 オプションはカーネルに構成されていません。doconfig コマンドを使用してカーネルを再構成します。詳細については、3.6.1 項を参照してください。

構成済みトンネルを使用する場合には、IP トンネルのサポートがカーネルに構成されているかどうかを確認します。次のコマンドを実行します。

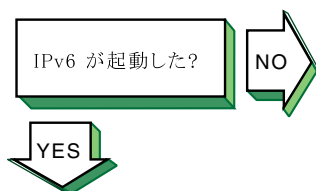
```
# sysconfig -s iptunnel | grep configured
```

何も表示されない場合には、IPTUNNEL オプションはカーネルに構成されていません。doconfig コマンドを使用してカーネルを再構成します。詳細については、3.6.1 項を参照してください。



rcmgr get IPV6 コマンドを実行し、IPv6 がシステムのブート時に起動するように構成されていることを確認します。IPv6 が構成されている場合には、yes が表示されます。

IPv6 が構成されていない場合には、ip6_setup ユーティリティを使用します。IPv6 のホストやルータの設定方法については、3.7 節を参照してください。



IPv6 ホストに問題がある場合は 10.4.1 項, IPv6 ルータに問題がある場合は 10.4.2 項, Mobile IPv6 に問題がある場合は 10.4.3 項に進みます。

次のコマンドを実行し, IPv6 が起動したことを確認します。

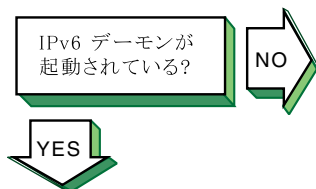
```
# ping ::1
```

host is unreachable というメッセージが表示された場合には, 次のコマンドを実行して IPv6 を起動します。

```
# /usr/sbin/rcinet start inet6
```

このコマンドは IPv6 インタフェースを作成して立ち上げ, IPv6 デーモンを起動します。

10.4.1 IPv6 ホストに関する問題の解決



次のコマンドを実行して, nd6hostd デーモンが動作しているか確認します。

```
# ps ax | grep nd6hostd
```

このデーモンが動作していない場合には, 次のコマンドを実行して, システムが IPv6 ホストとして構成されているか確認します。

```
# rcmgr get ND6HOSTD
```

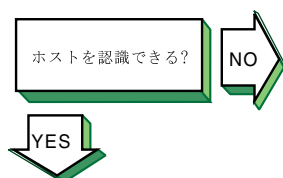
yes と表示されない場合には, ip6_setup ユーティリティを実行して, システムを IPv6 ホストとして構成します。構成の完了後, 次のコマンドを実行して IPv6 を再起動します。

```
# /usr/sbin/rcinet restart inet6
```

yes が表示された場合には, 次のコマンドを実行して, nd6hostd デーモンのデバッグ機能を使用可能にします。

```
# rcmgr set ND6HOSTD_FLAGS "-d -l /usr/tmp/nd6hostd.log"
```

IPv6 を再起動します。



リモート・ホストが未知の場合には, 次のメッセージが表示されます。

```
unknown host
```

次の手順で対処します。

1. リモート・ホストに到達できる有効なノード名を使用しているか確認します。

2. そのリモート・ノードが他のネーム・ドメインに属していることと、ユーザが完全ドメイン名を指定したことを確認します。
3. 名前からアドレスへの変換に DNS/BIND ネーム・サービスを使用しているサイトでは、`/etc/svc.conf` ファイルの内容を調べ、`hosts` データベース・エントリ用のサービスとして `bind` が指定されているか確認します。指定されていない場合には、システムを DNS/BIND クライアントとして構成します。詳細については、『ネットワーク管理ガイド：サービス編』を参照してください。

システムで IPv4 を実行しているか確認します。IPv4 を実行していない場合には、名前からアドレスへの変換にローカルの `/etc/ipnodes` ファイルを使用します。

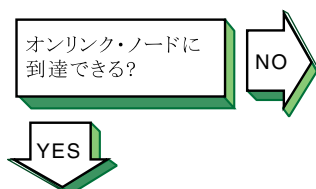
さらに、リモート・ノードに関する情報を DNS/BIND サービスが保有しているか確認します。『ネットワーク管理ガイド：サービス編』の「DNS/BIND クライアントに関する問題の解決」の手順を参照してください。

4. 名前からアドレスへの変換に NIS ネーム・サービスのみを使用しているサイトでは、ノード名用に別のサービスを使用する必要があります。これは、NIS が IPv6 アドレスをサポートしていないためです。

`/etc/svc.conf` ファイルを編集して、`hosts` データベース用のサービスとして、`bind` (DNS/BIND) または `local` (`/etc/ipnodes` ファイル) を追加します (リモート・ノードに関する情報を保有しているサービスの方を追加します)。

5. `/etc/svc.conf` ファイル内で名前からアドレスへの変換メカニズムとして `local` のみを指定している場合には、`/etc/ipnodes` ファイルを編集して、ノード名とアドレスが存在し正しいことを確認します。必要に応じて追加や修正をします。

また、ファイル内の編集箇所より前の各行にフォーマット・エラーが存在しないことを確認します。先頭のエントリから順に、指定されている各ノードに対して `ping` コマンドを実行して、フォーマット・エラーをチェックします。



オンライン・ノードに到達できない場合には、次のいずれかのメッセージが表示されます。

```
host is unreachable
network is unreachable
timeout
```

オンライン・ノードのホストまたはルータが存在する場合、ping コマンドを使用して、到達できるか確認します。コマンドに対して応答がないか、紛失するパケットが多い場合には、次の手順で対処します。

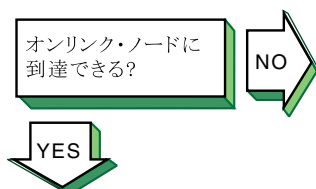
1. ノードが LAN に接続されている場合には、`netstat -I device -s` コマンドを使用して、データリンクのカウンタを調べます。調べるカウンタと、考えられる原因は次のとおりです。
 - 送信ブロック数または受信ブロック数がゼロの場合、ネットワーク・ハードウェアやケーブルに問題があると考えられます。
 - 高い衝突率は、ネットワークのケーブル接続が不適切であるか、ノードが過度のメッセージ・トラフィックを送信していることが考えられます。
 - データ・オーバランによるエラーと、バッファが利用できないというエラーは、システムの構成が不適切であることを示しています。
2. IPv6 と ICMPv6 のカウンタを、`netstat -p ipv6` コマンドと `netstat -p ipv6-icmp` コマンドを使用して調べます。調べるカウンタと、考えられる原因は次のとおりです。
 - ICMP エラーによって発生したエラーによって破棄されたパケットは、他のノードが不正なメッセージを生成していることを示します。他のカウンタに、より詳しい情報が表示されます。
 - 割り当てエラーは、過度のメッセージ・トラフィック、不適切なシステム構成、またはメモリを解放せずに繰り返し割り当てを行っているプログラムの存在を示します。
3. IPv6 ネットワーク・インタフェースが存在し、使用可能であり、`inet6` アドレスを持っていることを、`ifconfig -a` コマンドを使用して確認します。IPv6 ネットワーク・インタフェースに問題がある場合には、`/etc/rc.config` ファ

イル内の構成変数が正しいか確認します。エラーを修正するには、`ip6_setup` ユーティリティを実行します。

さらに、`/var/adm/syslog.dated/current/daemon.log` ファイル内で、`nd6hostd` エラーの有無を調べます。詳細については、11.9 節を参照してください。

インタフェースがグローバル・アドレスやサイト・ローカル・アドレスを持たない場合には、ローカル・ルータがリンク上でプレフィックスを通知しているかどうかをネットワーク管理者に依頼して確認してください。ローカル・ルータがない場合は、`ifconfig` コマンドを使用してプレフィックスを定義できます (3.8.5 項を参照)。

4. オンリンク・ノードが起動して動作していること、IPv6 用に正しく構成されていること、および使用しているアドレスがノード・インタフェース上で使用可能になっていることを、オンリンク・システムの管理者に依頼して確認します。
5. 両方のシステムに IPv4 が構成されている場合には、オンリンク・ノードの IPv4 アドレスに対して `ping` コマンドを実行します。このコマンドが成功した場合は、両方のシステム上で IPv6 構成の確認を行います。このコマンドに対して応答がない場合は、IPv4 ネットワークの問題を解決する必要があります。10.3 節の手順を参照してください。
6. 同じリンク上の他のノードに対して `ping` コマンドを実行し、問題が 1 つのノードだけで発生するのか、他のノードでも発生するかを調べます。問題が発生しない部分もある場合は、ネットワーク・デバイスや、リンク上のケーブルに障害が発生している可能性があります。
7. リンクが構成済みトンネルである場合には、次の手順を実行します。
 - a. `ifconfig -a` コマンドを使用して、トンネルの接続元アドレスと接続先アドレスを確認します。トンネルの接続先側ノードの管理者に連絡し、そのノードの接続先/接続元アドレスが、自分の接続元/接続先アドレスと一致しているか確認します。
 - b. トンネルの接続先アドレスに対して `ping` コマンドを実行します。このコマンドに対して応答がない場合には、IPv4 ネットワークの問題を解決する必要があります。10.3 節の手順を参照してください。



オフリンク・ノードに到達できない場合には、次のいずれかのメッセージが表示されます。

```
host is unreachable
network is unreachable
timeout
```

ping コマンドを使用して、オフリンク・ノードに到達できるか確認します。パケットの紛失率が 100% の場合には、次の手順を実行します。

1. ping コマンドを使用して、自分のシステムとオンリンク・ルータとの接続を確認します。このコマンドに対して応答がないか、紛失するパケットが多い場合は、「オンリンク・ノードに到達できる？」の手順に従ってください。ルータのアドレスを調べるには、次のコマンドを実行します。

```
# ping -I interface ff02::2
```

2. メッセージ送信に使用しているインタフェースに、使用可能なグローバル・ユニキャスト・アドレスまたはサイト・ローカル・ユニキャスト・アドレスがあるかを、`ifconfig -a` コマンドで確認します。使用可能なユニキャスト・アドレスがない場合には、ローカル・ルータがリンク上でプレフィックスを通知しているかどうかを、ネットワーク管理者に依頼して確認してください。

リンクが構成済みトンネルであり、ローカル・ルータがアドレス・プレフィックスの通知を行っていない場合には、`ip6_setup` ユーティリティを使用してトンネル用のプレフィックスを手動で定義できます。詳細については、3.7.1 項を参照してください。

3. リモート・システムが起動して正しく動作していること、IPv6 用に正しく構成されていること、および自分のシステムで使用している IPv6 アドレスとリモート・システムのインタフェースの IPv6 アドレスが一致することを、リモート・システムの管理者に依頼して確認します。アドレスが異なる場合には、`/etc/ipnodes` ファイルの内容を確認するか、リモート・システムの管理者に DNS エントリが正しいことを確認するように依頼します。
4. `netstat -rf inet6` コマンドを使用して、ネットワーク上のルータへの省略時の経路 (U フラグと G フラグが設定された経路) が存在するかどうかを確認します。存在しない場

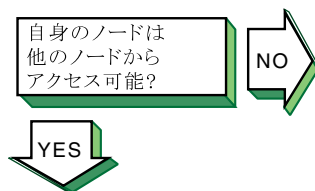
合には、そのルータが自分を省略時のルータとして通知しているかを、ルータ管理者に依頼して確認します。

さらに他のルータもチェックして、誤ったパスにメッセージが送られていないか確認します。

5. `tracert` コマンドを使用して、オフリンク・ノードへのパスをトレースします。詳細については、11.6 節と `tracert(8)` を参照してください。

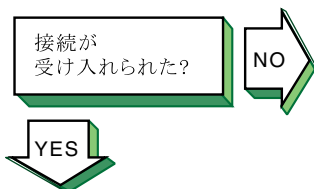
紛失するパケットが多い場合には、ネットワークが混雑しているか、断続的にルーティングの問題が発生している可能性があります。次の手順に従います。

1. `ping` コマンドを使用して、自分のシステムとオンリンク・ルータとの接続を確認します。
2. `tracert` コマンドを使用して、オフリンク・ノードへのパスをトレースします。詳細については、11.6 節と `tracert(8)` を参照してください。



他のノードから到達できないという報告を受けた場合には、次の手順に従います。

1. `ping` コマンドを使用して、相手のノードに到達できるか確認します。このコマンドに対して応答がない場合には、そのノードの位置に応じて、「オンリンク・ノードに到達できる?」または「オフリンク・ノードに到達できる?」の手順に従います。
2. 相手が DNS データベース内の名前を使用している場合には、DNS データベースに格納されている自分のノードのアドレスが、システムのインタフェースに構成されているアドレスのいずれかと一致することを確認します。DNS からアドレスを取り出すには `nslookup -type=AAAA node-name` コマンドを使用し、システムのアドレスを表示するには `ifconfig -a` コマンドを使用します。
3. 相手のノードが、相手のローカル `/etc/ipnodes` ファイルで定義したアドレスを使用している場合には、そのアドレスと、自分のシステムのインタフェースに構成されているアドレスを比較します。 `ifconfig -a` コマンドを使用します。

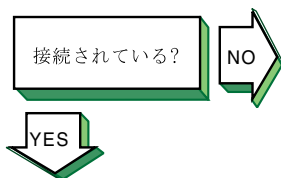


アプリケーションからの接続を受け入れるようにリモート・ノードが構成されていない場合は、次のメッセージが表示されることがあります。

```
connection refused
```

リモート・ノードのシステム管理者に、正しいソケット・ベースのサービス定義が `/etc/services` ファイルと `/etc/inetd.conf` ファイルに定義されているか確認するように依頼します。定義がないか、コメント・アウトされている可能性があります。

ローカルの `/etc/inetd.conf` ファイル内のサービスのプロトコル・フィールドに `tcp6` または `udp6` があるか確認します。



まだ問題がある場合はサービス担当者に報告してください。第 12 章を参照。

接続が異常終了したり、ネットワーク・アプリケーションがハングアップする場合には、次の手順に従います。

1. 障害の発生後、直ちに `ping` コマンドを実行し、リモート・ノードとのネットワーク接続を確認します。

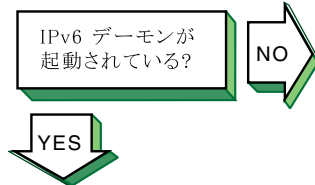
`ping` コマンドに対して応答がないか、パケット紛失率が高い場合には、そのノードの位置に応じて、「オンライン・ノードに到達できる?」または「オフリンク・ノードに到達できる?」の手順に従います。

2. アプリケーションが大量のデータをネットワーク送信する場合には、`ping -s 2000 nodename` コマンドを使用して、大きなメッセージや分割されたメッセージが正しく処理されているか確認します。

`ping` コマンドに対して応答がない場合には `tracert nodename 1200` コマンドを実行し、リモート・ノードへのパスを、1200 バイト長のパケットを使用してトレースします。すべての IPv6 リンクは、少なくとも 1280 バイトのメッセージ・サイズをサポートしなければなりません。このコマンドによって、ネットワーク上で問題が発生している位置を特定できることもあります。詳細については、11.6 節と `tracert(8)` を参照してください。

3. ネットワーク上の他のリンクにある他のクライアント・ノードとサーバ・ノードで、同じアプリケーションを実行します。

10.4.2 IPv6 ルータに関する問題の解決



次のコマンドを実行して、ip6rtrd デーモンが動作しているか確認します。

```
# ps ax | grep ip6rtrd
```

ip6rtrd デーモンが動作していない場合には次のコマンドを実行して、システムが IPv6 ルータとして構成されているかどうかを確認します。

```
# rcmgr get IP6RTD
```

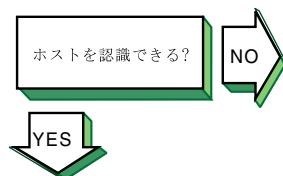
yes と表示されない場合には、ip6_setup ユーティリティを実行して、システムを IPv6 ルータとして構成します。構成の完了後、次のコマンドを実行して IPv6 を再起動します。

```
# /usr/sbin/rcinet restart inet6
```

yes と表示された場合には、次のコマンドを実行して、ip6rtrd デーモンのデバッグ機能を使用可能にします。

```
# rcmgr set IP6RTD_FLAGS "-d -l /usr/tmp/ip6rtrd.log  
/etc/ip6rtrd.conf"
```

IPv6 を再起動します。



リモート・ノードが未知の場合には、次のメッセージが表示されます。

```
unknown host
```

次の手順を実行します。

1. リモート・ノードに到達できる正しいノード名を使用しているか確認します。
2. そのリモート・ノードが他のネーム・ドメインに属していること、および完全ドメイン名を指定してアクセスを試みたことを確認します。
3. 名前からアドレスへの変換に DNS/BIND ネーム・サービスを使用しているサイトでは、/etc/svc.conf ファイルを参照して、hosts データベース・エントリ用のサービスとして bind が指定されているか確認します。bind が指定されていない場合には、システムを DNS/BIND クライアントとして構成します。詳細については、『ネットワーク管理ガイド：サービス編』を参照してください。

システムで IPv4 を実行しているか確認します。IPv4 を実行していない場合には、名前からアドレスへの変換に、`/etc/ipnodes` ファイルを使用します。

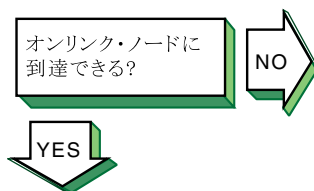
さらに、リモート・ノードに関する情報を DNS/BIND サービスが保有しているか確認します。『ネットワーク管理ガイド：サービス編』の「DNS/BIND クライアントの問題解決」を参照してください。

4. 名前からアドレスへの変換に NIS ネーム・サービス (yp) のみを使用しているサイトでは、ノード名用に別のサービスを使用する必要があります。これは、NIS が IPv6 アドレスをサポートしていないためです。

`/etc/svc.conf` ファイルを編集して、`hosts` データベース用のサービスとして、`bind` (DNS/BIND) または `local` (`/etc/ipnodes` ファイル) を追加します(リモート・ノードに関する情報を保有しているサービスの方を追加します)。

また、ファイル内の編集箇所より前の行にフォーマット・エラーが存在しないことを確認します。先頭のエントリから順に、指定されている各ノードに対して `ping` コマンドを実行して、フォーマット・エラーをチェックします。

5. `/etc/svc.conf` ファイル内で名前からアドレスへの変換メカニズムとして `local` のみを指定している場合には、`/etc/ipnodes` ファイルを編集して、ノード名とアドレスが存在し正しいことを確認します。必要に応じて追加や修正をします。



オンライン・ノードに到達できない場合には、次のいずれかのメッセージが表示されます。

```
host is unreachable
network is unreachable
timeout
```

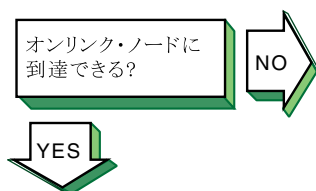
オンライン・ノードまたはルータが存在する場合、`ping` コマンドを使用して、到達できるか確認します。このコマンドに対する応答がないか、紛失するパケットが多い場合には、次の手順を実行します。

1. ノードが LAN に接続されている場合には、`netstat -I device -s` コマンドを使用して、データリンクのカウンタを調べます。調べるカウンタと、考えられる原因は次のとおりです。

- 送信ブロック数または受信ブロック数がゼロの場合、ネットワーク・ハードウェアやケーブルに問題があると考えられます。
 - 高い衝突率は、ネットワークのケーブル接続が不適切であるか、ノードが過度のメッセージ・トラフィックを送信していることが考えられます。
 - データ・オーバランによるエラーと、バッファが利用できないというエラーは、システムの構成が不適切であることを示しています。
2. IPv6 と ICMPv6 のカウンタを、`netstat -p ipv6` コマンドと `netstat -p ipv6-icmp` コマンドを使用して調べます。調べるカウンタと、考えられる原因は次のとおりです。
- ICMP エラーによって発生したエラーによって破棄されたパケットは、他のノードが不正なメッセージを生成していることを示します。他のカウンタに、より詳しい情報が表示されます。
 - 割り当てエラーは、過度のメッセージ・トラフィック、不適切なシステム構成、またはメモリを解放せずに繰り返し割り当てを行っているプログラムの存在を示します。
3. IPv6 ネットワーク・インタフェースが存在し、動作しており、`inet6` アドレスを持っていることを、`ifconfig -a` コマンドを使用して確認します。IPv6 ネットワーク・インタフェースに問題がある場合には、`/etc/rc.config` ファイルと `/etc/ip6rtrd.conf` ファイルが正しいか確認します。
- さらに、`/var/adm/syslog.dated/current/daemon.log` ファイル内で、`ip6rtrd` エラーの有無を調べます。詳細については、11.9 節を参照してください。
- エラーを修正するには、`ip6_setup` ユーティリティを実行します。
4. オンリンク・ノードが起動して動作していること、IPv6 用に正しく構成されていること、および使用しているアドレスがノードのインタフェース上で使用可能になっていることを、オンリンク・ノードの管理者に依頼して確認します。
5. 両方のシステムに IPv4 が構成されている場合には、オンリンク・ノードの IPv4 アドレスに対して `ping` コマンドを実行します。このコマンドが成功した場合は、両方のシステ

ム上で IPv6 構成の確認を行います。このコマンドに対して応答がない場合は、IPv4 ネットワークの問題を解決する必要があります。 10.3 節の手順を参照してください。

6. 同じリンク上の他のノードに対して ping コマンドを実行し、問題が 1 つのノードだけで発生するのか、他のノードでも発生するかを調べます。問題が発生しない部分もある場合は、ネットワーク・デバイスや、リンク上のケーブルに障害が発生している可能性があります。
7. リンクが構成済みトンネルである場合には、次の手順を実行します。
 - a. `ifconfig -a` コマンドを使用して、トンネルの接続元アドレスと接続先アドレスを確認します。トンネルの接続先側ノードの管理者に連絡し、そのノードの接続先/接続元アドレスが、自分の接続元/接続先アドレスと一致しているか確認します。
 - b. トンネルの接続先アドレスに対して ping コマンドを実行します。このコマンドに対して応答がない場合には、IPv4 ネットワークの問題を解決する必要があります。 10.3 節の手順を参照してください。



オフリンク・ノードにアクセスできない場合には、次のいずれかのメッセージが表示されます。

```
host is unreachable
network is unreachable
timeout
```

ping コマンドを使用して、オフリンク・ノードに到達できるか確認します。パケットの紛失率が 100% の場合には、次の手順を実行します。

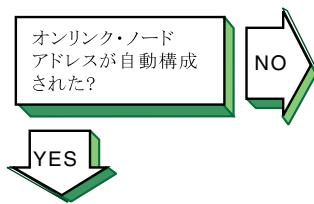
1. ping コマンドを使用して、オフリンク・ノードへのパス上にある次のルータとの接続を確認します。このコマンドに対して応答がないか、紛失するパケットが多い場合は、「オフリンク・ノードに到達できる？」の手順に従ってください。
2. メッセージ送信に使用しているインタフェースに、使用可能なグローバル・ユニキャスト・アドレスまたはサイト・ローカル・ユニキャスト・アドレスがあるかを、`ifconfig -a` コマンドで確認します。使用可能なユニキャスト・アドレスがない場合には、`/etc/ip6rtrd.conf` ファイル

(ip6rtrd.conf(4) を参照) 内でインタフェース・アドレス・プレフィックスが定義されているか確認します。プレフィックスを修正するには、ip6_setup ユーティリティを使用します。

3. リモート・システムが起動して正しく動作していること、IPv6 用に正しく構成されていること、および自分のシステムで使用している IPv6 アドレスとリモート・システムのインタフェースの IPv6 アドレスが一致することを、リモート・システムの管理者に依頼して確認します。アドレスが異なる場合には、ホスト・データベースを確認してください。

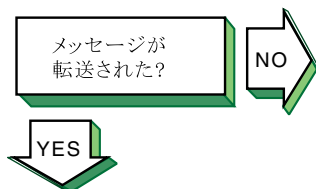
パケット紛失率が高い場合には、ネットワークが混雑しているか、断続的にルーティングの問題が発生している可能性があります。次の手順に従います。

1. ping コマンドを使用して、自分のシステムとオンリンク・ルータとの接続を確認します。
2. traceroute コマンドを使用して、オフリンク・ノードへのパスをトレースします。詳細については、11.6 節と traceroute(8) を参照してください。



IPv6 ホストは、リンク上のルータから提供されたアドレス・プレフィックスを使用して、自分のグローバル・ユニキャスト・アドレスおよびサイト・ローカル・ユニキャスト・アドレスを自動的に生成します。オンリンク・ノードが自分のアドレスを自動構成できない場合には、次の手順に従います。

1. ホストのリンク・ローカル・アドレスを指定して ping コマンドを実行し、ルータからホストへ到達できるか確認します。このコマンドに対して応答がないか、パケットの紛失率が高い場合には、「オンリンク・ノードに到達できる？」の手順に従います。
2. /etc/ip6rtrd.conf ファイルを編集して、正しいプレフィックスを通知するようにルータが構成されていること、タイマの値が適切であることを確認します。詳細については、3.8.11 項と ip6rtrd.conf(4) を参照してください。



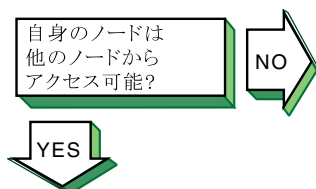
メッセージ送信がルータで失敗しているよだという報告を他のネットワークのユーザから受けた場合、次の手順に従います。

1. ルータが転送していないメッセージの送信元アドレスと宛先のアドレスを取得します。そして ping コマンドを使用して、ルータが各ノードに到達できるか確認します。どちらかのコマンドに対して応答がないか、パケットの紛失率が高い場合には、「オンリンク・ノードに到達できる？」または「オフリンク・ノードに到達できる？」の手順のうち、適切な方に従います。
2. ルータが RIPng プロトコルを実行している場合は、次のコマンドを実行して、IPv6 ルータ・デーモンが動作していることを確認します。

```
# ps ax | grep ip6rtrd
```

このデーモンが動作している場合には、
/etc/ip6rtrd.conf ファイルを編集して、各 IPv6 リンクで RIPng プロトコルが使用可能になっていることを確認します。RIPng プロトコルを使用可能にしないと、ノードが経路を正しく通知できない可能性があります。

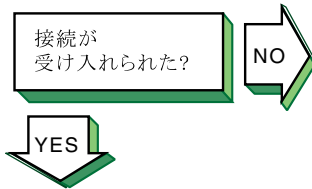
3. 手動経路を使用しているインタフェースと RIPng 経路を使用しているインタフェースが混在していないことを確認します。/etc/routes ファイルで定義された手動経路は、RIPng では他のルータに通知されません。



他のノードから到達できないという報告を受けた場合には、次の手順に従います。

1. ping コマンドを使用して、相手のノードに到達できるか確認します。このコマンドに対して応答がない場合には、そのノードの位置に応じて、「オンリンク・ノードに到達できる？」または「オフリンク・ノードに到達できる？」の手順に従います。
2. 相手が DNS データベース内の名前を使用している場合には、DNS データベースに格納されている自分のノードのアドレスが、システムのインタフェースに構成されているアドレスのいずれかと一致することを確認します。DNS からアドレスを取り出すには nslookup -type=AAAA node-name コマンドを使用し、システムのアドレスを表示するには ifconfig -a コマンドを使用します。

- 相手のノードが、相手のローカル `/etc/ipnodes` ファイルで定義したアドレスを使用している場合には、そのアドレスと、自分のシステムのインタフェースに構成されているアドレスを比較します。 `ifconfig -a` コマンドを使用します。

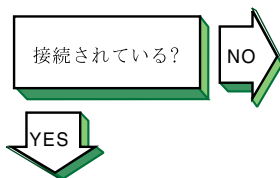


アプリケーションからの接続を受け入れるようにリモート・ノードが構成されていない場合は、次のメッセージが表示されることがあります。

```
connection refused
```

リモート・ノードのシステム管理者に、正しいソケット・ベースのサービス定義が `/etc/services` ファイルと `/etc/inetd.conf` ファイルに定義されているか確認するように依頼します。定義がないか、コメント・アウトされている可能性があります。

ローカルの `/etc/inetd.conf` ファイル内のサービスのプロトコル・フィールドに `tcp6` または `udp6` があるか確認します。



まだ問題がある場合はサービス担当者に報告してください。第 12 章を参照。

接続が異常終了したり、ネットワーク・アプリケーションがハングアップする場合には、次の手順に従います。

- 障害の発生後、直ちに `ping` コマンドを実行し、リモート・ノードとのネットワーク接続を確認します。

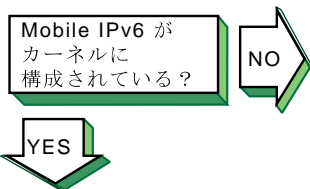
`ping` コマンドに対して応答がないか、パケットの紛失率が高い場合には、そのノードの位置に応じて「オンライン・ノードに到達できる?」または「オフリンク・ノードに到達できる?」の手順に従います。

- アプリケーションが大量のデータをネットワーク送信する場合には、`ping -s 2000 nodename` コマンドを使って、大きなメッセージや分割されたメッセージが正しく処理されているか確認します。

`ping` コマンドに対して応答がない場合には `traceroute nodename 1200` コマンドを実行し、リモート・ノードへのパスを、1200 バイト長のパケットを使用してトレースします。すべての IPv6 リンクは、少なくとも 1280 バイトのメッセージ・サイズをサポートしなければなりません。このコマンドによって、ネットワーク上で問題が発生している位置を特定できることもあります。詳細については、11.6 節と `traceroute(8)` を参照してください。

3. ネットワーク上の他のリンクにあるクライアント・ノードとサーバ・ノードで、同じアプリケーションを実行します。

10.4.3 Mobile IPv6 に関する問題の解決



Mobile IPv6 のサポートがカーネル内に構成されていることを確認します。次のコマンドを実行してください。

```
# sysconfig -q ipv6 mobileipv6_enabled
```

mobileipv6_enabled の属性が設定されていない場合、Mobile IPv6 はカーネル内に構成されていません。正しいカーネルを実行しているか確認してください。正しい場合、doconfig コマンドを使用してカーネルを再構成します。詳細は 3.6.1 項を参照してください。

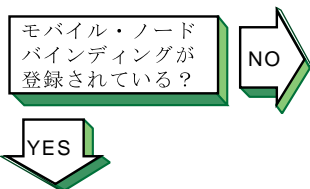
mobileipv6_enabled 属性が設定されているが 1 でない場合は、次のコマンドで再設定します。

```
# sysconfig -r ipv6 mobileipv6_enabled=1
mobileipv6_enabled: reconfigured
```

次のコマンドを実行して IPv6 を再起動します。

```
# /usr/sbin/rcinet restart inet6
```

このコマンドは IPv6 とそのデーモンを停止させ、IPv6 インタフェースを作成して起動し、IPv6 デーモンを開始します。



コレスポンデント・ノードに対して次のコマンドを実行して、コレスポンデント・ノードにモバイル・ノードに対するバインディングがあることを確認します。

```
# netstat -b | grep hostname
```

モバイル・ノードのエントリがなければ、コレスポンデント・ノードで次の手順を実行します。



まだ問題がある場合はサービス担当者に報告してください。第 12 章を参照。

1. tcpdump を実行して、Binding Update および Acknowledgement のパケットを探します。次の表に、拒否された Binding Updates の Status フィールドの値を示します (Status フィールドの値はゼロより大きな値になります)。

Status の値	理由
128	理由は不明
130	管理者により禁止

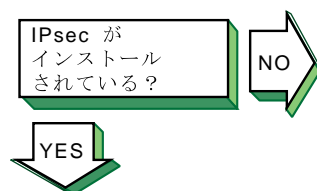
Status の値	理由
131	リソース不足
132	ホームの登録がサポートされていない
133	ホーム・サブネットではない
136	インタフェース識別子の長さが正しくない
137	このモバイル・ノードのホーム・エージェントではない
138	DAD (Duplicate Address Detection) の失敗
139	セキュリティ・アソシエーションがない
141	シーケンス番号が小さすぎる

2. 次のコマンドを実行して、デバッグを有効にします。

```
# sysconfig -r ipv6 mobileip_debug=1
mobileipv6_debug: reconfigured
```

このコマンドは基本的なバインディングの追加、変更、削除のメッセージを表示します。Mobile IPv6 のデバッグ・レベルについては sys_attrs_ipv6(5) を参照してください。

10.5 IPsec に関する問題の解決



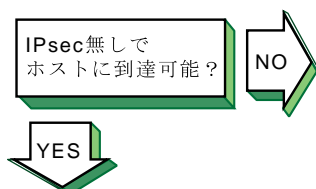
IPsec サブセットがインストールされていることを確認します。次のコマンドを入力してください。

```
# setld -i | grep OSFIPSECBASE
```

次のようなメッセージが表示されます。

```
OSFIPSECBASEnnn installed IPsec Base Components
(Network-Server/Communications)
```

OSFIPSECBASE サブセットがインストールされていない場合は、setld コマンドでインストールします。サブセットのインストールについては、『インストール・ガイド』を参照してください。



IPsec を使用していないときにリモート・ホストに到達できない場合には、次のいずれかのメッセージが表示されます。

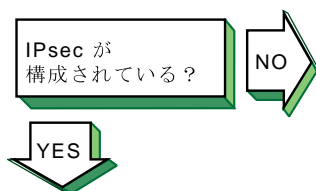
```
host is unreachable
network is unreachable
timeout
```

以下の手順を実行してください。

1. `ipsecd` デーモンがローカル・システムとリモート・システムのどちらでも実行されておらず、どちらのシステムも IP セキュア・モードでないことを確認します。Tru64 UNIX システムでは、次のコマンドを入力して IP セキュア・モードを確認します。

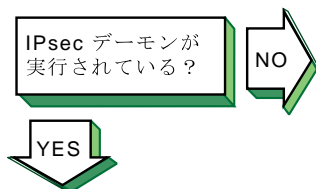

```
# sysconfig -q ipsec ip_secured
```


`ip_secured` の値が 0 の場合、システムは IP セキュア・モードではありません。詳細は `sys_attrs_ipsec(5)` を参照してください。
2. IPv4 接続の場合は、10.3 節の「ホストに到達できる？」の手順を参照してください。
3. IPv6 接続の場合は、10.4 節の「オンライン・ノードに到達できる？」および「オフリンク・ノードに到達できる？」の手順を参照してください。
4. ローカル・システムとリモート・システムがセキュア・ゲートウェイとして動作している場合は、各システムで IP 転送が有効になっていることを確認してください。



SysMan の IPsec アプリケーションを使用して、IPsec が構成されシステムの起動時に有効にされていることを確認します。IPsec が構成され有効になっていれば、メイン・ウィンドウの「Enable IP Security (IPsec)」ボックスがチェックされています。

IPsec が構成されていず有効になっていない場合は、SysMan Menu の IPsec アプリケーションを使用します。IPsec ホストやセキュア・ゲートウェイの設定については、4.7 節を参照してください。



次のコマンドを実行して、ipsecd デーモンが実行されていることを確認します。

```
# ps ax | grep ipsecd
```

デーモンが実行されていない場合は、次のコマンドで実行します。

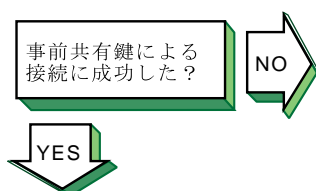
```
# /sbin/init.d/ipsec start
```

IPsec が起動または再起動されると、次のようなメッセージが /var/adm/messages ファイルに出力されます。

```
Apr 18 13:53:18 host1 vmunix: IPSEC: Attaching to the TCP/IP stack
```

問題が発生した場合は、/var/adm/syslog.dated/current/auth.log ファイル内のメッセージを参照してください。

IPsec メッセージの一覧は、付録 B を参照してください。



事前共有鍵を使用した接続に失敗した場合は、次の手順を実行します。

1. リモート・システム上で、IPsec が有効になり構成されていることを確認します。
2. リモート・システムに対して ping コマンドを実行するか、または適切なポートおよびプロトコルを用いてリモート・システムにトラフィックを送信します。失敗した場合は、/var/adm/syslog/dated/current/current/auth.log ファイルにエラーまたは警告メッセージが出力されていないか確認します。たとえば、ESP プロトコルを用いた正常な接続では、次のようなログ・メッセージが出力されます。

```
Jun 7 16:24:22 fddicon8 syslog: Phase-1 [initiator] done.  
Created SA between IDs ipv4(udp:500,[0..3]=16.140.64.106)  
and ipv4(udp:500,[0..3]=16.140.64.223).  
Jun 7 16:24:22 fddicon8 syslog: Phase-2 [initiator] done.  
Created 2 SA's by rule fddicon8-spaced(13):'ipsec  
ipv4(any:0,[0..3]=16.140.64.106)<->ipv4(any:0,[0..3]=16.140.64.223)'
```

ipsecd デーモンに対してデバッグと追加ログ・メッセージを有効にするには、次のコマンドを実行します。

```
# rcmgr set IPSEC_ARGS "-d -m 2"
```

次に、以下のコマンドで IPsec を停止して開始します。

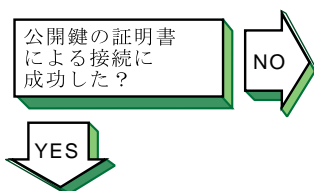
```
# /sbin/init.d/ipsec stop  
# /sbin/init.d/ipsec start
```

3. netstat -X -v コマンドを実行して、リモート・システムとのフェーズ 1 (IKE) SA が確立されたことを確認します。

フェーズ 1 SA が確立されなかった場合は、両方のシステムの構成について以下の項目を確認します。

- IPsec ポリシで正しい IP アドレスが使用され、それがシステムに構成されているアドレスに一致していることを確認します。トンネル・モードを使用している場合、このアドレスはローカルおよびリモートのセキュア・ゲートウェイのアドレスになることもあります。両方のシステムが、IPsec の保護が適用されるように構成されていることを確認してください。
- セキュア・ゲートウェイ構成では、保護されているトラフィックの仕様が、両方のシステムで完全に一致していることを確認します。たとえば、10.0.1.1/24 のサブネット仕様は 10.0.1.1 - 10.0.1.255 の範囲にも、10.0.0.27 のような特定のホストとも一致しません。
- 接続の事前共有鍵が両方のシステムで完全に一致していることを確認します。事前共有鍵が一致していないと、無効なペイロード・タイプやフォーマット・エラーなどとして報告されます。これは IKE プロトコル・データの暗号が正しく解読されないためです。また、ローカル ID がリモート・システムが想定しているものと一致していることも確認してください (通常は、ローカル・システムの、適切な IP アドレス)。
- 事前共有鍵を使用する認証を指定するプロポーザルが IKE プロポーザル・リストに含まれ、プロポーザル内の他のパラメータがリモート・システムのパラメータに一致していることを確認します。
- 接続に対して指定された IKE グループと PFS 設定が、リモート・システムが想定しているものと一致していることを確認します。省略時は PFS を持たない IKE グループ 2 です。
- 両方のシステムで同じ折衝モード (Main または Aggressive) が使用されていることを確認します。
- 2 つのホストの間に、IKE (UDP のポート 500) トラフィックをブロックしたり衝突するような NAT (Network Address Translator) やファイアウォールがないことを確認します。

4. 1 つまたは複数のフェーズ 2 (IPsec) SA が、`netstat -x -v` コマンドを用いてリモート・システムとの間に確立されていることを確認します。フェーズ 2 SA が 1 つも確立されていない場合は、両方のシステムの構成について以下の項目を確認してください。
 - IPsec プロポーザル・リストに、リモート・システム上のプロポーザルと一致するプロポーザルが少なくとも 1 つ含まれていることを確認します。
 - 接続に関する PFS 設定がリモート・システムでの設定と一致し、PFS が使用中であれば PFS グループが一致していることを確認します。
 - ローカル・システムとリモート・システムの SA 存続期間が一致していることを確認します。多くの場合、省略時の値として、要求される最短の存続期間になっています。ただし、IPsec の実装によっては、両方のシステムで同じ値にしたり、特定の範囲内の値にする必要があります。
5. フェーズ 1 とフェーズ 2 の SA がどちらも確立されている場合は、2 つのホストの間に、IPsec 保護 (AH または ESP) トラフィックをブロックしたり衝突するような NAT やファイアウォールがないことを確認します。
6. `/var/adm/syslog.dated/current/auth.log` ファイル内のメッセージが問題を示している場合は、IPsec SysMan アプリケーションを用いてセキュリティ・ポリシーを変更する必要があります。アプリケーションが多数のエラーを検出しても、その中には IPsec ポリシ・マネージャが実際にポリシーを使用して鍵と証明書を関連付けるまでは明らかにならないものがあります。IPsec メッセージのリストは、付録 B を参照してください。



まだ問題がある場合はサービス担当者に報告してください。第 12 章 を参照してください。

公開鍵の証明書を使用した接続に失敗した場合は、次の手順を実行します。

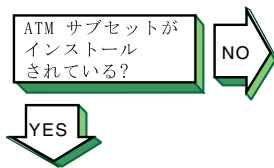
1. 証明書ベースの認証を使用する IKE プロポーザル・リストを選択して、適切な証明書ファイルを定義します。
2. リモート・システムに対して ping コマンドを実行するか、または適切なポートとプロトコルでリモート・システムにトラフィックを送信します。どちらも失敗した場合は、`/var/adm/syslog/dated/current/current/auth.log` ファイル内にエラーまたは警告メッセージが出力されていないか調べてください。エラーまたは警告メッセージがあったときには、以下の操作を実行します。
 - 両方のシステムで使用する CA 証明書が構成され CA 証明書としてマークされていることを確認します。証明書の階層内に複数のレベルがある場合、複数の証明書を構成する必要があります。
 - CRL ファイルが構成されていない場合は、CRL チェックが無効になっていることを確認します。
 - 暗号化フォーマット (PEM, Binary, HEXL) が、すべての証明書に対して正しく指定されていることを確認します。
 - ローカル・システムの証明書が構成され、構成された CA 証明書によって署名されていることを確認します。`ipsec_certview` ユーティリティを使用して、証明書の属性を調べます。
 - ローカル・システムの証明書に対して正しい非公開鍵ファイルが構成されていることを確認します。証明書と非公開鍵が実際に一致することを確認するには、`ipsec_keypaircheck` ユーティリティを使用します。
 - 証明書が有効期限内であることを確認します。CRL チェックが使用中の場合は、システムの証明書が取り消されていないか確認します。
 - ローカル・システムの証明書が正しい ID (IP アドレス、ドメイン名など) を含み、ID のタイプがリモート・システムが期待するものと一致していることを確認します。IPsec の実装によっては、証明書内の `subjectAltName` 属性を 1 つしか処理できないものがあります。

- IKE プロポーザル・リストに、適切な証明書タイプ (RSA または DSA) を使用する認証を指定するプロポーザルが含まれていることを確認します。また、プロポーザル内の他のパラメータがリモート・システムのもものと一致していることを確認します。
- RSA 暗号化モードを使用して認証が行われる場合、リモート・システムの ID 証明書がローカル・システムに構成されていることを確認します (RSA 署名モードでは、この証明書は自動的に IKE 経由で送られます)。また、RSA 暗号化モードでは、証明書に IP アドレスを含む subjectAltName 属性があることを確認します。IKE は、リモート・システムの IP アドレスだけが分かっているときに、正しい証明書を識別できなければなりません。

IPsec メッセージの一覧は、付録 B を参照してください。

3. /var/adm/syslog.dated/current/auth.log ファイル内のメッセージが問題を示している場合は、IPsec SysMan アプリケーションを用いてセキュリティ・ポリシーを変更する必要があります。アプリケーションが多数のエラーを検出しても、その中には IPsec ポリシ・マネージャが実際にポリシーを使用して鍵と証明書を関連付けるまでは明らかにならないものがあります。IPsec メッセージのリストは、付録 B を参照してください。

10.6 ATM に関する問題の解決



ATM サブセットがインストールされていることを確認します。
次のコマンドを入力します。

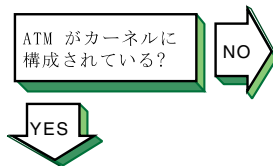
```
# setld -i | grep OSFATM
```

次のメッセージが表示されます。

```
OSFATMnnn installed ATM Commands
(Network-Server/Communications)
OSFATMBINnnn installed ATM Kernel
Modules (Kernel Build Environment)
OSFATMBINCOMnnn installed ATM Kernel
Header and Common Files
(Kernel Build Environment)
OSFATMBINOBJECTnnn installed ATM Kernel
Objects (Kernel Software Environment)
```

OSFATM、OSFATMBIN、および OSFATMBINCOM サブセットがインストールされていない場合は、setld コマンドを使用して

インストールします。これらのサブセットのインストール方法の詳細については、『インストール・ガイド』を参照してください。

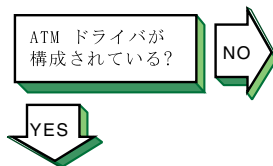


必要な ATM がカーネルに構成されていることを確認します。次のコマンドを入力します。

```
# sysconfig -q atm
```

何も表示されない場合は、ATM がカーネルに構成されていません。ATM オプション、および必要に応じて追加の ATM オプションを使用して、カーネルを再構成します。ATM カーネル・オプションのリストとカーネルを再構成する方法の詳細については、6.2.2 項を参照してください。

ATM が構成されている場合は、`sysconfig -q` コマンドを使用して、追加の ATM カーネル・オプションが構成されていることを確認します。必要に応じて、追加のオプションを使用してカーネルを再構成します。



`atmconfig drvlist` コマンドを使用して、ドライバが構成されていることを確認します。ドライバが構成されている場合は、次のような出力が表示されます。

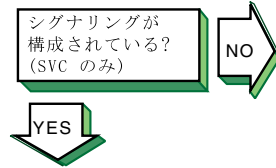
```
Name: lta0          Type: STS-3          State: UP
Driver ID: 1      ESIs: 8      PPAs: 9      VCs: 6
```

CLIP (Classical IP) については 10.6.1 項へ、LAN エミュレーションについては 10.6.2 項へ、また、IP スイッチングについては 10.6.3 項へ進んでください。

ドライバのエントリが存在しない場合は、`genvmunix` カーネルを使用してシステムをリブートしてから、`doconfig` ユーティリティを実行して、必要なドライバを使用してカーネルを構築します。

ドライバの状態が UP でない場合は、必要な ATM サービスについて `atmsetup` ユーティリティを実行します。CLIP (Classical IP) については 6.3.2.4 項を、LANE (LAN エミュレーション) については 6.3.3.3 項を、IP スイッチングについては 6.3.4.2 項をそれぞれ参照してください。

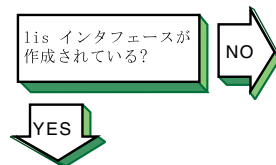
10.6.1 CLIP に関する問題の解決



シグナリングが構成されていることを確認します。次のコマンドを入力します。

```
# atmsig status driver=driver_name
```

UNI のバージョン番号が表示されない場合、または ILMI 状態が Unknown の場合は、atmsetup ユーティリティを実行して、シグナリングを構成します。詳細については、6.3.2.4 項を参照してください。

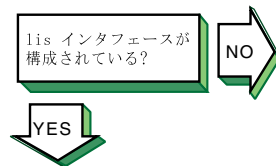


CLIP の lis インタフェースが作成されていることを確認します。次のコマンドを入力します。

```
# atmarp -h
```

lis インタフェースが作成されている場合は、作成された全部の LIS のステータス、およびホストが ARP クライアントか ARP サーバかを示すデータが表示されます。

LIS が作成されていない場合は、atmsetup ユーティリティを実行して CLIP を構成します。詳細については、6.3.2.4 項を参照してください。



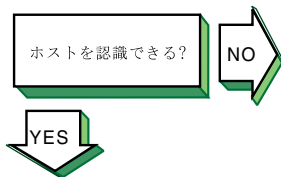
lis インタフェースが構成されていることを確認します。次のコマンドを入力します。

```
# ifconfig lissx
```

lis インタフェースが構成されている場合、次のような情報が表示されます。

```
lis0: flags=c23<UP,BROADCAST,NOTRAILERS,MULTICAST,SIMPLEX>  
inet 10.140.120.52 netmask ffffffff broadcast 10.140.120.255  
ipmtu 1500
```

lis インタフェースが構成されていない場合は、netconfig ユーティリティを実行してそれを構成するか、SysMan Menu から Interfaces アプリケーションを使用します。詳細については、6.3.2.5 項を参照してください。



リモート・ホストが認識されない場合は、次のメッセージが表示されます。

unknown host

この場合は、次の手順に従ってください。

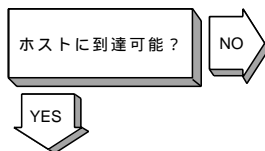
1. リモート・ホストに到達するために、ユーザが有効なホスト名を使用しているかどうか確認します。
2. リモート・ホストが他のネーム・ドメインに属すること、およびユーザが完全なドメイン名を指定していることを確認します。
3. 名前からアドレスへの変換に DNS を使用しているサイトの場合は、`/etc/svc.conf` ファイルの内容を調べ、`hosts` データベース・エントリのサービスとして `bind` が指定されているか確認します。指定されていない場合は、それを追加します。

また、DNS がリモート・ホストについての情報を持っていることも確認します。『ネットワーク管理ガイド：サービス編』の「DNS/BIND クライアントに関する問題の解決」の手順を参照してください。

4. 名前からアドレスへの変換に NIS ネーム・サービスを使用しているサイトの場合は、`/etc/svc.conf` ファイルの内容を調べ、`hosts` データベース・エントリのサービスとして `nis` が指定されているか確認します。指定されていない場合は、ファイルを編集してそれを追加します。

また、NIS サービスがリモート・ホストについての情報を持っていることも確認します。『ネットワーク管理ガイド：サービス編』の「NIS クライアントに関する問題の解決」の手順を参照してください。

5. `/etc/svc.conf` ファイルで、名前からアドレスへの変換メカニズムとして、`local` しか記載されていない場合は、`/etc/hosts` ファイルにリモート・ホストについての情報はありません。詳細については、`svc.conf(4)` を参照してください。

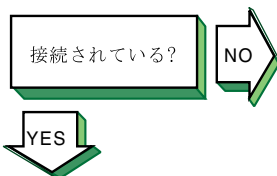


リモート・ホストに到達できない場合は、次のメッセージが表示されます。

```
host is unreachable
```

この場合は、次の手順に従ってください。

1. ローカル・ホストとスイッチ間のケーブルが正しく接続されており、ケーブルに損傷がないことを確認します。
2. `ping` コマンドを使用して、スイッチの IP コントローラへのネットワーク接続を確認します。このコマンドが失敗した場合は、`ifconfig` コマンド・パラメータが誤っているか、または IP コントローラがダウンしているかそのインタフェースに問題があることが考えられます。スイッチ管理者に問い合わせてください。
3. `ping` コマンドを使用して、対象のリモート・ホストへのネットワーク接続を確認します。コマンドが失敗する場合は、`traceroute` コマンドを使用してリモート・ホストへのルートを確認してください。



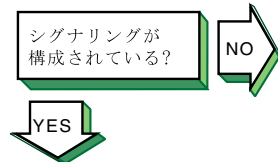
まだ問題がある場合は、サービス担当者に報告してください。第 12 章を参照。

接続が異常終了した場合は、次の手順に従ってください。

1. ネットワークをテストして、問題がローカル・ホストにあるのか、リモート・ホストにあるのか、またはそれらの間のパスにあるのかを判断します。詳細については、10.3 節を参照してください。
2. どのホストに問題があるかが分かったら、次の手順に従ってください。
 - a. ネットワーク・デバイスが正しく構成されていることを確認します。ローカル・ホストのブロードキャスト・アドレスおよびアドレス・マスクが正しいことを確認します。ネットワーク・デバイスの構成については、2.3 節を参照してください。
 - b. ローカル・ホストの `hosts` データベース中の IP アドレスが正しいことを確認します。
 - c. ローカル・ホストからネットワークへの配線に誤りがなく、正しく接続されていることを確認します。

- d. LAN 接続の場合は、ARP エントリが適切であること、およびシステムが LAN に正しく接続されていることを確認します。

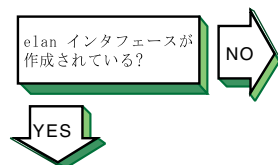
10.6.2 LANE に関する問題の解決



シグナリングが構成されていることを確認します。次のコマンドを入力します。

```
# atmsig status driver=driver_name
```

UNI (User-Network Interface) のバージョン番号が表示されない場合、または ILMI (Integrated Layer Management Interface) の状態が Unknown の場合は、atmsetup ユーティリティを実行して、シグナリングを構成します。詳細については、6.3.3.3 項を参照してください。



elan インタフェースが作成されていることを確認します。次のコマンドを入力します。

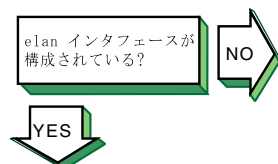
```
# atmelan show
```

elan インタフェースが作成されている場合は、次のような情報が表示されます。

```
⋮  
control state: S_OPERATIONAL  
⋮
```

制御状態が S_OPERATIONAL でない場合は、次の手順を実行します。

1. lane サブシステムのメッセージ・ロギング・レベルを上げます。詳細は、6.4.6 項を参照してください。
2. スイッチの UNI バージョンがシステムの UNI バージョンと一致していることを確認します。
3. スイッチ上の LES (LAN Emulation Server) が正しく構成されていることを確認します。



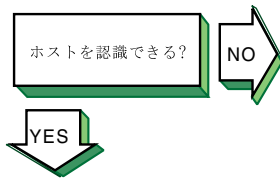
elan インタフェースが構成されていることを確認します。次のコマンドを入力します。

```
# ifconfig elanx
```

elan インタフェースが構成されている場合は、次のような情報が表示されます。

```
elan0: flags=c23<UP,BROADCAST,NOTRAILERS,MULTICAST,SIMPLEX>
      inet 10.140.120.52 netmask ffffffff broadcast 10.140.120.255
      ipmtu 1500
```

elan インタフェースが構成されていない場合は、netconfig ユーティリティを実行してそれを構成するか、SysMan Menu から Interfaces アプリケーションを使用します。詳細については、6.3.3.4 項を参照してください。



リモート・ホストが認識されない場合は、次のメッセージが表示されます。

unknown host

この場合は、次の手順に従ってください。

1. リモート・ホストに到達するために、ユーザが有効なホスト名を使用していることを確認します。
2. リモート・ホストが他のネーム・ドメインに属していること、およびユーザが完全なドメイン名を指定していることを確認します。
3. 名前からアドレスへの変換に DNS を使用しているサイトの場合は、`/etc/svc.conf` ファイルの内容を調べ、`hosts` データベース・エントリのサービスとして `bind` が指定されているか確認します。指定されていない場合は、それを追加します。

また、DNS がリモート・ホストについての情報を持っていることも確認します。『ネットワーク管理ガイド：サービス編』の「DNS/BIND クライアントに関する問題の解決」の手順を参照してください。

4. 名前からアドレスへの変換に NIS ネーム・サービスを使用しているサイトの場合は、`/etc/svc.conf` ファイルの内容を調べ、`hosts` データベース・エントリのサービスとして `nis` が指定されているか確認します。指定されていない場合は、ファイルを編集してそれを追加します。

また、NIS サービスがリモート・ホストについての情報を持っていることも確認します。『ネットワーク管理ガイド：サービス編』の「NIS クライアントに関する問題の解決」の手順を参照してください。

5. `/etc/svc.conf` ファイルで、名前からアドレスへの変換メカニズムとして、`local` しか記載されていない場合

は、`/etc/hosts` ファイルにリモート・ホストについての情報がありません。詳細については、`svc.conf(4)` を参照してください。

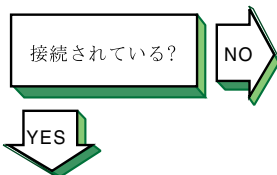


リモート・ホストに到達できない場合は、次のメッセージが表示されます。

`host is unreachable`

この場合は、次の手順に従ってください。

1. ローカル・ホストとスイッチ間のケーブルが正しく接続されており、ケーブルに損傷がないことを確認します。
2. `ifconfig elanx` コマンドを使用して、リンク上のアドレスが正しいことを確認します。
3. `ping` コマンドを使用して、対象のリモート・ホストへのネットワーク接続を確認します。コマンドが失敗する場合は、`traceroute` コマンドを使用してリモート・ホストへのルートを確認してください。



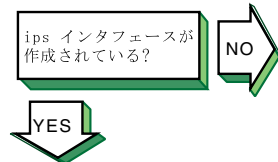
まだ問題がある場合は、サービス担当者に報告してください。第 12 章を参照。

接続が異常終了した場合は、次の手順に従ってください。

1. ネットワークをテストして、問題がローカル・ホストにあるのか、リモート・ホストにあるのか、またはそれらの間のパスにあるのかを判断します。詳細については、10.3 節を参照してください。
2. どのホストに問題があるかが分かったら、次の手順に従ってください。
 - a. ネットワーク・デバイスが正しく構成されていることを確認します。ローカル・ホストのブロードキャスト・アドレスおよびアドレス・マスクが正しいことを確認します。ネットワーク・デバイスの構成については、2.3 節を参照してください。
 - b. ローカル・ホストの `hosts` データベース中の IP アドレスが正しいことを確認します。
 - c. ローカル・ホストからネットワークへの配線に誤りがなく、正しく接続されていることを確認します。

- d. LAN 接続の場合は，ARP エントリが適切であること，およびシステムが LAN に正しく接続されていることを確認します。

10.6.3 IP スイッチに関する問題の解決



IP スイッチングの `ips` インタフェースが作成されていることを確認します。次のコマンドを入力します。

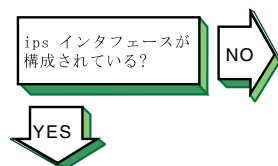
```
# atmifmp showips
```

`ips` インタフェースが作成されている場合は，作成された `ips` インタフェースごとに，次のような情報が表示されます。

```
ips0:
    Attached to driver lta0
    Default (SNAP) VC = 32
    IP Traffic VC = 1850 (Unused - peer does
        not support Flow Type 0)
    Min Tx VC = 1
    Max Tx VC = 2048
    Min Rx VC = 1
    Max Rx VC = 2048
    Driver Min Tx VC = 1
    Driver Max Tx VC = 2048
    Driver Min Rx VC = 1
    Driver Max Rx VC = 2048
    Peer does not support Flow Type 0
```

この例は，`ips0` インタフェースが作成され，ドライバ `lta0` にアタッチされていることを示します。

`ips` がまったく見つからない場合は，`ips` を 1 つまたはそれ以上作成します。詳細については，6.3.4 項を参照してください。



`ips` インタフェースが構成されていることを確認します。次のコマンドを入力します。

```
# ifconfig ipsx
```

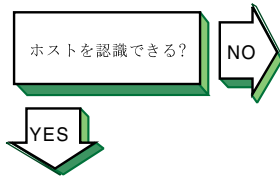
`ips` インタフェースが構成されている場合は，次のような情報が表示されます。

```
ips0: flags=4d1<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
    inet 16.142.128.129 --> 16.142.128.130 netmask ffffffff ipmtu 1500
```

この例は，インタフェースが起動されて動作中で，アドレスがポイント・ツー・ポイント・リンクの各エンドに対して構成されていることを示します。

`ips` インタフェースが構成されていない場合は，`netconfig` ユーティリティを実行してそれを構成するか，SysMan Menu

から Interfaces アプリケーションを使用します。詳細については、6.3.4.3 項を参照してください。



リモート・ホストが認識されない場合は、次のメッセージが表示されます。

unknown host

この場合は、次の手順に従ってください。

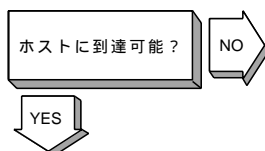
1. リモート・ホストに到達するために、ユーザが有効なホスト名を使用していることを確認します。
2. リモート・ホストが他のネーム・ドメインに属していること、およびユーザが完全なドメイン名を指定していることを確認します。
3. 名前からアドレスへの変換に DNS を使用しているサイトの場合は、`/etc/svc.conf` ファイルの内容を調べ、`hosts` データベース・エントリのサービスとして `bind` が指定されているか確認します。指定されていない場合は、ファイルを編集してそれを追加します。

また、DNS がリモート・ホストについての情報を持っていることも確認します。『ネットワーク管理ガイド：サービス編』の「DNS/BIND クライアントに関する問題の解決」の手順を参照してください。

4. 名前からアドレスへの変換に NIS ネーム・サービスを使用しているサイトの場合は、`/etc/svc.conf` ファイルの内容を調べ、`hosts` データベース・エントリのサービスとして `nis` が指定されているか確認します。指定されていない場合は、ファイルを編集してそれを追加します。

また、NIS サービスがリモート・ホストについての情報を持っていることも確認します。『ネットワーク管理ガイド：サービス編』の「NIS クライアントに関する問題の解決」の手順を参照してください。

5. `/etc/svc.conf` ファイルで、名前からアドレスへの変換メカニズムとして、`local` しか記載されていない場合は、`/etc/hosts` ファイルにリモート・ホストについての情報はありません。詳細については、『システム管理ガイド』を参照してください。

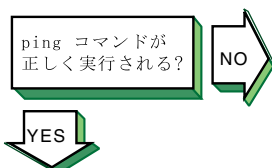


リモート・ホストに到達できない場合は、次のメッセージが表示されます。

```
host is unreachable
```

この場合は、次の手順に従ってください。

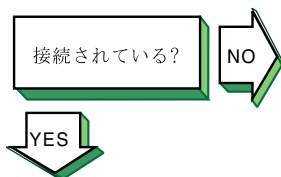
1. `ifconfig ipsx` コマンドを使用して、ポイント・ツー・ポイント・リンク上の、スイッチへのアドレスが正しいことを確認します。
2. `ping` コマンドを使用して、スイッチ上の IP コントローラへのネットワーク接続を確認します。このコマンドが失敗した場合は、ローカル・ホストの `ifconfig` コマンド・パラメータが誤っていることが考えられます。また、スイッチ上で IP コントローラがダウンしているか、そのインタフェースに問題があることも考えられます。スイッチ管理者に問い合わせてください。
3. `netstat -r` コマンドを使用して、リモート・ホストのサブネットへの `ips` ルートが存在することを確認します。



`ping` コマンドが失敗する場合、次の手順に従ってください。

1. ローカル・ホストとスイッチ間のケーブルが正しく接続されており、ケーブルに損傷がないことを確認します。
2. ローカル・ホストで指定されている SNAP (Subnetwork Attachment Point) VC (仮想回線) が、スイッチの SNAP VC に一致していることを確認します。
3. リモート・システムの管理者に連絡して、リモート・システムが起動されて動作中であり、IP スイッチングが正しく構成されていることを確認します。
4. `tracert` コマンドを使用して、リモート・ホストへのルートを確認します。出力の最初のホップが IP コントローラではなく省略時のネットワーク・インタフェースを示す場合、IP コントローラ経由でリモート・サブネットに至る静的ルートを、ルーティング・テーブルに追加します。変更内容の確認には、`netstat -r` コマンドを使用します。

ルートが IP コントローラに到達しているが、それより先に到達しない場合は、リモート・システムの管理者に連絡して、システムが正しく構成され、ルーティング・テーブルが正しいことを確認します。

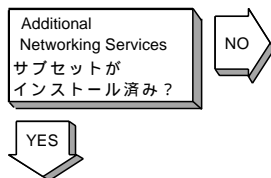


まだ問題がある場合は、サービス担当者に報告してください。第 12 章 を参照。

接続が異常終了した場合は、次の手順に従ってください。

1. ネットワークをテストして、問題がローカル・ホストにあるのか、リモート・ホストにあるのか、またはそれらの間のパスにあるのかを判断します。詳細については、10.3 節 を参照してください。
2. どのホストに問題があるかが分かったら、次の手順に従ってください。
 - a. ネットワーク・デバイスが正しく構成されていることを確認します。ローカル・ホストのブロードキャスト・アドレスおよびアドレス・マスクが正しいことを確認します。ネットワーク・デバイスの構成については、2.3 節 を参照してください。
 - b. ローカル・ホストの `hosts` データベース中の IP アドレスが正しいことを確認します。
 - c. ローカル・ホストからネットワークへの配線に誤りがなく、正しく接続されていることを確認します。

10.7 DHCP に関する問題の解決



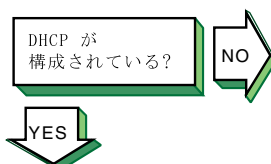
Additional Networking Services サブセットがインストールされていることを確認します。次のコマンドを入力します。

```
# setld -i | grep OSFINET
```

このサブセットがインストール済みであれば、次のメッセージが表示されます。

```
OSFINETnnn installed Additional Networking Services
(Network-Server/Communications)
```

サブセットがインストールされていない場合は、`setld` コマンドを使用してインストールします。このサブセットのインストール方法の詳細については、『インストール・ガイド』を参照してください。



次の手順を実行して、DHCP (Dynamic Host Configuration Protocol) がサーバとクライアントの両方で構成されていることを確認します。

1. `rcmgr` ユーティリティを使用して、DHCP サーバにある `/etc/rc.config.common` ファイルの `JOIND` エントリの値を表示します。

```
# rcmgr get JOIND
```

何も返されない場合は、SysMan Menu ユーティリティを実行して DHCP サーバを構成します。詳細については、7.3.7 項を参照してください。

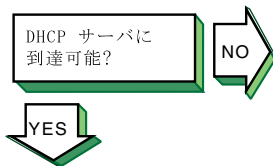
2. rcmgr ユーティリティを使用して、DHCP クライアントにある `/etc/rc.config` ファイルの `IFCONFIG_n` エントリの値を表示します。次に例を示します。

```
# rcmgr get IFCONFIG_0
```

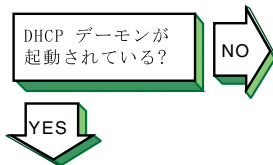
次のような値が表示されます。

```
DYNAMIC netmask n.n.n.n
```

このような値が返されない場合は、SysMan Menu ユーティリティを実行して DHCP クライアントを構成します。詳細については、2.3 節を参照してください。



ping コマンドを使用して、DHCP サーバが動作状態にあり、到達可能であることを確認します。



DHCP デーモン (joind) がサーバ上で動作状態にあることを確認します。次のコマンドを入力します。

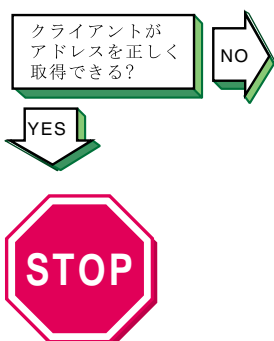
```
# ps -e | grep joind
```

または、SysMan Menu ユーティリティを使用して、DHCP デーモンのステータスを表示することも可能です。次のコマンドを入力すれば、「status」ダイアログ・ボックスに直接進むことができます。

```
# /usr/sbin/sysman dmnstatus
```

DHCP デーモンが動作状態にない場合、次のコマンドを使用して起動します。

```
# /usr/sbin/joind
```



まだ問題がある場合は、サービス担当者に報告してください。第 12 章を参照。

DHCP クライアントがサーバから DHCP 情報を取得できない場合は、次の手順に従ってください。

1. クライアントのために入力した MAC (Media Access Control) を確認します。特に Microsoft クライアントのユーザは、必ず 7.3.5 項を参照してください。Microsoft クライアントが MAC アドレスを DHCP サーバに送信する前に、MAC アドレスをどのように変更するかが説明されています。
2. 次の手順に従って、joind デーモンにデバッグ・フラグを付けて実行します。
 - a. `kill -HUP` コマンドを使用して、joind デーモンを停止します。

注意

`kill -9` コマンドで DHCP サーバ・デーモンを停止してはいけません。データベース・ファイルが破壊されるおそれがあります。

- b. 次のように、joind デーモンにデバッグ・フラグを付けて再起動します。

```
# /usr/sbin/joind -d4
```

joind を `/etc/inetd.conf` ファイルから実行している場合は、次の手順に従ってください。

- i. `/etc/inetd.conf` ファイルを編集して、`-d4` フラグを追加します。
 - ii. `kill -HUP` コマンドで joind デーモンを停止します。
 - iii. `inetd -h` コマンドで inetd デーモンを停止します。これにより、inetd デーモンが `/etc/inetd.conf` ファイルを再度読み取ります。

代わりに、SysMan Menu ユーティリティを使用して、デバッグ・オプションで DHCP サーバを構成することも可能です。詳細については、7.3.7 項を参照してください。

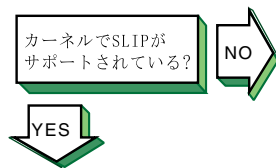
3. /var/join/log ファイルで、DHCP クライアントの問題の原因が解消されたか確認します。

以下は /var/join/log ファイル・メッセージの例で、DHCP がサーバ・システムにメッセージが到着したことを検出したが、IP サブネットワークのアドレス・レンジが未定義であることを示しています。

```
DHCPDISCOVER from HW address 08:00:2b:96:79:b6 :  
network not administered by server
```

この問題は、アドレス・レンジが定義されていても、
/etc/join/netmasks ファイルに、この IP ネットワークのサブネットワーク・マスク定義がない場合にも生じます。この場合はネットマスク・ファイルを編集し、サブネットワークのエントリを追加してから、DHCP サーバ /usr/sbin/joind を再起動します。

10.8 SLIP に関する問題の解決



netstat -in コマンドを使用して、正しい数の SLIP (Serial Line Internet Protocol) 擬似デバイスが、カーネルでサポートされていることを確認します。SLIP がサポートされている場合は、各インタフェースに対して次のような出力が表示されます。

```
sl0* 296 <Link> 0 0 0 0 0
```

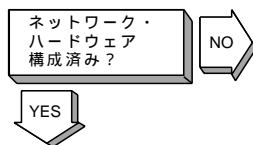
接頭文字 sl は、SLIP がシステムでサポートされていることを示します。この例では、SLIP 擬似デバイスは1つです。

SLIPインタフェースを追加する場合は、/etc/sysconfigtab ファイルで、net: サブシステムの下に nslip=x 属性を追加して指定します。SLIP インタフェースの追加についての説明は、『システム管理ガイド』を参照してください。

24 MB メモリのシステムでは、SLIP はカーネルに組み込まれません。SLIP をカーネルに追加する場合は、システム構成ファイル (/usr/sys/confhostname) を編集して次のようなエントリを追加してください。

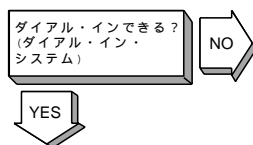
```
options SL
```

詳細については、『システム管理ガイド』を参照してください。



ネットワーク・ハードウェアを次のように構成します。

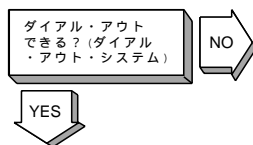
- 正しいハードウェアを使用していることを確認します。詳細は 8.1.2.1 項を参照してください。
- モデムが次のように構成されていることを確認します。
 - パリティなしの 8 ビット文字を使用していること。
 - ソフトウェアのフロー制御 (XON/XOFF) を禁止していること。
 - ダイヤル・イン・システムの場合は、8.1.3.1 項のガイドラインに従う。
 - ダイヤル・アウト・システムの場合は、8.1.3.2 項のガイドラインに従う。



リモート・システムが正しくダイヤル・インできない場合は、次の手順に従います。

1. `/usr/spool/locks` ディレクトリ内で `LCK..tty nn` ロック・ファイルの有無を調べます。SLIP 用に構成している端末デバイスのロック・ファイルがあれば、それを削除してください。

端末デバイス経由で接続を確立すると、他のアプリケーションによって接続が切られないようにするために、システムがロック・ファイルを生成します。この接続が正しい手続きを経ずに切断されると、ロック・ファイルが残り、新しい接続が確立できなくなります。
2. `/etc/slhosts` ファイルを編集して、ログインできないログイン・エントリに `debug` オプションを追加します。詳細については、`slhosts(4)` を参照してください。
3. リモート・ユーザに再度ダイヤル・インするよう指示します。
4. `/var/adm/syslog.dated/current/daemon.log` ファイル内で、ダイヤル・イン・システムでの SLIP の問題に関する情報を調べます。詳細については、11.9 節を参照してください。



リモート・システムにダイアル・アウトできない場合は、次の手順に従います。

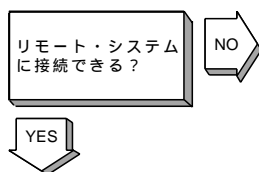
1. `/usr/spool/locks` ディレクトリ内で `LCK..ttynn` ロック・ファイルの有無を調べます。SLIP 用に構成している端末デバイスのロック・ファイルがあれば、それを削除してください。

端末デバイス経由で接続を確立すると、他のアプリケーションによって接続が切られないようにするために、システムがロック・ファイルを生成します。この接続が正しい手続きを経ずに切断されると、ロック・ファイルが残り、新しい接続が確立できなくなります。

2. モデムが正しく動作していることを確認します。

`/etc/acucap` ファイルを編集してモデムのエントリに `db` オプションを含めます。このオプションにより、新しいエントリのデバッグに役立つ情報が出力されます。詳細については、`acucap(4)` を参照してください。

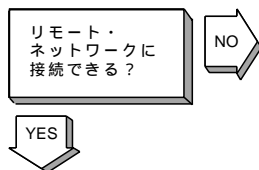
3. 次の手順で、SLIP の設定を確認します。
 - a. `startslip` ダイアル・アウト・スクリプト・ファイルを編集して `debug` サブコマンドとデバッグ・ログ・ファイルを指定します。
 - b. 再度ダイアル・アウトを試みます。
 - c. デバッグ・ログファイル内で、SLIP ダイアル・アウトに関する情報を調べます。



リモート・ホストと通信できず、デバッグ・メッセージがエラーを表示しない場合は、次の手順に従ってください。

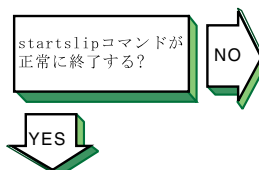
1. 接続している両方のシステムで、IP アドレスとネットマスクが正しく設定されていることを確認します。
2. 接続している両方のシステムで、次の SLIP 構成パラメータを調べます。
 - ICMP (Internet Control Message Protocol) 通信量抑制
ローカル・エンドまたはリモート・エンドで可能にされていると、`ping` コマンドは異常終了します。
 - TCP ヘッダ圧縮

ローカル・エンドまたはリモート・エンドの一方で可能にされている場合は、他方でも TCP ヘッダ圧縮を可能にするか、または自動で可能にしておく必要があります。



リモート・ホストとは通信できるが、そのリモート・ホストが接続されているネットワークと通信できない場合は、次の手順に従います。

1. ローカル・システムがリモート・システムをゲートウェイ・システムとして使用している場合、ローカル・システムで `netstat -rn` コマンドを実行して、リモート SLIP アドレスが省略時のゲートウェイであることを確認します。
2. ゲートウェイ・システム (リモート・システム) で `iprsetup -d` コマンドを実行して、`ipforwarding` と `ipgateway` 変数がオンになっているかどうか調べます。オフになっている場合は、`iprsetup -s` コマンドでオンにします。
3. ゲートウェイ・システムで `gated` デーモンが実行されているか確認します。詳細については `gated(8)` を参照してください。

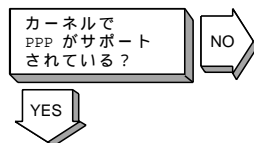


まだ問題がある場合はサービス担当者に報告してください。第 12 章 を参照。

`startslip` コマンドが異常終了する場合は、次の手順に従ってください。

1. `PACKETFILTER` オプションを指定してカーネルを構築します。
2. `tcpdump` コマンドを使用して、SLIP インタフェースを介して送受信されたパケットを調べます。詳細については、`tcpdump(8)` を参照してください。

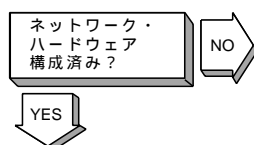
10.9 PPP に関する問題の解決



`sysconfig -s | fgrep ppp` コマンドを使用して、PPP (Point-to-Point Protocol) がカーネルでサポートされていることを確認します。PPP がサポートされている場合は、次のような出力が表示されます。

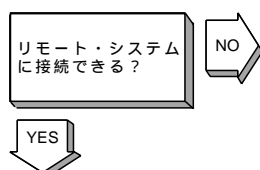
```
ppp: loaded and configured
```

PPP がサポートされていない場合、PPP オプションを `/sys/conf/MACHINE` システム構成ファイルに追加し、カーネルを再構築します。



ネットワーク・ハードウェアを次のように構成します。

- リモート・ホストへの直接接続
ヌル・モデム・ケーブルまたはモデム・エリミネータ・ケーブルを使用して、システムをリモート・ホストと接続します。
- リモート・ホストへの電話回線接続
2本のケーブルを使用して、モデムと電話回線、システムとモデムをそれぞれ接続します。使用するモデムは、リモート・ホストのモデムと互換性がなければなりません。モデムを次のように構成します。
 - パリティなしの 8 ビット文字を使用する。
 - すべてのフロー制御を禁止する。



メッセージをコンソールへ出力するよう設定している場合、リンクが正常に行われるとコンソールに次のメッセージが表示されます。

```
Local IP address: xx.xx.xx.xx  
Remote IP address: yy.yy.yy.yy
```

リンクが確立されない場合は、次の手順を実行します。

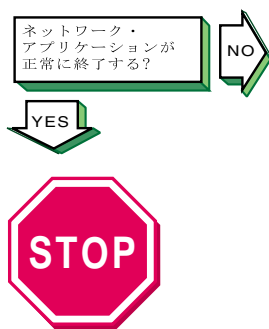
- `/usr/spool/locks` ディレクトリ内で `LCK..ttynn` ロック・ファイルの有無を調べます。PPP 用に構成している端末デバイスのロック・ファイルがあれば、それを削除してください。

端末デバイス経由で接続を確立すると、他のアプリケーションによって接続が切られないようにするために、システムがロック・ファイルを生成します。この接続が正しい手

続きを経ずに切断されると、ロック・ファイルが残り、新しい接続が確立できなくなります。

- シリアル接続が正常に設定されていることを確認します。
`chat -v` コマンドを実行して、`chat` プログラムが送受信する文字をログに取ります。
- リモート・システムで `pppd` デーモンが起動されていることを確認します。`chat -v` コマンドを実行して、`chat` プログラムが送受信する文字をログに取ります。
- 2 つのピア間の PPP 折衝を調べます。`pppd` コマンドを `debug` オプション付きで実行して、送受信されるすべての制御パケットの内容をログに取ります。
- MRU の値が正しく設定されていることを確認します。MRU の値が小さすぎると、トラフィックはリンク上を正しく流れません。IPv4 の場合、最小値は 128 バイトですが、値を 296 にすることをお勧めします。IPv6 の場合、最小値は 1298 バイトですが、値を 1500 にすることをお勧めします。

カーネルで IPv6 が有効になっている場合、使用するしないにかかわらず、PPP は自動的に IPv6 アドレスを構成します。そのため、MRU の値は 1298 またはそれ以上に設定する必要があります。あるいは、PPP リンクで IPv6 を使用しない場合は、`noip6` オプションを指定します。



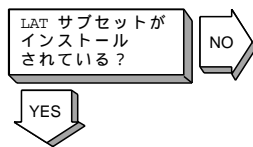
まだ問題がある場合はサービス担当者に報告してください。第 12 章を参照。

ネットワーク・アプリケーションが異常終了する場合、これは IP アドレス割り当て問題またはルーティング問題を示しています。次の手順に従ってください。

1. `netstat -i`, `netstat -r`, `ping`, `traceroute` の各コマンドを使って問題を診断します。
2. ピア・マシンとは通信できるが、ピア・マシンを越えてネットワーク内の他のマシンと通信できない場合は、ルーティング問題が発生しています。たとえば、ローカル・マシンがピアを介してインターネットと接続される場合は、次のことを実行します。
 - a. リモート・マシンと同じサブネットの IP アドレスをローカル・マシンに割り当てます。
 - b. ローカルの `pppd` デーモンを `defaultroute` オプション付きで実行します。

- c. リモートの `pppd` デーモンを `proxyarp` オプション付きで実行します。
- d. ピア・システム (リモート・システム) で `iprsetup -d` コマンドを実行して、`ipforwarding` および `ipgateway` 変数がオンになっていることを確認します。オフの場合は、`iprsetup -s` コマンドでオンにします。

10.10 LAT に関する問題の解決



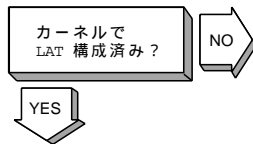
LAT のサブセットがインストールされていることを確認します。次のコマンドを入力します。

```
# setld -i | grep OSFLAT
```

このサブセットがインストールされている場合は、次のメッセージが表示されます。

```
OSFLATnnn installed Local Area Transport (LAT)
(General Applications)
```

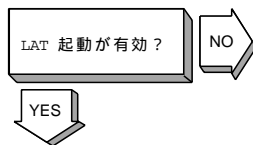
サブセットがインストールされていない場合は、`setld` コマンドを使用してインストールします。サブセットのインストールについての説明は、『インストレーション・ガイド』を参照してください。



カーネルにローカル・エリア・トランスポートが構成されていることを確認します。次のコマンドを入力します。

```
# sysconfig -q lat
```

何も表示されない場合は、LAT がカーネルに構成されていません。LAT オプションを使用してカーネルを再構成します。カーネルの再構成についての説明は、『システム管理ガイド』を参照してください。



`rcmgr` ユーティリティを使用して、`/etc/rc.config` ファイル内の `LAT_SETUP` エントリの値を表示します。

```
# rcmgr get LAT_SETUP
```

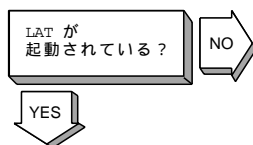
0 が返された場合は、`latsetup` ユーティリティを実行します。詳細については、9.3.1 項を参照してください。



latsetup ユーティリティが新しいLAT tty を作成しようとする
と異常終了する場合は、/usr/sbin ディレクトリが検索パスに
含まれていることを確かめます。次のコマンドを入力します。

```
# echo $PATH
```

含まれていない場合は、それを PATH 環境変数に指定します。
次に、latsetup コマンドを使用して新しいLAT tty を作
成します。



LAT がスタートしていることを確認します。次のコマンド
を入力します。

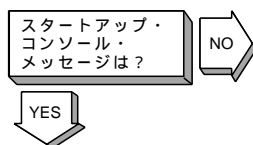
```
# latcp -d
```

LAT がスタートしている場合は、次の行が表示されます。

```
LAT Protocol is active
```

LAT がスタートしていない場合は、スタートさせます。次
のコマンドを入力します。

```
# latcp -s
```



LAT がスタートしてメッセージがシステム・コンソールに連
続的に表示される場合は、次の各メッセージを探し、必要な手
順に従ってください。

メッセージ 1

```
getty: cannot open "/dev/lat/xx".  
errno: 2
```

これは、LAT ターミナル・デバイス・ファイル (tty) が存在しな
いにもかかわらず、このファイルのエントリが /etc/inittab
ファイルに存在することを示します。また、latsetup ユー
ティリティによって、使用可能な LAT エントリがないことが
報告されます。次のことを行います。

1. /etc/inittab ファイルを編集し、LAT getty エントリを
削除します。
2. LAT ターミナル・デバイスが必要な場合は、latsetup コマ
ンドを使用して、LAT ターミナル・デバイス・ファイルを
作成し、それに対応するエントリを /etc/inittab ファ
イル内に作成します。詳細については、latsetup(8) を
参照してください。

メッセージ 2

```
getty: cannot open "/dev/lat/xx".  
errno: 19
```

これは、カーネルが LAT オプションを使用して構成されなかったにもかかわらず、最低でも 1 つの LAT getty エントリが、`/etc/inittab` ファイルに存在していることを意味します。次のいずれかを行います。

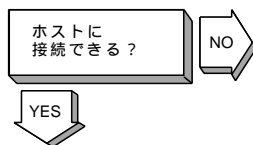
- LAT を組み込んでカーネルを構成します。LAT を組み込むカーネルの構成については、『システム管理ガイド』を参照してください。
- 手動によって、または `latsetup` コマンドを使用して、LAT getty エントリを `/etc/inittab` ファイルから削除します。

メッセージ 3

```
INIT: Command is respawning too rapidly.
```

このメッセージは、次のいずれかのことを示します。

- `lattelnet` などのオプション・サービスを使用しようとしているが、不正なサービス名が定義されています。次の手順に従ってください。
 1. `latcp -d` コマンドを使用して、`latcp -A` コマンドによって定義されたオプション・サービス名が正しいことを確認します。
 2. `/etc/inittab` ファイルを編集し、LAT エントリに指定されているオプション・サービス名が正しいことを確認します。
- 存在しない LAT ターミナル・デバイス (tty) を使用しようとしました。次の手順に従ってください。
 1. `/etc/inittab` ファイルを編集し、存在しないターミナル・デバイス名が記述されているエントリを削除します。
 2. LAT ターミナル・デバイスが必要な場合は、`latsetup` コマンドを使用して、LAT ターミナル・デバイス・ファイルを作成し、それに対応するエントリを `/etc/inittab` ファイル内に作成します。詳細については、`latsetup(8)` を参照してください。



ユーザがターミナル・サーバから LAT を介して、サービスに接続できないか、またはサービスを表示できない場合は、Tru64 UNIX システムで次の手順に従ってください。

1. `latcp -d` コマンドを使用して、サービス名が正しいことを確認します。サービス名が不正な場合は、そのサービスを削除します。次のコマンドを入力します。

```
# latcp -D -aservice_name
```

次に、サービスを正しい名前で登録します。次のコマンドを入力します。

```
# latcp -A -aservice_name
```

詳細については、`latcp(8)` を参照してください。

2. `latcp -d` コマンドを使用して、接続しようとしているサービスのグループ・コードを表示します。ターミナル・サーバで、`show port` コマンドによって表示されるグループと一致するグループ・コードがあるかどうかを確かめます。一致するグループ・コードがない場合は、次のいずれかを行います。

- そのポートに対して表示されたグループの中から最低でも 1 つ、サービスに追加してみます。次のコマンドを入力します。

```
# latcp -glist -aservice_name
```

- サービスと一致するグループを追加して、ターミナル・サーバのポート特性を変更します。

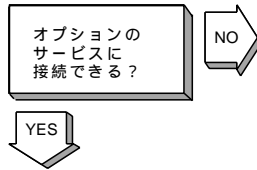
詳細については、`latcp(8)` を参照してください。

3. LAT がシステムでスタートしているかを確かめます。スタートしていなければ、スタートさせます。次のコマンドを入力します。

```
# latcp -s
```

4. それでも問題が解決しない場合は、LAT を再起動させます。次のコマンドを入力します。

```
# latcp -s
```

オプション・サービスを使用すると問題が発生する場合は、次の手順に従ってください。

1. そのサービスがオプション・サービスとして追加されたことを確認します。次のコマンドを入力します。

```
# latcp -d
```

次の行を探します。

```
Service name: name (Optional)
```

Optional が表示されない場合は、このオプション・サービスが -o オプションによって定義されていなかったことになります。このサービスを削除します。次のコマンドを入力します。

```
# latcp -D -aservice_name
```

次に、正しい名前と -o オプションを指定して、サービスを追加します。次のコマンドを入力します。

```
# latcp -A -aservice_name -o
```

詳細については、latcp(8) を参照してください。

2. オプション・サービス名が /etc/inittab ファイルに定義されている名前と一致することを確認します。一致しない場合は、次のいずれかを行います。

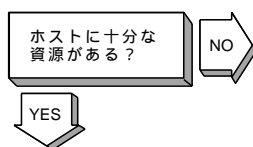
- /etc/inittab ファイルを編集して、オプション・サービス名を指定します。
- そのサービスを削除します。次のコマンドを入力します。

```
# latcp -D -aservice_name
```

次に、正しい名前と -o オプションを指定して、サービスを追加します。次のコマンドを入力します。

```
# latcp -A -aservice_name -o
```

詳細については、latcp(8) を参照してください。



LATを使用してもホストに接続できない場合は、次のメッセージが表示されます。

```
Connection
to node-name not established.
Service in use.
```

/etc/inittab ファイル内の getty エントリの数が不足しています。latsetup コマンドを使用して、LAT ターミナル・デバイス (tty) を追加作成し、対応するエントリを /etc/inittab ファイルに追加します。次に、LAT を再起動して、使用できるサービスをアダプタイズさせてみます。次のコマンドを入力します。

```
# latcp -s
```

詳細については、9.3.1 項を参照してください。



ホストから開始される接続が失敗する場合は、ポート、ホスト、およびサービス名が正確に指定されていることを確認します。次のコマンドを入力します。

```
# latcp -d -P -L
```

これらの名前が正しく指定されていない場合は、不正な名前のアプリケーション・ポートを削除します。次のコマンドを入力します。

```
# latcp -D -pport_name
```

次に、正確なスペルを使用してアプリケーション・ポートを追加します。LAT ターミナル・デバイスのマッピング先となるリモート・ポートを指定してアプリケーション・ポートを作成するには、次のコマンドを使用します。

```
# latcp -A -plocal_port -Hnode -Rrem_port
```

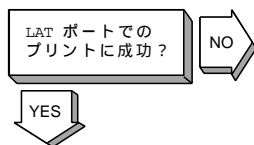
LAT ターミナル・デバイスのマッピング先となるリモート・サービス名を指定してアプリケーション・ポートを作成する場合には、次のコマンドを使用します。

```
# latcp -A -plocal_port -Hnode -Vsvc_name
```

詳細については、latcp(8) を参照してください。

注意

LAT プリンタのアプリケーション・ポートを削除した場合に、現在実行されているプリント動作が継続されるのは、プリンタ・バッファが空になるまでです。プリント・ジョブが終了しないこともあります。



LAT アプリケーション・ポートに接続された，オンラインになっているプリンタへファイルをプリントしてもプリントが実行されない場合は，プリント・キューの状態をチェックします。次のコマンドを入力します。

```
# lpc status
```

次の行が表示されます。

```
waiting for printer to become ready (offline ?)
```

この行が表示された場合は，LAT がスタートしていることを確認します。次のコマンドを入力します。

```
# latcp -d
```

LAT がスタートしていない場合は，それをスタートします。次のコマンドを入力します。

```
# latcp -s
```

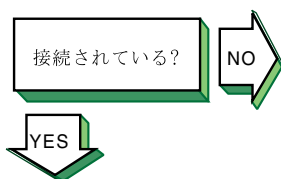


LAT/Telnet ゲートウェイの問題が検出された場合は，`/var/adm/syslog.dated/current/daemon.log` ファイル内にエラー・メッセージがあるか探します。そして，そのエラー・メッセージを使用して問題を診断します。`daemon.log` ファイルについては，11.9 節を参照してください。

`lattelnet` ユーティリティは，`LOG_INFO` の `syslog` メッセージ・プライオリティを使用します。たとえば，ターミナルの `getty` プロセスの処理中に，`/etc/inittab` ファイル内の LAT ターミナル・エントリを編集してそれを `lattelnet` に再び割り当て，LAT/Telnet に接続しようとする，接続は失敗します。`daemon.log` ファイルに，次のエラー・メッセージが記録されます。

```
No such file or directory
```

ターミナル・ポートの `getty` プロセスを終了します。



まだ問題がある場合はサービス担当者に報告してください。第 12 章 を参照。

LAT 接続が失敗する場合は、次の手順に従ってください。

1. LAT ターミナル・デバイス (tty) ファイル内で、副デバイス番号の重複の有無を調べます。次のコマンドを入力します。

```
# ls -l /dev/lat/*
```

重複している副デバイス番号が存在する場合は、重複しているデバイス・ファイルを削除してオリジナルのファイルを残します。

2. /etc/inittab ファイル内で、LAT エントリの重複の有無を調べます。重複しているエントリを削除して、オリジナルのエントリを残します。

問題解決ツールの使用

ネットワーク接続とネットワーク・ハードウェアの問題解決を支援するため、このオペレーティング・システムは、次の各タスクを実行するツールを備えています。

- ネットワーク・インタフェースに関する情報の表示 (11.1 節)
- ネットワーク・インタフェースの障害の検出 (11.2 節)
- インターネット上にあるネットワーク・ホストへの接続テスト (11.3 節)
- ネットワーク統計の表示 (11.4 節)
- インターネット/イーサネット間変換テーブルの表示と変更 (11.5 節)
- ネットワーク・ホストまでのデータグラムの経路の表示 (11.6 節)
- ネットワーク上のパケットのヘッダの表示 (11.7 節)
- エラー・ログ・ファイルの表示 (11.8 節)
- syslogd デモンのメッセージ・ファイルの表示 (11.9 節)

以下の節では、これらのタスクに関連するツールの使用方法について説明します。ネットワーク・サービスの診断に使用できるその他のツールについては、『ネットワーク管理ガイド：サービス編』を参照してください。

11.1 ネットワーク・インタフェースに関する情報の表示

ネットワーク・インタフェースに関する情報を表示するには、`ifconfig` および `hwmgrr` ユーティリティを使用します。

`ifconfig` コマンドは、物理的なネットワーク・アダプタ (`tu` や `ee` など) と論理的なネットワーク・インタフェース (`nr` や `lag` など) の基本的なネットワーク・パラメータを表示します。

システムで使用できるすべてのネットワーク・インタフェースに関する情報を表示するには、次のように `ifconfig -a` コマンドを実行します。

```
# ifconfig -a
ee0: flags=c63<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,SIMPLEX>
    inet 18.141.116.139 netmask ffffffff00 broadcast 18.141.116.255
    ipmtu 1500

ee1: flags=c63<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,SIMPLEX>

ee2: flags=c63<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,SIMPLEX>

lo0: flags=100c89<UP,LOOPBACK,NOARP,MULTICAST,SIMPLEX,NOCHECKSUM>
    inet 127.0.0.1 netmask ff000000 ipmtu 4096
```

この出力は、3 枚の ee イーサネット・カード (ee(7) を参照) がシステムにインストールされていることを示します。構成されアクティブになっているインタフェース・カードは ee0 のみです。アクティブなインタフェースに対する出力には、IP アドレス、ネットワーク・マスク、ブロードキャスト・アドレス、最大伝送ユニット設定が含まれています。

lo0 エントリは、すべてのシステムに存在する標準のループバック論理インタフェースに対する表示です。

特定のネットワーク・インタフェースに関する情報を表示するには、次のように、ネットワーク・インタフェースの名前を引数にして ifconfig コマンドを実行します。

```
# ifconfig tu0
tu0: flags=c63<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,SIMPLEX>
    inet 18.141.116.142 netmask ffffffff00 broadcast
    18.141.116.255 ipmtu 1500
```

ifconfig コマンドでは、ネットワーク・インタフェースを構成することもできます。詳細については ifconfig(8) を参照してください。

システムにインストールされている物理ネットワーク・アダプタに関するその他の情報を表示するには、次のように hwmgr コマンドを入力します。

```
# hwmgr get attribute -category network
18:
    name = ee0
    category = network
    sub_category = Ethernet
    model = Intel 82558
    hardware_rev = 5
    firmware_rev =
    MAC_address = 00-08-02-3E-C5-A5
    MTU_size = 1500
    media_speed = 10
```

```
media_selection = Automatic
media_type = Unshielded Twisted Pair (UTP)
loopback_mode = 0
promiscuous_mode = 0
full_duplex = 0
multicast_address_list = CF-00-00-00-00-00 01-00-5E-00-00-01 \
                        33-33-FF-3E-C5-A5 33-33-00-00-00-01 \
                        09-00-2B-00-00-0F 09-00-2B-02-01-04

interface_number = 1
link = Up
autoneg_enable = 1
registration_time = Mon Jul 22 10:23:24 2002
user_name = (null) (settable)
location = (null) (settable)
software_module = (null)
state = available
state_previous = unknown
state_change_time = none
event_count = 0
last_event_time = none
access_state = online
access_state_change_time = none
capabilities = 0
indicted = 0
indicted_probability = (null)
indicted_urgency = (null)
disabled = 0
est_seconds = 0
est_bytesent = 2144929
est_bloksent = 7401
est_mbytesent = 1496342
est_mbloksent = 3873
est_deferred = 322
est_single = 68
est_multiple = 44
est_collis = 0
est_unrecog = 0
est_userbuf = 0
est_latecoll = 0
est_excesscoll = 0
est_carrierfail = 0
est_shortcirc = 0
est_opencirc = 0
est_sndlong = 0
est_sendfail = 0
est_bytercvd = 1131389693
est_blokrvd = 7146273
est_mbytercvd = 1130918879
est_mblokrvd = 7141764
est_overrun = 1
```

```
est_sysbuf = 0
est_unaligned = 0
est_longframe = 0
est_shortframe = 0
est_fcsfail = 0
est_badframe = 0
est_symbolerror = 0
est_rcvfail = 1
```

上記の例では、システムにインストールされているネットワーク・アダプタは 1 つだけです。hwmgr の出力は、ハードウェア情報、低水準の構成設定、このデバイスに対する統計情報のカウンタを表示します。低水準の構成設定の変更については、ifconfig(8) と lan_config(8) を参照してください。ネットワークの統計情報については、11.4 節 と 付録 A を参照してください。

システムに別のネットワーク・インタフェース・カードがインストールされている場合は、次のように表示されます。

```
18:
  name = ee0
  category = network
  sub_category = Ethernet
  model = Intel 82558
.
.
19:
  name = ee1
  category = network
  sub_category = Ethernet
  model = Intel 82558
.
.
56:
  name = ee2
  category = network
  sub_category = Ethernet
  model = Intel 82559
.
.
```

上記の例では、各カードの前に、18、19、56 のような一意のハードウェア ID が表示されています。必要に応じて、次のようにこの ID を使用して特定のカードに関する情報を表示することができます。


```
# hwmgr get attribute -id 56
56:
  name = ee2
  category = network
  sub_category = Ethernet
  model = Intel 82559
.
```

hwmgr ユーティリティの詳細については、『ハードウェア管理ガイド』と hwmgr(8) を参照してください。

11.2 ネットワーク・インタフェースの障害の検出

NIFF (Network Interface Failure Finder) デモン (niffd) を使用すると、ネットワーク・インタフェースやその接続で発生する障害を検出して報告させることができます。

特定のネットワーク・インタフェースの監視を有効にすると、システムがそのインタフェースの packets・カウンタの追跡を開始します。このカウンタの値が増加している限り、ネットワーク・インタフェースは正常に動作しているものと見なされます。カウンタの値が増加しないまま一定時間が経過すると、niffd デモンによって当該インタフェースを経由するトラフィックが生成され、インタフェースの接続状態がチェックされます。その結果、カウンタの値が増加しなければ、niffd はインタフェースが正しく機能していないものと認識し、問題の発生を Event Manager サブシステムに通知します。

パケット・カウンタに関連するログは、イベント・ビューアで確認できます。Event Manager の他のユーティリティを使用して、接続の問題をリアルタイムで監視することも可能です。

この節では NIFF の手動構成を通じて、ネットワーク・インタフェースを個別に監視する方法を説明します。インタフェースのフェイルオーバーについては、ここでは取り上げません。NIFF には、NetRAIN (Redundant Array of Independent Network Adapters) にインタフェースの障害発生を通知するメカニズムがありますが、NIFF 自体がフェイルオーバー機能を備えているわけではありません。NetRAIN セットを構成してネットワーク・インタフェース間の自動フェイルオーバーを実現する方法については、2.1.1.2 項を参照してください。

11.2.1 NIFF の構成と構成解除

ネットワーク・インタフェースの監視を有効にするには、`niffconfig` コマンドを次のように実行します。

```
# niffconfig -a interface-id
```

`interface-id` の部分に、監視対象とするネットワーク・インタフェースのデバイス名 (`tu0` など) を指定します。複数のインタフェースを空白文字で区切って指定することも可能です。

さらに、次のコマンドを実行して `niffd` デーモンを `rc.config` ファイル内で有効にするようにすれば、同デーモンによるインタフェースの監視を、システムのリブート後も自動的に継続させることができます。

```
# rcmgr set NIFFD "YES"
# rcmgr set NIFFC_FLAGS "-a interface-id"
```

`niffd` デーモンが監視している各インタフェースは、次のように `niffconfig` コマンドをオプションなしで実行すれば表示できます。

```
# niffconfig
Interface:  tu0, status: UP
```

監視されているインタフェースに対して次のコマンドを実行すれば、そのインタフェースの監視を無効にできます。

```
# niffconfig -r interface-id
```

インタフェースの監視がリブート後に自動的に開始されるようにシステムを設定している場合、上記のコマンドで無効にしたインタフェースをリブート後も監視対象から除外するには、`rcmgr` コマンドを実行して `NIFFC_FLAGS` を更新します。さらに、すべての監視を無効にするには、次のコマンドを実行します。

```
# rcmgr delete NIFFD "YES"
# rcmgr delete NIFFC_FLAGS
```

NIFF の構成についての詳細は、`niffconfig(8)` および `niffd(8)` を参照してください。

11.2.2 NIFF イベントの表示

1 つ以上のネットワーク・インタフェースを対象に NIFF を有効にすると、これらのインタフェースに関連するイベントをイベント・ビューアで表示できます。次にその手順を示します。

1. SysMan Menu から [Monitoring and Tuning View events] を選択してイベント・ビューアを表示します。

イベント・ビューアは、コマンド行で次のコマンドを実行して表示することもできます。

```
# /usr/bin/sysman event_viewer
```

特に指定しなければ、イベント・ビューアには `syslogd` デーモンがログ出力したすべてのイベントが表示されるため、イベント数が数百、あるいは数千にも達する可能性があります。このため、フィルタを作成して NIFF が生成したイベント以外を抑制する必要があります。

2. NIFF イベント用のフィルタを作成するには、まず [フィルタ...] を選択します。「フィルタ」ダイアログ・ボックスが表示されます。
3. 「イベント名」チェック・ボックスを選択し、続いて対応する「一致するもの」チェック・ボックスを選択します。
4. 「イベント名」テキスト・フィールドに `sys.unix.hw.net.niff.*` という文字列を入力します。この文字列によって、NIFF が生成したイベントのみが選別されます。
5. さらに、次の手順でイベントの優先度に基づくフィルタを設定すれば、NIFF が生成した情報メッセージや警告も抑制し、インタフェース障害のみを表示することも可能です。
 - a. 「プライオリティ」チェック・ボックスを選択し、対応する「一致するもの」チェック・ボックスを選択した後、続いて「範囲」チェック・ボックスを選択します。
 - b. 「範囲」テキスト・フィールドに、範囲として 600-700 と入力します。

インタフェース障害は優先度が 600 なので表示されます。情報メッセージと警告はいずれも優先度が 200 なので、表示対象から除外されます。

6. [了解] を選択し、設定したフィルタを保存して適用します。

NIFF によって生成されたイベントが存在すれば、それがイベント・ビューアに表示されます。

イベント・ビューアに表示されるのは、通知済みのイベントのみです。表示後に通知されたイベントを表示に反映させるには、[更新] を選択して表示を更新する必要があります。ただし、niffd デーモンが EVM に通知する接続関連の警告は、ローカル・コンソール上のターミナルに直接出力させることも可能です。そのための手順は次のとおりです。

1. ローカル・コンソール上で新しいターミナル (dtterm や xterm など) を開きます。
2. このターミナルで次のいずれかのコマンドを実行します。

NIFF で生成された全イベント (情報メッセージ、警告、および障害) を表示する場合

```
# evmwatch | evmshow -f "[name sys.unix.hw.net.niff.*]"  
-t "@timestamp [@priority] @@"
```

障害のみを表示する場合

```
# evmwatch -f "[priority >= 600]" | evmshow -f "[name  
sys.unix.hw.net.niff.*]" -t "@timestamp [@priority] @@"
```

niffd デーモンからイベントが通知されると、それが直ちにターミナルに表示されます。適切な優先度のイベントが通知されるまで、このターミナルには新しい情報はなにも表示されません。

このターミナルでは、Ctrl/c を押してプロセスを終了させない限り、新たなコマンドは実行できません。

なお、niffd デーモンが動作しているシステムのネットワーク・インタフェースが 1 つだけの場合、上記の方法でリモート・ホストを通して、ネットワーク・インタフェースの接続を監視することはできません。この場合、ローカル・コンソールで実行する必要があります。

EVM についての詳細は、『システム管理ガイド』を参照してください。

11.3 インターネット・ネットワーク・ホストへの接続テスト

システムがインターネット上のホストに接続できるかどうかをテストするには、ping コマンドを使用します。ping コマンドの構文は、次のとおりです。

`/usr/sbin/ping [options...] hostname`

表 11-1 に、`ping` コマンドのオプションの一部を示します。

表 11-1: `ping` コマンドのオプション

オプション	機能
<code>-c count</code>	送信および受信する ECHO RESPONSE パケットの数を指定します。
<code>-I interface</code>	パケット送信に使用するインタフェースを指定します。
<code>-R</code>	送信パケットに RECORD_ROUTE オプションを指定して、受信パケットに入れることのできるパス・バッファを表示します。
<code>-r</code>	ローカル・ホストに直接接続されたホストに対して <code>ping</code> コマンドを実行します。このオプションを使用すると、 <code>ping</code> コマンドは通常のパス・テーブルを経由しないで、接続されたネットワーク上にあるホストに直接要求を送信します。直接接続されたネットワーク上にホストがない場合は、ローカル・ホストに対してエラー・メッセージが返されます。
<code>-v</code>	ホスト名が IPv4 アドレスと IPv6 アドレスの両方を持つ場合に、リゾルバが返却するアドレスを IP のバージョン番号 (4 または 6) で指定します。特に指定しなければ、 <code>ping</code> コマンドはホスト名を IPv6 アドレスとして解決してみても、IPv4 アドレスとして解決してみます。

`ping` コマンドは、ICMP (Internet Control Message Protocol) のエコー要求を、指定されたホスト名宛に送信します。要求が成功した場合には、リモート・ホストはローカル・ホストにデータを返します。リモート・ホストが要求に応答しない場合、`ping` コマンドは何も表示しません。

`ping` コマンドの出力を終了するには、`Ctrl/c`を押します。終了する場合、`ping` コマンドは送信パケットおよび受信パケットについての統計情報、欠落したパケットのパーセンテージ、ならびにパケットの往復にかかった時間の最小値、平均、および最大値を表示します。

`ping` コマンドの出力は、ホストに到達できない、接続タイムアウト、ネットワークに到達できないなどの、直接ルーティングおよび間接ルーティングに関する問題の原因を調べるのに使用できます。

問題の原因を突き止めるために `ping` コマンドを使用する場合は、最初にローカル・ホストが作動していることを確認します。ローカル・ホストからデータが正しく返されたら、`ping` コマンドを使用してローカル・ホストからより離れた位置にあるリモート・ホストを順次テストしていきます。

コマンド・オプションを指定しないと、ping コマンドは、それぞれの ICMP 要求の結果 (送信順)、リモート・ホストから受け取ったバイト数、および 1 回の要求の往復にかかる時間を表示します。

次に、host1 という名前のホストに対して ping コマンドを実行した場合の出力例を示します。

```
% ping host1
PING host1.corp.com (16.20.32.2): 56 data bytes
64 bytes from 16.20.32.2: icmp_seq=0 ttl=255 time=11 ms
64 bytes from 16.20.32.2: icmp_seq=1 ttl=255 time=3 ms
64 bytes from 16.20.32.2: icmp_seq=2 ttl=255 time=7 ms
64 bytes from 16.20.32.2: icmp_seq=3 ttl=255 time=3 ms
64 bytes from 16.20.32.2: icmp_seq=4 ttl=255 time=7 ms
64 bytes from 16.20.32.2: icmp_seq=5 ttl=255 time=3 ms
Ctrl/c
----host1.corp.com PING Statistics---
6 packets transmitted, 6 packets received, 0% packet loss
roundtrip (ms) min/avg/max = 3/5/11 ms
```

ping のコマンド行には、IPv4 アドレス、IPv6 アドレス、またはノード名が指定できます。IPv6 アドレスを指定した場合の例を、次に示します。

```
# ping -c 2 5F00:2100:108C:4000:8C40:800:2B2D:2B2
PING (5F00:2100:108C:4000:8C40:800:2B2D:2B2): 56 data bytes
64 bytes from 5F00:2100:108C:4000:8C40:800:2B2D:2B2: icmp6_seq=0
    hlim=58 time=17 ms
64 bytes from 5F00:2100:108C:4000:8C40:800:2B2D:2B2: icmp6_seq=1
    hlim=58 time=17 ms
----5F00:2100:108C:4000:8C40:800:2B2D:2B2 PING Statistics----
2 packets transmitted, 2 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 17/17/17 ms
```

このコマンドは、使用されているアドレスの種類に応じて、適切な ECHO_REQUEST パケットを送信します。1 つのノード名が IPv4 と IPv6 の両方のアドレスで解決できる場合には、-v4 オプションまたは -v6 オプションを指定して、使用するアドレスの種類を指定できます。

また、-I フラグを使用すると、強制的に特定のインタフェースを使用することもできます。次に例を示します。

```
# ping -I ln0 FE80::800:2B2D:2B2
```

このコマンドとオプションについての詳細は、ping(8) を参照してください。

11.4 ネットワーク統計情報の表示

netstat コマンドを使用すれば、ソケット、インタフェース、およびルーティング・テーブルに関するネットワーク統計情報を表示することができます。これらの情報はいくつかの形式で表示することが可能であり、それぞれの形式ごとに強調する情報の種類を指定できます。

表 11-2 に netstat コマンドのオプションを示します。

表 11-2: netstat コマンドのオプション

オプション	機能
-A	関連するプロトコル制御ブロックのアドレスを表示します。
-a	すべてのソケットの情報を表示します。
-f <i>address_family</i>	指定された種類のアドレスに関する統計情報またはアドレス制御ブロック情報を表示します。たとえば、inet (IPv4)、inet6 (IPv6)などを指定します。
-I <i>interface</i>	指定されたインタフェースの情報を表示します。
-i	自動構成されたインタフェースの状態に関する情報を表示します。
-m	メモリ管理の使用状況に関する情報を表示します。
-n	ネットワーク・アドレスを (シンボル形式ではなく) 数値形式で表示します。
-r	ルーティング・テーブルを表示します。
-s	プロトコルごとの統計情報を表示します。
-t	インタフェース監視ルーチンが起動するまでの時間を表示します。(-i オプションと併用します。)

-I オプションは、指定されたインタフェースの統計情報を表示します。付録 A には、-I オプションによるイーサネット、FDDI (Fiber Distributed Data Interface)、およびトークン・リングの各インタフェースの監視例と、カウンタ、状態、および属性の説明が記載されています。

-i オプションは、構成されている各ネットワーク・インタフェースの統計情報を表示します。発信パケット・エラー (Oerrs) はローカル・ホストの問題、受信エラー (Ierrs) はインタフェースが接続されているネットワークの問題をそれぞれ示します。

-f inet は IPv4 のデータのみ、-f inet6 は IPv6 のデータのみをそれぞれ表示するオプションです。たとえば、netstat -f inet6 -rn コマンドを実行すると、IPv6 のルーティング・テーブルのエントリのみが表示されます。特に指定しなければ、IPv4 と IPv6 の両方のエントリが表示されます。

netstat -s コマンドは、IPv6 や ICMPv6 を含む全プロトコルの統計情報を表示します。

次の例は、netstat コマンドを -i オプション付きで実行した場合の典型的な出力を示しています。

```
% netstat -i
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Coll
ln0 1500 <Link> 8324125 0 8347463 0 237706
ln0 1500 16.31.16 host1 8324125 0 8347463 0 237706
fza0* 4352 <Link> 0 0 0 0 0
sl0* 296 <Link> 0 0 0 0 0
sl1* 296 <Link> 0 0 0 0 0
tra0 4092 <Link> 34 0 20 0 0
tra0 4092 16.40.15 host21 34 0 20 0 0
lo0 1536 <Link> 909234 0 909234 0 0
lo0 1536 loop localhost 909234 0 909234 0 0
```

この出力では Ierrs と Oerrs はどちらも表示されていません。したがって、ネットワーク接続に問題が発生していないことがわかります。

netstat コマンドとそのオプションについての詳細は、netstat(1) と 付録 A を参照してください。

11.5 インターネット (IPv4) アドレスから MAC アドレスへのアドレス変換テーブルの表示および変更

アドレス解決プロトコル (ARP) が使用する、インターネット・アドレスから MAC (Media Access Control) アドレスへの変換テーブルの内容を表示および変更し、次の場合に発生する IPv4 ダイレクト・ルーティングの問題の診断に役立てることができます。

- ソース・ホストがデスティネーション・ホストの誤ったイーサネット・アドレス情報を保持している場合。
- 同じ IPv4 アドレスを持つホストが 2 つある場合。

この問題は変換テーブルを修正すれば回避できますが、アドレスの衝突を恒久的に解決するために、一方のホストの IPv4 アドレスを変更してください。

インターネット・アドレスから MAC アドレスへの変換テーブルのエントリを表示するには、`arp -a` コマンドを使用します。変換テーブルに変更を加えるには、`root` でログインして、`arp` コマンドを次のように使用します。

```
/usr/sbin/arp [ options ] hostname
```

次に、`host1` という名前の IPv4 ホストのイーサネット・アドレスの例を示します。システムの応答によると、`host1` のイーサネット・アドレスが `aa-00-04-00-8f-11` であることがわかります。

```
# /usr/sbin/arp host1
host1 (16.20.32.2) at aa:0:4:0:8f:11 permanent trailers
```

次の例に、`host9` を一時的にシステム変換テーブルに追加する方法を示します。

```
# /usr/sbin/arp -s host9 0:dd:0:a:85:0 temp
```

次の例に、`host8` をシステム変換テーブルから削除する方法を示します。

```
# /usr/sbin/arp -d host8
```

このコマンドについての詳細は、`arp(8)` を参照してください。

11.6 ネットワーク・ホストまでのデータグラムの経路の表示

ネットワークのテスト、測定、および管理を手動で行うために、ネットワーク・ホストまでのデータグラムのパスを表示できます。

データグラムのパスを表示するには、次の構文に従って `traceroute` コマンドを使用してください。

```
traceroute [ options... ] hostname [ packetsize ]
```

表 11-3 に、`traceroute` コマンドのオプションを示します。

表 11-3: `traceroute` コマンドのオプション

オプション	機能
<code>-m max_ttl</code>	発信されるプローブ・パケットで使用する <code>ttl</code> (time-to-live) の最大値を設定します。 <code>ttl</code> パラメータは、パケットがデスティネーションに達するために取ることができる最大ホップ数を指定します。省略時の値は 30 ホップです。
<code>-n</code>	ホップのアドレスを、数字と記号の併用ではなく数字だけで表示します。

表 11-3: traceroute コマンドのオプション (続き)

オプション	機能
-p <i>port</i>	発信されるプローブ・パケットで使用する UDP (User Datagram Protocol) のベース・ポート番号を設定します。省略時の値は 33434 です。省略時の範囲にあるポートがすでに使用されている場合は、ポート情報を使用して未使用のポート範囲を選択します。
-r	通常のルーティング・テーブルを経由しないで、接続されているネットワーク上のホストにプローブ・パケットを直接送信します。直接接続されたネットワーク上にホストがない場合は、traceroute コマンドによってエラーが返されます。
-s <i>IP_address_number</i>	発信されるプローブ・パケットのソース・アドレスとして、指定された IP アドレスを使用します。2 つ以上の IP アドレスを持つホストに対してこのオプションを使用すると、traceroute コマンドは、他のアドレスを使用しないで必ず指定されたソース・アドレスを使用します。指定した IP アドレスが、受信側のホストのインタフェース・アドレスのいずれにも一致しない場合は、エラーが返され、プローブ・パケットは送信されません。
-t <i>type-of-service value</i>	プローブ・パケットのサービス・タイプを指定された値に設定します。省略時の値は 0 です。値は 0 ~ 255 の範囲の 10 進数の整数です。このオプションは、サービスが異なるとパスも異なるかどうかをユーザに示します。このオプションが使用できるのは、バークレー UNIX (4.4BSD) の環境だけです。すべてのサービス・タイプが正当、または有効というわけではありません。このオプションで有効な値は、16 (低ディレイ) および 8 (高ディレイ) です。サービス・タイプについての詳細は、RFC 791 の『Internet Protocol』を参照してください。
-v	詳細な出力を表示します。つまり、time exceeded および port unreachable 以外の、受信された ICMP パケットも表示します。
-V <i>version</i>	ホスト名が IPv4 アドレスと IPv6 アドレスの両方で解決できる場合に、リゾルバが返却するアドレスを、IP のバージョン番号 (4 または 6) で指定します。省略すると、traceroute コマンドはホスト名を IPv6 アドレスとして解決してみても、次に IPv4 アドレスとして解決してみます。

表 11-3: traceroute コマンドのオプション (続き)

オプション	機能
<code>-w wait_time</code>	プローブに対する応答を待つ時間 (秒) を設定します。省略時の値は 3 秒です。
<code>packetsize</code>	プローブ・パケットのパケット・サイズ (バイト単位) を設定します。省略時のサイズは 38 バイトです。

traceroute コマンドは、UDP パケット(プローブ・パケット) をリモート・ホストの未使用ポートに送信し、IP ルータからの ICMP 応答を待ちます。プローブ・パケットは、小さな ttl パラメータを指定して送信されます。ttl パラメータは、パケットがそのデスティネーションに達するために取ることができる最大のホップ数を指定します。traceroute コマンドは、ttl を最初に 1 に指定して、プローブ・パケットを 1 つ送信するたびに ttl を 1 つずつ増加させます。パケットがデスティネーションに達するかまたは、ttl がホップの最大数に達するまでプローブ・パケットの送信を続けます。

traceroute コマンドは、各プローブ・パケットへの応答として、次のいずれかの ICMP メッセージを受信します。

- time exceeded
プローブ・パケットを受信した IP ルータが、ttl 値の指定によりそれ以上パケットを転送できないことを示します。このメッセージによって、パケットを処理している IP ルータが判明します。
- port unreachable
意図した宛先にプローブ・パケットが到着したが、意図したポートにはアクセスできなかったことを示します。

traceroute コマンドは、各 ttl 設定に対してプローブ・パケット (データグラム) を 3 つ送信すると、以下の項目を示す情報を 1 行表示します。

- ttl
- 応答したホストまたはルータの IP アドレス
- 各プローブ・データグラムまたは ICMP 応答の往復時間

複数の IP ルータがプローブ・データグラムに応答する場合には、traceroute コマンドは、各 IP ルータのアドレスを表示します。3 秒 (省略

時の待ち時間) で応答が得られない場合は、`traceroute` コマンドはそのプロープ・データグラムに関してアスタリスク (*) を表示します。

次に、`host2` に対する `traceroute` コマンドの成功例を示します。

```
% traceroute host2
traceroute to host2 (555.55.5.5), 30 hops max, 40 byte packets
 1  host3 (555.55.5.1) 2 ms 2 ms 2 ms
 2  host5 (555.55.5.2) 5 ms 6 ms 4 ms
 3  host7 (555.55.5.3) 7 ms 7 ms 6 ms
 4  host2 (555.55.5.5) 12 ms 8 ms 8 ms
```

`traceroute` コマンドを `host` 引数付きで実行すると、パケットが IPv4 ホストと IPv6 ホストの両方に到着するまでに使用した経路が表示されます。

このコマンドとオプションについての詳細は、`traceroute(8)` を参照してください。

11.7 ネットワーク上のパケット・ヘッダの表示

特定のネットワーク・サービスに関係するネットワーク・トラフィックをモニタリングしたい場合は、いつでもネットワーク上のパケット・ヘッダを表示させることができます。これは、要求が受け取られているかあるいは認識されているかを調べるため、またはネットワークの性能が低い場合にネットワーク要求のソースを調べるために行います。

ネットワーク・インタフェースのパケット・ヘッダを表示するには、`tcpdump` コマンドを使用します。このコマンドを使用すると、調べるインタフェース、パケット転送の方向、表示するプロトコル・トラフィックのタイプを指定することができます。また、パケットのソースを調べることもできます。詳細については、`tcpdump(8)` を参照してください。

注意

`tcpdump` コマンドを使用するためには、カーネルに `packetfilter` オプションを構成してシステムをリブートする必要があります。詳細については、`packetfilter(7)` を参照してください。

11.8 エラー・ログ・ファイルの表示

カーネルとハードウェアのエラー診断するには、エラー発生前に記録されたシステム・イベントを参照します。カーネルとシステム・ハードウェアに関連

するエラー・メッセージや、システムの状態、スタートアップ、および診断に関する情報メッセージなどの、システム・イベントによるメッセージは、エラー・ログ・ファイル (/var/adm/binary.errlog) に記録されます。

このログ・ファイルはバイナリ形式で格納されているため、オペレーティング・システムには専用ユーティリティ (Compaq Analyze と DECevent) が用意されています。これらのユーティリティは、バイナリ・ログ・ファイルを読み取り、データを変換して情報を表示します。Compaq Analyze と DECevent についての詳細は、それぞれ ca(8) と dia(8) を参照してください。

デフォルトでは、これらのユーティリティはオペレーティング・システムにインストールされません。個別にインストールしなければなりません。

Compaq Analyze は、Associated Product CD-ROM に収録されている WEBES (Web-Based Enterprise Services) キット (診断ユーティリティのセット) の一部です。WEBES キットについての詳細は、次の URL を参照してください。

<http://www.compaq.com/support/svctools/webes>

DECevent は、Associated Product CD-ROM に収録されているほか、Web サイトからダウンロードすることもできます。DECevent キットについての詳細は、次の URL を参照してください。

<http://www.compaq.com/support/svctools/decevent>

Compaq Analyze と DECevent で変換したエラーをイベント・ビューアで表示する方法については、『システム管理ガイド』を参照してください。また、これらのユーティリティを使用しないで表示する方法については、uerf(8) を参照してください。

11.9 syslogd デーモンのメッセージ・ファイルの表示

IPv4 (Internet Protocol Version 4) や IPv6 (Internet Protocol Version 6) のアクセス制御の問題など、セッション層で発生した問題の診断には、syslogd デーモンが役立ちます。

syslogd デーモンは、システムのブート時と、システムがハングアップ・シグナルを受信したときに起動されます。このデーモンは特に指定しなければ、これらのイベントのシステム・メッセージを、/var/adm/syslog.dated ディレクトリ内のファイル群に (/etc/syslog.conf ファイルの指定に応じ

て) 記録します。システム・メッセージは、メッセージに含まれている優先順位コードに応じて、エラー状況や警告を示します。

システム・メッセージ・ファイルの内容はコマンド行から参照することもできますが、ファイルへのアクセスが簡単になることや、特定の問題を見つけやすくなることから、SysMan Menu ユーティリティの一部であるイベント・ビューアを使用して表示します。イベント・ビューアを起動するには、1.2.1 項で説明されている手順に従って SysMan Menu を起動し、[Monitoring and Tuning View events] を選択します。次のコマンドをコマンド行で実行してイベント・ビューアを起動することもできます。

```
# /usr/bin/sysman event_viewer
```

イベント・ビューアが表示されると、ログ・エントリのソートや、エントリのフィルタ(確かなイベント名、優先レベル、ポストしているホストまたは日付について)、個々のエントリについてのさらに詳細な情報を得るのに使用することができます。

イベント管理とシステム・ログ・ファイルへのアクセス方法についての詳細は、`evm(5)`、`syslogd(8)`、『システム管理ガイド』、およびオンライン・ヘルプを参照してください。

ネットワークに関する問題の報告

ネットワークまたはネットワーク・サービスの重大な問題を解決できない場合は、次の手順に従ってください。

1. 製品のリリース・ノートを読んで、その問題が既知の問題であるかどうかを確認します。既知の場合には、記載されている解決策に従ってください。
2. 製品が保証期間中であるかどうか、または製品のサポート契約を結んでいるかどうかを確認します。
3. 上記の条件を満たしている場合は、次のいずれかの処置を行なってください。
 - a. オンライン・サービス・データベースを購入している場合は、オンライン・サービス・データベースにアクセスして、問題が報告されているかどうかを確認めます。報告されていない場合は、問題を記録しておいてください。
 - b. サービス担当者に問い合わせて、発生した問題について説明してください。
4. 問題に関する情報を求められた場合は、必要な情報を集めて提出してください。

問題を報告する際には、関連情報の提出が求められる場合があります。提出した情報は、問題が発生したシステム領域の特定と、問題解決の迅速化に役立てられます。基本的な情報はすべて、`system.information` という名前のファイルに入れておくとい良いでしょう。そうしておけば、そのファイルをすぐに問題報告書に添付できます。

以降の項では、提出を求められる可能性があるいくつかの情報について説明します。

12.1 一般情報の収集

使用しているシステムについて、次の情報を収集します。

- オペレーティング・システムのバージョンおよびリビジョン番号 (/etc/motd ファイルにあります)。この情報を `system.information` ファイルに追加します。
- エラーが発生する前のシステムの実行状態についての説明。
- 実行したコマンド行の正確なリスト、およびその出力。
- ユーザ作成アプリケーションを実行した場合は、そのアプリケーションのソース・コードのコピー。できれば問題を再現できるサンプル・テスト・プログラムを添付してください。

12.2 ハードウェア・アーキテクチャに関する情報の収集

ハードウェア・アーキテクチャについて、次の情報を収集します。

- グラフィック・コントローラのタイプ (ワークステーションの場合)、メモリの総量、ワークステーションまたはサーバのモデル (/usr/sys/conf/HOSTNAME ファイルにあります)、他社製のハードウェアについて。

- X サーバについて。

実行している X サーバのタイプは、次のコマンドで調べます。

```
# ps ax | grep /usr/bin/X >> system.information
```

- 使用しているディスク、およびスワップ・パーティションのサイズについて。

たとえば、システム・ディスクがユニット 0 の場合に、この情報を `system.information` ファイルに追加するには、`root` で次のコマンドを入力します。

```
# disklabel -r /dev/rrz0a >> system.information
# echo df: >> /system.information
# df >> /system.information
# echo mount: >> /system.information
# mount >> /system.information
# echo xdpinfo: >> /system.information
# xdpinfo >> /system.information
```

- すべてのネットワーク情報。

この情報を system.information ファイルに追加するには、次のコマンドを入力します。

```
# echo netstat: >> /system.information
# netstat -i -n >> system.information
# netstat -r -n >> /system.information
# echo nslookup: >> /system.information
# nslookup localhost >> /system.information
```

- すべてのイベント・ログ情報。

この情報を system.information ファイルに追加するには、次のコマンドを入力します。

```
# uerf -R -o full | head -200 >> /system.information
```

12.3 ソフトウェア・アーキテクチャに関する情報の収集

ソフトウェア・アーキテクチャについて、次の情報を収集します。

- インストールされているソフトウェア・サブセット。

この情報を system.information ファイルに追加するには、次のコマンドを入力します。

```
# echo setld: >> /system.information
# setld -i >> /system.information
```

- ログ・ファイル setld の出力。

この情報を system.information ファイルに追加するには、次のコマンドを入力します。

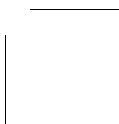
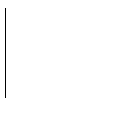
```
# pr /usr/adm/smllogs/setld.log >> /system.information
```

- 自動リブート・ファイル。

この情報を system.information ファイルに追加するには、次のコマンドを入力します。

```
# pr /etc/rc.config* >> /system.information
# pr /sbin/rc[023] >> /system.information
# pr /sbin/init.* >> /system.information
```

- インストールされているレイヤード・プロダクトについて。



ネットワーク・インタフェースの監視

netstatコマンドは、イーサネット、FDDI (Fiber Distributed Data Interface)、およびトークン・リングのネットワーク・インタフェースの監視にたいへん便利です。次の各節では、システム出力のサンプルを示し、各ネットワーク・インタフェースの情報について説明します。

A.1 イーサネット・インタフェースの監視

イーサネット・カウンタのリストを表示させるには、netstat -I ln0 -s コマンドを実行します。次に、このコマンドによるシステム出力のサンプルを示します。

```
ln0 Ethernet counters at Thu Nov 6 07:33:00 1992
    1289 seconds since last zeroed
16812469 bytes received
4657308 bytes sent
    42555 data blocks received
    28418 data blocks sent
860360 multicast bytes received
    7710 multicast blocks received
    546 multicast bytes sent
    13 multicast blocks sent
    0 blocks sent, initially deferred
    1864 blocks sent, single collision
    5542 blocks sent, multiple collisions
    6 send failures, reasons include:
        Excessive collisions
    0 collision detect check failure
    3 receive failures, reasons include:
        Block check error
        Framing Error
    0 unrecognized frame destination
    0 data overruns
    0 system buffer unavailable
    0 user buffer unavailable
```

次の各項目では、上記のサンプルの各フィールドをアルファベット順にリストし、それぞれのフィールドについて説明します。

blocks sent, initially deferred

最初の送信でフレームの送信が遅延された回数。衝突のないイーサネット・コンテンツの測定に使用されます。

blocks sent, multiple collisions

通常の衝突が発生した後、3 回目以降でフレームを正常に送信した回数。

blocks sent, single collision

最初の送信で通常の衝突が発生した後、2 回目でフレームを正常に送信した回数。

bytes received

正常に受信したバイト数。

bytes sent

正常に送信したバイト数。

collision detect check failure

送信後に衝突の検出が検知されなかった回数。

data blocks received

正常に受信したフレーム数。

data blocks sent

正常に送信したフレーム数。

data overruns

受信バッファを使用できなかったためにフレームが破棄された回数。

multicast blocks received

マルチキャスト・フレームで正常に受信したフレーム数。

multicast blocks sent

マルチキャスト・フレームで正常に送信したフレーム数。

multicast bytes received

マルチキャスト・フレームで正常に受信したバイト数。

multicast bytes sent

マルチキャスト・フレームで正常に送信したバイト数。

receive failures, reasons include:

受信エラーが発生した回数。各受信エラーは、次のうちいずれか 1 つに分類されます。

- Block check error
- Framing error
- Frame too long

seconds since last zeroed

関連するカウンタの属性が 0 に設定されてからの秒数。

send failures, reasons include:

送信エラーが発生した回数。各送信エラーは、次のうちいずれか 1 つに分類されます。

- Excessive collisions
- Carries check failed
- Short circuit
- Open circuit
- Frame too long
- Remote failure to defer

system buffer unavailable

リンク・バッファを使用できなかったためにフレームが破棄された回数。

unrecognized frame destination

データ・リンク・ポートがなかったためにフレームが破棄された回数。この回数に含まれるのは物理アドレスで受信されたフレーム数だけです。マルチキャスト・アドレスまたはブロードキャスト・アドレスで受信されたフレームは数えません。

```
user buffer unavailable
```

ユーザ・バッファを使用できなかったためにフレームが破棄された回数。

A.2 FDDI インタフェースの監視

FDDI (Fiber Distributed Data Interface) インタフェースのカウンタ, 状態, および特性のリストを表示させるには, `netstat -Iinterface -s` コマンドを実行します。次に, `fza0` インタフェースのこのコマンドによるシステム出力のサンプルを示します。アダプタのエラー・メッセージについては, `faa(7)`, `fta(7)`, `fza(7)`, および `mfa(7)` を参照してください。

```
fza0 FDDI counters at Wed Jun 12 14:02:44 1992
      89 seconds since last zeroed
6440875 ANSI MAC frame count
      0 ANSI MAC frame error count
      0 ANSI MAC frames lost count
37488 bytes received
39005 bytes sent
      447 data blocks received
      479 data blocks sent
30170 multicast bytes received
      321 multicast blocks received
29163 multicast bytes sent
      360 multicast blocks sent
      0 transmit underrun errors
      0 send failures
      0 FCS check failures
      0 frame status errors
      0 frame alignment errors
      0 frame length errors
      0 unrecognized frames
      0 unrecognized multicast frames
      0 receive data overruns
      0 system buffers unavailable
      0 user buffers unavailable
      0 ring reinitialization received
      0 ring reinitialization initiated
      0 ring beacon process initiated
      0 ring beacon process received
      0 duplicate tokens detected
      0 duplicate address test failures
      0 ring purger errors
      0 bridge strip errors
      0 traces initiated
```

```
0 traces received
0 LEM reject count
0 LEM events count
0 LCT reject count
0 TNE expired reject count
1 completed connection count
0 elasticity buffer errors
```

fza0 FDDI status

Station State:	On
Last Station ID:	Not Implemented
Station UID:	00-00-08-00-2B-A2
Link State:	On ring running
Link UID:	08-00-2B-A2-B5-84
Negotiated TRT:	7.987 ms
Duplicate Address Test:	Absent
Upstream Neighbor Address:	08-00-2B-18-B3-D7
Old Upstream Neighbor Address:	08-00-2B-1E-C0-3E
Upstream Neighbor Dup Addr Flag:	Unknown
Downstream Neighbor Address:	08-00-2B-1E-C0-3E
Old Downstream Neighbor Address:	08-00-2B-1E-C0-3E
Ring Purger State:	Purger off
Frame Strip Mode:	Source Address Match
Ring Error Reason:	No reason
Loopback Mode:	False
Ring Latency:	0.000 ms
Ring Purge Address:	Not Implemented
Physical Port State:	In use
Physical Port UID:	08-00-2B-A2-B5-84
Neighbor Physical Port Type:	Master
Physical Link Error Estimate:	15
Broken Reason:	None
Reject Reason:	No reason

fza0 FDDI characteristics

Station ID:	00-00-08-00-2B-A2
Station Type:	SAS
SMT Version ID:	2
SMT Max Version ID:	2
SMT Min Version ID:	2
Link Address:	08-00-2B-A2-B5-84
Requested TRT:	8.000 ms
Valid Transmission Time:	2.621 ms
Restricted Token Timeout:	1000.000 ms
Ring Purger Enable:	FALSE
Physical Port Type:	Slave
PMD Type	ANSI multimode
LEM Threshold:	8

ダウンストリームの近隣のアドレス (Downstream Neighbor Address) と制限付きトークン・タイムアウト (Restricted Token Timeout) は、DEFZA ファームウェアがリビジョン 1.2 以降の場合のみに報告されます。

次の各項では、上記のサンプルの各フィールドをアルファベット順にリストし、それぞれのフィールドについて説明します。

A.2.1 FDDI カウンタ

この項では、FDDIカウンタをアルファベット順にリストします。

ANSI MAC frame count

このリンク内にあるフレーム(トークン・フレームを除く)の総数。

ANSI MAC frame error count

メディア・アクセス制御 (MAC) によって、フレーム内のEインディケータが R から S に変更された合計の回数。

ANSI MAC frames lost count

フレーム (トークン・フレームを除く) が異常終了した回数の合計。

bridge strip errors

トークンを受信することで、フレームの内容に依存しないストリップ操作が終了した回数。

bytes received

正常に受信したバイト数。

bytes sent

正常に送信したバイト数。

completed connection count

物理 (PHY) ポートが初期化処理を完了し、In Use 状態に入った回数。

data blocks received

正常に受信したフレーム数。

data blocks sent

正常に送信したフレーム数。

duplicate address test failures

二重アドレス・テストに失敗した回数。

duplicate tokens detected

二重トークン検出アルゴリズムによって、またはトークン保留中に別のトークンを受信することによって、MAC が二重トークンを検出した回数。

elasticity buffer errors

PHYポートで Elasticity Buffer 機能がオーバフローまたはアンダフローした回数。

FCS check failures

受信したフレームが FCS (Frame Control Status) 検査に失敗した回数。

frame alignment errors

受信したフレームでアライメント・エラーが発生した回数。

frame length errors

受信したフレームの長さが不適切だった回数。

frame status errors

CRC (cyclic redundancy check) は正常だったが、受信したフレームに不正な E インディケータがあった回数。

LCT reject count

物理的な接続のどちらかの末端で LCT (link confidence test) に失敗したために、この物理ポートの接続がリジェクトされた回数。

LEM events count

リンク・エラー・モニタ (LEM) によって検出された物理層のエラー数。

LEM reject count

この物理ポートの有効な接続が、LEM によって物理的な接続のこの端でリジェクトされたために、切断された回数。

multicast blocks received

マルチキャスト・フレームで正常に受信したフレーム数。

multicast blocks sent

マルチキャスト・フレームで正常に送信したフレーム数。

multicast bytes received

マルチキャスト・フレームで正常に受信したバイト数。

multicast bytes sent

マルチキャスト・フレームで正常に送信したバイト数。

receive data overruns

受信バッファを使用できなかったためにフレームが破棄された回数。

ring beacon process initiated

リング・ビーコン処理が、このリンクで開始された回数。

ring beacon process received

リング・ビーコン処理の再初期化が、別のリンクで開始された回数。

ring purger errors

リング・パージャが、リング・パージ状態の間にトークンを受信した回数。

ring reinitialization initiated

リングの再初期化が、このリンクで開始された回数。

ring reinitialization received

リングの再初期化が、別のリンクで開始された回数。

seconds since last zeroed

リンク要素が作成された時間。この値は、関連するカウンタ属性が0に設定されてからの秒数です。

send failures

送信エラーが発生した回数 (送信アンダーランを除く)。

system buffers unavailable

リンク・バッファを使用できなかったためにフレームが破棄された回数。

TNE expired reject count

この物理ポートの有効な接続が、ノイズ・タイマ (TNE) の終了によってリジェクトされたために切断された回数。

traces initiated

PCトレース処理がこのリンクで開始された回数。

traces received

PCトレース処理が別のリンクで開始された回数。

transmit underrun errors

送信アンダーラン・エラーが発生した回数。これは、フレームの送信中に、転送先いれ先出し (FIFO) バッファが空になったことを示します。

unrecognized frames

データ・リンク・ポートがなかったために、受信ずみの個々にアドレス指定された LLC (logical link control) フレームが破棄された回数。

unrecognized multicast frames

データ・リンク・ポートがなかったために、受信ずみの、マルチキャスト・アドレス指定された LLC フレームが破棄された回数。

user buffers unavailable

ユーザ・バッファを使用できなかったためにフレームが破棄された回数。

A.2.2 FDDI の状態

この項では、FDDI の状態をアルファベット順にリストします。

Broken Reason

物理ポートが Broken 状態にある理由 (非 SAS 局)。このフィールドは、次のいずれかの値が入ります。

Broken

物理ポートが壊れています。

None

物理ポートは Broken 状態ではありません。

Downstream Neighbor Address

リングのダウストリーム側にある局の 48 ビット・ハードウェア・アドレス。

Duplicate Address Test

局の FDDI MAC 要素が実行した二重アドレス・テストの結果。このフィールドには、次のうちいずれか 1 つの状態が入ります。

Absent	FDDI MAC 要素は、リング内に自分の回線アドレスの重複がないと判定しました。
Present	FDDI MAC 要素は、リング内に自分の回線アドレスの重複があると判定しました。論理的なリングの障害が解決されるまで、データの送信や受信はできません。
Unknown	FDDI MAC 要素が二重アドレス・テストを実行して、リング内の別の局に自分の回線アドレスと同じアドレスがあるかどうかを判定中です。

Frame Strip Mode

局が使用するフレーム・ストリップ・モード。このフィールドには、次の値のうちいずれか 1 つが入ります。

Source Address Match	局は、自分のアドレスを含むソース・アドレス・フィールドを持っているフレームを、リングから取り除きます。
Bridge Strip	局は、トークンを取得した後に送信したフレームのカウントを保持し、送信が完了した場合に無効フレームを 1 つ送信します (リング・パージャの場合は無効フレームを 2 つ)。さらに、送信したフレームのカウントが 0 になるまで、返ってくるフレームをリングから取り除きます。ブリッジは、所有者のないフレームを検知し、ソース・アドレス・フィールドに自分のアドレスを含んでいないフレームを頻繁に送信するため、ブリッジではブリッジ・ストリップが使用されます。
Unknown	そのリングでは、その局は機能していません。

Last Station ID

インプリメントされている場合は、PMF (Parameter Management Frame) の変更、追加、あるいは削除を最後に実行した局の 48 ビット

ト・アドレスです。インプリメントされていない場合は、“Not implemented” というメッセージが表示されます。

Link State

局の FDDI MAC 要素の作動状態。このフィールドには、次の値のうちいずれか 1 つが入ります。

Broken	ハードウェアに問題があります。
Off Fault Recovery	FDDI MAC 要素は、二重アドレス・テストの失敗、ローカルまたはリモートのビーコン・ハング状態、リング動作の振動など、リングの論理的な障害から回復中です。
Off Maintenance	FDDI MAC 要素は、ループバック・テストとオンライン診断を実行中です。
Off Ready	FDDI MAC 要素は、作動の準備はできていますが、リングに論理的には接続されていません。
On Ring Initializing	FDDI MAC 要素が、論理的なリングに接続しているところです。
On Ring Running	FDDI MAC 要素は、論理的なリングに接続されて正常に作動しています。
Unknown	FDDI MAC エンティティはリングには接続されていません。

Link UID

データ・リンクの物理ポートの 48 ビット・アドレス。

Loopback Mode

リンク・エンティティのループバック・モードの作動状態。このフィールドには、次のいずれかの値が入ります。

False	ループバック・モードはオフ。リンク・エンティティは、リング上あるいは物理ポートのループバック・テストを実行するために転送フレームを受けとるようには設定されていません。
True	ループバック・モードはオン。リンク・エンティティは、リング上あるいは物理ポートのループバック・テストを実行するために転送フレームを受けとるようには設定されています。

Negotiated TRT

折衝 TTRT (Target Token Rotation Time) の値が、ANSI FDDI 仕様の T_Neg として参照されます。折衝は、トークン請求処理中に行われます。

Neighbor Physical Port Type

近隣の物理ポートのタイプ。このフィールドには、次の値のうちいずれか 1 つが入ります。

A	FDDI デュアル・リングの着信一次リングと発信二次リングに接続する、デュアル・アタッチメント・ワイヤ・コンセントレータ (DAC) またはデュアル・アタッチメント局 (DAS) の物理ポート。
B	FDDI デュアル・リングの発信一次リングと着信二次リングに接続される、デュアル・アタッチメント・ワイヤ・コンセントレータ (DAC) またはデュアル・アタッチメント局 (DAS) の物理ポート。
Master	DECbridge 500 デバイスなどのシングル・アタッチメント局 (SAS) に接続される、ワイヤ・コンセントレータ上の物理ポートの 1 つ。
Slave	ワイヤ・コンセントレータまたは別の SAS に接続される、SAS 上の物理ポート。
Un-known	接続が確立されていません。

Old Downstream Neighbor Address

リングのダウンストリーム側にあった局の 48 ビット・ハードウェア・アドレス。

Old Upstream Neighbor Address

リングのアップストリーム側にあった局の 48 ビット・ハードウェア・アドレス。

Physical Link Error Estimate

リンク・エラー・モニタ (LEM) によって求められるリンクの現在のエラーの割合。値が n の場合は、実際の割合は 1×10^{-n} になります。

Physical Port State

物理ポートの作動状態。このフィールドには、次の値のうちいずれか 1 つが入ります。

Broken	物理ポートは、診断テストに失敗したために作動できません。
Failed	物理ポートが最低1回は異常終了したこと以外は、Waitingと同じです。これは、初期化中にリンク信頼性テスト (LCT) に失敗したか、作動中にリンク・エラー・モニタ (LEM) のしきい値を超えてしまったか、違法なトポロジーの一部を構成していたためです。
In use	物理ポートは、接続を確立して作動中です。
Off maintenance	物理ポートは、診断テストとループバック用に予約されています。
Off ready	物理ポートは、使用できません。
Starting	物理ポートは、近隣の物理ポートからの応答を受信して情報を交換し、接続を完了する前にリンク信頼性テスト (LCT) を実行しています。
Unknown	物理ポートの状態が不明です。
Waiting	物理ポートが接続を確立し、近隣の物理ポートからの応答を待っています。
Watching	物理ポートが最低1回は異常終了したこと以外は、Startingと同じです。これは、初期化中にリンク信頼性テスト (LCT) に失敗したか、作動中にリンク・エラー・モニタ (LEM) のしきい値を超えてしまったか、または違法なトポロジーの一部を構成していたためです。

Physical Port UID

物理ポートの 48 ビット・アドレス。

Reject Reason

物理ポート上の最新の接続が失われた理由。このフィールドは、物理ポートが Failed 状態と Watching 状態を交互に繰り返すたびに更新されます。このフィールドには、次の値のうちいずれか 1 つが入ります。

LCT Both	この物理ポートと近隣の物理ポートで、リンク信頼性テスト (LCT) に失敗しました。
LCT Local	この物理ポートでのリンク信頼性テスト (LCT) に失敗しました。
LCT Remote	近隣の物理ポートでのリンク信頼性テスト (LCT) に失敗しました。

LEM Failure	物理ポートのビット誤り率が、リンク・エラー・モニタ (LEM) のしきい値を超えてしまいました。LEM は、作動中のリンクの品質を監視します。
No Reason	物理ポートは初期化中です。この値は、物理ポートが In Use 状態になるとクリアされます。
Remote Reject	近隣の物理ポートが、原因不明で接続を切断しました。
Standby	物理ポートは使用できません。初期化中です。
TNE Expired	シングル・ノイズ・イベントが 1.31072 ミリ秒以上続いたため、ノイズ・タイマが終了しました。ノイズ・タイマは、物理ポートが In Use の場合にだけ作動します。
Topology Rules	A と A、または Master と Master などのように、近隣の物理ポートがこの物理ポートとルールに反して一致しています。
Trace in Progress	物理ポートの初期化中に、PC トレースが発生しました。PC トレースが発生すると、接続を確立していない物理ポートはシャットダウンされて、トポロジが変更できなくなります。
Trace Received-Trace Off	物理ポートの PC トレース機能が禁止されている場合に、物理ポートが PC トレースを受信したため、そのポートが一時的に使用できなくなりました。Trace Disable スイッチは、PC トレース・アルゴリズムの不完全な実装から物理ポートを保護するために設計されたものです。Trace Disable スイッチは、リモートでは管理できません。

Ring Error Reason

リングにエラー状態がある理由。このフィールドには、次の値のうちいずれか 1 つが入ります。

Bridge Strip Error	ブリッジ・フレーム・ストリップを使用する局が、Sent のカウントを 0 に設定する前に、トークンを受信しました。ブリッジ・ストリップ・モードで、局は、トークンを取得してから送信されたフレームのカウントを保持し、そのフレームが 1 つずつ返されるたびにカウントを減少させます。
Directed Beacon Received	ビーコン処理でハングしている局が、指定のビーコン・マルチキャスト・アドレスにフレームを送信し、リング・ブレークの原因となった可能性があることを示しています。FDDI MAC 要素が、ANSI FDDI パラメータの T_Stuck で定義されるよりも長い時間ビーコン処理を行った場合は、局がビーコン処理でハングします。これが、PC トレースの開始前の、最後の回復処理です。

Duplicate Address Detected	局が、自分のアドレスの重複を検出しました。
Duplicate Token Detected	局が、トークンの保持中に同じトークンを受信しました。
No Reason	リングは正常に作動しています。
PC Trace Initiated	ビーコン処理でハングしている局が、アップストリーム側の隣接する局にセルフ・テストを実行させました。FDDI MAC 要素が、ANSI FDDI パラメータの T_Stuck で定義されるよりも長い時間ビーコン処理を行った場合は、局がビーコン処理でハングします。PC トレースは、最もドラスチックな障害回復処理です。
PC Trace Received	局は、セルフ・テストの開始を指示する PC トレース・フレームを受信しました。
Beaconing Initiated	トークン請求処理がリングが回復する前に TRT タイマが時間切れになったので、局はリングのビーコン処理を開始しました。ビーコン処理は、リング・ブレークの位置を突き止めます。ブレークから見てダウンストリームにある局は、ビーコン処理でハングします。FDDI MAC 要素が、ANSI FDDI パラメータの T_Stuck で定義されるよりも長い時間ビーコン処理を行った場合は、局がビーコン処理でハングします。
Ring Init Initiated	構成の変更および紛失したトークンを検出したため、この局の FDDI MAC 要素がトークン請求処理を開始しました。
Ring Init Received	別の局が、構成の変更および紛失したトークンを検出したため、トークン請求処理を開始しました。
Ring OP Oscillation	リングが、リング OP (作動) 振動で不安定になっています。つまり、立ち上がっても一時的で、再び初期化の実行に戻ってしまい、これの繰り返しになります。この問題は、二重アドレス状態の場合、頻繁に発生します。
Ring Purge Error	リング・パージャとして動作していた局が、予期していなかった時点でトークンを受信しました。局がリング・パージャとして動作している場合は、無効なフレーム 2 つを受信した後ではじめてトークンを 1 つ受信することを予期します。

Ring Latency

単一の要素がリング全体に行き渡るまでの総時間 (ミリ秒単位)。

Ring Purge Address

リング・パージャとして現在選ばれている局の 48 ビット・データ・リンクアドレス。

Ring Purger State

局の FDDI MAC 要素用リング・パージャ・アルゴリズムの状態。このフィールドには、次の値のうちいずれか 1 つが入ります。

Candidate	リングは作動中で、FDDI MAC 要素は、リング・パージャのマルチキャスト・アドレスに Candidate Hello フレームを送信することで、リング・パージャになることを要求しています。リング・パージャになるのは、最高の局 ID を持つ局です。
Non Purger	リングは作動中ですが、別の局が候補要求で勝ったか、またはこの回線が二重アドレスであるか、いずれかの原因で、FDDI MAC 要素がリング・パージャになれませんでした。
Purger	リングが作動中で、FDDI MAC 要素は、リング・パージャとして動作し、リングからフラグメントおよび所有者のないフレームを定期的にパージしています。局は、リング・パージャのマルチキャスト・アドレスに Ring Purger Hello フレームを定期的送信します。
Purger Off	リングが実行中ではないため、リング・パージャ・アルゴリズムは無効です。

Station State

局の状態。このフィールドには次のいずれかの値が入ります。

Loopback	ループバック・モード。リングには接続しません。
Off	局が無効です。
On	通常の動作モード。

Station UID

局の FDDI ポートの 48 ビット ID。最初の 2 バイトはゼロ (0) です。残りのバイトは、局の最初の MAC のリンク・アドレス値です。

Upstream Neighbor Address

この局から見てリングのアップストリーム側にある局の48ビット・ハードウェア・アドレス。

Upstream Neighbor Dup Addr Flag

アップストリーム隣接局のアドレス重複状況。このフィールドには、次のいずれかの値が入ります。

Absent	重複アドレス・テストをパスしました。
Present	重複アドレス・テストに失敗しました。

A.2.3 FDDI の特性

この項では、FDDI の特性をアルファベット順にリストします。

LEM Threshold

物理ポート用に設定されたリンク・エラー・モニタ (LEM) のしきい値。LEM は、物理ポートの通常の動作時のビット誤り率 (BER) を監視します。ビット誤り率が LEM のしきい値を超えると、局は物理ポートを使用できないようにして、リングが混乱しないようにします。

LEM のしきい値は、ビット誤り率の指数の絶対値として表現されます。しきい値の正しい範囲は 5 ~ 8 で、ビット誤り率の範囲に対応しています。ビット誤り率の範囲は、1 秒あたり $1 \times 10^{-5} \sim 1 \times 10^{-8}$ (0.0001 ~ 0.00000001) です。

Link Address

この FDDI ネットワーク・インタフェースの 48 ビット・ハードウェア・アドレス。

Physical Port Type

隣接物理ポートのタイプ。このフィールドには、次のいずれかの値が入ります。

A	FDDI デュアル・リングの着信 1 次リングおよび発信 2 次リングに接続する DAC (dual attachment wiring concentrator) あるいは DAS (dual attachment station) の物理ポート。
B	FDDI デュアル・リングの発信 1 次リングおよび着信 2 次リングに接続する DAC あるいは DAS の物理ポート。
Master	DECbridge 500 デバイスなどの SAS (single attachment station) に接続するワイア・コンセントレータの物理ポートの 1 つ。
Slave	ワイア・コンセントレータあるいは他の SAS に接続する SAS の物理ポート。
Unknown	接続されていません。

PMD Type

この物理ポートを接続できる物理メディアのタイプ。このフィールドには、次の値のうちいずれか 1 つが入ります。

ANSI Multimode	発光ダイオード (LED) ソースと PIN (P-type intrinsic N-type) 検出器に接続している、低価格の太軸コア・ファイバ。
ANSI Singlemode Type 1	レーザー・ダイオード・ソースとアバランシェ・フォトダイオード (APD) 検出器に接続している、高価格の細軸コア・ファイバ。
ANSI Singlemode Type 2	レーザー・ダイオード・ソースとアバランシェ・フォトダイオード (APD) 検出器に接続している、高価格の細軸コア・ファイバ。
ANSI SONET	同期光ネットワーク

Requested TRT

ANSI MAC パラメータの T_{req}。トークン巡回タイマには、この値が必要です。省略時の値は、8.0 ミリ秒です。

Restricted Token Timeout

この値は、単一の制限付きモード・ダイアログのタイムアウトを定義します。

Ring Purger Enable

True の場合、このリンクはリング・パージャ候補に含まれます。選択されたリンクはリング・パージャ機能を実行します。

SMT Max Version ID

サポートされる最も高い SMT バージョン ID 値。値 1 は、SMT Revision 6.2 に相当します。

SMT Min Version ID

サポートされる最も低い SMT バージョン ID 値。値 1 は、SMT Revision 6.2 に相当します。

SMT Version ID

FDDI の局管理部 (SMT) プロトコルのバージョン番号。

Station ID

局管理部 (SMT) に対する FDDI ネットワーク・インタフェースの 48 ビット ID。最初の 2 バイトは 0 で、残りのバイトは局の最初の MAC のリンク・アドレス値です。

Station Type

局のタイプ。このフィールドには次のいずれかの値が入ります。

DAS

DAS (dual attachment station)。1 つあるいは 2 つのリンクと 2 つの物理ポート、タイプ A の 1 つおよびタイプ B の 1 つを持つ局。

SAS

SAS (single attachment station)

Valid Transmission Time

FDDI MAC 要素が使用する有効転送時間 (TVX)。FDDI MAC 要素が有効フレームまたは制限なしのトークンを有効転送時間内で受信しない場合は、リングを初期化します。省略時の値は、2.621 ミリ秒です。

A.3 トークン・リング・インタフェースの監視

トークン・リングのカウンタおよびその他の属性のリストを表示するには、`netstat -I tra0 -s` コマンドを実行します。次に、このコマンドによるシステム出力のサンプルを示します。

```
tra0 Token ring counters at Thu Mar 24 07:33:00 1993
      82502 seconds since last zeroed
```

```

2230 bytes received
1704 bytes sent
  34 data blocks received
  20 data blocks sent
288 multicast bytes received
  8 multicast blocks received
306 multicast bytes sent
  13 multicast blocks sent
  0 unrecognized frames
  0 unrecognized multicast frames
  0 transmit failures
  0 transmit underrun errors
  1 line errors
  9 internal errors
  4 burst errors
  0 ARI/FCI errors
  0 abort delimiters transmitted
  3 lost frame errors
  0 receive data overruns
  0 frame copied errors
  0 token errors
  9 hard errors
  3 soft errors
  1 adapter resets
  1 signal loss
  5 beacon transmits
  2 ring recoveries
  0 lobe wire faults
  0 removes received
  0 single stations
  0 self test failures
tra0 Token ring and host information:
MAC address:                00-00-C9-19-4A-F3
Group address:               00-C0-00-80-00-00
Functional address:          00-C0-00-00-00-00
Physical drop number:        0
Upstream neighbor address:    00-00-10-C9-F5-3B
Upstream physical drop number: 0
Transmit access priority:     0
Last major vector:            Standby monitor present
Ring status:                  No problems detected
Monitor contender:            Yes
Soft error timer value:       2000 ms
Local ring number:            0
Reason for transmitting beacon: No beacon
Reason for receiving beacon:   No beacon
Last beacon upstream neighbor address: 00-00-10-C9-F3-4A
Beacon station physical drop number: 0
Ring speed:                    4Mbps
Early token release:           False

```

Open status:
Token ring chip:

Open
TMS380C26

A.3.1 トークン・リング・カウンタ

この項では、トークン・リング・カウンタをアルファベット順にリストします。

abort delimiters transmitted

データの送信中に強制終了デリミタが送信された回数。

adapter resets

アダプタがリセットされた回数。

ARI/FCI errors

SMP (standby monitor present) MAC フレームまたは AMP (active monitor present) MAC フレームの番号が受信されて、アドレス認識標識 (ARI) またはフレーム・コピー標識 (FCI) のビットが0にセットされた後に、別の SMP MAC フレームが受信されて ARI および FCI のビットが 0 にセットされた回数。

beacon transmits

送信されたビーコン処理 MAC フレームの数。

burst errors

バースト・エラーが検出された回数。

bytes received

正常に受信したバイト数。

bytes sent

正常に送信したバイト数。

data blocks received

正常に受信したフレーム数。

data blocks sent

正常に送信したフレーム数。

frame copied errors

局を認識するアドレスを持つフレームによって、フレーム・コピー標識 (FCI) がセットされた回数。

hard errors

ストリーム・エラー，周波数エラー，シグナル損失エラー，または内部エラーが検出された回数。

internal errors

回復可能な内部エラーが検出された回数。

line errors

フレームが繰り返しコピーされたか，着信フレーム内のエラー検出標識 (EDI) が 0 になったか，または次のうちのいずれかが発生した回数。

- フレームの開始デリミタと終了デリミタの間でのコード違反
- トークンでのコード違反
- フレーム・チェック・シーケンス (FCS) エラー

lobe wire faults

ワイヤ障害状態が検出された回数。

lost frame errors

アダプタがデータを送信したが，送信したフレームの終端を受信できなかった回数。

multicast blocks received

マルチキャスト・フレームで正常に受信したフレーム数。

multicast blocks sent

マルチキャスト・フレームで正常に送信したフレーム数。

multicast bytes received

マルチキャスト・フレームで正常に受信したバイト数。

multicast bytes sent

マルチキャスト・フレームで正常に送信したバイト数。

receive data overruns

フレームを受信したが、使用できるバッファ・スペースが局になかった回数。

removes received

リング局削除 MAC フレームを受信した回数。

ring recoveries

リングの回復が発生した回数。

seconds since last zeroed

関連するカウンタの属性が 0 に設定されてからの秒数。

self test failures

セルフ・テストに失敗した回数。

signal loss

リングの破損、ワイヤ・コンセントレータの障害、送信タスクまたは受信タスクの誤動作が検出された回数。

single stations

リング上に局が 1 つしかなかった回数。

soft errors

エラーの MAC フレームが送信された回数。

token errors

アクティブ・モニタが、トークンの送信を必要とするエラー状態を認識した回数。

transmit failures

送信エラーが発生した回数 (送信アンダーランを除く)。

transmit underrun errors

送信アンダーラン・エラーが発生した回数。これは、フレームの送信中に、転送先いれ先出し (FIFO) バッファが空になったことを示します。

unrecognized frames

データ・リンク・ポートがなかったために、受信ずみの個々にアドレス指定された LLC (logical link control) フレームが破棄された回数。

unrecognized multicast frames

データ・リンク・ポートがなかったために、受信ずみの、マルチキャスト・アドレス指定された LLC フレームが破棄された回数。

A.3.2 トークン・リングおよびホストの情報

この項では、トークン・リングおよびホストの情報をアルファベット順にリストします。

Beacon station physical drop number

ビーコンを送信したアップストリーム側の局の物理的位置。

Early token release

このフィールドには、次の値のうちいずれか 1 つが入ります。

- True 局は、フレームの送信を完了すると、トークンを解放します。省略時の値は、16Mb/s リングです。
- False 局は、送信されたフレーム・ヘッダを受信すると、トークンを解放します。省略時の値は、4 Mb/s リングです。

Functional address

局の機能を示すアドレス。ローカルで管理され、特定の意味を付与したビットによって定義済みデバイス群を識別するグループ・アドレスです。デバイスの例を、次に示します。

アクティブ・モニタ	C0 00 00 00 00 01
リング・パラメータ・サーバ (RPS)	C0 00 00 00 00 02
リング・エラー・モニタ (REM)	C0 00 00 00 00 08
構成レポート・サーバ (CRS)	C0 00 00 00 00 10
ソース・ルート・ブリッジ (SRB)	C0 00 00 00 01 00

Group address

局のグループ・アドレス。

Last beacon upstream neighbor address

ビーコンを送信したアップストリーム局のアドレス。

Last major vector

アダプタが実行する機能。このフィールドには、次の値のうちいずれか 1 つが入ります。

Active monitor present	アクティブ・モニタが、隣接するダウンストリーム側の近隣に、待機モニタ提供 MAC フレームを要求しました。
Beacon	アダプタによるビーコン処理に使用します。
Change parameters	ネットワーク・マネージャがアダプタ・パラメータを変更しています。
Claim token	アダプタによる、モニタ送信権の争奪処理に使用します。
Duplicate address test	アダプタが、リング内でアドレスがユニークであることを確認しています。
Initialize ring station	リング・パラメータ・サーバが、アダプタ・パラメータを設定しています。
Lobe media test	アダプタが、ループバック・パスでワイヤの連続性をテストしています。
Remove ring station	ネットワーク・マネージャが、アダプタにリングから脱退するように要求しています。
Report error	アダプタが、リング・エラー・モニタにソフト・エラー・イベントを報告しています。
Report monitor error	アダプタが、アクティブ・モニタに問題が発生したか、または局アドレスが二重になっている可能性があることを、リング・エラー・モニタに報告しています。
Report new monitor	送信権を取得した後、アクティブ・モニタ・アダプタが、この状態をネットワーク・マネージャに報告しています。
Report ring poll failure	アクティブ・モニタが、リング・エラー・モニタにリング・ポーリング処理の失敗を報告しています。

Report station address	アダプタが、局アドレスをネットワーク・マネージャに報告しています。
Report station attachment	アダプタが、アタッチメントの状態をネットワーク・マネージャに報告しています。
Report station state	アダプタが、自分の状態をネットワーク・マネージャに報告しています。
Report SUA change	アダプタが、SUA (stored upstream address)の変更をネットワーク・マネージャに報告しています。
Report transmit forward	アダプタが、送信されて取り除かれたフレームをネットワーク・マネージャに報告しています。
Request initialization	アダプタが、リング・パラメータ・サーバに操作パラメータを要求しています。
Request station address	ネットワーク・マネージャが、局アドレス報告 MAC フレームをアダプタに要求しています。
Request station attachment	ネットワーク・マネージャが、局アタッチメント報告 MAC フレームをアダプタに要求しています。
Request station state	ネットワーク・マネージャは、局状態報告 MAC フレームをアダプタに要求しています。
Response	アダプタが、応答を必要とするフレームに肯定応答を送信しているか、または MAC フレーム内の構文エラーを報告しています。
Ring purge	アクティブ・モニタによるリング・パージ処理に使用します。
Standby monitor present	アダプタが、アクティブ・モニタ提供 MAC フレームまたは待機モニタ提供 MAC フレームに応答しています。
Transmit forward	転送処理に使用します。

Local ring number

局のローカル・リング番号。

MAC address

局の MAC アドレス。

Monitor contender

局が、モニタ送信権の争奪処理を行っているかどうかを示します。このフィールドには、次の値のうちいずれか 1 つが入ります。

- No 局は、モニタ送信権の争奪処理を行いません。
- Yes 局は、モニタ送信権の争奪処理を行います。

Open status

リング上でのアダプタの状態。このフィールドには、次の値のうちいずれか 1 つが入ります。

- Close アダプタはリング上で作動していません。
- Open アダプタはリング上で作動しています。

Physical drop number

局の物理的位置。

Reason for receiving beacon

アダプタがビーコン処理 MAC フレームを受信している理由。このフィールドには、次の値のうちいずれか 1 つが入ります。

- Bit streaming アダプタが、モニタ送信権争奪送信モードでトークン請求 MAC フレームを受信する前に、モニタ送信権争奪タイムアウトが発生しました。
- Contention streaming アダプタが、モニタ送信権争奪モード (送信または受信) で 1 つ以上のトークン請求 MAC フレームを受信している間に、モニタ送信権争奪タイムアウトが発生しました。
- No beacon アダプタは、ビーコン処理 MAC フレームを受信していません。
- Signal loss アダプタは、シグナルの損失を検出しました。

Reason for transmitting beacon

アダプタがビーコン処理 MAC フレームを送信する理由。このフィールドには、次の値のうちいずれか 1 つが入ります。

- Bit streaming アダプタが、モニタ送信権争奪送信モードでトークン請求 MAC フレームを受信している間に、モニタ送信権争奪タイムアウトが発生しました。

Contention streaming	アダプタが、モニタ送信権争奪モード (送信または受信) でトークン請求MACフレームを 1 つまたは複数受信している間に、モニタ送信権争奪タイムアウトが発生しました。
No beacon	アダプタは、ビーコン処理 MAC フレームを送信していません。
Signal loss	アダプタは、リング上でシグナルの損失を検出しました。

Ring speed

リングの速度: 4Mb/s または 16Mb/s。

Ring status

アダプタがドライバに報告した状態。このフィールドには、次の値のうちいずれか 1 つが入ります。

Auto removal error	アダプタが、ローブ・ラップ・テストに失敗し、リングから脱退します。
Counter overflow	アダプタのエラー・カウンタのうちの 1 つが最大値を超えています。
Hard error	アダプタが、ビーコン処理フレームをリングに送信しているか、またはリングからビーコン処理フレームを受信しています。
Lobe wire fault	アダプタが、アダプタとワイヤ・コンセントレータを接続するケーブルで、開放回路または短絡を検出しました。
No problems detected	リングが正常に作動しています。
Remove received	アダプタが、リング局脱退の MAC フレーム要求を受信し、リングから脱退しました。
Ring recovery	アダプタが、リング上のトークン請求 MAC フレームを観察しています。
Signal loss	アダプタが、リング上でシグナルの損失を検出しました。
Single station	アダプタが、リング上で自分だけが唯一の局であることを検知しました。

Soft error アダプタが、エラー報告 MAC フレームを送信しました。

Transmit beacon アダプタが、リング上でビーコン処理フレームを送信しています。

Soft error timer value

アダプタが、ソフト・エラーを検出してからエラー報告 MAC フレームをリング・エラー・モニタに送信するまでの経過時間 (ミリ秒)。

Token ring chip

送信する局が使用したチップのタイプ。

Transmit access priority

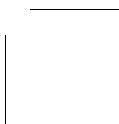
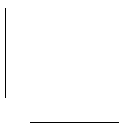
この局がリングにアクセスできる優先順位レベル。このフィールドには、0 (最低の優先順位) ~ 7 (最高の優先順位) の値が入ります。

Upstream neighbor address

アップストリーム側の局のアドレス。

Upstream physical drop number

アップストリーム側の局の位置。



B

IPsec のメッセージ

IPsec のメッセージには次のようなタイプがあります。

- 正常なステータス・メッセージ (B.1 節)
- 起動時のエラー・メッセージ (B.2 節)
- IKE 折衝のエラー・メッセージ (B.3 節)
- ipsecd デモンのメッセージ (B.4 節)

B.1 正常なステータス・メッセージ

以下のメッセージは、IPsec が正しくインストールされ、有効になっていることを示します。

IPSEC: Initializing engine

説明: IPsec モジュールがカーネルにロードされ、初期化されています。

IPSEC: Attaching to the TCP/IP stack

説明: IPsec モジュールは IP パケットを処理しています。システムは IP セキュア・モードです。

IPSEC: Detaching from the TCP/IP stack

説明: IPsec モジュールは IP パケットを処理していません。システムは IP セキュア・モードではありません。

B.2 起動時のエラー・メッセージ

ここには、一般的な起動時のエラー・メッセージと、手動鍵接続のエラー・メッセージを記載します。

B.2.1 一般的な起動時のエラー・メッセージ

次のようなエラー・メッセージが、画面やコンソールに出力されるか、または syslogd デモンに送られます。

Can not open connection with the packet processing engine. Check that the engine module is loaded into kernel, the device used on communication exists, and you have permission to open that device. This process must be run on super-user privileges.

説明: 次のような原因が考えられます。

- デーモンがすでに実行されている。
- デバイス特殊ファイルの `/dev/ipsec_engine` が削除されている。
- IPsec サブセットのインストールで問題が発生した。

Could not read configuration file '*file*': not reconfiguring

説明: IPsec の再構成が指示されたが、IPsec ポリシ・ファイルのいずれかが存在しないか、読み取れなくなっています。

Could not start the cryptography system

説明: IPsec が、CDSA (Common Data Security Architecture) サブシステムと通信できないために起動できません。CDSA サブセットが削除されているか、CDSA ライブラリまたはデータベースが壊れている可能性があります。

Dropping *IPprotocol* packet *source->dest proto:port->port*

説明: どのセキュア接続とも一致しないパケットのロギングが有効になり、IPsec が IPsec ポリシのどの規則とも一致しないパケットを受信しました。

SPD: could not decode certificate '*name*': *number*

説明: 証明書ファイルのフォーマットが無効です。

SPD: Could not decode local-address of connection '*name*'

説明: 接続のローカル・アドレスが有効な IPv4 または IPv6 アドレス、サブネット、アドレス・レンジではありません。

SPD: Could not decode remote-address of connection '*name*'

説明: 接続のリモート・アドレスが有効な IPv4 または IPv6 アドレス、サブネット、アドレス・レンジではありません。

SPD: Could not handle local-address of type *n* for connection '*name*'

説明: 接続のローカル・アドレスが有効な IPv4 または IPv6 アドレス , サブネット , アドレス・レンジではありません。

SPD: Could not handle remote-address of type *n* for connection '*name*'

説明: 接続のリモート・アドレスが有効な IPv4 または IPv6 アドレス , サブネット , アドレス・レンジではありません。

SPD: could not read certificate '*name*' of the connection '*name*'

説明: root が証明書ファイルを読み取れません。

SPD: could not read CRL '*name*'

説明: CA 証明書に CRL (Certificate Revocation List) があるというマークがついていますが , IPsec が CRL ファイルを読み取れません。

SPD: could not read private key '*name*'

説明: IPsec が非公開鍵ファイルを読み取れません。このファイルは root による読み取りが可能で , 有効な非公開鍵を含んでいなければなりません。

SPD: Invalid local-gw specification *id*

説明: ローカル・ゲートウェイの指定が無効な IPv4 または IPv6 アドレスになっています。

SPD: Invalid remote-gw specification *id*

説明: リモート・ゲートウェイの指定が無効な IPv4 または IPv6 アドレスになっています。

SPD: local and remote selectors specify different IP protocol ID. Skipping connection '*name*'

説明: 接続にローカル IPv4 アドレスとリモート IPv6 アドレス (またはその逆) が指定されていますが無効です。接続は無視されます。

SPD: no certificate file name specified for the certificate '*name*'

説明: 証明書定義内のファイル名が無効です。

SPD: no private key file specified for the authentication certificate '*name*'

説明: このホストの認証に証明書を使用していますが、非公開鍵ファイルを指定していません。非公開鍵ファイルは root による読み取りが可能で、有効な非公開鍵を含んでいなければなりません。

SPD: Policy not instantiated due to errors.

説明: SPD (Security Policy Database) ファイルに重大なエラーが見つかりました。IPsec はこのセキュリティ・ポリシでは起動しません。

SPD: port selectors specified for protocol '*proto*' which is not TCP or UDP: port selectors ignored for connection '*name*'

説明: 接続にポート番号を指定しましたが、プロトコルとして TCP や UDP 以外のものを指定しています。

SPD: the certificate '*name*' is a CA certificate but is not marked as trusted. The certificate is not configured in the certificate manager.

説明: 証明書の内部属性では、これは CA 証明書であるとされていますが、IPsec 構成ではそのようなマークが付いていません。証明書は無視されます。

SPD: the private key '*name*' is broken

説明: IPsec が非公開鍵ファイルを読み取れません。非公開鍵ファイルは root による読み取りが可能で、有効な非公開鍵を含んでいなければなりません。

SPD: the trusted certificate '*name*' does not contain the Basic Constraints extension. This is against RFC-2459. However, forcing the certificate as a point of trust because of the flag '*trusted*'.

説明: 証明書には CA (Certification Authority) 証明書であるというマークが付いていますが、通常 CA 証明書にあるような内部属性がありません。この証明書は、CA 証明書として信頼されます。

B.2.2 手動鍵接続のエラー・メッセージ

ここで述べるエラー・メッセージはセキュリティ・アソシエーション (SA) の作成時のメッセージなので、起動時に表示されます。

AH or ESP authentication key is not long enough for the specified algorithm at connection *id*

説明: 接続に指定された手動鍵が有効な長さではありません。各暗号化アルゴリズムや HMAC アルゴリズムには、鍵の長さが規定されています。

ESP cipher key is not long enough for the specified algorithm at Connection *id*: got *n*, minimum *n*

説明: 接続に指定された手動鍵が有効な長さではありません。各暗号化アルゴリズムや HMAC アルゴリズムには、鍵の長さが規定されています。

SPD: Algorithms for manually keyed connection *id* can not be determined. The proposal-list is missing, or it does not contain exactly one proposal.

説明: 手動鍵による接続には、プロポーザルを 1 つだけ含むプロポーザル・リストが必要です。プロポーザルはチェーンになることもありますが、プロトコルのインスタンスを 1 つだけ含んでいなければなりません (AH, ESP, IPcomp など)。各プロトコルには、受信と送信の鍵を指定する必要があります。

SPD: invalid number of cipher or HMAC algorithm names in proposal '*name*' for manually keyed connection '*name*'

説明: プロポーザルに、必要な数の暗号化アルゴリズムまたはハッシング・アルゴリズムの名前がありません。手動鍵による接続には、プロポーザルを 1 つだけ含むプロポーザル・リストが必要です。プロポーザルはチェーンになることもありますが、プロトコルのインスタンスを 1 つだけ含んでいなければなりません (AH, ESP, IPcomp など)。各プロトコルには、受信と送信の鍵を指定する必要があります。

SPD: invalid number of compression algorithm names in proposal '*name*' for manually keyed connection '*name*'

説明: プロポーザルに、必要な数の圧縮アルゴリズム名がありません。手動鍵による接続には、プロポーザルを 1 つだけ含むプロポーザル・リストが必要です。プロポーザルはチェーンになることもありますが、プロトコルのインスタンスを 1 つだけ含んでいなければなりません (AH, ESP, IPcomp など)。各プロトコルには、受信と送信の鍵を指定する必要があります。

SPD: invalid number of HMAC names in proposal 'name' for manually keyed connection 'name'

説明: プロポーザルに、必要な数のハッシング・アルゴリズム名がありません。手動鍵による接続には、プロポーザルを 1 つだけ含むプロポーザル・リストが必要です。プロポーザルはチェーンになることもありますが、プロトコルのインスタンスを 1 つだけ含んでいなければなりません (AH, ESP, IPcomp など)。各プロトコルには、受信と送信の鍵を指定する必要があります。

SPD: invalid number of proposals in the proposal list 'name' of the manually keyed connection 'name'

説明: 指定されたプロポーザル・リストに必要な数のプロポーザルがありません。手動鍵による接続には、プロポーザルを 1 つだけ含むプロポーザル・リストが必要です。プロポーザルはチェーンになることもありますが、プロトコルのインスタンスを 1 つだけ含んでいなければなりません (AH, ESP, IPcomp など)。各プロトコルには、受信と送信の鍵を指定する必要があります。

SPD: invalid transform type in transform 'name' for manually keyed connection 'name'

説明: 手動鍵による接続には、プロポーザルを 1 つだけ含むプロポーザル・リストが必要です。プロポーザルはチェーンになることもありますが、プロトコルのインスタンスを 1 つだけ含んでいなければなりません (AH, ESP, IPcomp など)。各プロトコルには、受信と送信の鍵を指定する必要があります。

SPD: The number of keys *n* for connection *id* does not match protocol count *n*

説明: 指定された手動鍵の数が、接続に指定されたプロトコルの数と一致しません。手動鍵による接続には、プロポーザルを 1 つだけ含むプロポーザル・リストが必要です。プロポーザルはチェーンになることもありますが、プロトコルのインスタンスを 1 つだけ含んでいなければなりません (AH, ESP, IPcomp など)。各プロトコルには、受信と送信の鍵を指定する必要があります。

SPD: too few keys for manually keyed connection 'name'

説明: 接続に必要な数の鍵を指定していません。各プロトコルには、受信と送信の鍵を指定する必要があります。

SPI for connection *id* is not specified or is less than 256.

説明: この手動鍵接続の鍵のいずれかに対する SPI 値が存在しないか、無効になっています。有効な値は、256 より大きい値です。

Transport endpoints not specified for Connection *id*.
For IKE these can be left out, but for manually keyed connection they must be present.

説明: 接続のローカル・アドレスまたはリモート・アドレス、あるいはその両方が指定されていません。手動鍵接続のパラメータは、接続に定義しなければなりません。

Truncating key name ciph len *n* to required *n* bits

説明: 接続に指定した手動鍵が有効な長さではありません。各暗号化アルゴリズムや HMAC アルゴリズムには、鍵の長さが規定されています。

B.3 IKE 折衝のエラー・メッセージ

ここには、IKE フェーズ 1 およびフェーズ 2 の折衝に関するエラー・メッセージを記載します。

B.3.1 フェーズ 1 のエラー・メッセージ

フェーズ 1 折衝の問題に関するメッセージを以下に示します。

Can not decode certificate out from BER encoded blob.
The certificate may be corrupt, or should be decoded
to binary BER blob before inserting (file format
may be wrong?)

説明: セキュリティ・ポリシで指定した証明書ファイルが読み取れないか、無効になっています。証明書は無視されます。

Can not decode CRL out from BER encoded blob. The
CRL input may be corrupted, or should be decoded to
binary BER blob before inserting (file format may be
wrong?).

説明: セキュリティ・ポリシで指定した CRL ファイルが読み取れないか、無効になっています。CRL は無視されます。

Can not get policy for *id* <-> *id*

説明: リモート・システムが IKE 折衝を開始しましたが、ローカル IKE はリモート・システムに一致するポリシを見つけることができませんでした。

Can not get subject name from a CA certificate. This certificate is not usable as an IPsec authenticator, and is not inserted into local list of trusted roots.

説明: セキュリティ・ポリシーに指定された CA 証明書に、IPsec で使用するための正しい情報がありません。

Certificate contains bad IP address: length=*n*

説明: IP アドレスを含む無効な subjectAltName 属性が証明書に含まれています。

CRL issuer name does not appear at the CRL. Can not check the CRL validity. Discarding the CRL.

説明: セキュリティ・ポリシーに指定された CRL ファイルが読み取れないか無効です。CRL は無視されます。

CRL issuer public key was not found from the local database. Can not check the CRL validity. Discarding the CRL.

説明: CRL に関連する CA 証明書が構成されていません。

Phase-1 [<initiator/responder>] between *id* and *id* failed;
reason

説明: IKE は、表示された理由でフェーズ 1 SA の折衝ができません。

Phase-1 lifetime is too short (prop=*n*, min=*n*)

説明: フェーズ 1 の存続期間が短すぎます。要求された存続期間は、最低限の値に置き換えられます。

Phase-1 notify *string* "(size *n* bytes) from *string:string*
for protocol=*n* spi(*n*)=*string*"

説明: リモート・システムが、表示した理由で IKE 折衝を拒否または変更するという通知メッセージを送信しました。

Policy manager didn't find private key

説明: IPsec は、認証の証明書に合った非公開鍵を見つけることができませんでした。非公開鍵ファイルが構成されていないか、間違ったファイルが使用されています。

Policy manager didn't find public key

説明: IKE は、証明書ベースの IKE 交換を認証するための、正しい公開鍵を見つけることができませんでした。必要な証明書または CA 証明書が構成されていないか、または証明書の ID が間違っています。

Received error notify from remote address : reason.
Deleting ISAKMP SA.

説明: リモート・システムは、表示した理由で IKE 折衝を拒否したという通知メッセージを送信しました。

Sending notification to remote-address : reason

説明: ローカル IKE は IKE 折衝を拒否または変更し、リモート IKE に通知を送信しています。

SPD: Phase-1 policy; No security policy available.

説明: IKE が実行中で、リモート・ピアからメッセージを受信しましたが、有効なローカル・セキュリティ・ポリシーがロードされていません。

SPD rejected conn using selectors id <-> id

説明: IKE 折衝を受信しましたが、指定されたリモート・アドレスに合うポリシーがありません。

The Phase-1 remote id is not an IP-address, check the peer/gw address.

説明: 構成されたアドレスが IP アドレスではありません。セレクトとゲートウェイ・アドレスに対して IP アドレスを指定する必要があります。IPsec ポリシを変更する必要があります。

B.3.2 フェーズ 2 のエラー・メッセージ

フェーズ 2 折衝の問題に関するメッセージを以下に示します。

IKE Phase-2; Could not select any protocols from IPSEC SA n

説明: ローカル・ノードとリモート・ノードのセキュリティ・ポリシーの間に、IPsec 保護に関する共通のプロポーザルがありません。どちらかを変更する必要があります。

IKE Quick-Mode negotiation between id <-> id failed:
reason

説明: 提示した理由で IPsec SA の折衝が失敗しました。

Phase-2 [role] for *id* and *id* failed; *reason*.

説明: 提示した理由で、指定されたシステム (開始システムと応答システム) 間のフェーズ 2 折衝が失敗しました。

Phase-2 lifetime is too short, reset to min (prop=*n*, min=*n*)

説明: リモート・システムが要求するフェーズ 2 存続期間が短すぎます。適用できる最短期間を代わりに使用します。

QM notification *n* (*reason*) (size *n* bytes) from
remote-address for protocol=*n* spi(*n*)=*spi-value*

説明: リモート・システムが、提示した理由でフェーズ 2 折衝を拒否または変更したことを示す通知メッセージを送信しました。

Received responder lifetime notification: "life_secs=*n*,
life_kbytes=*n*"

説明: リモート・システムは、フェーズ 2 SA に対して間違った存続期間の値を選択しました。

Requested to delete SA protocol[*spi-value*]

説明: リモート・システムが、指定された SA を削除するようにという要求を送信しました。これは、リモートが IPsec の処理をシャットダウンしたか停止したことを示します。

SA-per-host specified and the remote requested addresses
range or subnet -> rejecting connection.

説明: ローカル・ポリシーは、接続ルールに一致する各ホストに対して一意の SA を作成するように指定しています。ただし、リモート・ポリシーでは一致する全ホストに対して単一の SA を使用するようになっています。

SA-per-host specified without remote addresses given and
the remote did not request QM for itself -> rejecting
connection.

説明: ローカル・ポリシーでは、認証されたすべてのリモート・ホストに対してこの接続の使用を許可しています。これを安全に行うには、リモート・ポリシーでは自分のアドレスに関してのみ、SA の折衝を行う必要があります。これにより、リモート VPN ゲートウェイは、受信する予定のないパケットを要求することがなくなります。

The bundle *n* to be installed does not contain any inbound SA's. Not installing it.

説明: フェーズ 2 折衝で何らかの問題が発生して完了しなかったため, SA が作成されていません。この問題は, 手動鍵接続にエラーがあった場合にも発生します。

The bundle *n* to be installed does not contain any outbound SA's. Not installing it.

説明: フェーズ 2 折衝で何らかの問題が発生して完了しなかったため, SA が作成されていません。この問題は, 手動鍵接続にエラーがあった場合にも発生します。

Tunnel endpoints not specified for Connection *id*

説明: IKE は, 指定された接続のセキュア・ゲートウェイ・アドレスとして省略時の値を選択できませんでした。いずれか, または両方のセキュア・ゲートウェイのアドレスを, 接続に指定する必要があります。

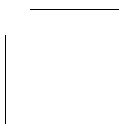
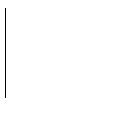
B.4 ipsecd デーモンのメッセージ

以下のメッセージは, ipsecd デーモンが一時的に過負荷になっているか, IPsec カーネル・モジュールからの情報に応答していないことを示しています。これらの状態は, 必ずしも問題を示しているとは限りませんが, これらのメッセージが高い頻度で表示される場合, ipsecd デーモンがハングアップして, 再起動が必要であるという可能性があります。

```
ssh_send to ipm:  queue full, priority message dropped,  
len=n type=n queue_size=n
```

```
ssh_send to ipm:  dropping entry to make space for  
important packet
```

```
ssh_send to ipm:  WARNING: queue full, important packet  
dropped len=0xn, type = n
```



用語集

Diffie-Hellman

公開鍵暗号化を用いた鍵生成方法。Diffie-Hellman アルゴリズムは、2 人のユーザが公開情報を交換することで開始されます。各ユーザは、次に相手の公開情報を数学的に自分の非公開情報に連結し、共有非公開値を計算します。この非公開値は、セッション鍵、またはランダムに生成されるセッション鍵を暗号化するための暗号鍵として使用できます。この方式では、双方のユーザが保持している公開情報と非公開 (シークレット) 情報に基づいて、セッション鍵が生成されます。

DSA

電子署名アルゴリズム (Digital Signature Algorithm)。電子署名のための公開鍵アルゴリズム。詳細は、Bruce Schneier 著『*Applied Cryptography*』を参照してください。

DSS

電子署名標準 (Digital Signature Standard)。DSA 公開鍵アルゴリズムと SHA ハッシュ・アルゴリズムを使用する電子署名の標準である、米国政府の電子署名標準。

HMAC

ハッシュ・メッセージ認証コード (Hash Message Authentication Code)。データの送信元の認証と、2 者間で送信されるパケットのデータ保全の両方に使用される、非公開鍵認証アルゴリズム。ただし、これを行うためには、送信元と宛先のみが HMAC 鍵を知っているようにしなければなりません。HMAC が正しければ、送信元によって追加されたことが保証されます。

MD5

メッセージ・ダイジェスト・アルゴリズム (RFC 1321 に記載されている)。ドキュメントの安全で不可逆な強力な暗号化能力を備えたハッシュ値を計算します。ほとんどの場合、SHA-1 アルゴリズムの方が安全であると考えられます。SHA を参照してください。

事前共有鍵

IKE での認証方式。2 つのピアが共有のパスワードを構成し、暗号化によってエンドポイントを認証する際に、そのパスワードを使用します。送信者が暗号化したパケットを受信者が解読できる場合、受信者は送信者が同じシークレット情報を知っていることがわかります。この認証方式は、ホスト数が限られている場合にはうまくいきます。ホストの数が多い場合は、証明書ベースの認証を使用してください。

公開鍵暗号化

各ホストが、非公開鍵と公開鍵という 2 つの鍵を持つ方式。非公開鍵は、送信メッセージへの署名と受信メッセージの暗号解読に使用します。公開鍵は、特定のホストから送られる署名付きメッセージの信憑性を他者が確認するためと、その特定ホストに送られるメッセージを暗号化するために使用します。非公開鍵は文字どおり非公開です。所有者以外に使わせてはなりません。これに対して、公開鍵は信頼できるチャンネルを通して誰にでも配付できます。

RSA

公開鍵暗号化と電子署名のアルゴリズム。詳細は、Bruce Schneier 著の『*Applied Cryptography*』を参照してください。

SHA-1

Secure Hash Algorithm バージョン 1。強力な暗号化能力を備えたハッシュ・アルゴリズム (FIPS PUB 180-1 に記載されている)。国家安全保障局 (NSA) が設計し、米国の電子署名標準の一部になっています。MD5 を参照してください。

SPI

セキュリティ・パラメータ・インデックス。宛先のアドレスやセキュリティ・プロトコルと組み合わせて、SA を一意に識別するために使用する任意の値。これによって、受信側システムは、受信した IP パケットの処理にどの SA を使用するかを決定できます。

索引

数字および記号

6bone

アドレス割り当て 3-13

接続 3-63

6to4 トンネル 3-17

A

acucap ファイル 8-47

Address Resolution Protocol

(ARP を参照)

AH

認証アルゴリズム 4-9

保護 4-6

モード 4-6

ARP

サーバ ATM アドレスの指定 . 6-12

サーバの IP アドレスの指定 . 6-12

システムの役割の指定 6-12

arp コマンド 11-12

ARP サーバ

/etc/atmhosts ファイル 6-20

ARP テーブル

CLIP との関係 6-31

LANE に対する表示 6-32

エントリの削除 6-31

エントリの作成 6-31

ATM

CLIP を使用した構成 6-19

ESI の指定 6-9

ILMI の指定 6-10

LANE を使用した構成 6-24

UNI バージョンの指定 6-10

VC 計算の指定 6-10

環境の管理 6-30

カーネル・オプションの確認 . 6-7

構成 6-17

構成に必要な情報 6-8

構成の準備 6-8

サブセットがインストールされてい
ることの確認 6-6

シグナリングの管理 6-31

シグナリングの指定 6-10

スイッチングを使用した構成 6-27

デバイス・ドライバの無効化 6-31

デバイス・ドライバの有効化 6-31

トラブルシューティング ... 10-33

ネットワーク情報の表示 6-31

ネットワーク層の指定 6-9

フロー制御の指定 6-9

メッセージ 6-33

メッセージ・レベルの変更... 6-33

atmarp コマンド 6-31

atmconfig コマンド 6-31

atmelan コマンド 6-32

atmhosts ファイル

CLIP のための編集 6-20

LANE のための編集 6-24

および ARP サーバ.....	6-20
atmifmp コマンド	6-32
atmsig コマンド	6-31
ATM 設定アプリケーション	6-17
CLIP の構成	6-22
IP スイッチングの構成.....	6-28
LANE の構成	6-25

B

Binding Acknowledgement ...	5-5
Status フィールドの値.....	10-26
Binding Update	5-5
BOOTP	
DHCP	7-26
クライアントの登録.....	7-25
BSD デバイス	
LAT.....	9-6

C

CDSL	1-9
Certificate Revocation List	
(CRL を参照)	
Challenge Authentication Protocol	
(CHAP を参照)	
CHAP	
chap-secrets ファイル. 8-19, 8-34	
PPP とともに使用	8-18
chat スクリプト	8-15
CIDR	3-4
Classical IP	
(CLIP を参照)	
Classless Inter-Domain Routing	
(CIDR を参照)	

CLIP

ATM 設定アプリケーションの実	
行	6-22
ATM を使用した構成.....	6-19
ATM を使用した構成の計画..	6-10
/etc/atmhosts ファイルの編集	6-20
/etc/hosts ファイルの編集	6-21
LIS インタフェースの構成 ...	6-23
PVC の設定	6-22
スタティック・ルートの追加	6-24
説明	6-2
トラブルシューティング ...	10-35
リモート・ホスト・サポートの指	
定	6-12
Compaq Analyze	11-16
Compaq Insight Manager	1-8
connection refused メッセージ	
IPv6 ホスト.....	10-17
IPv6 ルータ.....	10-25

CRL

の使用	4-14
-----------	------

D

DECevent	11-16
DHCP	7-1
joind デーモン	7-20
xjoin	7-14
アドレス割り当ての無効化...	7-26
クライアントの起動.....	7-22
クライアントのモニタリング	7-23
構成中のサーバの識別	2-12
構成に必要な情報.....	7-5
構成の計画.....	7-3
構成ワークシート.....	7-5, 7-10

サーバの起動 7-20
サーバの構成 7-14
セキュリティ 7-5, 7-25
トラブルシューティング ... 10-44
ネットワーク構成時の指定... 2-12
ハードウェア・アドレスのマッピン
グ 7-24
Diffie-Hellman グループ 4-43
(グループも参照)
DNS
IPv6 のデータ・フォーマット 3-12
IPv6 のレコード・タイプ 3-12
逆引きルックアップ用のドメイ
ン 3-12
Domain Name System
(DNS を参照)
Dynamic Host Configuration
Protocol
(DHCP を参照)

E

ELAN
elan インタフェースの構成 .. 6-27
/etc/hosts ファイルとの関係 .. 6-25
名前の指定 6-14
番号の指定 6-14
Emulated LAN
(ELAN を参照)
Encapsulating Security Payload
(ESP を参照)
ESI
ATM アダプタに対する指定... 6-9
削除 6-31

作成 6-31
ESP
認証アルゴリズム 4-9
保護 4-6
モード 4-7
/etc/acucap ファイル
(acucap ファイルを参照)
/etc/inittab ファイル
LAT 用のカスタマイズ 9-11
/etc/remote ファイル
(remote ファイルを参照)
/etc/slhosts ファイル
(slhosts ファイルを参照)
/etc ファイル
(ファイルを参照)

F

FDDI
netstat による監視 11-11
インタフェース・カウンタ... A-6,
A-9
インタフェースの状態 . A-9, A-17
インタフェースの特性 A-17, A-19
監視 A-4
構成 2-24
構成に必要な情報 2-10
情報の表示 2-45
パラメータの修正 2-45
パラメータの表示 2-45
fddi_config コマンド 2-45
Fiber Distributed Data Interface
(FDDI を参照)
FTP

IPsec 接続に対する構成 4-58

G

gated.conf ファイル 2-19

gated デーモン

構成 2-29

定義 2-18

gateways ファイル 2-17

H

HEXL

説明 4-14

host is unreachable メッセージ

オフリンク・ノード (IPv6 ホスト) 10-15

オフリンク・ノード (IPv6 ルータ) 10-22

オンリンク・ノード (IPv6 ホスト) 10-13

オンリンク・ノード (IPv6 ルータ) 10-20

hosts.equiv ファイル 2-22

構成 2-33

hosts ファイル

CLIP のための編集 6-21

ELAN ホストとの関係 6-25

IP スイッチングのための編集 6-27

LANE のための編集 6-25

hwmgr ユーティリティ 11-1

I

ICMP メッセージ 11-15

ID

の問題 4-16

ifaccess.conf ファイル 2-45

ifconfig コマンド 2-45

IPv6 アドレスの削除 3-66

IPv6 アドレスの追加 3-65

IPv6 インタフェース ID の割り当て 3-64

IPv6 インタフェースの削除 .. 3-64

IPv6 インタフェースの初期化 3-63

NIC 情報の表示 11-1

IKE

アグレッシブ・モード 4-11

クイック・モード 4-12

存続期間 4-36

定義 4-11

フェーズ 1 交換 4-11

フェーズ 2 交換 4-12

メイン・モード 4-11

IKE オプション

ワークシート 4-42

IKE プロポーザル

カスタム・ワークシート 4-35

省略時の 4-34

名前の形式 4-34

ワークシート 4-32

IKE プロポーザル・リスト

省略時の 4-33

ILMI

ATM アダプタに対する指定 .. 6-10

inittab ファイル

LAT 用のカスタマイズ 9-11

Insight Manager 1-8

Integrated Layer Management

Interface

(ILMI を参照)

Internet Key Exchange

(IKE を参照)

Internet Protocol Security

(IPsec を参照)

Internet Protocol Version 6

(IPv6 を参照)

InterNIC

IP アドレス 2-13

IP MTU のサイズ 2-50

ip6_setup ユーティリティ

ホストの構成 3-46

ルータの構成 3-54

ip6rtrd.conf ファイル 3-70

ip6rtrd デモン

デバッグ情報のロギング 5-11

デバッグ情報のログ取得 3-71

動作していない 10-19

ログ・ファイル 3-71, 5-11

ips

インタフェースの構成 6-29

IPsec

エラー・メッセージ B-1

鍵交換 4-10

環境 4-1

カーネルに必要なサポート... 4-18

起動時のエラー・メッセージ . B-1

クラスタ・ポリシ 4-18

計画 4-17

構成されていない 10-28

構成に必要な情報 4-20

構成例 4-1

構成例のワークシート 4-47

構成ワークシート 4-20

採用のステップ 4-19

サブセットがインストールされてい

ない 10-27

事前共有鍵接続の失敗 10-29

証明書 4-13

証明書接続の失敗 10-31

制限 4-4

セキュア・ゲートウェイの構

成 4-63

セキュア接続 4-4

セキュリティ・アソシエーショ

ン 4-9

全トラフィックを通す 4-58

存続期間 4-31

デモンが開始されていない 10-28

トラブルシューティング ... 10-27

ノードに到達できない 10-27

プロトコル 4-5

ホストの構成 4-59

モニタリング 4-71

ipsecd デモン

起動 4-68

再ロード 4-69

追加ログ・メッセージの取得 10-29

停止 4-69

デバッグの有効化 10-29

IPsec 接続

FTP の構成 4-58

SysMan の省略時の接続 4-5

全トラフィックを通す構成... 4-58

特定のトラフィックに対する構

成 4-58

とセキュリティ・ポリシ 4-12

名前の指定 4-23

ワークシート	4-22	サポートされているインタフェース	3-19
IPsec の規則		サポートされているコマンド	3-19
の構成要素.....	4-4	プランニング	3-24
IPsec プロポーザル		ホストの構成	3-46
カスタム・ワークシート	4-29	メッセージ.....	3-71
名前の形式.....	4-29	問題の解決.....	10-10
の順序	4-29	用語	3-2
ワークシート	4-25	ルータの構成	3-54
IPsec プロポーザル・リスト		ipv6forwarding 属性	3-67
省略時の	4-26	ipv6router 属性	3-67
iptunnel コマンド	3-65	IPv6 アドレス	
IPv4 アドレス		6to4 トンネル	3-29
6to4 トンネル	3-29	構成済みトンネル.....	3-30
構成済みトンネル.....	3-30	IPv6 構成済みトンネル	
IPv4 構成済みトンネル		(構成済みトンネル を参照)	
(構成済みトンネル を参照)		IPv6 サブシステム	
IPv4 互換 IPv6 アドレス.....	3-6	チューニング	3-71
IPv4 射影 IPv6 アドレス.....	3-7	IP アドレス	2-13
IPv6		DHCP のための構成	7-15
6bone ネットワーク	3-63	NIC	2-13
Mobile IPv6 にはカーネルのサポー		取得	2-13
トが必要	5-8	ネットワーク数	2-14
rc.config ファイルの編集	3-68	リモートの指定	4-23
アドレスの自動構成.....	3-11	ローカルの指定	4-24
アドレスの種類	3-4	IP スイッチング	
アドレッシング	3-3	ATM 設定アプリケーションの実	
インタフェースからの削除... 3-64		行	6-28
インタフェースでの初期化... 3-63		ATM を使用した構成.....	6-27
カーネルでのサポートの必要		ATM を使用した構成の計画.. 6-15	
性	3-24	/etc/hosts ファイルの編集 6-27	
カーネル内のサポートの構成 3-67		ips インタフェースの構成 6-29	
構成済みトンネルの作成	3-65	管理	6-32
構成に必要な情報	3-25	統計値の表示	6-32
構成例	3-32	特徴	6-4
構成ワークシート	3-25		

トラブルシューティング ...	10-41
無効化	6-32
有効化	6-32
ルートの追加	6-29
IP セキュア・モード	4-68
IP 別名	2-35
IP ルータ	2-19
システムの構成	2-30
定義	2-19
要求	2-30

J

joind デーモン	7-20
-------------------------	------

L

lag	2-7
------------------	-----

LAN

RIPng の使用	3-31
-----------------	------

LAN Emulation

(LANE を参照)

LAN Emulation Configuration

Server

(LECS を参照)

LAN Emulation Server

(LES を参照)

LANE

ARP テーブルの表示	6-32
ATM 設定アプリケーションの実 行	6-25
ATM を使用した構成	6-24
ATM を使用した構成の計画 ..	6-13
elan インタフェースの構成 ..	6-27

/etc/atmhosts ファイルの編集	6-24
/etc/hosts ファイルの編集	6-25
環境の管理	6-32
特徴	6-3
トラブルシューティング ...	10-38
メッセージ・レベルの変更 ...	6-33

LAT

DLB サポートの確認	9-5
-------------------	-----

 /etc/inittab ファイルのカスタマイ

 ズ

LAN サービス

 専用の作成方法

LAT/Telnet サービスの定義方

 法

latsetup コマンド

latsetup によるこうせい

NetRAIN

アクセスの制御

回線制御規則

ゲートウェイ・サービス

構成に必要な情報

構成の計画

構成例

サーバ・ノード

サーバ名を定義

サービスのタイプ

サービス・ノード

サービス・ノード・グループ .

自動スタートアップおよびシャット

 ダウン

スタートアップ・ファイルの作

 成

接続のタイプ

- セットアップ 9-8
- 専用サービスの作成方法 9-20
- 端末での専用 tty デバイス ... 9-22
- ターミナル・サーバのポート設
定 9-13
- デバイスのタイプ 9-6
- デバイスの追加 9-8
- トラブルシューティング ... 10-53
- パスワードの保護 9-4
- 発信接続 9-18
- 負荷分散 9-5
- 複数のネットワーク・アダプタの構
成 9-12
- プリンタ設定のテスト方法 ... 9-14
- プリンタの設定 9-12, 9-16
- テスト方法 9-16
- プリンタの設定をテスト 9-16
- プリンタ・ハードウェアの特
性 9-13
- プリント・スプーラの設定方
法 9-15
- ホストが開始する接続
 プログラム・インタフェー
 ス 9-17
- ホスト側が開始する接続 9-16
- ホスト側が開始する接続の設
定 9-16
- ポート名を定義 9-14
- ユーザ作成の LAN サービス . 9-20
- スタートアップ 9-21
- 設定 9-21
- LAT/Telnet** ゲートウェイ 9-19
- スタートアップ 9-19
- 設定 9-19
- latsetup** コマンド 9-8

- latstartup.conf** ファイル 9-9
- learp** コマンド 6-32
- LEC**
 - 構成 6-32
 - 作成 6-32
 - 状態の表示 6-32
- LECS**
 - ATM アドレスの指定 6-14
- LES**
 - ATM アドレスの指定 6-14
 - /etc/atmhosts ファイルとの関
係 6-24
- LIS**
 - LIS インタフェースの構成 ... 6-23
 - 作成 6-31
 - 定義 6-2
 - 番号の指定 6-11
- Local Area Transport**
(LAT を参照)

M

- MAC** アドレス
 - インタフェース ID 3-5
- Microsoft Challenge**
Authentication Protocol
(MS-CHAP を参照)
- Microsoft RAS** サーバ 8-36
 - CHAP 認証の問題の解決 8-38
 - 構成 8-37
- Mobile IPv6** 5-1
 - インストールの準備 5-7
 - 環境 5-2
 - カーネルのサポートが必要 5-8
 - 経緯 5-2

コレスポンデント・ノードの構成	5-9
制限	5-1
動作	5-3
モニタリング	5-10
ルータの構成	5-9
MS-CHAP	
PPP とともに使用	8-18
MTU	
サイズの指定	6-15

N

nd6hostd デーモン	
デバッグ情報のログ取得	3-71
ログ・ファイル	3-71
NetRAIN	2-5
LAG	2-36
LAT	2-36
MAC アドレスに基づくライセンス 認証	2-6
インタフェースの監視	2-41
インタフェースの構成	2-36
ハードウェア制限	2-36
メンバの設定	2-15
netstat コマンド. 5-10, 11-11, A-1	
IPsec のモニタリングに使用 . 4-71	
SA のモニタリングに使用 4-69	
Network Information Center (NIC を参照)	
network is unreachable メッセージ オフリンク・ノード (IPv6 ホス ト).....	10-15

オフリンク・ノード (IPv6 ルー タ).....	10-22
オンリンク・ノード (IPv6 ホス ト).....	10-13
オンリンク・ノード (IPv6 ルー タ).....	10-20
networks ファイル	2-23
niftd デーモン	11-5
nonce	4-12
nr インタフェース	2-5

P

PAP	
PPP とともに使用	8-18
pap-secrets ファイル... 8-19, 8-33	
Password Authentication Protocol (PAP を参照)	
PEM	
説明	4-14
PFS	
IKE に対する指定.....	4-43
ping コマンド.....	11-8
Point-to-Point Protocol (PPP を参照)	
PPP	
chap-secrets ファイル. 8-19, 8-34	
chat スクリプト.....	8-15
Microsoft RAS サーバ.....	8-36
pap-secrets ファイル.. 8-19, 8-33	
pppd の実行のガイドライン.. 8-36	
オプション・ファイル 8-32, 8-40	
ゲートウェイ	8-39
構成のサンプル	8-13

構成ワークシート	8-22
セキュリティ	8-18
接続のガイドライン	8-22
接続の終了	8-41
接続のモニタリング	8-41
設定に必要な情報	8-22
ダイアル・アウト・システムの構成	8-30
ダイアル・イン・システムの構成	8-38
トラブルシューティング ...	10-51
pppd デーモン	
オプション	8-17, 8-22
実行のガイドライン	8-36
PPP リンク	
RIPng の使用	3-31
PVC	
CLIP のための構成	6-22
削除	6-31
作成	6-31
作成の確認	6-24

Q

QoS	
定義	2-51

R

rc.config ファイル	
IPv6 変数	3-68
NetRAIN	2-36
rcmgr ユーティリティでの編集	1-10
remote ファイル	8-47
Resource ReSerVation Protocol	

(RSVP を参照)

RIPng	
PPP リンク上での使用	3-31
トンネルで使用する	3-30
routed デーモン	2-16
構成	2-27
定義	2-16
route コマンド	
ルータの削除 (IPv6)	3-66
ルータの追加 (IPv6)	3-66
RSA 暗号化	
と証明書	4-16
RSVP	
管理	2-53
起動	2-53
終了	2-53
定義	2-51
rwhod デーモン	2-16
構成	2-27
定義	2-16

S

SA	
定義	4-9
モニタリング	4-69
SDH	
ATM アダプタに対する指定 ...	6-9
Security Policy Database	
(SPD を参照)	
slhosts ファイル	8-7
SLIP	
IP アドレス	8-5
startslip コマンド	8-6
ゲートウェイ	8-10
構成	8-8

構成に必要な情報	8-4
構成のサンプル	8-1
構成の準備	8-2
接続ガイドライン	8-43
接続の終了	8-12
ダイアル・アウト・システムの構成	8-10
ダイアル・イン・システムの構成	8-9
トラブルシューティング ...	10-47
モデムのガイドライン	8-3
SNAP	
省略時の VCI の設定	6-17
SONET	
ATM アダプタに対する指定 ...	6-9
SPD	
送信パケットの処理	4-5
SPI	
と SA	4-9
と手動鍵	4-45
srconfig コマンド	2-47
startppp コマンド	
ダイアル・イン接続での使用	8-39
startslip コマンド	
サブコマンド	8-6
スクリプト・ファイルからのサブコマンドの呼び出し	8-11
ダイアル・イン接続に使用	8-9
Subnetwork Attachment Point (SNAP を参照)	
SVC	
削除	6-31
SVR4 デバイス	
LAT	9-6

Synchronous Data Hierarchy

(SDH を参照)

Synchronous Optical Network

(SONET を参照)

syslogd デーモン	11-17
SysMan Menu	1-3
ATM の構成	6-17
gate デーモンの設定	2-29
hosts.equiv ファイルの設定 ..	2-33
IP ルータの構成	2-30
LAT の構成	9-8
PPP chap-secrets ファイルの変更	8-34
PPP pap-secrets ファイルの変更	8-33
PPP オプション・ファイルの作成	8-32, 8-40
route デーモンの設定	2-27
rwho デーモンの設定	2-27
syslogd メッセージ・ファイルの表示	11-17
起動	1-3
クイック・セットアップ	1-4
静的ルート・ファイルの設定	2-31
ネットワーク・インタフェースの構成解除	2-26
ネットワーク・インタフェースの設定	2-24
ネットワーク・セットアップ・ウィザード	1-6
ネットワーク・ファイルの設定	2-34
ホスト・ファイルの設定	2-33

T

- tcpdump** コマンド..... 5-10, 11-16
- timeout** メッセージ
 - オフリンク・ノード (IPv6 ホスト)..... 10-15
 - オフリンク・ノード (IPv6 ルータ)..... 10-22
 - オンリンク・ノード (IPv6 ホスト)..... 10-13
 - オンリンク・ノード (IPv6 ルータ)..... 10-20
- tip** コマンド 8-31, 8-44
- Token Ring**
 - アダプタの速度 2-15
- traceroute** コマンド..... 11-13

U

- uerf** コマンド 11-16
- UNI**
 - ATM アダプタのバージョン番号 6-10
- unknown host** メッセージ
 - IPv6 ホスト..... 10-12
 - IPv6 ルータ..... 10-19
- User-Network Interface (UNI)**
 - (UNI を参照)

V

- VC**
 - ATM アダプタに対する計算.. 6-10
 - 監視 6-31
- VCI**
 - PVC に対する指定 6-12

Virtual Private Network

(VPN を参照)

VPI

PVC に対する指定 6-12

VPN..... 4-2

X

xjoin コーティリティ 7-14

あ

アクション

指定 4-25

定義 (IPsec) 4-4

アグレッシブ・モード

IKE に対する指定..... 4-43

のメッセージ 4-11

アダプタ

(ネットワーク・インタフェース を参照)

宛先プレフィックス 3-32

アドレス

6bone テスト用 3-13

CIDR 3-4

IPv6 3-3

エニーキャスト 3-9

サイズ 3-3

自動構成されない..... 10-23

テキスト表記 3-3

名前へのマッピング..... 3-12

マルチキャスト 3-9

ユニキャスト 3-5

割り当て..... 3-13

アドレス解決プロトコル, **ARP** を参照..... 11-12

アドレスの自動構成	
DHCPv6.....	3-12
ステートフル	3-12
ステートレス	3-11
アドレス・プレフィックス	3-11
トンネル経由の通知.....	3-30
トンネル上で公開.....	3-29
リモート・ネットワーク	3-32
リンク上での通知.....	3-31
暗号化	
IKE アルゴリズム.....	4-35
暗号鍵.....	4-10
IPsec 鍵に対する指定	4-45
アンバウンド対話式サービス ...	9-20

い

イベント・ビューア	
syslogd メッセージ・ファイルの表 示	11-17
インストレーション・クローニン グ.....	1-10
インタフェース	
(ネットワーク・インタフェー スを参照)	
インタフェース ID	
IPv6 インタフェースへの割り当 て	3-64
MAC アドレス	3-5
ユニキャスト・アドレス	3-5
インターネット・アドレスから MAC アドレスへの変換テーブル. 11-12	
インターネット・プロトコルのアド レス	

(IP アドレス を参照)	
イーサネット	
構成	2-24
構成に必要な情報.....	2-10
イーサネット・インタフェース	
カウンタ.....	A-1, A-4
監視	A-1, A-4
イーサネット・カウンタ	A-1

え

エニーキャスト・アドレス	3-9
エラー・メッセージ	10-1
(トラブルシューティング; 問題 も参照)	
IPsec.....	B-1
エラー・ログ・ファイル	
表示	11-16
エンド・システム	6-2
エンド・システム識別子	
(ESI を参照)	

お

オプション	
IKE のワークシート	4-42
PPP のワークシート	8-22
オプション・サービス.....	9-20
オプション・ファイル... 8-32, 8-40	
オフリンク・ノード	
到達できない (IPv6 ホスト) 10-15	
到達できない (IPv6 ルータ) 10-22	
オンリンク・ノード	
アドレスを自動構成できない 10-23	

到達できない (IPv6 ホスト) 10-13
到達できない (IPv6 ルータ) 10-20
オンリンク・プレフィックス
用の経路の追加 3-67

か

回線制御規則 9-17
カウンタ
イーサネット A-1
トークン・リング A-21
カウンタ, **FDDI** A-6
鍵
暗号化 4-10
交換 4-10
事前共有 4-39
手動 4-10
と IKE 4-11
認証 4-10
鍵交換
IPsec 4-10
仮想回路
(VC を参照)
仮想チャネル識別子
(VCI を参照)
仮想パス識別子
(VPI を参照)
カーネル
ATM の構成 6-7
IPv6 ルーティングの構成 3-67
Mobile IPv6 が構成されてい
ない 10-26
の PPP 構成 8-22
カーネル, **LAT** 用の構成 9-5

き

気付アドレス
モバイル・ノードにバインディング
を登録できない 10-26
キーブアライブ
IKE SA に対する指定 4-42

く

クイック・セットアップ 1-4
クイック・モード
交換 4-12
クライアント
DHCP 7-2
DHCP のモニタリング 7-23
IP アドレスの取得 2-12
クラスタ
IPsec ポリシ 4-18
グループ
IKE に対する指定 4-43
PFS に対する指定 4-43
クローニング
インストレーションと構成... 1-10

け

経路
オンリンク・プレフィックス用の追
加 3-67
静的 3-28, 3-32, 3-65
他のルータとの交換 3-31
トンネル経由の交換 3-30
ゲートウェイ 4-63
(セキュア・ゲートウェイ も参
照)

PPP.....	8-39
SLIP.....	8-10
ケーブル	
ヌル・モデム	8-3
モデムとともに使用する場合のガイ ドライン	8-43

こ

公開鍵証明書	
root に対する指定	4-40
構成	
BOOTP クライアント	7-25
DHCP	7-17
DHCP サーバ	7-16
SLIP ダイアル・アウト・システ ム	8-10
SLIP ダイアル・イン・システ ム	8-9
構成クローニング	1-10
構成済みトンネル	3-18
RIPng を使用する	3-30
構成例	
セキュア・ゲートウェイ対セキュ ア・ゲートウェイ	4-2
ホスト対セキュア・ゲートウェ イ	4-3
ホスト対ホスト	4-2
コマンド	
arp	11-12
ifconfig	2-45
srconfig	2-47
startslip	8-6
tip	8-44

コレスポンデント・ノード	
Mobile IPv6 の構成	5-9
定義	5-2
バインディングのモニタリン グ	5-10
コンテキスト依存のシンボリック・ リンク	
(CDSL を参照)	

さ

サイト・プレフィックス	
6to4 トンネル	3-29
サイト・ローカル・アドレス	3-8
サブネット	
多重インタフェース	2-3
サブネット・マスク	2-14
IP スイッチング	6-6
定義	2-14
ネットワーク・クラス	2-14
サブネットワーク	
複数のインタフェース	2-35
サブネットワーク , DHCP	7-17
サーバ	
DHCP	7-2
DHCP 用の構成	7-14
LAT	9-1
からの IP アドレスの取得	2-12
サービス	
品質	2-51
サービスのタイプ , LAT	9-20
サービス品質	
(QoS を参照)	

し

事前共有鍵	
IKE に対する指定.....	4-39
自動トンネル.....	3-16
周知のマルチキャスト・アドレ ス.....	3-10
手動鍵.....	4-10
ワークシート	4-44
準備	
Mobile IPv6	5-7
状態	
FDDI	A-9
証明書	
IPsec.....	4-13
エンコーディングのタイプ...	4-14
ガイドライン	4-15
作成	4-16
タイプ	4-13
定義	4-13
ローカル・ホストの指定	4-38
ワークシート	4-40
シークレット・ファイル	8-33

す

スイッチ	6-1
スタティック・ルート.....	2-20

せ

制限	
IPsec.....	4-4
Mobile IPv6	5-1
静的経路	3-28, 3-65
静的ルート	2-31

性能

チューニング	3-71
セキュア・ゲートウェイ	
IPsec に対する構成	4-63
IP ルーティングの有効化	4-63
定義	4-2
セキュア接続	
IPsec.....	4-4
省略時の	4-5
定義	4-4
セキュリティ	
DHCP	7-5, 7-25
PPP.....	8-18
インタフェースへのアクセスの制 御	2-45
セキュリティ・アソシエーション (SA を参照)	
IPsec.....	4-9
接続.....	4-23
(IPsec 接続 も参照)	
IPsec のテスト.....	4-19
LAT ホスト側が開始する接続	9-16
SLIP の終了	8-12
異常終了 (IPv6 ホスト)	10-18
異常終了 (IPv6 ルータ)	10-25
ダイアル・アウト・アクセス用のシ ステムの構成	8-47
ダイアル・イン・アクセス用のシ テムの構成	8-44
発信	
LAT	9-18
セレクタ	
定義 (IPsec)	4-4
専用サービス.....	9-20

そ

存続期間	
IKE に対する指定.....	4-36
IPsec に対する指定	4-31
プロポーザルを優先.....	4-44
ソース・ルーティング.....	2-47

た

ダイアル・アウト接続.....	8-47
PPP.....	8-30
ダイアル・イン接続	8-44
PPP.....	8-38
端末での専用 tty デバイス	9-22

ち

チューニング	
IPv6 サブシステム	3-71

て

デバイス	
LAT.....	9-6
データグラム	
ネットワーク経路の表示 ...	11-13
デーモン	
pppd.....	8-17

と

特性, FDDI	A-17
トラフィック制御	2-52
トラブルシューティング	10-1

(エラー・メッセージ も参照)

ATM.....	10-33
CLIP.....	10-35
DHCP	10-44
IPsec.....	10-27, B-1
IP スイッチング	10-41
LANE.....	10-38
LAT.....	10-53
PPP.....	10-51
SLIP.....	10-47
ツール	11-1
トランキング	
(リンク・アグリゲーション を参照)	
トランク・グループ	2-7
トランスポート・モード	
AH.....	4-7
ESP.....	4-8
トンネル	
6bone への	3-63
6to4.....	3-17, 3-28
構成済み.....	3-18, 3-28
構成での指定	3-32
作成	3-65
自動	3-16, 3-28
トンネル・モード	
AH.....	4-7
ESP.....	4-8
トークン・リング	
IP MTU サイズの修正	2-50
IP MTU サイズの表示	2-50
IP MTU のサイズ	2-50
netstat による監視.....	11-11
カウンタ.....	A-21

構成	2-24
構成に必要な情報	2-10
ソース・ルーティング	2-47
ホストの情報	A-24
トークン・リング IP MTU サイズ	2-50
トークン・リング・インタフェース, 監視	A-19
トークン・リングのソース・ルーティング	2-47
トークン・リングのソース・ルーティングの管理	2-47

な

名前	
アドレスへのマッピング	3-12

に

認証	
IKE に対するタイプ指定	4-38
IKE のワークシート	4-37
PPP	8-18
IKE 方式	4-36
認証アルゴリズム	
AH	4-9
ESP	4-9
認証鍵	4-10
IPsec 鍵に対する指定	4-46
認証ヘッダ	
(AH を参照)	

ぬ

ヌル・モデム・ケーブル	8-3
-------------------	-----

ね

ネット構成アプリケーション ...	2-23
ネットワーク・アダプタ	
(ネットワーク・インタフェースを参照)	
ネットワーク・アダプタ, LAT の構成	9-12
ネットワーク・インタフェース..	2-1
IPv6 ID の割り当て	3-64
IPv6 アドレスの削除	3-66
IPv6 アドレスの追加	3-65
IPv6 の削除	3-64
IPv6 用の初期化	3-63
NetRAIN	2-5, 2-15
Token Ring	2-15
アクセスの制御	2-45
同じサブネットとの多重インタフェース接続	2-3
同じサブネットワーク内の複数の	2-35
監視	2-41, 11-5, 11-11, A-1
管理	2-35
構成	2-24
構成解除	2-26
構成に必要な情報	2-10, 6-8
情報の表示	11-1
タイプ	2-11
パケット・ヘッダの表示 ...	11-16
フェイルオーバー用の多重構成	2-36
リンク・アグリゲーション...	2-15
ネットワーク・インタフェースの監視	11-5
ネットワーク・セットアップ・ウィザード	1-6

ネットワーク・データの構造
 netstat コマンドでの表示 .. 11-11
ネットワークに関する問題
 情報の収集..... 12-1
 報告 12-1
ネットワーク , ネットワーク操作する
 ためのシステムの構成 2-10
ネットワークの問題 10-1
 (問題; 問題の解決 も参照)
 解決用のツール 11-1
ネットワーク・ファイル
 構成 2-34
ネットワーク・マスク
 (サブネット・マスク を参照)
ネットワーク問題の解決手順の開
 始..... 10-2

の

ノード..... 10-13, 10-17, 10-24
 (オフリンク・ノード; オンリン
 ク・ノード; ローカル・ノー
 ド も参照)
 定義 3-2

は

バイナリ
 証明書のエンコーディング... 4-14
バインディング
 モニタリング 5-10
バウンド対話式サービス 9-20
パケット
 モニタリング 5-10, 11-16

リモート・ホストによるリジェク
 ト 2-50
パスワードの保護 , LAT..... 9-4
ハッシュ・アルゴリズム
 IKE に対する指定..... 4-36
発信接続 9-18
パーマネント仮想回路
 (PVC を参照)

ひ

非同期転送モード
 (ATM を参照)

ふ

ファイル
 chap-secrets..... 8-19, 8-34
 gated.conf 2-19
 gateways 2-17
 hosts.equiv 2-33
 ip6trd.conf..... 3-70
 latstartup.conf 9-9
 pap-secrets 8-19, 8-33
 rc.config 1-9, 2-36, 3-68
 slhosts..... 8-7
 オプション..... 8-32, 8-40
 手動による編集 1-9
 シークレット 8-33
 ネットワーク 2-34
 ホスト 2-33
 リモート..... 8-48
 ルート 2-31
フォーマット・プレフィックス. 3-11

負荷分散	
LAT.....	9-5
プリンタ	
LAT での使用方法	9-12
プリンタの設定	
LAT.....	9-13, 9-16
テスト	9-16
テスト方法.....	9-16
プロトコル	
IPsec.....	4-5
プロポーザル	
(IKE プロポーザル, IPsec プロ	
ポーザル を参照)	
定義 (IPsec)	4-4
フロー.....	6-4
情報の表示.....	6-32
ブロードキャスト・アドレス	
(マルチキャスト・アドレス を	
参照)	

ほ

ポイント・ツー・ポイント接続	
(PPP, SLIP を参照)	
ガイドライン	8-43
タイプ	8-1
方向	
アクションの指定.....	4-25
ホスト.....	10-12
(ノード も参照)	
DHCP 用のリストの作成.....	7-16
IPsec に対する構成	4-59
IPv6 構成変数.....	3-68
IPv6 用の構成.....	3-46
インターネットへの接続テス	
ト	11-8

静的経路.....	3-28
定義	4-1
未知 (IPv6 ホスト)	10-12
ホスト・ファイル	2-21
構成	2-33
ホスト名	
ネットワーク・インタフェースの構	
成	2-12
ホーム・エージェント	
定義	5-2

ま

マルチキャスト・アドレス	3-9
一時的な.....	3-10
グループ.....	3-10
周知の	3-10

み

未指定アドレス	3-6
---------------	-----

め

メイン・モード	
と電子署名.....	4-11
のメッセージ	4-11
メッセージ	
Binding Acknowledgement	5-5
Binding Update	5-5
IPsec の起動	B-1

も

モデム	
acucap ファイル	8-47

SLIP とともに使用する場合... 8-3
 ガイドライン 8-43
 ケーブルのガイドライン 8-43
 ダイアル・アウト・アクセス用コマ
 ンド 8-10
 ダイアル・イン・アクセス用のコマ
 ンド 8-45
 モバイル・ノード
 定義 5-2
 バインディングのモニタリン
 グ 5-10
 バインディングを登録できな
 い 10-26
 問題
 IPsec がインストールされてい
 ない 10-27
 IPsec が構成されていない.. 10-28
 IPsec デーモンが開始されてい
 ない 10-28
 Mobile IPv6 がカーネルにな
 っていない 10-26
 オンリンク・ノードがアドレスを自
 動構成できない..... 10-23
 事前共有鍵接続の失敗 10-29
 証明書接続の失敗 10-31
 接続拒否 10-17, 10-25
 接続の異常終了 10-18, 10-25
 接続の時間切れ 10-9
 動作していないネットワーク・デー
 モン 10-6
 動作していないルータ・デーモ
 ン 10-19

到達できないオフリンク・ノー
 ド 10-15, 10-22
 到達できないオンリンク・ノー
 ド 10-13, 10-20
 到達できない自ノード 10-17,
 10-24
 到達できないネットワーク... 10-6
 到達できないホスト..... 10-8
 ネットワーク・ソフトウェアの未構
 成 10-6
 ノードに到達できない
 (IPsec) 10-27
 未知のリモート・ホスト 10-7,
 10-12, 10-19
 モバイル・ノードにバインディング
 を登録できない..... 10-26
 ルータがメッセージを転送してい
 ない 10-23
 問題解決 11-1
 (エラー・メッセージ も参照)
 ツール 11-1
 問題の解決 10-1
 診断マップ..... 10-1

ゆ

ユニキャスト・アドレス
 IPv4 互換 IPv6 アドレス 3-6
 IPv4 射影 IPv6 アドレス 3-7
 サイト・ローカル・アドレス . 3-8
 定義 3-5
 未指定アドレス 3-6
 リンク・ローカル・アドレス . 3-7
 ループバック・アドレス 3-6

り

- リジェクトされたパケット 2-50
- リソース・レコード 3-12
- リモート・ノード
 - 接続拒否 (IPv6 ルータ) 10-25
- リモート・ファイル 8-44, 8-48
- リモート・ホスト 10-12
 - (ホスト も参照)
- 接続拒否 (IPv6 ホスト) 10-17
- 未知 (IPv6 ルータ) 10-19
- リンク・アグリゲーション 2-7
 - LAT 2-12, 2-43
 - 構成 2-42
 - ポート 2-15
- リンク・ローカル・アドレス 3-7

る

- ルータ
 - IPv6 構成ファイルの編集 3-70
 - IPv6 構成変数..... 3-68
 - IPv6 用のカーネル・サポートの構成 3-67
 - IPv6 用の構成..... 3-54
 - IPv6 用の省略時設定の削除 .. 3-66
 - IPv6 用の省略時設定の追加 .. 3-66

- Mobile IPv6 の構成 5-9
- 静的経路..... 3-28
- 動作していないデーモン ... 10-19
- メッセージを転送していない 10-23
- ルータ通知
 - 目的 3-70
- ルーティング..... 2-20
 - スタティック 2-20
 - 静的 2-31
 - ソース 2-47
 - 動的 2-16, 2-18
- ルート
 - スタティック 2-20
 - 静的 2-31
- ルートの最適化 5-7
- ルート・ファイル
 - 構成 2-31
 - 定義 2-20
- ループバック・アドレス 3-6

ろ

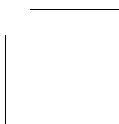
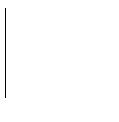
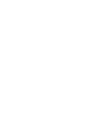
- ログ・ファイル 11-17
 - (メッセージ も参照)
- ローカル・ノード
 - 到達できない (IPv6 ホスト) 10-17
 - 到達できない (IPv6 ルータ) 10-24

Tru64 UNIX ドキュメントの購入方法

Tru64 UNIX ドキュメントのご購入については、弊社担当営業または日本ヒューレット・パッカートの各営業所/代理店にお問い合わせください。

各ドキュメント・キットの注文番号は以下のとおりです。ドキュメント・キットに含まれるマニュアルの内容については『ドキュメント概要』を参照してください。

キット名	注文番号
Tru64 UNIX Documentation CD-ROM	QA-6ADAA-G8
Tru64 UNIX Documentation Kit	QA-6ADAA-GZ
End User Documentation Kit	QA-6ADAB-GZ
- Startup Documentation Kit	QA-6ADAC-GZ
- General User Documentation Kit	QA-6ADAD-GZ
- System and Network Management Documentation Kit	QA-6ADAE-GZ
Developer's Documentation Kit	QA-6ADAF-GZ
Reference Pages Documentation Kit	QA-6ADAG-GZ
TruCluster Server Documentation Kit	QA-6BRAA-GZ
Tru64 UNIX 日本語ドキュメント・キット	QA-6ADJB-GZ
スタートアップ・ドキュメント・キット	QA-6ADJC-GZ
一般ユーザ・ドキュメント・キット	QA-6ADJD-GZ
システム/ネットワーク管理ドキュメント・キット	QA-6ADJE-GZ
プログラミング・ドキュメント・キット	QA-6ADJF-GZ
CDE 翻訳ドキュメント・キット	QA-6ADJG-GZ
TruCluster Server 日本語ドキュメント・キット	QA-05SJA-GZ
Advanced Server for UNIX 日本語ドキュメント・キット	QA-5U2JA-GZ



マニュアルに対するご意見

Tru64 UNIX

ネットワーク管理ガイド: 接続編

AA-RQ30B-TE

弊社のマニュアルに関して、ご意見、ご要望、または内容の不明確な部分など、お気づきの点がございましたら、下記にご記入の上、弊社社員にお渡しくださるようお願い申し上げます。

マニュアルの採点：

	大変良い	良い	普通	良くない
正確さ (説明どおりに動作するか)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
情報量 (十分か)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
分かり易さ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
マニュアルの構成	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
図 (役立つか)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
例 (役立つか)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
索引 (項目の検索性)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ページ・レイアウト (情報の検索性)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

内容の不明確な部分がありましたら、以下にご記入ください：

ペー ジ

その他お気づきの点がございましたら、以下にご記入ください：

ご使用のソフトウェアのバージョン： _____

貴社名/部課名 _____

御名前 _____

記入日 _____

(注) 当用紙を受け取った弊社社員は、すみやかに下記にお送りください。

ビジネスクリティカルシステム統括本部 **BCS** 技術本部 **Alpha** ソフトウェア技術部